DEPARTAMENTO DE ECONOMÍA FINANCIERA

Y DIRECCIÓN DE OPERACIONES

UNIVERSIDAD DE SEVILLA

# "VALORACIÓN DE INTANGIBLES PARA LA CIBERSEGURIDAD EN LA NUEVA ECONOMÍA"

Tesis doctoral presentada por:
CARMEN SÁNCHEZ MONTAÑÉS

Dirigida por:
Profesor Doctor D. FÉLIX JIMÉNEZ NAHARRO

UNIVERSIDAD DE SEVILLA.

**AGRADECIMIENTOS**

A mi familia por su apoyo, paciencia, cariño y comprensión en cada momento para que esta tesis llegue a buen puerto.

A mi director de tesis, Dr. D. Félix Jiménez Naharro, gracias a su inteligencia, paciencia, sabiduría y por estar siempre dispuesto a ayudarme, por su ánimo constante, por sus valores en el ámbito de la docencia, investigación y la gestión, porque siempre está ahí cuando lo necesito, y para mí es un ejemplo a seguir en todos los sentidos.

Al profesor Dr. D. Fernando Gutiérrez Hidalgo por su apoyodesinteresado en momentos difíciles y en el desarrollo de este trabajo, por su ánimo. Universidad Pablo de Olavide.

Al profesor Dr. D. Tomás Escobar Rodríguez por su ayuda, por su ánimo, por su colaboración. Universidad de Huelva.

Al profesor Dr. D. E. Bonson por su ayuda y por ser un pionero importante en el nuevo paradigma digital.

Al profesor Dr. D. José Cristóbal Riquelme Santos, Red Española de Minería de Datos y Aprendizaje. Universidad de Sevilla.Por su aportación en las entrevistas relacionadas con la encuesta sobre seguridad de la información de esta tesis.

A los profesores: Dr. D. Vicente Pérez Chamorro (Universidad Pablo de Olavide), a la Dra. Araceli Casasola-Balsells (Universidad Pablo de Olavide), Dr. D. Juan Demetrio Gómez Moreno (Universidad de Sevilla), Dr. D. Juan Gómez Álvarez (Universidad de Huelva) por sus comentarios en el desarrollo de esta tesis.

A Doña Begoña Rodríguez Mondragón del Instituto Tecnológico y de Estudios Superiores de Monterrey (México).

A Don Reynaldo Frausto Mena, supervisor académico del Instituto Politécnico Nacional, México, D.F.

A Doña Teresa Álamo Cantarero, responsable de auditoría interna de IBM, Londres.

A Don Carlos Orlando Rico Bonilla, Universidad Nacional de Colombia.

A Don Manuel Pineda Villegas, directivo de la Compañía Telefónica.

Muchas gracias a todos.

**INDICE GENERAL:**

# Contenido

# CAPÍTULO 1 JUSTIFICACIÓN, OBJETIVOS Y ESTRUCTURA

## 1.1. LA CIBERSEGURIDAD EN LOS MEDIOS DE COMUNICACIÓN

**El 96% de las empresas no están preparadas para un ciberataque.**Las restricciones presupuestarias son la principal barrera para satisfacer las expectativas de seguridad, junto con la falta de recursos especializados. Y eso a pesar del crecimiento en el número de amenazas, como señala un estudio de Ernst & Younghttp://cso.computerworld.es/seguridad-en-cifras/el-96-de-las-empresas-no-estan-preparadas-para-un-ciberataque

**Hacienda admite el fallo de cruce de datos entre contribuyentes.**Al colapso sufrido en la web durante el primer día de la campaña de la declaración de la renta 2015, se le unió un error que provocó que numerosas personas recibieran el borrador de otros contribuyentes, cruzando los datos personales. La organización Facua[1] considera escandaloso el grave fallo de seguridad, y anuncia acciones legaleshttp://cso.computerworld.es/seguridad-en-cifras/hacienda-admite-el-fallo-de-cruce-de-datos-entre-contribuyente

**Nuevo phishing que aprovecha la declaración de la renta para suplantar a la Agencia Tributaria.**Estamos en plena campaña de la declaración de la renta y los ciberdelincuentes están utilizando esto para enviar mensajes de correo electrónico de phishing suplantando a la Agencia Tributaria. INCIBE[2] recuerda que hay que desconfiar de los mensajes recibidos de organismos públicos solicitando datos personales.http://cso.computerworld.es/alertas/nuevo-phishing-que-aprovecha-la-declaracion-de-la-renta-para-suplantar-a-la-agencia-tributaria

**El 97% de los usuarios son incapaces de identificar correos de phishing.**En una encuesta realizada a usuarios de 144 países, España fue el quinto país con los mejores resultados de detección de phishing. Intel Security recuerda que los indicios de phishing típicos incluyen gramática incorrecta y gráficos pobreshttp://cso.computerworld.es/seguridad-en-cifras/el-97-de-los-usuarios-son-incapaces-de-identificar-correos-de-phishing

**Los ataques a la Administración y empresas de interés crecerán un 40%.**Así lo destaca el último informe sobre ciberamenazas y tendencias realizado por el Centro Criptológico Nacional CCN-CERT, el cual prevé un incremento del 40% en los ciberataques a la Administración y a empresas de interés estratégico. Los ataques DDoS[3], el cryptoware[4] y el ransomware[5] serán una constante.http://cso.computerworld.es/seguridad-en-cifras/los-ataques-a-la-administracion-y-empresas-de-interes-creceran-un-40

**A casi medio billón de dólares asciende el coste de la ciberdelincuencia.**La evolución de los riesgos cibernéticos obliga a las empresas a desarrollar una cultura de ciberseguridad en la que diferentes actores compartan conocimientos sobre gestión de riesgos. AGCS[6] prevé que las primas de los ciberseguros se dispararán en 10 años.http://www.networkworld.es/seguridad/a-casi-medio-billon-de-dolares-asciende-el-coste-de-la-ciberdelincuencia

[1] FACUA Andalucía-Consumidores en Acción.
[2] Instituto Nacional de Ciberseguridad.
[3] Ataque de denegación.
[4] Captura de pantalla de un dispositivo que ha sido objeto de ataque con ransomware.
[5] Es un tipo de programa informático mal intencionado que restringe el acceso a determinadas partes o archivo del sistema infectado, y pide un rescate (bitcoins) a cambio de quitar esta restricción.
[6] Allianza Risk Barometer sobre ciberseguridad.

**Solo una cuarta parte de las empresas utiliza ciberaseguradoras.**El aumento de los costes asociados a las brechas de seguridad y los ciberataques está llevando a cada vez más empresas a transferir más riesgos a aseguradoras, aunque aún representa un pequeño porcentaje, señala ABI Research[7]. http://www.networkworld.es/seguridad/solo-una-cuarta-parte-de-las-empresas-utiliza-ciberaseguradoras

**Falta madurez en las empresas para afrontar los riesgos de la ciberseguridad.**El 75% de los encuestados en el RSA[8] Cybersecurity Poverty Index carecen del nivel de madurez necesario para afrontar este tipo de retos. http://www.ciospain.es/industria-y-utilities/falta-madurez-en-las-empresas-para-afrontar-los-riesgos-de-la-ciberseguridad

**Transformación digital: cómo sobrevivir.**Puede ser la estrategia que permitirá a las empresas ser disruptivas e innovadoras y crear nuevos modelos de negocios digitales. Y quién sabe si ser los próximos Amazon o Uber.http://www.ciospain.es/industria-y-utilities/transformacion-digital-como-sobrevivir-y-prosperar

**Transformación digital de la banca: hacia nuevos modelos.**Pocos sectores tienen por delante tantos desafíos como la banca a la hora de adaptar a su actual operativa al nuevo entorno digital. Transformarse para mejorar la experiencia de cliente va más allá del rediseño de infraestructuras operativas y procesos, requiere la adopción de nuevas tecnologías, modelos de negocio y alianzas con nuevos 'entrants'.http://www.ciospain.es/finanzas/transformacion-digital-de-la-banca-hacia-nuevos-modelos

**Fabricación conectada: el reto de la cuarta revolución industrial.**Las TI y el Internet de las Cosas (IoT) perfilan infinitas posibilidades de negocio, lo que está empujando a la industria a una transición digital para no quedarse fuera del mercado.http://www.ciospain.es/industria-y-utilities/fabricacion-conectada-el-reto-de-la-cuarta-revolucion-industrial

**¿Cómo impactan en la banca la automatización y los modelos de digitalización?**La transformación digital producirá cambios importantes en el mercado laboral, pero las soluciones tecnológicas también generarán nuevos puestos de trabajo. La banca es uno de los sectores que más invierte en automatización y servicios digitales. ¿Qué ventajas están consiguiendo con este esfuerzo?http://www.ciospain.es/finanzas/como-impactan-en-la-banca-la-automatizacion-y-los-modelos-de-digitalizacion

**El 43% de las empresas utilizará soluciones IoT a finales 2016, según Gartner.**Actualmente sólo un 29% de las empresas utiliza tecnología IoT y un 14% quiere introducirlas este año, según un estudio de Gartner[9]. Los datos indican que el ritmo de adopción de Internet de las Cosas es rápido, aunque hay un alto porcentaje de empresas que no tienen planes en este ámbitohttp://www.ciospain.es/movilidad/el-43-de-las-empresas-utilizara-soluciones-iot-a-finales-2016-segun-gartner

**Enisa confía en el mercado de ciberaseguradores para concienciar a las empresas.**Enisa ha publicado un informe en el que confirma que la Unión Europea confía en el fortalecimiento del mercado de ciberaseguradoras para concienciar a las empresas. En su informe, Enisa destaca la gran diferencia entre el mercado de EEUU y el

[7] https://www.abiresearch.com,

[8] https://www.rsa.com>security-perspectives

[9] www.gartner.com

europeo.http://cso.computerworld.es/seguridad-en-cifras/enisa-confia-en-el-mercado-de-ciberaseguradores-para-concienciar-a-las-empresas

**Los riesgos cibernéticos podrían provocar un shock global similar a la crisis de 2008.** La dependencia de las nuevas tecnologías de la información ha creado una compleja red de riesgos interconectados que dificulta su gestión. Por lo menos eso es lo que asegura un estudio de Zurich Seguros que advierte a las empresas de su exposición a riesgos externos de los que en ocasiones ni siquiera son conscientes.http://cso.computerworld.es/cibercrimen/los-riesgos-ciberneticos-podrian-provocar-un-shock-global-similar-a-la-crisis-de-2008

**España es el tercer país más castigado por los ciberataques.**Un estudio de S21sec[10] destaca que la actividad del malware bancario entre julio y septiembre decreció en España. A pesar de esto, tras Estados Unidos y Reino Unido, España es el tercer país más castigado.http://cso.computerworld.es/cibercrimen/espana-es-el-tercer-pais-mas-castigado-por-los-ciberataques

**Cuáles son los sectores empresariales más vulnerables ante un ciberataque.**S2 Grupo[11] acaba de presentar su tercer Informe Técnico sobre Protección de Infraestructuras Críticas, en el que, además de analizar cuál es la situación de la información disponible en Internet sobre las infraestructuras, revela cuáles son los sectores más vulnerables ante un ciberataque.http://cso.computerworld.es/seguridad-en-cifras/cuales-son-los-sectores-empresariales-mas-vulnerables-ante-un-ciberataque

**Las empresas sufren un ciberataque cada 1,5 segundos.**El último informe de FireEye revela que las empresas sufren, de media, un ataque cada 1,5 segundos. El informe desvela que los ataques de malware ya afectan a 206 países. Estados Unidos, Alemania, Corea del Sur, China, Países Bajos, Reino Unido y Rusia fueron los países más afectados.http://cso.computerworld.es/seguridad-en-cifras/las-empresas-sufren-un-ciberataque-cada-15-segundos

**Más de la mitad de las empresas españolas sufrieron ataques de malware y spam.**Con un 71% de compañías españolas afectadas, los ataques de virus, gusanos, spyware u otro tipo de programa malicioso son la principal amenaza de seguridad corporativa, seguidos de los ataques de spam y de phishing. http://cso.computerworld.es/seguridad-en-cifras/mas-de-la-mitad-de-las-empresas-espanolas-sufrieron-ataques-de-malware-y-spam

**Repuntan el 'ransomware' y el 'malware' móvil.**¿Alguien se extraña? tras algo más de tres trimestres de caída, el número total de muestras de nuevo 'malware' creció en el último trimestre de 2015. Lo mismo ocurrió con el 'ransomware' que repuntó un 26% coincidiendo con el cierre del año. Son datos recogidos de un informe realizado por Intel Security.http://cso.computerworld.es/seguridad-en-cifras/repuntan-el-ransomware-y-el-malware-movil

**Aplicaciones, parches y monetización del malware, los principales riesgos para las empresas.**En su informe anual sobre delitos cibernéticos CyberRiskReport 2016, Hewlett Packard Enterprise (HPE) identifica la vulnerabilidad de las aplicaciones, los parches de seguridad y la creciente monetización del malware como las principales áreas de riesgo en la seguridad de las empresas.http://cso.computerworld.es/cibercrimen/aplicaciones-parches-y-monetizacion-del-malware-los-principales-riesgos-para-las-empresas

[10] https://www.s21sec.com(empresa líder en ciberseguridad).

[11] Es una de las principales compañías a nivel nacional especializadas en CiberSeguridad y explotación de sistemas de misión crítica. https://www.s2grupo.es

**Telefónica incorpora Faast a su portfolio IoT de ciberseguridad.** La solución Faast permite detectar las vulnerabilidades presentes en los procesos de autentificación o autorización, así como la falta de cifrado en el transporte de la información. Se une a las herramientas ya existentes en IoT que detectan comportamientos anómalos en base al tráfico desplegado en la red.http://cso.computerworld.es/proteccion-de-datos/telefonica-incorpora-faast-a-su-portfolio-iot-de-ciberseguridad

**La ciberseguridad en IoT vista por Chema Alonso (directivo de la filal de Telefónica para la ciberseguridad).**Chema Alonso, CEO de ElevenPaths[12], filial de ciberseguridad de Telefónica, nos cuenta que "es necesario que las compañías apliquen ciclos de análisis y auditorias de seguridad revisables constantemente a cada uno de los dispositivos que formen parte de los nuevos ecosistemas IoT". No te pierdas su punto de vista.http://www.idgtv.es/entrevistas/la-ciberseguridad-en-iot-vista-por-chema-alonso

## 1.2. LA JUSTIFICACIÓN DEL TRABAJO

Cuanto más conectamos nuestros dispositivos y nuestras vidas a las redes de información global, ya sea a través de teléfonos móviles, redes sociales, ascensores o coches autodirigidos, más vulnerables nos volvemos frente a quienes saben cómo funcionan las tecnologías subyacentes y cómo explotarlas en beneficio propio y en detrimento del común de los mortales. En pocas palabras; cuando todo está conectado, todo el mundo es vulnerable. La tecnología que aceptamos de manera rutinaria en nuestras vidas, sin cuestionarnos nada ni analizarla, puede volverse contra nosotros.

El crimen organizado, los hackers o piratas informáticos, los gobiernos corruptos de las entidades y los terroristas compiten por controlar las nuevas tecnologías en beneficio propio.

La tecnoautopía prometida por Silicon Valley tal vez sea posible, pero no aparecerá por arte de magia. Será necesario que ciudadanos, gobiernos, empresas y organizaciones no gubernamentales para el desarrollo (ONGDs) inviertan en ella: una implicación, un esfuerzo y una lucha fuerte y constante para garantizar que llegue a buen puerto. Ha dado comienzo una nueva contienda entre quienes aprovecharán la tecnología en beneficio de la humanidad y quienes prefieren subvertir esas herramientas, al margen del daño que provoquen al prójimo.Estamos ante una batalla por el alma de la tecnología y su futuro. Se propaga en el fondo, de manera encubierta y oculta del ciudadano corriente. Si somos previsores, es posible anticipar e impedir hoy los delitos del mañana, antes de alcanzar un punto de no retorno. Las generaciones futuras volverán la vista atrás y juzgarán nuestros esfuerzos por domeñar estas amenazas de seguridad y salvaguardar el alma de la tecnología.

Siguiendo a Michael Weissenstein, “Mexico´s Cartels Build Own National Radio System”. En: Associated Press, 27 de diciembre de 2011:“Los delincuentes actualizan de manera permanente sus técnicas para incorporar las últimas tecnologías a sus modus operandi. Construyen sus propios sistemas de radio telecomunicaciones móviles encriptadas de alcance nacional, como los emplean los cárteles del narcotráfico en México”.

Las organizaciones ilegales se han consagrado como las principales asimiladoras de las nuevas tecnologías. Los delincuentes utilizaban Internet mucho antes que la policía ni siquiera contemplara hacerlo, y desde entonces han sacado ventajas a las autoridades. Los titulares de prensa vienen repletos de noticias sobre cuentas online de millones de dólares pirateadas. El avance de estos delitos es alarmante y siguen acelerando por el mal camino.

[12]https://www.elevenpaths.com(@chemaalonso.1d)

Los delincuentes han rebasado los ciberdelitos de hoy en día y se han internado en nuevos campos emergentes de la tecnología: como la robótica, la realidad virtual, la inteligencia artificial, la impresión 3D y la biología sintética.

Siguiendo a "Gartner Says Worlwide Security Software Market Grew 3.7 percent in 2015" (Analysts to focus on top Security Trends and Gartner Security and Risk Management Summits 2016 in Sao Paulo, Sydney. Mumbay and London); septiembre Steve Johson. "Cybersecurity Business Booming in Silicon Valley". En: San José Mercury News, 13 de de 2013. Cada año, clientes y empresas del todo el mundo depositan su fe en la industria del software de seguridad informática para que los protejan de la amenaza creciente y cada día más sofisticada del software malicioso. De acuerdo con un estudio por el Grupo Gartner, el gasto mundial en software de seguridad rondaba los 20.000 millones de dólares en 2012 y la previsión es que ascienda a 94.000 millones en 2017.

Para Imperva (http://www.Imperva.com).(Imperva/Press Release/ Http/2: Imperva Hacker Intelligence Iniciatitive Report Reveals Four High-Profile Flaws en the Latest Version of the worldwide Web´s Underlying Protocol, Las Vegas, Aug.03, 2016, Globe newawire) Hacker Intelligence Initiative, Monthly Trend Report 14. Diciembre 2012. Researchers at Imperva, una empresa de seguridad de datos con sede en Redwood Shores, California, y los alumnos del Technios-Israel Institute of Technology decidieron comprobar las herramientas antivirus estándar. Recopilaron ochenta y dos nuevos virus informáticos y sometieron aquellos programas de software maliciosos a los motores de detección de amenazas de más de cuarenta de las principales empresas de antivirus del mundo, incluidas entre ellas, Symantec, McAfee y Kaspersky Lab., Trend Micro, Microsoft. El resultado: La tasa de detección de amenazas inicial fue de sólo un cinco por ciento, lo cual implicaba que el 95% restante del malware pasaba completamente desapercibido. También significa que el software antivirus que se ejecuta en el ordenador personal probablemente sólo evite el cinco por ciento de las amenazas contra la máquina.

El centro de la cuestión es que los delincuentes y los programadores de virus sacan una enorme ventaja en materia de innovación y astucia a la industria de los antivirus establecida para protegernos ante las amenazas. Peor aún, la tasa de tiempo para la detección o, lo que es lo mismo, el tiempo que se tarda desde que lanza un software malicioso al ancho mundo hasta que es descubierto está aumentando. Por ejemplo, en 2012, los investigadores del Kaspersky Lab de Moscú descubrieron un malware sumamente complejo bautizado como Flame que había estado hurtando datos de los sistemas de información de todo el mundo durante más de cinco años de ser detectado.

En Tom Simonite. "The antivirus Era is Over". En MIT Technology Review, 11 de junio de 2012. Mikko Hypponen al frente de la investigación en la empresa de seguridad informática F-Secure, afirmó que Flame era un fracaso de la industria de los antivirus y destacó que él y sus colegas podían haber quedado "desclasificados de sus ligas en su propio juego". Pese a que millones de personas en todo el mundo confían en estas herramientas, está bastante claro que la era de los antivirus ha tocado a su fin.

Uno de los motivos que explican esto es la gran cantidad de ataques y de amenazas tecnológicas, la expansión de los ataques llamados "ataques de día cero"[13].Un ataque de día cero aprovecha una vulnerabilidad previamente desconocida de una aplicación informática

[13] Zero day attack, es un nataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para la gente y fabricante del producto.

antes de que los programadores y el personal de seguridad tengan tiempo para subsanarla. En lugar de buscar una actitud proactiva ante estas vulnerabilidades por cuenta propia. Las empresas de software antivirus sólo analizan puntos de referencias conocidos. Cada vez se generan más días ceros para una amplia gama de productos tecnológicos que usamos de manera habitual en nuestras vidas y que afectan a cualquier cosa, desde el sistema operativo Microsoft Windows hasta routers Linksys o los programas PDF Reader o Flash Player de Adobe. Ahora lo que impera es la clandestinidad y el sigilo de los hackers como si tuviésemos una célula durmiente dentro del ordenador.

Miles de ataques con éxito perpetrados contra grandes empresas, ONGDs y gobiernos del todo el mundo revelan, que pese al capital que invierten, no consiguen proteger su información mucho mejor que el común de los mortales.

De acuerdo con 2013 Data Breach Investigations Reports de Verizon[14], la mayoría de las empresas han demostrado ser simple y llanamente incapaces de detectar cuándo un hacker se introduce en sus sistemas de información. Esta encuesta fue realizada por los servicios empresariales de Verizon en colaboración con los servicios secretos de Estados Unidos, la Policía Nacional Holandesa y la Unidad de los delitos cibernéticos de la Policía del Reino Unido, informó de que un promedio del 62% de las intrusiones contra empresas tardaba aproximadamente dos meses en detectarse, Verizon 2013 Data Breach Investigations Reports.

Un estudio similar de Trustwave Holdings 2013, Glogal Security Report revelaba que el tiempo promedio desde la infiltración inicial en la red de una empresa hasta la detección de tal intrusión era de 210 días. Impresionante. Ya se trate de una mafia, de la competencia o de un gobierno extranjero, merodeando a sus anchas por una red corporativa robando secretos, aprovechando los conocimientos de la competencia, infiltrándose en sistemas financieros y hurtando datos personales identificativos de los clientes, como los números de las tarjetas de créditos. Y finalmente, cuando las empresas se dan cuenta de que tienen un espía digital en su seno y de que sus sistemas de información vitales han quedado expuestos, un lamentable 92% de las veces no es el gerente de las Tecnologías de la Información de la empresa ni el equipo encargado de seguridad ni el administrador del sistema quien descubre la infracción, Verizon Risk Team, 2012, “Data Breach Investigations Reports, páginas 3 y 51. Normalmente, los cuerpos de seguridad del Estado, un cliente enfadado, o un contratista notifican el problema a la víctima.

Si los hackers son capaces de penetrar tan fácilmente en las mayores corporaciones mundiales, empresas que de manera colectiva invierten millones de dólares en ciberdefensa y cuentan con departamentos exclusivos de profesionales que trabajan lasveinticuatro horas del día de la semana para proteger sus redes, las perspectivas de que los usuarios domésticos protejan su información se antojan como mínimo agoreras.

¿Cuánto cuesta infiltrarse en un sistema informático normal?, según el estudio de Verizon, una vez que los hackers ponen la vista en la red de alguien, en un 75% de las ocasiones son capaces de penetrar sus defensas en cuestión de minutos. El mismo estudio apunta que sólo el 15% de las veces tardan más de unas cuantas horas en franquear el sistema.

El coste de nuestra ciberseguridad continúa ascendiendo. Si bien la inversión de las empresas multinacionales en todo un abanico de medidas de seguridad para software y hardware

[14] 2017 Data Breach Investigations Repor-Verizon Enterprise Solutions (www.verizonenterprise.com>dbir)

rondará los cien mil millones de dólares en 2017, esa cifra no es más que la fragilidad tecnológica de las empresas.

Pongamos por ejemplo la ciberhuelga que se convocó en 2007 contra TJX, la empresa madre de las tiendas al por menor de T.J. Maxx y Marshalls en Estados Unidos y T.K. Maxx en Europa. En aquel caso los hackers robaron los datos de las tarjetas de crédito de más de cuarenta y cinco millones de clientes, lo cual lo convirtió en el caso de pirateo informático de tiendas minoristas más sonado de su época, Mark Jewell. "T.J. Maxx Theft Believed Largest Hack Ever". Associated Press, 30 de marzo de 2007.

En los documentos presentados posteriormente ante los tribunales se reveló que el número real de víctimas rozaba los noventa y cuatro millones, pese a que TJX alcanzó un acuerdo con Visa, MasterCard y sus clientes por la cantidad de 256 millones de dólares, muchos analistas creen quelos costes reales podrán haber ascendido fácilmente a los mil millones de dólares, Julianne Pepitone. "5 of the Biggest Ever Credit Card Hacks". CNN, 12 de enero de 2014.

Ross Kerber. "Banks Claim Credit Card Hack Breach affected 94 Millions Accounts". New York Times, 24 de octubre de 2007. Una de las fuentes más fiables en materia del coste del hurto de datos es el Ponemon Institute, que lleva a cabo investigaciones independientes acerca de protección de datos y políticas de seguridad de la información.

A la hora de calcular infracciones a la seguridad en el ciberespacio, el Ponemon Institute recalca que es importante extender el análisis de pérdidas bastante más allá de las cantidades sustraídas a los clientes directos. Ponemon Institute, página de inicio de su página web en 2014: http://www.ponemon.org.

Por ejemplo, la empresa víctimas de los ataques, en este caso, TJX, debe hacer una inversión cuantiosa en detectar la infracción, contener a los atacantes, investigar el asunto, identificar a los perpetradores y reparar y recuperar su red informática. Además, suelen producirse graves caídas de ventas, pues el público, receloso, tiene miedo de utilizar los servicios de una empresa que se percibe como insegura. Súmese a ello el precio de las tasas de sustitución de las tarjetas de crédito, unos 5,10 dólares por tarjeta, los servicios de monitorización del crédito de los clientes que debe adquirir la empresa víctima para impedir nuevos fraudes contra sus clientes con las tarjetas de crédito y las primas cada vez más cuantiosas de los ciberseguros y nos damos cuenta enseguida de la rapidez con la que dichas pérdidas ascienden. De ahí que muchas empresas rehúsen admitir que las han pirateado y otras intenten negar la infracción durante el máximo tiempo posible.

Hay otros costes adicionales, más graves, a tener en cuenta, incluido cómo los mercados bursátiles castigan a las empresas víctimas con desplomes precipitados en el precio de sus acciones ante un ciberataque. En una ocasión, Global Payment vió como su valoración en el mercado se recortaba con un nueve por ciento en solo un día hasta que finalmente la Bolsa de Nueva York dejó de vender sus acciones, Robin Sidel y Andrew R. Johnson, "Data Breach Sparks Worry" en: Wall Street Journal, 30 de marzo de 2012. Además de los quebraderos de cabeza económicos que entrañan estos casos, están las demandas colectivas subsiguientes de los clientes, accionistas y reguladores. Dicho lo anterior, Ponemon Institute calcula que las empresas afrontan unos costes de 188 dólares por cada registro robado. Multipliquemos esa cantidad por los cerca de cien millones de registros de cuentas de TJX y enseguida obtendremos una idea de cómo crecen exponencialmente los costes de estas infracciones, Ponemon Institute (esponsorizado por Symantec), 2013. Cost of Data Breach Study: Global Analysis, mayo de 2013.

Las sumas gastadas en medidas de prevención, en su mayoría ineficaces, es pagada por la sociedad en general. Y lo que es aún peor, nuestra creciente conexión al mundo virtual y nuestra radical dependencia concomitante de tecnologías completamente penetrables pueden hacernos mucho daño para nuestros bolsillos colectivos.

Internet ha perdido su inocencia. Nuestro mundo interconectado se está volviendo un lugar cada vez más peligroso y cuantas más tecnologías expugnables incorporemos a nuestras vidas, más vulnerables nos volveremos. La revolución de la información está en marcha con consecuencia a gran escala aún imprevista para nuestra seguridad personal y global.

En el horizonte se perfilan nuevas tecnologías, incluidas la robótica, la inteligencia artificial, la genética, la biología sintética, la nanotecnología, la fabricación en 3D, la ciencia del cerebro y la realidad virtual, todas ellas con repercusiones de gran calado en nuestro mundo y plantearán una panoplia de amenazas a la seguridad que hará que los ciberdelincuentes habituales de hoy en día parezcan un juego de niños. Estas innovaciones desempeñarán papeles esenciales en nuestras vidas diarias en cuestión de pocos años y, pese a ello, todavía no se ha realizado ningún estudio abarcador en profundidad que nos ayude a entender los riesgos colaterales que plantean.

La profundidad y el alcance de estas transformaciones y de sus riesgos concomitantes suelen pasar desapercibidos a la mayoría de las personas, pero, antes de que nos demos cuenta, en nuestra sociedad global habrá conectados a internet tres mil billones de dispositivos nuevos, que permearán cada aspecto de nuestras vidas. Estas conexiones permanentes nos vincularán a hombres y máquinas a lo ancho y largo del planeta, para bien o para mal. La cornucopia de tecnología a la que hemos dado cabida, con poca o nula reflexión ni examen a conciencia, puede volverse en nuestra contra. Estos riesgos presagian la nueva normalidad, un futuro para el cual no estamos preparados, Marc Goodman (2015), “Los delitos del futuro”. Editorial Ariel.

## 1.3. OBJETIVOS, ESTRUCTURA Y METODOLOGÍA

**Transversalidad de la investigación.**Las actuaciones por una mayor protección de la seguridad de la información no sólo afecta a la tecnología, también está relacionado con las finanzas nacionales e internacionales, la valoración de empresas, con aspectos organizativos, con actividades del control interno en el marco de la auditoría interna (responsabilidad de la comisión de auditoría en el informe de buen gobierno de las empresas), con el informe de auditoría externa considerando los riesgos y amenazas de la información como parte importante del mismo, con las actividades institucionales de las compañías, con el informe de responsabilidad corporativa, con el mapa de riesgos, con la información cualitativa como la carta del presidente, también afecta a los activos intangibles de las empresas, con la contabilidad analítica de explotación (robotización de las cadenas de producción), sociología y antropología social. También afecta esta transversalidad a la Contabilidad de gestión: La integración en las empresas del diseño asistido por ordenador(C.A.D.), la fabricación orientada por ordenador (C.A.M.), la planificación asistida por ordenador (C.A.P.), la planificación y el control de la producción (P.P.C.), el control numérico computerizado (C.N.C.), los robots industriales (R.I), y los propios sistemas flexibles de fabricación (F.M.S), son una buena muestra de las posibilidades de aplicación de la IT en Bonson, Escobar, Canay y Gago (2000).

En otro orden de cosas, esta investigación está relacionada con el Derecho Internacional Público y sus instituciones (la guerra del espacio y los desechos de satélites en la atmósfera en las capas más cercanas a la tierra), afecta al Derecho Mercantil, al Derecho del Trabajo, al Derecho Tributario, al Derecho Constitucional, también afecta a la privacidad de los

particulares, de las empresas y a las altas instituciones en sus órganos unipersonales y colegiados nacionales e internacionales.

En el contexto actual de transformación digital, no podemos ignorar las amenazas en materia de ciberseguridad. Si hablamos de innovación y de cómo esta se está llevando a cabo en los bancos, las compañías de telecomunicaciones o las empresas de distribución, no podemos obviar hablar a su vez de cibercrimen, uno de los sectores más innovadores en materia de delitos informáticos, y que actualmente mueve millones de dólares diariamente, gozando de una estructura perfectamente organizada. Los directorios o las reuniones de los diferentes comités de las empresas han ido incorporando paulatinamente aspectos de ciberseguridad en sus agendas, dentro de proyectos e iniciativas de innovación.

Todo esto pone de relieve que la seguridad se convierte en un tema estratégico que afecta y tiene que considerar toda la organización, considerando aspectos de procesos, personas y estructuras; no se trata de un mero tema técnico, delegado en el departamento de TI. Gracias a este giro estratégico, la ciberseguridad se convierte en un asunto que ayuda a las compañías a ser más ágiles, a reducir riesgos y a diferenciarse de la competencia.

En este sentido es clave considerar tres aspectos: los grandes riesgos se pueden reducir en gran parte aplicando medidas de seguridad básicas; las empresas no pueden proteger al mismo nivel todos sus activos, por lo que hay que hacer un análisis de riesgos riguroso estableciendo prioridades; y, por último, hay que empezar a considerar las herramientas de ciberinteligencia como un aspecto clave de la estrategia de defensa. Tenemos que anticiparnos a los cibercriminales, aprendiendo del mercado, de nuestro sector y otras empresas similares.

La seguridad de la información y la ciberseguridad debe tratarse como un proceso sistemático más de la organización, imprescindible para alcanzar los objetivos del negocio, y éste se debe revisar de manera continua para alcanzar los objetivos del mismo. Esta responsabilidad estratégica, en un marco de liderazgo basado en valores, corresponde a los miembros del Consejo de Administración en el marco del Buen Gobierno de las empresas.

En el mismo sentido del párrafo anterior, las cuentas anuales: el balance de situación, la cuenta de resultados, la memoria, el estado de flujo de efectivo, el estado de cambio en patrimonio neto, el informe de gestión (como prolongación de las cuentas anuales) no sólo deben contemplar las operaciones tradicionales sino desglosar todas las transacciones en operaciones online de las que no lo son. La digitalización de la empresa es hoy una realidad y los directivos deben contemplar el nuevo paradigma digital (ecosistema digital). Los profesores Bonson[15], Escobar[16] y Gagohacen alusión al nuevo pradigma digital AECA (2000).La profesora Luna Huertas, P. (2003)[17]

La longevidad de la organización en un marco global y de competitividad, como veremos en el desarrollo de esta tesis, está relacionada, entre otras cosas, con el liderazgo en valores de los miembros del Consejo de Administración, con su preparación en materia de seguridad de la información, deben garantizar la integridad, confidencialidad, disponibilidad y seguridad de la información teniendo en cuenta unos mínimos normativos y deseables que maximicen los controles internos de salvaguarda de la información.

[15] Contabilidad Digital Universidad-Empresa, mayo de 2003. Simposium, celebrado en la Universidad de Huelva. Dedicado al recuerdo del prof. Moisés García García: La valentía de la investigación.

[16] La demanda de la información contable en internet: un estudio empírico.

[17] Códigos de Conducta en internet (2003) Universidad de Huelva, Prof. Luna Huertas, P. y D. Enrique Álvarez Merida, auditor Webtrust.

**Alcance y contenido del concepto de ciberseguridad.**Dejemos claro, aunque a lo largo de la tesis volveremos a ello con más profundidad, algunos términos: la ciberseguridad asociado a ciberespacio, ciberamenazas u otros conceptos. En determinadas ocasiones, se usa como sinónimo de seguridad de la información, seguridad informática o seguridad de cómputo, pero esta idea no es la correcta. La ciberseguridad busca proteger la información digital en los sistemas interconectados. Está comprendida dentro de la seguridad de la información. Según Information Systems Audit and Control Association (ISACA), (welivesecurity.com) la ciberseguridad es definida como "protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

La norma ISO 27001 define activo de información "como los conocimientos o datos que tienen valor para la organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma. Por tanto, la ciberseguridad tiene como foco la protección de la información digital que vive en los sistemas interconectados, enconsecuencia está comprendida dentro de la seguridad de la información.

El propósito de la seguridad de la información es reducir riesgos hasta un nivel que sea aceptable para los interesados en mitigar amenazas latentes, se entiende también como todas aquellas actividades encaminadas a proteger cualquier tipo de peligro. La información puede encontrarse de diferentes maneras, por ejemplo: en formato digital (a través de archivos en medios electrónicos u ópticos), en forma física (ya sea escrita o impresa en papel) así como de manera no representada como puede ser las ideas, conocimientos y valores de las personas.

La información puede encontrarse en diferentes estados (almacenada, procesada, o transmitida): en formato electrónica, de manera verbal o a través de mensajes escritos o impresos. La información requiere protección adecuada en función de su importancia y criticidad. La seguridad de cómputo se limita a la protección de los sistemas y equipos que permiten el procesamiento de la información, mientras que la seguridad informática involucra los métodos, procesos o técnicas para el tratamiento automático de la información en formato digital, teniendo un alcance mayor, ya que incluye la protección de las redes e infraestructura tecnológica.

Cuando se busca proteger al hardware, redes, software, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o ciberseguridad. La seguridad de la información tiene un alcance mayor que la ciberseguridad, dado que la primera busca proteger la información de riesgos que puedan afectarla en sus diferentes formas y estados. La ciberseguridad se enfoca principalmente a la información de tipo digital y los sistemas interconectados que lo procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.

La seguridad de la información se sustenta en metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnologías y otros elementos, que soportan la idea de protección en las distintas facetas de la información; también involucra la aplicación y gestión de medidas de seguridad apropiadas a través de un informe holístico. Lo importante es la protección de la información ante la gran dependencia tecnológica de las empresas y los particulares.

**Objetivo, hipótesis de partida, metodología, estructura de la investigación, conclusiones.**El objetivo de esta tesis tiene varios apartados:

Estudiar la problemática existente relacionada con los riesgos y amenazas de ciberseguridad que sufren las empresas en el nuevo paradigma/realidad digital actual.

Los incrementos de valoración de las compañías a través de mayor grado de protección de la ciberseguridad incrementando los flujos de beneficios y flujos de efectivo operativos por operaciones digitales, dado que habría mayor grado de confianza.

Analizar la problemática del ciberseguro.

Estudiaractuaciones proactivas continuada de algunas empresas del Ibex-35 en la protección de los riesgos por ciberseguridad, a través de los informes anuales, incluso la carta del presidente e información voluntaria.

Establecer una propuesta de mínimos informativos deseables por encima de los mínimos establecidos actualmente que generen seguridad de la información en beneficio del principio de puesta en funcionamiento y de la eficiencia de la protección de los datos de todos los stakeholder relacionados con la misma.

**Hipótesis de partidas**:Entre las hipótesis de partida se destacan:

La actitud proactiva y conocimientos de seguridad de la información de la alta dirección y la implicación de todos los stockholders pueden mejorar mucho la reputación y la valoración de las empresas.

Que las empresas de ciberseguros podrían ayudar a las organizaciones empresariales a través de los distintos tipos de cobertura a hacer frente a los riesgos de ataques maliciosos cibernéticos, fallos técnicos y recursos humanos. Las primas estarán en función de la actitud de la alta dirección de las empresas (estática, dinámica, proactiva) y de los activos de información expuestos.

Que un buen control interno continuo, bajo la responsabilidad de una comisión de ciberseguridad, dependiente del Consejo de Administración, colaborando al unísono con los responsables de la comisión de auditoría interna, ayudaría a mejorar la problemática de ciberseguridad y facilitaría el proceso de auditoría interna y externa. Dando así importancia estratégica a la ciberseguridad.

Si en el informe de auditoría interna y externa, existiera un párrafo de riesgos relacionado con la ciberseguridad, ayudaría a concienciarnos de la importancia de la seguridad de la información e incrementaría el valor de la empresa.

La planificación estratégica, táctica y operativa, de la ciberseguridad incrementaría el valor de la empresa. La importancia la podríamos medir a través de la información cualitativa en la carta del presidente de la compañía que aparece cada año en el informe anual. Cuantitativamente podríamos medir la importancia de la ciberseguridad a través de los datos expuestos a ciberamenazas y vulnerabilidades en las cuentas anuales y el informe anual.

Que la presentación de todas las cuentas anuales desglosadas en operaciones digitales de las no digitales ayudaría a los usuarios y stakeholders a entender mejor la información que presentan las empresas ante la nueva realidad digital (paradigma digital), también percibiríamos mejor la mayor exposición de información digital y, por tanto, mediríamos mejor la vulnerabilidad que sufren las empresas ante ciberataques (A mayor grado de exposición de datos online en los informes anuales mayor vulnerabilidad y ciberamenazas).

Si existe actitud proactiva continua por parte de la empresa ante los riesgos de ciberseguridad (buen gobierno de las empresas y responsabilidad social corporativa), las redes sociales y la sociedad en general reflejarían positivamente esta actitud directiva y de esta manera incrementaría el valor de la empresa, se fomentaría los niveles de transparencias, el respeto a los demás, mayores niveles de confianza de la sociedad hacia la empresa, evitando actitudes maliciosas, mayor grado de convivencia de lo tradicional con la realidad digital. No se puede huir de los ataques maliciosos de ciberseguridad, simplemente se deben afrontar. La nueva realidad digital basada en valores humanos es buena para la sociedad en general y para las empresas cuyos objetos sociales estén basados en esos mismos valores.

**Metodología:**Creemos que podemos encuadrar la investigación dentro de las conceptuaciones que se sitúan en el paradigma de utilidad de la información, haciendo énfasis en la utilidad de los intangibles. Resulta conveniente plantearse si el modelo contable utilizado en la actualidad es adecuado, ya que puede no reflejar el valor de todos los elementos que intervienen en la creación de valor en la empresa (Cañibano et al., 1999). Éste es el caso de la relevancia asumida por los intangibles en las últimas décadas.

Tomando el paradigma de la utilidad, podemos decir que los intangibles, como parte de la contabilidad, deberían suministrar información relevante para las decisiones que tomen sus usuarios. Pero si realmente se pretende que la información sobre intangibles de las empresas sea útil para los usuarios, debería valorarse e integrarse en el sistema contable, de forma que la información integrada sirva para reflejar la imagen fiel de su patrimonio, situación financiera, resultados y actuaciones en materia de intangibles, según Cañibano et al. (1999), Tua (1989, 2006).

Numerosos estudios que han relacionado la inversión en los elementos intangibles de una empresa con los precios de mercado de las acciones de la misma, demuestran la pérdida de relevancia y fiabilidad de los estados financieros, dada la subjetividad que entraña la valoración de estos intangibles.

La aparición de la nueva economía puede llevarnos a considerar que la capacidad de una empresa para crear valor, parece no depender exclusivamente de su capacidad financiera y de producción. Si bien, desde hace algunos años, la información y los intangibles han sido consideradas una de las fuentes para la creación de renta y riqueza en las entiades.

Las empresas deben buscar elementos de diferenciación que les permitan tomar decisiones útiles para alcanzar los objetivos planteados de manera eficiente. Así, puede ser habitual encontrar entre los usuarios externos de las empresas, demandas crecientes de información sobre intangibles con altas dosis de utilidad, con el objetivo de intentar conseguir el máximo nivel de adecuación entre la decisión elegida y el objetivo estratégico planteado. Uno de esos intangibles estratégicos son los relacionados con seguridad de la información, generando una diferencia competitiva importante. Ignorar este intangible significaría ir contra el principio de empresa en funcionamiento.Para validar las hipótesis que se han señalado se pueden utilizar dos enfoques:

**Positivo-inductivo** En primer lugar, el enfoque positivo-inductivo en el desarrollo de los distintos informes que presentan algunas empresas más internacionales del Ibex-35 y la revelación voluntaria en ellos contenida relacionada con la seguridad de la información. Se analizarán también la información emitida por las institucionales nacionales e internacionales, para proteger a las empresas.

N**ormativo-deductivo.**En segundo lugar, normativo-deductivo, apoyándonos también en la literatura económico-social-financiera-contable; en el análisis de la normativa; en el análisis de las encuestas a través de un tratamiento estadístico; en las hojas de trabajo realizadas para observar en la información integrada las referencias a los intangibles relacionados con la seguridad de la información; en la aplicación del modelo de Sharpe a las empresas del Ibex-35 objeto del trabajo de investigación. Para ejecutar este estudio, hemos confeccionado una hoja de trabajo, donde aparecen los items relacionados con la ciberseguridad con el objetivo de establecer unos mínimos deseables por encima de los ítems actuales.

**Estructura de la investigación:**

Con el fin de conseguir los objetivos establecidos en nuestro trabajo de investigación hemos estudiado como estructura de la investigación los siguientes capítulos.

Con referencia al capítulo primero:justificación, objetivos y estructura de la investigación.

Capítulo segundo: revisión bibliográfica dela valoración de inmovilizados tangibles e intangibles. Desde el modelo de negocio hasta el capital intelectual. También hemos incluido la bibliografía novedosa relacionada con la valoración de las empresas de internet y su importancia en un paradigma digital.

En el tercer capítulo, estudiamos los aspectos conceptuales de la ciberseguridad, así como alcance y contenido de la misma, las vulnerabilidades de los sistemas informáticos,los organismos internacionales de seguridad informática en la Unión Europea, España, Alemania, Estados Unidos, México.

Los nuevos delitos informáticos en España, tras la reforma del Código Penal a través de la ley orgánica 1/2015 de 30 de marzo.

La legislación vigente para salvaguardar el derecho de los usuarios en la red.

La directiva comunitaria en materia de ciberseguridad. Directiva UE 2016/1148-eur-lex-europa.eu, sobre el incremento de los niveles de seguridad en redes y sistemas de información para establecer, promover, impulsar los mecanismos para conseguir un ciberespacio económico, industrial y social seguro.

La problemática del seguro, la situación actual del ciberseguro en España, incluyendo los gastos derivados de investigación forense, la notificación a los clientes, la gestión de la reputación, cobertura en caso de fraude informático por transferencia de fondos, cobertura en caso de extorsión, descontaminación de malware, medidas relativas a la protección de datos.

La problemática del ciberseguro alcance y contenido. La importancia del importe de las primas de ciberseguros.

Los activos de información (propiedad intelectual, propiedad industrial, marcas, bases de datos, aplicaciones informáticas, etc.) y su importancia en base a los pronunciamientos de los Organismos Internacionales Privados.

Las funciones de las comisiones de auditoría interna y la comisión de tecnología al unísono en base al nuevo código de buen gobierno 2016 y a la responsabilidad social corporativa, como es el caso de BBVA a través de los correspondientes reglamentos, pueden ayudar a hacer frente a la problemática de la ciberseguridad.

Capítulo cuarto: los activos intangibles y su importancia estratégica en la empresa, ligados al logro de las ventajas competitivas. La seguridad de la información, nueva ventaja competitiva en las organizaciones. Nos detendremos en la teoría de los recursos y de las capacidades. Recursos y capacidades como activos intangibles y su impacto en el valor de la empresa. Los criterios para implementar una estrategia. Enfoque estructural y teoría de los recursos y capacidades. Activos tangibles e intangibles. La gestión del capital intelectual. Los activos de información como base de la ventaja competitiva. El plan director de seguridad de la información en las empresas como ventaja competitiva. Esquema de mínimos informativos. Consideraciones finales. La ciberseguridad considerada como cuestión estratégica de la empresa.Breves referencias a la Norma Internacional de Contabilidad (NIC) 38.

El capítulo quinto, se refiere a los métodos de valoración de empresas, con especial énfasis en los métodos de valoración de intangibles y más en concreto en el método de valoraciones por opciones reales.

El capítulo sexto, está relacionado con la encuesta sobre valoración de empresas y ciberseguridad. Aparecen los resultados y comentarios de la investigación en base a una encuesta dirigida a directivos, auditores internos y externos, de determinadas empresas al objeto de extraer unos mínimos deseables para dar solución en parte, ya que la seguridad absoluta es imposible, a los problemas de ciberseguridad de las empresas y a partir de ahí, sacar posteriormente las conclusiones de la tesis en consonancia con las hipótesis de partida y objetivos.

El capítulo séptimo,contempla la métrica de los intangibles, la información cualitativa en la valoración de intangibles, las hojas de trabajo de las empresas más internacionales de España, según la bolsa de valores.

El capítulo ocho, trata sobre la valoración de Telefónica como empresa precursora en materia de ciberseguridad y de seguridad de la información, Jiménez Naharro, F. (2017) e igualmente en otras materias a lo largo de su historia desde 1924, Gutiérrez Hidalgo[18], F[19]. at al. (2013). Jiménez Naharro, F[20].(2010)

Por último, las conclusiones y las futuras investigaciones

## 1.4. BIBLIOGRAFÍA

BONSON PONTE, E., CANAY PAZOS, J.R., ESCOBAR RODRÍGUEZ, T., GAGO RODRÍGUEZ, S. (2000): "Contabilidad de Gestión y Tecnologías de la Información: ¿Pérdida de Relevancia? I Encuentro Iberoamericano de Contabililidad de Gestión. Valencia. Noviembre de 2000

[18] La Legitimación de Telefónica, S.A. a través de sus informes anuales (1924-2004). "Reflexiones sobre apariencias y contenido en los informes históricos de Telefónica". "Es necesario buscar en el pasado de las compañías para conocer su presente", según Hopwood (1987). V Encuentro de Trabajo de Historia de la Contabilidad. Universidad Castilla La Mancha. Abril de 2005.

[19] "Evolución histórica de la contabilidad de costes y de gestión (1885-2005). En la página 114, "en la década de los ochenta las empresas redescubrieron el papel crítico que la producción jugaba en la generación de ventaja competitiva", cita como ejemplos, entre otros: "la introducción de las operaciones productivas controladas por ordenador el CIM o entorno de producción integrado por ordenador".

[20] Valoración de las empresas Biotecnológicas. Coordinador Andalucía Business Angels Networks. UPO 2010

BONSON, E., ESCOBAR RODRÍGUEZ, T., GAGO RODRÍGUEZ, S. (2001) "Los sistemas de Reporting Digital. Hacia un nuevo Enfoque de la Contabilidad Financiera".

CAÑIBANO ET AL., (1999): "La relevancia de los intangibles para la valoración y la gestión de empresas: Revisión de la literatura" Revista Española de Financiación y Contabilidad, vol. 28, nº 100, pp.17-88.

GÓMEZ ÁLVAREZ, J. (2016): "Análisis de la información sobre gobiernocorporativo proporcionado por las empresas mediante un estudio de casos longitudinal". Tesis Doctoral. Diciembre 2016.

GUTIÉRREZ HIDALGO, F., CASASOLA BALSELLS, M. A., PÉREZ CHAMORRO, V.A., SÁNCHEZ BARRIOS, M. (2013): "Valoración contable de la inversión extranjera: el caso de la Compañía Nacional de España y la cantidad neta invertida (1924-1932). Revista Española de Historia de la Contabilidad, número 19, diciembre 2013. Págs. 48-75.

JIMENEZ NAHARRO, F., DE LA TORRE GALLEGOS, A. (2017): "Valoración de empresas y análisis bursátil". Editorial Pirámide, S.A. Ediciones. ISBN: 9788436836905. Idioma: varios. Enero de 2017.

MARC GOODMAN (2015), "Los delitos del futuro". Editorial Ariel.

MARK JEWELL. (2007) "T.J. Maxx Theft Believed Largest Hack Ever". Associated Press, 30 de marzo de 2007.

MICHAEL WEISSENSTEIN (2011), "Mexico´s Cartels Build Own National Radio System". En: Associated Press, 27 de diciembre de 2011.

PONEMON INSTITUTE (esponsorizado por Symantec), (2013): "Cost of Data Breach Study: Global Analysis", mayo de 2013.

ROBIN SIDEL Y ANDREW R. JOHNSON (2012): "Data Breach Sparks Worry" en: Wall Street Journal, 30 de marzo de 2012.

ROSS KERBER. (2007): "Banks Claim Credit Card Hack Breach affected 94 Millions Accounts". New York Times, 24 de octubre de 2007.

STEVE JOHSON (2013): "Cybersecurity Business Booming in Silicon Valley". En: San José Mercury News, 13 de de 2013.

TOM SIMONIT E. (2012): "The antivirus Era is Over". En MIT Technology Review, 11 de junio de 2012.

TRUSTWAVE HOLDINGS 2013, Glogal Security Report.

TUA PEREDA, J. (1989): "Información Pública y Sistemas informativo en las entidades de depósitos". Revista Española de Financiación y Contabilidad, Vol. 19, nº 58, pp.97-128.

TUA PEREDA, J. (2006): "Ante la reforma de nuestro ordenamiento: nuevas normas, nuevos conceptos: Un ensayo", Revista de Contbilidad ASEPUC, vol. 19, nº 18, pp. 145-175

VERIZON RISK TEAM, 2012, "Data Breach Investigations Reports, páginas 3 y 51.

http://cso.computerworld.es/seguridad-en-cifras/el-96-de-las-empresas-no-estan-preparadas-para-un-ciberataque

http://cso.computerworld.es/seguridad-en-cifras/hacienda-admite-el-fallo-de-cruce-de-datos-entre-contribuyente

http://cso.computerworld.es/alertas/nuevo-phishing-que-aprovecha-la-declaracion-de-la-renta-para-suplantar-a-la-agencia-tributaria

http://cso.computerworld.es/seguridad-en-cifras/el-97-de-los-usuarios-son-incapaces-de-identificar-correos-de-phishing

http://cso.computerworld.es/seguridad-en-cifras/los-ataques-a-la-administracion-y-empresas-de-interes-creceran-un-40

http://www.networkworld.es/seguridad/a-casi-medio-billon-de-dolares-asciende-el-coste-de-la-ciberdelincuencia

http://www.networkworld.es/seguridad/solo-una-cuarta-parte-de-las-empresas-utiliza-ciberaseguradoras

http://www.ciospain.es/industria-y-utilities/falta-madurez-en-las-empresas-para-afrontar-los-riesgos-de-la-ciberseguridad

http://www.ciospain.es/industria-y-utilities/transformacion-digital-como-sobrevivir-y-prosperar

http://www.ciospain.es/finanzas/transformacion-digital-de-la-banca-hacia-nuevos-modeloshttp://www.ciospain.es/industria-y-utilities/fabricacion-conectada-el-reto-de-la-cuarta-revolucion-industrial

http://www.ciospain.es/finanzas/como-impactan-en-la-banca-la-automatizacion-y-los-modelos-de-digitalizacion

http://www.ciospain.es/movilidad/el-43-de-las-empresas-utilizara-soluciones-iot-a-finales-2016-segun-gartner

http://cso.computerworld.es/seguridad-en-cifras/enisa-confia-en-el-mercado-de-ciberaseguradores-para-concienciar-a-las-empresas

http://cso.computerworld.es/cibercrimen/los-riesgos-ciberneticos-podrian-provocar-un-shock-global-similar-a-la-crisis-de-2008

http://cso.computerworld.es/cibercrimen/espana-es-el-tercer-pais-mas-castigado-por-los-ciberataques

http://cso.computerworld.es/seguridad-en-cifras/cuales-son-los-sectores-empresariales-mas-vulnerables-ante-un-ciberataque

http://cso.computerworld.es/seguridad-en-cifras/las-empresas-sufren-un-ciberataque-cada-15-segundos

http://cso.computerworld.es/seguridad-en-cifras/mas-de-la-mitad-de-las-empresas-espanolas-sufrieron-ataques-de-malware-y-spamhttp://cso.computerworld.es/seguridad-en-cifras/repuntan-el-ransomware-y-el-malware-movil

http://cso.computerworld.es/cibercrimen/aplicaciones-parches-y-monetizacion-del-malware-los-principales-riesgos-para-las-empresas

http://cso.computerworld.es/proteccion-de-datos/telefonica-incorpora-faast-a-su-portfolio-iot-de-ciberseguridad

http://www.idgtv.es/entrevistas/la-ciberseguridad-en-iot-vista-por-chema-alonso

(http://www. Imperva.com). (Imperva/Press Release/ Http/2: Imperva Hacker Intelligence Iniciatitive Report Reveals Four High-Profile Flaws en the Latest Version of the worldwide Web´s Underlying Protocol, Las Vegas, Aug.03, 2016, Globe newawire)

# CAPÍTULO 2.- REVISIÓN BIBLIOGRÁFICA SOBRE LA VALORACIÓN DE EMPRESAS

## 2.1 INTRODUCCIÓN

En este capítulo desarrollaremos una revisión bibliográfica que nos ayude a entender la problemática de la valoración de empresas en general y en particular la valoración de empresas basada en los activos intangibles como elementos estratégicos claves que marcan una ventaja competitivaen el desarrollo del negocio con respecto a las empresas de su entorno. Este entorno está cada día más conectado a sistemas informáticos.

La infraestructura del tendido eléctrico, los gasoductos, los sistemas de emergencias, el control del tráfico aéreo, el mercado bursátil, el agua potable, el alumbrado público, los hospitales y los sistemas de saneamiento y salud pública dependen de tecnologías y de internet para funcionar. Las transacciones, propias del negocio de las empresas, en un mundo global, efectuadascon tarjeta de crédito, las terminales de pago en los puntos de venta y los cajeros automáticos que mantienen el flujo mundial de comercio y un capitalismo tecnológico en mano de los más fuertes (en estos momentos hemos sacado al ser humano del organismo y hemos convertido a la máquina en la columna vertebral de la civilización) se frenarían en seco sin los ordenadores que ejecutan la red.Por tanto, a la hora de hablar de valoración de empresas debemos tener en cuenta en nuevo paradigma digital en el que nos encontramos inmerso.

La mayoría de las infraestructuras básicas del mundo utilizan sistemas de supervisión, control y adquisición de datos para funcionar, se trata de sistemas informáticos especializados en su mayoría anticuados que controlan equipamiento físico con funciones tan dispares como hacer circular los trenes por las vías, distribuir la energía en una ciudad, Clay Wilson (2008).

Hemos tomado como referencia la información referida a la valoración de empresas establecida en la tesis doctoral “propuesta metodológica de valoración del sector biotecnológico y sus intangibles de Santiago Moreno, I[21]. (2015) y le hemos añadido información específica sobre la valoración de empresas en internet.

Posteriormente, nos dedicaremos a repasar la bibliografía sobre la valoración de empresas, desde el punto de vista de la teoría financiera. Vamos a comenzar refiriéndonos a los distintos significados del término valor, objetivo financiero y también nos vamos a referir a los distintos trabajos que relacionan el capital intelectual con la valoración de empresas.

La definición de empresa ha tenido distintos significados según las posturas adoptadas por los distintos autores, tanto nacionales como extranjeros, que han tratado el concepto: Brealey y Myers (1999), Brigham (1985), Durbán (1993, 2008), Ruiz y Gil (2004), Loring (1997), Cuervo (1979), Bueno Campos (1991) y Suárez Suárez (1981, 1988), Ruiz y Jiménez (1999a, 1999b) y Arruñada (1990).

Atendiendo a las diferentes definiciones de empresa dadas por los autores citados anteriormente, podemos resumir éstas como aquella entidad que integra y coordina diversos factores productivos, conel propósito de hacer frente a una demanda insatisfecha, para lo cual

[21] “Propuesta metodológica de valoración del sector biotecnológico y sus intangibles”. Tesis dirigida por el profesor Jiménez Naharro, F. Universidad de Sevilla.

necesitará realizar inversiones,para lo que habrá de disponer de recursos para poder financiarlas.

Según Suárez Suárez (1996), siempre se ha considerado en el mundo económico capitalista que el objetivo fundamental de la empresa es la obtención del máximo beneficio o lucro. Este único objetivo ha recibido duras críticas.

Para Ruiz y Jiménez (1999a, 1999b) el objetivo financiero de una empresa es la maximización del valor de la empresa en el mercado, que se traducirá a la larga en crecimiento y mejora de la situación económica y patrimonial, cosa que no tiene por qué ocurrir con la maximización del beneficio. Este objetivo se resume en conseguir una buena relación entre rentabilidad y riesgo. Por tanto, la empresa debe elegir las decisiones que combinen la mejor relación entre rentabilidad y riesgo, al objeto de llevar al máximo el valor de la empresa para el accionista.

Nosotros entendemos que la creación de valor tiene su origen en las ventajas competitivas sostenibles de la empresa, entendiendo éstas como cualquier recurso y/o capacidad de la empresa que la diferencia de otras, colocándola en una posición relativa superior que sus competidoras, permitiendo a la compañía obtener una tasa de beneficios persistentemente mayor que éstas.

Según Grant (2002), para que un recurso o capacidad proporcione una ventaja competitiva deben darse dos condiciones. Primera, que el recurso o capacidad sea escaso. En segundo lugar, el recurso o capacidad debe ser relevante (Grant, 2002).

El mantenimiento de las ventajas competitivas de una compañía dependerá, según Hill y Jones (2009), de tres factores: barreras a la imitación, las posibilidades de la competencia para imitar la ventaja competitiva y el dinamismo de la industria que hace transitoria las ventajas competitivas empresariales (debido a la intensidad de los cambios, la innovación en producto y los ciclos de vida acortados de los productos/servicios).Entendemos que la estrategia empresarial y su puesta en acción en el modelo de negocio, deben recoger tales ventajas competitivas sostenibles, articuladas éstas en los recursos y capacidades de la organización.

## 2.2 DE LA ESTRATEGIA AL MODELO DE NEGOCIO, EL VALOR DE LA VENTAJA COMPETITIVA

La cuestión que nos ocupa no es otra que la incidencia del modelo de negocio en la valoración de empresas, para ello debemos empezar por conocer la estrategia y los cimientos de la seguridad de la información de una organización, como núcleo en un nuevo paradigma digital, y los diversos conceptos que nos permiten entender, con claridad y detalle, el modelo de negocio de una compañía. Hoy el modelo de negocio está íntimamente relacionado con su seguridad.

Existen diversos autores, tanto nacionales como extranjeros que han estudiado tanto el concepto *estrategia* como el *modelo de negocio*. Por lo que respecta al primero, entre los autores extranjeros destacamos los siguientes: Porter (1987 y 1982), Hamel y Pahalad (1999), Kaplan y Norton (2008, 2006, 2004, 2001, 2002), Collins y Porras (1996), Collins (2001), Treacy y Wieserma (2004), Kim y Mauborgne (2002, 2005), Newman y Morgerstern (1944), Drucker (1954), Chandler (1962), Ansoff (1965), Quinn (1980), Grant (2002), Magretta (2002), Mintzberg (1990), Zook y Allen (2012), Ohmae (2004), Evered (1983), Dixit y Nalebuff (1991) y Schelling (1980). Entre los autores nacionales cabe mencionar los siguientes: Bueno y Morcillo (1997), Navas y Guerras (2012), Fernández (1987), Martínez y Milla (2005), Castro et al (2009), Martínez (2013), Bueno (1998).

Por lo que respecta a los diversos autores extranjeros que han estudiado el concepto *modelo de negocio*, destacamos a los siguientes: Osterwalder y Pigneur (2011), Osterwalder et al. (2012, 2015), Maurya (2014), Hamel (2000), Zook y Allen (2012), Zott y Amitt (2010), Viscio y Paternack (1996), Timmers (1998), Afuah & Tucci (2000), Eisenmann et al. (2001), Schmid et al. (2001), Chesbrough y Rosenbloom (2002), Sandulli y Chesbrough (2009), Magretta (2002), Afuah (2004), Davenport, Leibold y Voelpel (2006), Christensen, Johnson y Kagermann (2008), Skarzynski y Gibson (2008), Demil y Lecoq (2010), Itami y Nishino (2010), Gambardella y McGahan (2010), Teece (2010), Yunus, Moingeon y Lehmann (2010), Mullins y Komisar (2010), Ghemawat (1991), Liberty, Boulton y Samek(2001), Palacios y Duque (2011).

A nivel nacional mencionamos a los siguientes autores: Freije (2014), March y Seoane (2006), López (2012), Martínez (2013), Jiménez et al (2013), Escudero (2013), Casadesus-Massanell (2004), Casadesus-Massanell y Ricart (2007, 2010), March et al (2007), López et al. (2013).

A continuación, explicaremos con más detenimiento esa aproximación al valor de la empresa que consideramos, tanto de la estrategia inicialmente, y cómo se pone en acción tal estrategia con el modelo de negocio.

### 2.2.1 La Estrategia empresarial. Los conceptos que permiten su definición y desarrollo

En un contexto económico global, rápidamente cambiante como el actual, donde la gestión empresarial está cada vez más influenciada por los avances tecnológicos y donde el talento es escaso, se hace necesario que las empresas sepan adaptarse, con flexibilidad, a un entorno de demanda cambiante, aprendiendo y actuando según su razón de ser, sabiendo a dónde quieren llegar, contando con la disponibilidad de unos recursos y unas capacidades generadas por el personal de la empresa. Todo esto nos lleva al concepto de la estrategia y a quién corresponde su aplicación: el líder empresarial.

Desde nuestro punto de vista, una buena definición de estrategia debe de contemplar la inclusión de una serie de conceptos que permitan a la empresa obtener ventajas competitivas sostenibles, nos referimos a los siguientes: liderazgo, aprendizaje, flexibilidad, recursos, capacidades y competencias.

En relación al *liderazgo* encontramos los siguientes autores, tanto extranjeros como nacionales: Drucker (2000), Bennis (1995), Kotter (1990, 2000, 2007, 2015), Goleman (2013); Goleman et al. (2007); Covey (2004, 2014); Yukl (2008), Lencioni (2002); Boyatzis y Mckee (2006), Blanchard y Johnson (2002); Maxwell (2007), Hemphill y Coons (1957), Katz y Kahn (1978), Rauch y Behling (1984), Richards y Engle (1986), Jacobs y Jaques (1990), Schein (1992), Drarth y Palus (1994), Zook y Allen (2012), Collins (2001), Word et al. (1974), Vroom y Yetton (1973), Gladstein (1984), Hackman, Brosseau y Weiss (1976), Hewett, O´Brien y Hornik (1974), McGrath (1991), Pearce y Ravlin (1987), Wofford Y Goodwin (1994), Zaccaro, Ritman y Marks (2001), Podsakoff, Mackenzie y Ahearne (1997), Ancona (1990), Ancona y Caldwell(1992), Galbraith (1973), Sundstrom, DeMeuse y Futrell (1990), Bandura (2000), Guzzo, Yost, Campbell y Shea (1993), Campion, Papper y Medsker (1996), Chen y Bliese (2002), Gibson, Randel y Earley (2000), Gully et al. (2002), Mulvey y Klein (1998), Pearce, Gallagher y Ensley (2002), Castro et al. (2009), Heifetz et al. R. A. (2012), Zaccaroa et al. (2001), Day et al. (2004, 2006), Heldal y Antonsen (2014), Funke y Knott (2014), Mehra et al. (2006).

Por lo que respecta a el *aprendizaje* encontramos los siguientes autores, tanto extranjeros como nacionales: Kogut y Zander (1992), Ventura et al. (2003), Agryris y Schön (1978), Daft y Weick (1984), Fiol y Lyles (1985), Levit y March (1988), Stata (1989), Slater y Narver (1995),

Scwandt y Marquardt (2000), Dibella et al. (1996), Garvin (1993), Mayo y Lank (1994), Senge (1993, 1999), Burgelman (1990), Martínez (2001), Crossan, Lane y White (1999), Pedler et al. (1991), Argyris (1999), Nonaka y Takeuchi (1995), Helleoid y Simonin (1994), Mowerly y Oxley (1995), Kim (1998), Cohen y Levinthal (1994), Zahra y George (2002) y Rodríguez y García (2004); Ordóñez y Parreño (2005).

En relación a la *flexibilidad* encontramos los siguientes autores, tanto extranjeros como nacionales: Bettis y Hitt (1995); Nandakumar et al. (2014); Hitt, Keats y DeMarie (1998), Ansoff (1965, 1980), Overholt (1997), Thompson (1967), Perrow (1970), Mascarenhas (1982), Kogut (1985), Harrigan (1982, 1985), Hitt et al. (1998), Paik (1991), Sanchez (1993, 1997), Volberda (1996, 1997), Evans (1982), Leeuw y Volberda (1996), Lund y Gjerding (1996), Upton (1994), Youndt, Snell, Dean y Lepak (1996), MacDuffie (1995), Beer et al. (1990), Wright y Snell (1998), Keiser y Ferris (1997), Lau (1996), Teece, Pisano y Shuen (1997), Aaker y Mascarenhas (1984), Piore y Sabel (1984), Evans (1991), Sánchez (1997), Shimuzu y Hitt (2004), Tamayo 2006), Dyer y Shafer (1999), Abbot y Banerji (2003), Stopford y Baden- Fuleer (1990), Malone (1986), Kulatilaka y Marks (1988) y Mahavan (1996), Krijnen (1979, 1985), Frazer (1985), Keiser y Ferris (1997) y Weick, (1979).

Refiriéndonos a los *recursos, capacidades y competencias* encontramos los siguientes autores, tanto extranjeros como nacionales: Grant (2002), Barney (1991, 2007), Porter (1991, 1987), Prahalad y Hamel (1990), Itami (1987), Navas y Guerras (2012), López Sintas (1996), Nelson y Winter (1982), Selznick (1957), Ansoff (1965), Hamel y Prahalad (1999), Fernández Rodríguez (1993), Salas (1996), Bueno (1998), Bueno y Morcillo (1997), Bueno et al. (2012, 2003)

Una vez reflejado los conceptos que consideramos fundamentales para diseñar una estrategia, con capacidad para generar ventajas competitivas sostenibles, nos centraremos en las diversas definicionesque dan los diversos autores sobre el término *estrategia*, en el cual no existe un claro consenso sobre su significado.

Ronda y Guerras (2012) realizaron un estudio cienciométrico sobre el concepto de estrategia a partir de 91 definiciones relevantes desde el año 1962 hasta el año 2008, que permitió elaborar una definición de consenso a partir de las palabras más repetidas en las distintas definiciones. Así, se consideró que la estrategia representaba “la dinámica de la relación de la empresa con su entorno y las acciones que emprende, para conseguir sus objetivos y/o mejorar su rendimiento mediante el uso racional de recursos” (Navas y Guerras, 2012).

El concepto de estrategia es introducido en el campo económico y académico por Newman y Morgerstern(1944, Theory of Games and Economic Behavior, Princeton University Press, Princeton, Nueva Jersey) con la teoría de los juegos, en ambos casos la idea básica es la competición.

Posteriormente, fue introducida en el ámbito empresarial por Drucker (The Practice of Management,1954). Para este autor, la estrategia es un intento por organizar información cualitativa y cuantitativa, que permita la toma de decisiones efectivas en circunstancias de incertidumbre (basadas más en criterios y análisis objetivos que en las experiencias o la intuición) y que da respuesta a dos preguntas: ¿Qué es nuestro negocio? Y ¿Qué debería ser?Alfred Chandler JR. (1962) define la estrategia como la determinación de metas y objetivos básicos de largo plazo de la empresa, la adopción de los cursos de acción y la asignación de recursos necesarios para lograr dichas metas.

Igor Ansoff (1965) considera a la estrategia como el lazo común entre las actividades de la organizacióny las relaciones producto-mercado, tal que definan la esencial naturaleza de los negocios en que está la organización y los negocios que ésta planea para el futuro.

Para Quinn (1980), una estrategia es el modelo o plan que integra los principales objetivos, políticas ysucesión de acciones de una organización en un todo coherente.Una estrategia bien formulada ayuda a ordenar y asignar los recursos de una organización de una forma singular y viable basada en sus capacidades y carencias internas relativas, en la anticipación a los cambios del entorno y en las eventuales maniobras de los adversarios inteligentes (Grant, 2002).

Para Andrews (1987), la estrategia es el modelo de objetivos, propósitos o metas y de las principalespolíticas y planes para alcanzarlos, planteados de tal manera que definen en qué negocio está o va a estar la compañía y la clase de compañía que es o que va a ser.

Para Ohmae (2004), la estrategia empresarial, en una palabra, es ventaja competitiva. El propósito de laplanificación estratégica es permitir que la empresa obtenga una ventaja sostenible sobre sus competidores.

Las estrategias exitosas (Grant, 2002) se centran en el análisis de dos elementos: losRecursos/Capacidades empresariales y el Entorno. Este enfoque corresponde con el conocido análisis DAFO, en el que la estrategia se formula en relación a cuatro grupos de consideraciones: Debilidades y Fortalezas (recursos y capacidades), y Amenazas y Oportunidades (entorno externo).

Para Grant (2002) las estrategias fructíferas se componen de cuatro elementos clave: están basadas en un entendimiento profundo del entorno; están dirigidas hacia objetivos precisos a largo plazo, están implantadas con resolución, coordinación y eficaz aprovechamiento de las capacidades y compromiso de todos los miembros de la organización; están fundadas en un detallado conocimiento de las capacidades internas de la organización.

Según Zook y Allen (2012), la estrategia tiene cada vez menos que ver con un plan rígido en busca de mercados en crecimiento y más con el desarrollo de una dirección general construida en torno a unas competencias profundas y de enjundia distintiva, capaces, en todo momento, de aprender, mejorar, ponerse a prueba y adaptarse de forma progresiva.

Una estrategia competitiva (Magretta, 2002) explica el método que va a emplear la empresa para hacer las cosas mejor que sus competidores, siendo distintos a sus rivales e inimitables.

En resumen, podemos definir Estrategia como un conjunto de actividades, metas y recursos que se analizan, organizan y plantean, de tal manera que permitan hacer un desarrollo de actividades estructuradas, de acuerdo a los recursos y capacidades de la organización, ligadas éstas al mercado en donde se actúa, con el fin de cumplir con los objetivos empresariales y de obtener ventajas competitivas, distintas a sus rivales e inimitables.La estrategia también nos tiene que mostrar un camino claro para el futuro de la compañía, contemplando sus distintas deviaciones económicas. Para ello, ésta debe contar con características especiales, tales como liderazgo, aprendizaje, flexibilidad, innovación continua y la gestión del cambio y del capital humano.

## 2.2.2. El Modelo de negocio como elemento generador de valor

Las organizaciones son sistemas abiertos (Bueno, 1982), y por tanto no se pueden entender de forma aislada, sino interactuando mutuamente con el entorno.

Además, éstas son dinámicas y están retroalimentándose continuamente, en función de sus experiencias, aprendiendo de sus fracasos y maximizando sus éxitos.

Para Chesbrough y Rosenbloom (2002) hay tres grandes diferencias entre Estrategia y Modelos de Negocio. En primer lugar, El modelo de negocio está enfocado en la creación de valor y nos muestra como la organización va a capturar ese valor. La estrategia va más allá, preocupándose de cómo hacer sostenible esta ventaja competitiva. En segundo lugar, el modelo de negocio es una arquitectura para convertir la innovación de las actividades en valor económico, pero no se preocupa del impacto en el valor para el accionista. La estrategia por el contrario va más allá. Finalmente, la estrategia maneja mucha más variables procedentes del entorno.

Con el diseño del modelo de negocio no solamente vamos a definir cómo hacer las actividades de una forma más eficaz o eficiente, sino también se buscará que tales actividades estén relacionadas entre sí con un doble objetivo: el ser coherentes con la propuesta de valor de la organización y que ésta sea diferente a las de la competencia (López, 2012).

Según Teece (2010) y Casadesus-Masanell y Ricart (2007, 2010) un modelo de negocio describe el diseño o la arquitectura de la forma de crear valor, entregarlo al cliente y los mecanismos para capturar valor para la organización.

Para López (2012), las organizaciones se preocupan cada vez más del análisis de su modelo de negocio, como herramienta para conseguir una ventaja competitiva sostenible. Para este mismo autor, desde una perspectiva estratégica se está tomando conciencia de la importancia que tiene la coherencia del modelo de negocio para la sostenibilidad de la ventaja competitiva.

Un modelo de negocio debe explicar cómo funciona una organización y debe responder a tres preguntas: ¿Quién es el cliente? ¿Qué valora el cliente? Y ¿Cómo se va a generar dinero en este negocio? (Drucker, 1992). Yunus et al. (2010) también considera que un modelo de negocio radica en la forma de generar valor, mediante una proposición de valor y una fórmula de generación de beneficios que captura valor para la organización.

Para Christensen, Johnson y Kagermann (2008) son cuatro los elementos interrelacionados que componen un modelo de negocio: la proposición de valor para el cliente, la fórmula de obtención de beneficios, los recursos y capacidades clave y los procesos clave. Mediante estos cuatro elementos interrelacionados las organizaciones crean y entregan valor para los clientes, así como capturan valor para ellas mismas.

Para Skarzynski y Gibson (2008) un modelo de negocio describe como una compañía crea, entrega yextrae valor.

Davenport, Leibold y Voelpel (2006) consideran que un modelo de negocio es simplemente, la forma enla que una organización ha decidido hacer las cosas. Creando y entregando valor a los clientes yobteniendo un beneficio de esa actividad, así como una rentabilidad para sus accionistas.

Para Demil y Lecocq (2010), la definición de modelo de negocio se centra en la realización de actividadesrelacionadas con la producción de una proposición de valor para los consumidores. Itami y Nishino (2010) proponen que un modelo de negocio está compuesto por dos

elementos: un sistema de negocio (sistema de producción y entrega) y un modelo de beneficios.

Para Zott y Amit (2010), un modelo de negocio es un sistema de actividades por lo que se debedeterminar cómo es el contenido, estructura y gobierno de éstas. Asimismo, se deben diseñar de acuerdo a cuatro características temáticas: Contenido innovador, capacidad de retención de stakeholders, complementariedades y eficiencia.

Los recursos y capacidades están muy unidos al concepto de modelo de negocio, como apuntan Zott yAmit (2010), el concepto de modelo de negocio está muy ligado al de un sistema de actividades como unión de recursos y capacidades.

Para Chesbrough (2010), el modelo de negocio debe de cubrir las siguientes funciones: articular la proposición de valor; identificar el segmento de mercado; estructurar la cadena de valor requerida para crear y distribuir la oferta y los activos complementarios necesarios para soportar su posición en la cadena de valor; detallar los mecanismos de ingresos por los que la firma obtendrá el pago por el producto o servicio; estimar los costes de estructura y el potencial de beneficios; describir la posición de la organización dentro de la red generadora de valor junto con clientes y proveedores; formular la ventaja competitiva por la que la organización innovadora conseguirá y mantendrá ésta sobre sus rivales.

Eisenmann et al. (2001) consideran que un modelo de negocio se refiere a la naturaleza de los servicios que las firmas proveen a sus consumidores, y las actividades que se realizan para entregar esos servicios. Schmid et al. (2001) concretan los elementos del modelo de negocio en seis componentes genéricos y de consideración conjunta: La misión, la estructura, los procesos, los ingresos, los temas legales y la tecnología.

Para Timmers (1998) la definición de modelo de negocio incorpora tres conceptos: la arquitectura del producto, el servicio, y la información que fluye. Viscio y Pasternack (1996) consideran que un modelo de negocio se compone de cinco elementos: identidad, liderazgo, capacidades, misión y control de la misión.

Para Magretta (2002), los modelos de negocio describen un sistema, el modo de funcionar de las piezas de una empresa y su forma de encajar. Sin olvidarse nunca de la competencia. Esta misma autora asimila el concepto de modelo de negocio como historias que explican de qué forma funcionan las empresas: se comienza con una hipótesis, después se comprueba en la práctica y se modifica si hace falta. Cuando los modelos de negocio no funcionan, es porque el argumento no se ratifica en la práctica (la historia no tiene sentido) o porque las cifras no se materializan (la cuenta de resultados no cuadra).

Según Osterwalder y Pigneur (2011), un modelo de negocio describe las bases sobre las que una empresa crea, proporciona y capta valor. Para estos autores, la mejor manera de describir un modelo de negocio es dividirlo en nueve módulos básicos (segmentos de mercado, propuestas de valor, relaciones con el cliente, canales, fuentes de ingresos, recursos claves, actividades claves, asociaciones claves y estructura de costes) que reflejen la lógica que sigue una empresa para conseguir ingresos. Estos nueve módulos cubren las cuatro áreas principales de un negocio: clientes, oferta, infraestructura y viabilidad económica.

Para López (2012) un modelo de negocio es un sistema generador de valor para el cliente y para lapropia organización, que utiliza una serie de recursos y capacidades para realizar unas actividades interdependientes que conforman la arquitectura organizacional y que son el reflejo de la estrategia realizada.

El modelo de negocio (Escudero, 2013) es una herramienta previa al plan de negocio que permitirá definircon claridad qué se va a ofrecer al mercado, cómo se va a hacer, a quién se vende, cómo se vende y de qué forma se van a generar ingresos. El modelo de negocio es una visión de conjunto de todo lo que es un negocio, es decir, cómo una empresa crea, desarrolla y captura valor.

Mullins y Komisar (2010) se refieren al modelo de negocio como el patrón de la actividad económica quedetermina si una empresa se queda sin liquidez, o no, y si ofrece, o no, un rendimiento atractivo a sus inversores. En resumen, el modelo de negocio es el apuntalamiento económico de la empresa en todas sus facetas.

Según Mullins y Komisar (2010), todo modelo de negocio comprende cinco elementos clave, queconsiderados en conjunto, determinan su viabilidad económica: el modelo de ingresos (el dinero que se recibe de los clientes a cambio de algo que se les vende), el modelo de margen bruto (se calcula a partir de la diferencia entre los ingresos y todos los gastos directamente relacionados con la fabricación o distribución de los productos o servicios comercializados), el modelo de gastos de explotación (todos los gastos cotidianos en el que debe incurrir una empresa, además de los gastos directamente relacionados con la producción y la comercialización), el modelo de capital circulante (suma de dinero que una empresa necesita tener a su disposición a corto plazo para que el negocio siga funcionando) y el modelo de inversión (dinero para poner en marcha la actividad de la empresa, incluyendo un modesto colchón de liquidez de reserva).

Hamel (2000) considera que los conceptos de modelo de negocio y el concepto de negocio son lo mismo.Un modelo de negocio es un concepto de negocio que se ha llevado a la práctica de forma efectiva.

ParaHamel (2000) un concepto de negocio se compone de cuatro partes: la estrategia clave (misión empresarial, el ámbito de producto/mercado y la base para la diferenciación), los recursos estratégicos(competencias clave, los activos estratégicos y los procesos clave), la relación con el cliente y las conexiones de valor (proveedores, los asociados y las coaliciones).

Entre estos cuatro componentes los elementos que cohesionan el concepto de negocio son: los beneficios para el consumidor, la configuración de competencias (es la forma única en que las competencias, los activos y los procesos se combinan e interrelacionan respaldando a la estrategia) y los límites de la organización (se refiere a las decisiones referentes a lo que la empresa hace y lo que se prefiere contratar de su sistema de valor).

Para Zook y Allen (2012), un modelo de negocio se define como un plano que traduce la estrategia endecisiones y acciones claves, y cuyos componentes son evidentes y se refuerzan a sí mismos. El modelo de negocio lleva a la estrategia a la acción.

En base a las diversas definiciones dadas por los diversos autores, tanto nacionales como extranjeros,sobre el concepto modelo de negocio intentaremos sintetizar una propia definición, donde vengan recogidos las diferentes aportaciones realizadas por los autores anteriormente citados.

Entendemos que el modelo de negocio es una herramienta para conseguir una ventaja competitivasostenible, mediante la descripción de las bases sobre las que una empresa crea, proporciona y capta valor.

Estas bases se asientan sobre la identificación del cliente (segmento del mercado); la articulación de unapropuesta de valor diferencial basado en lo que valora este cliente; la

disponibilidad de los recursos, capacidades y procesos clave que hacen posible una propuesta de valor accesible a los clientes y bien conocida por éstos y una fórmula de obtención de beneficios (atendiendo a la estructura de ingresos y costes contemplada en tal modelo de negocio).

## 2.3 EL CAPITAL INTELECTUAL COMO FUENTE DE VALOR DEL MODELO DE NEGOCIO

El concepto que nos ocupa está estrechamente vinculado al apartado anterior donde estudiamos la importancia de la estrategia y el modelo de negocio. Consideramos que el Capital Intelectual debe ser la fuente de ventajas competitivas sostenibles que desarrolle la empresa en el mercado.

Este tema lo han tratado con profundidad diversos autores, tanto nacionales como extranjeros, tales como:

Wiederhold (2014); Bontis (1996, 1998); Brennan y Connell (2000); Brooking (1998); Bueno (1998, 2000, 2003, 2012, 1991); Bueno et al. (2003, 1997); Cañibano et al. (1999, 2002); Jiménez el al. (2013); Edvinsson y Malone (1999); Euroforum (1998); Omar (2005); García (2008); Kaplan y Norton (1997, 2001, 2002, 2004, 2006 y 2008); Lev (200, 2001); Nomen (2005); Petrash (1996); Rojo y Sierra (2000); Martínez y García (2005); Roos et al. (2001, 2006); Roos y Roos (1997); Saint-Onge (1996); Sotomayor y Larrán (2005); Stewart (1997); Sullivan (2001); Sveiby (2000); Pricewaterhousecoopers (1999); Hormiga et al. (2008); Ventura et al. (2003); Nevado y López (2002 y 2006); Castro et el. (2009); Sotomayor (2005); Bueno y Salmador (2000); Andriessen (2004).

En las economías desarrolladas, los inversores son conscientes de que la mayor parte de los recursos productivos de los negocios empresariales son intangibles y en mayor medida en los sectores tecnológicos, donde la innovación es la clave para poder competir.

La primera gran potencialidad de los intangibles es su capacidad de diferenciación. En la actualidad, casi todo tiene una calidad muy similar, un precio muy parecido y se encuentra en los mismos puntos de venta. Las elecciones de compra de los consumidores se reducen a short lists de marcas o empresas de cada sector de consumo, que ellos almacenan en su mente. Llegar a formar parte de esas tres o cuatro marcas o empresas es lo difícil y eso cada vez se consigue menos a través de las propiedades funcionales de la oferta y más porque algún atributo intangible puede ser decisivo en el proceso de compra.

En los últimos años se han realizado numerosos esfuerzos en la búsqueda de metodologías y modelos que contribuyan a mejorar la identificación y medición del Capital Intelectual. Esto ha provocado la aparición de modelos y métodos que pretenden conocer el valor y evolución en el tiempo de los intangibles generadores de valor.

A continuación, vamos a recoger las distintas definiciones de Capital Intelectual realizadas por diversosautores expertos, tanto nacionales como extranjeros.

Para Petrash (1996) existe una correlación directa entre cómo se han gestionado los activos intelectuales de una corporación y su éxito financiero. La oportunidad radica en ser capaces de visualizarlos, medirlos mejor y gestionarlos.

Kaplan y Norton (2002) consideran que el Capital Intelectual es el conocimiento que existe en una organización para crear una ventaja diferencial, basada en que las capacidades de los empleados de una organización satisfagan las necesidades de los clientes de ésta.

Sullivan (2001) afirma que capital intelectual es el conocimiento que puede ser convertido en beneficio.

Según Bueno (1998), el capital intelectual es el conjunto de competencias básicas distintivas de carácter intangible que permiten crear y sostener ventajas competitivas.

Roos et al. (2006) definen el Capital intelectual como todo recurso no-monetario y no-físico que es total o parcialmente controlado por la empresa y que contribuye a la creación de valor de la compañía.

Para Stewart (1997), el Capital Intelectual es el paquete de conocimiento útil o conocimientos, información, propiedad intelectual, experiencia que se puede poner en uso para generar riqueza.

Según Roos y Roos (1997), el Capital Intelectual es la suma de los activos “ocultos” de la compañía, no totalmente capturados en el Balance General e incluye el conocimiento de los empleados en la organización que dejan en la compañía cuando ellos se van.

Cañibano et al. (2002) definen capital intelectual como las fuentes no monetarias de beneficios económicos futuros, sin sustancia física, controlados, o al menos influidos por la empresa, como resultado de acontecimientos y transacciones pasadas (producidos por la empresa, comprados o adquiridos de cualquier otra manera) y que pueden o no ser vendidos separadamente de otros activos de la empresa.

Para Brooking (1998), el Capital Intelectual es la combinación de diferentes activos inmateriales (activos de mercado, activo humano, activos de propiedad intelectual y activos de infraestructura) que permiten funcionar a la empresa.

Cabrera y Rincón (2001) manifiestan que el Capital Intelectual es la principal fuente de ventaja competitiva para la empresa. Esto último, más todo lo expresado por los diferentes autores que hemos recogido, viene a corroborar nuestro fundamento, de que el capital intelectual debe ser el núcleo principal de la fuente de generación de valor de cualquier organización y que debe contenerse prioritariamente en el modelo de negocio de la empresa.

Atendiendo a las diversas definiciones dadas por el concepto que estamos tratando por los diversos autores aquí citados, podemos decir que el capital intelectual es el conocimiento útil (el liderazgo, el aprendizaje, la capacidad de adaptación y de ser ágiles, el conocimiento del personal, las relaciones con los proveedores y clientes, las patentes, las marcas, los procesos internos y la capacidad de I+D, etc.) formado por los recursos y activos intangibles, con capacidad de crear valor y obtener rentas superiores a la competencia, cuando tales intangibles se fundamentan en la ventaja competitiva sostenible de una organización.

## 2.4. UNA APROXIMACIÓN AL VALOR

En este apartado veremos en profundidad las definiciones de valor y precio, llevadas a cabo por diversos autores, tanto nacionales y extranjeros. Para ello, hemos realizado la pertinente revisión bibliográfica de tales conceptos, considerados fundamentales en nuestro estudio de investigación sobre modelos de valoración de empresas.

La problemática que nos ocupa, que no es otra que la valoración de empresas, empieza por conocer el concepto que le da origen, que es el del "valor" para después continuar con el término "precio". Existen diversos autores, tanto nacionales como extranjeros que han estudiado el concepto. Por lo que respecta a los autores extranjeros destacamos los siguientes: Carl Menger (1996); Screpanti y Zamagni (1997); Brilman y Maire (1990); Omar (2005), Adam Smith (1997); David Ricardo (1997); Karl Marx (1976); Jaensch (1974), PriceWaterhouseCoopers (1999). En el ámbito nacional destacamos a los siguientes: Santandreu y Santandreu (1998); Méndez (1996); Pérez-Carballo (1998); Caballer (1998); Beltrán (1976); Fernández Pirla (1974); Ruíz y Gil (2004); De la Torre y Jiménez (2012, 2014); Gil (2009); Fernández (2002); Fabregat (2009); Morales y Martínez (2006); Revello de Toro (2004), García (2008); Irimia et al. 2003).

Los términos valor y precio no son coincidentes y su diferenciación es el punto de partida obligado de cualquier proceso de valoración (Morales y Martínez, 2006).

A continuación, recogemos las diversas descripciones del concepto valor realizadas por diversos autores (nacionales y extranjeros) que recogemos a continuación:

Según Gil (2009), el sentimiento del valor trata de sopesar la utilidad y el perjuicio, la ventaja y el sacrificio, de escoger, tasar y clasificar. La percepción, basada en un sentimiento de valor, se combina con otras percepciones existentes al mismo tiempo que ella, con lo que el sentimiento entra en lucha con otros sentimientos. De esta manera, el objeto valorado se clasifica según un ideal y conforme determinadas reglas.

Para De la Torre y Jiménez (2012), el valor de un objeto lo determina la utilidad que tenga para el que lo adquiera, por lo que estaríamos ante una medida subjetiva del valor, ya que en la determinación del mismo intervendrían las características particulares de cada sujeto.

Revello de Toro (2004) considera que el valor es una cantidad obtenida mediante un procedimiento más o menos técnico y que se fundamenta en unos datos objetivos y contrastables (Morales y Martínez, 2006).

Brillman y Maire (1990) entienden por valor aquella cualidad convencional del objeto que le es atribuida como consecuencia de un cálculo o de una peritación. El valor no es un hecho, sino una opinión.

Para estos mismos autores, el valor busca su apoyo en un fundamento lógico o matemático lo más riguroso posible. Busca la objetividad, la neutralidad y la independencia frente a las partes, las relaciones de fuerzas en el mercado e incluso la propia situación del mercado.

De la Torre y Jiménez (2012) consideran que el valor es el resultado de un enfoque teórico que puede limitarse a realizar una simple comparación o a recurrir a una referencia, o por el contrario puede ser elresultado de un cálculo más o menos complejo mediante la aplicación de un método o de una fórmula.

Para estos mismos autores, el valor busca su apoyo en un fundamento lógico o matemático lo más riguroso posible. Busca la objetividad, la neutralidad y la independencia frente a las partes, las relaciones de fuerzas en el mercado e incluso la propia situación del mercado.

Según Fabregat (2009), el valor es por definición subjetivo, ya que depende de la utilidad de un bien para un inversor. Por lo tanto, no existirán valores únicos ni indiscutibles. El precio, si existe, es fruto de un acuerdo y, por tanto, sí que será único.

Respecto al término valor (García, 2008), podemos destacar las siguientes acepciones: valor de mercado: es el precio que marca el mercado, depende de la demanda y de la oferta de acciones (valor bursátil); valor contable: es el que corresponde según la contabilidad, valor intrínseco: es el que se obtiene después de que un analista haya examinado todos los datos relevantes de la empresa.

Es fundamental aclarar que no se puede confundir el concepto valor con el precio.

Fernández (2002) estima que el precio es la cantidad a la que el vendedor y comprador acuerdan realizar una operación de compra-venta de una empresa.

Para Revello de Toro (2004), el precio es la cantidad resultante de un proceso de negociación a partir de valores obtenidos en una metodología, y en el que se ponen de acuerdo las dos partes negociadoras: compradores y vendedores (Morales y Martínez, 2006). El comprador trata de minimizarlo y el vendedor, por el contrario, pretende maximizarlo.

Brillman y Maire (1990) consideran que el precio es consecuencia de una transacción (pago efectivo), es un hecho tangible.

Según Fabregat (2009), para llegar al precio es preciso empezar por la valoración y continuar con una fase de negociación.

PriceWaterhouseCoopers (1999) considera obvio que sobre el precio inciden multitud de factores,relacionados tanto con los propios intervinientes en su fijación (comprador y vendedor) como con las circunstancias exógenas que concurren en dicha transacción.

Entre los factores que habitualmente influyen en la determinación del precio de una empresa, seencuentran los siguientes (PriceWaterhouseCoopers, 1999):

Relacionados con el comprador: justificación estratégica de la operación, posibles sinergias, urgencia para realizar la operación, escasez de información sobre la empresa a adquirir y mejor información que el mercado sobre la empresa objeto; relacionadas con el vendedor: necesidad de vender por parte del accionista, urgencia en realizar la operación, mejor/peor información sobre desarrollos futuros del negocio, falta de sucesión empresarial y búsqueda de viabilidad futura a un negocio en declive.

Relacionados con circunstancias exógenas: recientes o previsibles nuevas regulaciones sectoriales que afectan al negocio, modificaciones sustanciales en tipos de interés, alteraciones sustanciales de los precios de los insumos y mayor o menor presión de otros competidores en la compra-venta.

El proceso negociador (Revello de Toro, 2004) debe iniciarse no en único valor, por muy exacto o sofisticado que parezca, sino en un rango de valoración más o menos amplio, que se determina en base a diferentes escenarios o hipótesis, que incluye análisis de sensibilidad de las variables claves. A partir del rango de valoración se va negociando el precio con la

incorporación de todos aquellos matices y factores subjetivos de muy difícil cuantificación que tiene cada parte involucrada en la transacción (Morales y Martínez, 2006).

Para García (2008), el resultado que se obtenga de una técnica de valoración siempre será un resultado referencial que puede guiar la discusión en una transacción.

Una vez contempladas las diversas definiciones dadas por los diversos autores aquí mencionados, en los conceptos valor y precio, podemos resumirlos de la siguiente manera.

En relación al valor, la mayor parte de las opiniones sobre el concepto se sustentan bajo la idea de que el valor viene representado por las expectativas de renta futura que un inversor espera conseguir de la empresa o proyecto de inversión, descontadas a una tasa que sea representativa del riesgo que ofrecedicha empresa y/o proyecto. Para ello se contemplan las dos variables fundamentales: *rentabilidad yriesgo*, con las cuales un buen analista debe buscar siempre el equilibrio adecuado.

Concretando, el *valor* recoge las opiniones que tienen el oferente y el demandante sobre la utilidad quetiene un objeto (tangible o intangible). Estaríamos pues ante una medida subjetiva del concepto en cuestión, ya que en la determinación del mismo se considerarían las características particulares de cada sujeto.

Respecto al precio y atendiendo a las diversas definiciones recogidas en nuestro estudio, podemosresumir su descripción como un hecho real fruto del acuerdo, en una negociación, entre el oferente (al alza) y el demandante (a la baja) del objeto (tangible o intangible), y que se suele tomar en consideración, en tal subasta, el empleo de una metodología de valoración que marque las reglas de la misma.

En resumen, mientras que el valor no deja de ser una opinión el precio es un hecho.

## 2.5. MODELOS DE VALORACIÓN DE EMPRESAS

A continuación, vamos a recoger la definición que dan diversos autores del concepto valoración de empresas, para posteriormente poder mostrar los diversos métodos de valoración de empresas que vamos a considerar en nuestro estudio de investigación. Para ello realizaremos la revisión bibliográfica pertinente, tanto de autores nacionales como extranjeros.

Para Fernández (2014a), la valoración de una empresa es un ejercicio de sensatez que requiere de unos conocimientos técnicos y que mejora con la experiencia. La sensatez y los conocimientos técnicos nos permiten saber para qué y para quién se está haciendo la valoración, el qué se está haciendo y el por qué se realiza de una forma determinada ésta.

En relación a la definición de valoración de empresas, consideramos lo siguiente.

PriceWaterhouseCoopers (1999) considera que las dificultades de aplicación de ciertos métodos devaloración, la vulnerabilidad de algunos instrumentos utilizados (proyecciones financieras) y los problemas para entender las diferencias entre precio y valor, producen un cierto escepticismo sobre el resultado de las valoraciones, que pueden llevar a concluir que cualquier resultado es posible al valorar un negocio, ya que, en el fondo, la valoración es un proceso absolutamente subjetivo.

Hay que admitir (PriceWaterhouseCoopers, 1999), en todo caso, que toda valoración tiene un ciertocomponente de subjetividad. Pero ésta puede y debe ser minorada mediante el análisis

riguroso de los datos de partida utilizados, el contraste de las hipótesis de futuro con las opiniones de los expertos y la utilización simultánea de más de un método de valoración.

En este sentido, el analista financiero (García, 2008) busca la "objetividad", la neutralidad y laindependencia frente a las partes, a través de un fundamento matemático o lógico lo más riguroso posible, es decir de un método normalizado que puede consistir en el resultado de una simple comparación o del cálculo de una fórmula (Ruiz y Gil, 2004).

Ruiz y Gil (2004) plantean una cuestión importante, en relación a si el concepto valor de la empresa esúnico o, por el contario, se pueden determinar diversos valores para una misma compañía.

Para estos mismos autores, es necesario tener en cuenta en el proceso de valoración los siguientes aspectos:

El procedimiento de cálculo del valor de una empresa supone la necesidad de predecir escenarios futuros, por lo que será imposible determinar un único valor, como consecuencia de la incertidumbre existente en dicha predicción, lo que nos llevaría a establecer un rango de valores entre los que se encontrará el valor más probable de la empresa;

El valor va a estar siempre influido por las características particulares del sujeto que está llevando a cabo la valoración;

Se debe de tener en cuenta cuál es el objetivo de la valoración, ya que en función del mismo podemos llegar a obtener distintos valores (De la Torre y Jiménez, 2012).

En definitiva, valorar es fundamentalmente (PriceWaterhouseCoopers, 1999) formarse un juicio, profesional e independiente, en base a la aplicación de un conjunto de metodologías y a la experiencia profesional.

Para De la Torre y Jiménez (2012), la valoración de una empresa es un proceso que busca la cuantificación de los elementos que constituyen el patrimonio de una empresa, su actividad, su potencialidad o cualquier otra característica de la misma susceptible de ser valorada.

Según Jiménez et al (2013), la valoración es un proceso de negociación en la que cada una de las partes esgrimirá las razones por las que está dispuesto a ceder, o adquirir, el objeto de la valoración, por no menos o por no más del precio establecido. Para apoyar estas razones en la negociación, se pueden emplear diversas metodologías de valoración, en donde cada uno intentará hacer prevalecer aquel método que mejor le sirva para justificar el valor que está dispuesto a pagar o cobrar.

Para AECA (1997), es indispensable el conocimiento de la valoración de empresas en el mundo de lasfinanzas, que considera las siguientes premisas: el objetivo de cualquier empresa es maximizar su valor; el valor de cualquier empresa viene determinado por su capacidad de generar renta; cualquier proceso de valoración debe consistir en transformar renta en valor.

Aceptar que el objetivo principal (García, 2008) de cualquier empresa es maximizar su valor, debeentenderse bajo la actual percepción de que la generación de riqueza se entiende asociada al desarrollo y mantenimiento de ventajas competitivas de naturaleza intangible. La práctica demuestra que una empresa que no presta atención a aspectos tales, como a sus empleados o a sus clientes, encontrará que su valor será inferior al de otra empresa que sí los considera (Cornell, 1993).

Una de las fases más importantes en la valoración (García, 2008) es obtener información. El analistaencargado de la valoración García, 2008), además de la información de la organización, debe buscar información del sector y los mercados, utilizando otras fuentes ajenas a la empresa objeto de valoración.

Lo más práctico será emplear las herramientas informáticas oportunas para estructurar la información entres niveles: información macroeconómica, sectorial y de la propia de la empresa.

En la práctica (Jiménez et al., 2013), los analistas, en numerosas ocasiones, no saben utilizar ni el métodode valoración adecuado ni aplicarlo en el momento adecuado. Esto es debido a que en los últimos años han surgido numerosas técnicas relacionadas con el ámbito de la valoración. Por ello, cada vez resulta más complicado dilucidar qué técnica está, o no, encuadrada dentro de cada uno de los bloques metodológicos de la valoración; y dentro de éstos, cuáles y cuándo son válidos en su aplicación.

Para Robinson (1986) los modelos de valoración de empresas (MVE) no son más que artefactos intelectuales basados en las teorías que a través de supuestos, simplifican la realidad.

En la actualidad, la importancia de los MVE (Omar, 2005) radica en que son un instrumento clave para medir el desempeño de la empresa. Identificar los “value drivers”, elaborar estrategias de planificación basadas en el valor de la empresa y ayudar a establecer los métodos de vinculación de una parte de la compensación administrativa con la creación de valor de la empresa (Weston y Copeland, 1995).

El concepto que ahora nos atañe, la valoración de una empresa es un proceso de formación de un juicio de valor sensato, basado en la experiencia y en el empleo de metodologías normalizadas (aceptadas por el mercado), que permitan la identificación de las fuentes de creación, destrucción y transmisión de valor.

Estas fuentes de valor las encontramos principalmente en el modelo de negocio, donde se pone en acción la estrategia empresarial competitiva y en donde se concentran los value drivers, que permitirán a obtención de ventajas competitivas sostenibles, las cuales ayudarán a justificar, en gran medida, tal valoración empresarial.

En resumen, la valoración dependerá de la situación de la empresa, del momento de la transacción y del método empleado.

Los modelos que ahora explicaremos y revisaremos bibliográficamente, son los siguientes: ModelosEstáticos, Modelos Mixtos, Modelos basados en múltiplos comparables, Modelos basados en el descuento de flujos, Modelos de valoración de intangibles, Modelos basados en la creación de valor para el accionista y las opciones reales.

Por último, y recalcando la recomendación del principio de Fernández (2014a), el método de valoraciónque se elija debe permitirnos saber a quién y para qué se hace tal valoración, el qué se está haciendo y el por qué se realiza de una forma determinada tal valoración.

## 2.5.1. Los Modelos de Valoración Estáticos

Los modelos de valoración estáticos basan la valoración empresarial en la situación histórica de la compañía, utilizando papa ello el balance como principal instrumento.

Los métodos con enfoque estático toman como referencia las cuentas y las cifras que conforman el Balance de la empresa (información contable a una fecha determinada), ya sea para aceptarlas como valor probable o para corregirlas y compararlas con el valor de mercado del subyacente que está representado (Omar, 2005).

Dentro de estos tipos de valoración estática destacamos los siguientes modelos: Valor contable o valor en libro (Book Value); valor contable ajustado, corregido o regularizado; valor de reposición sustancial; valor de liquidación; valor basado en los capitales permanentes empleados.

De este modelo parten diversos métodos desarrollados por diferentes autores, tanto nacionales como extranjeros, tales como:

El método de valor contable(Amat, 2011; García, 2008; Fernández, 2002 y 2014; Santandreu y Santandreu, 1998; Termes, 1998; Caballer, 1998; Martín y Trujillo, 2000; Cornell, 1993; De la Torre y Jiménez, 2012 y 2014; Ruiz y Gil, 2004; García, 2008; AECA, 1997; Omar, 2005; Fundación de Estudios Bursátiles y Financieros, 2009; Jiménez et al., 2013);El método del valor contableajustado(Amat, 2011; García, 2008; Termes, 1998; Caballer, 1998; Fernández, 2000, 2002 y 2014; AECA, 1997; De la Torre y Jiménez, 2012 y 2014; Ruiz y Gil, 2004; García, 2008; Omar, 2005; Fundación de Estudios Bursátiles y Financieros, 2009; Jiménez et al., 2013; Rojo, 2007*);*

El método del valor dereposición o substancial(Amat, 2011; García, 2008; ACCID, 2009; Omar, 2005; Barnay y Calba, 1977; Brilman y Maire, 1990; Jaensch, 1974; Caballer, 1998; Santandreu y Santandreu, 1998; Fernández, 2002 y 2014a; Martín y Ruiz, 1992; De la Torre y Jiménez, 2012 y 2014; Ruiz y Gil, 2004; García, 2008; Jiménez et al., 2013; Fundación de Estudios Bursátiles y Financieros, 2009; Rojo, 2007*);*

El método del valor deliquidación(Amat, 2011; Omar, 2005; Barnay y Calba, 1977; Brilman et al., 1990, Weston yCopeland,1995; Fernández, 2002 y 2014; Rojo, 1996 y 2007; De la Torre y Jiménez, 2012 y 2014; Ruizy Gil, 2004; Fundación de Estudios Bursátiles y Financieros, 2009);

El método del valor basado en loscapitales permanentesnecesarios(Omar, 2005; Martín y Trujillo, 2000; Santandreu y Santandreu, 1998;Rojo, 1996; Barnay y Calba, 1977; De la Torre y Jiménez, 2012 y 2014; Ruiz y Gil, 2004, Jiménez et al.,2013).

Este enfoque cuenta con una debilidad a considerar, la cual consiste en que no tiene en cuenta lasexpectativas de generación de renta de la organización ni la influencia del factor tiempo. Por lo que estos métodos infravaloran siempre a las empresas con expectativas.

Otras limitaciones generales importantes que encontramos en tales modelos, son: la incapacidad que se le imputa a la información contable en su modelo actual, para recoger, procesar y proporcionar información sobre determinados aspectos de la realidad económico-financiera de las empresas (Caballer, 1998); los datos de la Contabilidad histórica mostrados en el Balance no sirven para hacer valoraciones basadas en las expectativas (Rappaport, 2005); los ajustes y las regularizaciones que se proponen a las partidas del Balance para corregirlo no son factibles desde el punto de vista práctico ni tampoco del económico, puesto que no existen los mercados eficientes de donde se puedan extraer tales valores (Caballer, 1998); No tiene en cuenta:el valor del dinero en el tiempo; las posibilidades futuras de creación del mismo (Martín y Trujillo, 2000); la evolución futura de la empresa; las perspectivas del sector en el que está inserta; la situación de recursos humanos; la estructura organizacional; la planificación y las decisiones estratégicas (Fernández, 2002).

## 2.5.2. Los Modelos Mixtos de Valoración de Empresas

En este tipo de modelos (Omar, 2005) se prescinde de considerar el valor de la empresa en términos exclusivamente estáticos y se pasa a reconocer el valor dinámico de la misma.

Para Omar (2005), se parte del principio de que el valor de la empresa está compuesto por el importe inicial de las inversiones realizadas, llamado valor sustancial (Vs) y el valor emanado de su capacidad de generar rendimientos superiores a los exigibles, en función de su nivel de riesgo, llamado fondo de comercio (Adserà y Viñolas, 2003).

Valor de la empresa= Valor estático + Plusvalía potencial

Dentro de estos tipos de valoración destacamos los siguientes modelos de valoración: método clásico; método de la Unión de Expertos Contables europeos (UEC); método Simplificado de la formulación de la UEC; método Evolucionado de la formulación de la UEC; método Indirecto o de los Prácticos; método Directo o anglosajón; método de Compra de los resultados anuales; método de la Tasa sin Riesgo y con Riesgo; método de Barnay y Calba; modelo de valoración Ohlson; modelo de valoración Ohlson y Feltham; modelo de valoración de Edwards, Bell y Ohlson.

De todos estos diversos modelos parten diversos métodos desarrollados por diferentes autores, tanto nacionales como extranjeros, los cuales mostramos a continuación:

El método clásico(Termes, 1998; Brilman y Maire, 1990; Fernández, 2002 y 2014a; Adserá y Viñolas, 2003; Barnay y Calba, 1977; Rojo, 1996; Omar, 2005; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003).

El método de la UEC(UEC, 1962; Sanjurjo y Reinoso, 2003; PriceWaterhouseCoopers, 1999; Fernández, 2000; Martínez y García, 2005; De la Torre y Jiménez, 2014 y 2012; Omar, 2005; Fernández, 2002 y 2014a; Adserá y Viñolas, 2003; Barnay y Calba,1977; Rojo, 1996; García, 2008).

El método simplificado de la formulaciónde la UEC(Sanjurjo y Reinoso, 2003; PriceWaterhouseCoopers, 1999; Omar, 2005; Adserá y Viñolas, 2003; Fernández, 2002 y 2014; Brilman y Maire 1990; Martín y Trujillo, 2000; Barnay y Calba, 1977; De la Torre y Jiménez, 2014 y 2012).

El método evolucionado de la formulación de la UEC(Jiménez et al., 2013; De la Torre y Jiménez, 2014 y 2012; García, 2008; Ruiz y Jiménez, 1999a).

El método indirecto ode los prácticos(PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003; Fernández, 2000; Adserá yViñolas, 2003; Barnay y Calba, 1977; Brilman y Maire, 1990; Omar, 2005; Fernández, 2002 y 2014).

El método directo o anglosajón(Sanjurjo y Reinoso, 2003; Fernández, 2000; Rojo, 1996; Adserá y Viñolas,2003; Fernández, 2002 y 2014a; Omar, 2005; PriceWaterhouseCoopers, 1999).

El método de compra de los resultados(Fernández, 2000; Termes, 1998; Omar, 2005; Adserá y Viñolas, 2003; Fernández, 2002y 2014a).

El método de la tasa con riesgo y sin riesgo(Fernández, 2002 y 2014a; Omar, 2005; Adserá yViñolas, 2003).

El método de Barnay y Calba(Brilman y Maire 1990; Barnay y Calba,1977; Omar, 2005).

Modelo de valoración Ohlson (Ohlson, 1989 y 1995; Milla, 2010; Martínez y García, 2005; AECA, 2006; McCrae y Nilsson, 2001; Lo y Lys, 1999; Ota, 2000 y 2002; Rojo, 2007; Huang y Wang, 2008).

Modelo de valoración Feltham y Ohlson (Milla, 2010; Martínez y García, 2005; Iñiguez y Giner, 2006; Feltham y Ohlson, 1995; Bernard, 1995); Modelo de valoración de Edwards, Bell y Ohlson (Milla, 2010; Martínez y García, 2005; García- Ayuso y Monterrey, 1998).

### 2.5.3. Los Modelos de Valoración basados en indicadores

Este tipo de métodos de valoración (Omar, 2005) se utilizan para establecer analogías entre el valor de la empresa objeto y el de empresas similares cuyo precio es conocido.

La principal finalidad (De la Torre y Jiménez, 2012 y 2014) del modelo de valoración por ratios no consiste tanto en establecer un valor absoluto de lo que estemos valorando sino la comparación entre ellos con una referencia.

Son denominados por algunos autores como de valoración relativa (Martín y Trujillo, 2000; Adserà y Viñolas, 2003; Damodaran, 2002 y 2006; Fernández, 2002 y 2014a; Martínez y García, 2005) o de valoración bursátil (Caballer, 1998; Santandreu y Santandreu, 1998; Rojo, 1996; Brilman y Maire, 1990; Martínez y García, 2005; Fernández, 2002 y 2014a; Fernández y Carabias, 2013, Jiménez et al., 2013) debido a que el precio con que se relaciona el valor de la empresa está tomado del mercado de capitales.

Sin embargo, su aplicación práctica no se restringe a este ámbito, sino que también es de aplicación en variadas transacciones de empresas.

Destacamos los siguientes indicadores más empleados en valoración por comparables, aunque no los únicos:

De este modelo parten diversos métodos desarrollados por diferentes autores, tanto nacionales como extranjeros, tales como:

Q Tobin*:* Tobin, 1969 y 1978; Martín y Trujillo, 2000; Adserá y Viñolas, 2003; García, 2008; Martínez y García, 2005; Milla, 2010; Omar, 2005; Sennetti et al., 2004; Ruiz y Gil, 2004; Valhondo, 2003; Andriessen, 2004, Vélez-Pareja, 2013.

PER*:* Mascareñas, 2011; Ruiz y Jiménez, 1999a; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003; Rosenbaum y Pearl, 2013; Amat, 2011; Milla, 2010; Copeland et al., 2010; Rojo, 1996 y 2007; Keegan, 2008; Titman y Martin, 2009; Revello de Toro, 2004 y 2013; Damodaran, 2006, 2012; Martín y Trujillo, 2000; Brilman y Maire, 1990; Omar, 2005; Irimia et al., 2003; Milla, 2010; Fundación de Estudios Bursátiles y Financieros, 2009; García, 2008; De la Torre y Jiménez, 2014 y 2012; Martínez y García, 2005; ACCID, 2009; Adserá y Viñolas, 2003; Fernández, 2002 y 2014a; Joos y Zhdanov, 2005; Martínez, 2001; Ruiz y Gil, 2004; Fernández y Carabias, 2013; Jiménez et al., 2013; Keegan, 2008; Sahoo y Rajib, 2013; Penman, 1996.

PEG*:* Lev, 2013; Titman y Martin, 2009; Keegan, 2008; Revello de Toro, 2004 y 2013; Damodaran, 2006; De la Torre y Jiménez, 2014 y 2012; Martínez y García, 2005.

Ratio Precio sobre Ventas*:* Mascareñas, 2011; PriceWaterhouseCoopers, 1999; Amat, 2011; Titman y Martin, 2009; Damodaran, 2006, 2012; Omar, 2005; Adserá y Viñolas, 2003; Fernández, 2002 y 2014a; De la Torre y Jiménez, 2014 y 2012; Martínez y García, 2005; ACCID, 2009; Adserá y Viñolas, 2003; Fundación de Estudios Bursátiles y Financieros, 2009; Sanjurjo y Reinoso, 2003; Ruiz y Gil, 2004; Jiménez et al., 2013.

Ratio Price to Book:Mascareñas, 2011; Ruiz y Jiménez, 1999a; Titman y Martin, 2009; Keegan, 2008; Sennetti et al., 2004; Revello de Toro, 2004 y 2013; Damodaran, 2006, 2012; Omar, 2005; Martín y Trujillo, 2000; Termes, 1998; Adserá y Viñolas, 2003; Fernández, 2002 y 2014a; Milla, 2010; García, 2008; De la Torre y Jiménez, 2014 y 2012; Martínez y García, 2005; ACCID, 2009; Fundación de Estudios Bursátiles y Financieros, 2009; Irimia et al., 2003; Sanjurjo y Reinoso, 2003; Copeland et al., 2010; Ruiz y Gil, 2004; Ruiz y Gil, 2004; Andriessen, 2004; Jiménez et al., 2013.

Ratio valor de la empresa sobre Ebitda*:* Mascareñas, 2011; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003; Titman y Martin, 2009; Amat, 2011; Keegan, 2008; Damodaran, 2006; Omar, 2005; Fernández, 2002 y 2014; De la Torre y Jiménez, 2014 y 2012; Martínez y García, 2005; ACCID, 2009; Fundación de Estudios Bursátiles y Financieros, 2009; Revello de Toro, 2004 y 2013.

Ratio valor de la empresa sobre Ebit: Mascareñas, 2011; PriceWaterhouseCoopers, 1999; Revello de Toro, 2013; Keegan, 2008; Damodaran, 2006; Omar, 2005; Fernández, 2002 y 2014a; De la Torre y Jiménez, 2014 y 2012; Martínez y García, 2005; ACCID, 2009; Sanjurjo y Reinoso, 2003.

Ratio Dividend Yield: Damodaran, 2012; Adserá y Viñolas, 2003; Fundación de Estudios Bursátiles y Financieros, 2009; Revello de Toro, 2004; Omar, 2005.

Estos métodos de valoración poseen la ventaja de que son bastantes intuitivos y nada complejos, perosi se desconocen se pueden utilizar no adecuadamente y pueden llevarnos a errores. Para evitar estas dificultades tenemos que tener presente los siguientes aspectos: las ratios deben ser consistentes y mantenerse estables durante cierto tiempo, además el analista debe de trabajar con criterio, empleando datos homogéneos y calculados según los mismos criterios (De la Torre y Jiménez, 2012 y 2014).

## 2.5.4. Los Modelos de Valoración basados en descuentos de flujos

Estos tipos de métodos de valoración basados en los flujos descontados, se encuadrarían en un enfoque dinámico, los cuales valoran la empresa en función de las expectativas de renta generadas por ésta, es decir, con la suma actualizada de la renta que la empresa generará en el futuro.

Los métodos incluidos en este enfoque son de los más utilizados por la mayoría de los analistas. Dentro de los métodos de valoración dinámicos, como son los de flujos descontados, destacamos los siguientes modelos:

De este enfoque dinámico de valoración parten diversos métodos desarrollados por diferentes autores, tanto nacionales como extranjeros, los cuales exponemos a continuación:

Modelo del dividendo: Mascareñas, 2011; Lütolf-Carrol et al., 2009; Adsera y Viñolas, 2003; De la Torre y Jiménez, 2012, 2014; García, 2008; Milla, 2010; Ruiz y Gil, 2004; Revello de Toro, 2004 y 2013; Martínez y García, 2005; Damodaran, 2006 y 2012; Fernández, 2002, 2014a;

Fundación de Estudios Bursátiles y Financieros, 2009; Amat, 2011; Sanjurjo y Reinoso, 2003; Ruiz y Jiménez, 1999a.

Modelo del Valor en función de las oportunidades de crecimiento: Fundación de Estudios Bursátiles y Financieros, 2009; De la Torre y Jiménez, 2012, 2014; Jiménez et al, 2013; Ruiz y Jiménez, 1999a.

El Capital Cash Flow: Omar, 2005; García, 2008; Revello de Toro, 2004 y 2013; Fernández, 2002, 2014a, 2014b, 2014c.

El Free Cash Flow: Mascareñas, 2011; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003; Amat, 1999, 2011; Ruiz y Gil, 2004; Fundación de Estudios Bursátiles y Financieros, 2009; Razgaitis, 2003 y 2009; Damodaran, 2009, 2006 y 2012; Copeland et al., 2010; Revello de Toro, 2004 y 2013; Adsera y Viñolas, 2003; Omar, 2005; García, 2008; Milla, 2010; De la Torre y Jiménez, 2012, 2014; Irimia et al., 2003; Jiménez et al, 2013; Martínez y García, 2005; Rojo, 2007; Keegan, 2008; Smith, 1997; Smith y Parr, 2000 y 2005; Lütolf-Carrol et al., 2009; Bogdan y Villiger, 2007; Boer, 1999; Titman y Martin, 2009; Fernández, 2002, 2014a, 2014b, 2014c; ACCID, 2009; Murphy et al., 2012; Rosenbaum y Pearl, 2013; Ruiz y Jiménez, 1999a y 1999b; Chiu, 2013, Vélez-Pareja, 2013; Festel, Wuermseher y Cattaneo, 2013.

El Cash Flow disponible para los accionistas: Omar, 2005; Revello de Toro, 2004 y 2013; Martínez y García, 2005; Fernández, 2000, 2002, 2014a, 2014b, 2014c; ACCID, 2009; Amat, 1999; Sanjurjo y Reinoso, 2003; Adserà y Viñolas, 2003.

Uno de los temas de mayor dificultad y cuyo resultado influye cardinalmente en el valor probable de la empresa es la determinación de la tasa con la que se han de descontar los flujos de fondos proyectados.

Esta variable se vuelve crítica cuando la organización a valorar tiene diversas unidades productivas. Paradescontar el valor de los distintos flujos necesitamos una tasa apropiada.

La rentabilidad exigida para cada unidad de negocio y para la empresa en su conjunto, es un tema demáxima importancia. Por ello, será necesario incorporar como parte del ejercicio de valoración, una evaluación del riesgo de los flujos de caja libre, lo que se logra a través de la utilización del Modelo de Valoración de los Activos de Capital, Capital Asset Pricing Model (Sharpe, 1976; Dubán, 2008, Lintner, 1965; Mossin, 1968; Suárez Suárez, 1996; Ruiz y Gil, 2004; De la Torre y Jiménez, 2014, Fernández, 2014c; Bogdan y Villiger, 2007; Keegan, 2008 Chiu, 2013; Wirtz, 2012; Lütolf-Carrol et al., 2009; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003; Copeland et al., 2010; Ruiz y Jiménez, 1999ª y 1999b; Mascareñas, 2011).

Para descontar el valor de los distintos flujos necesitamos una tasa apropiada. Para definirla se debe proceder en forma coherente con lo que representa y, por tanto, no se puede definir independientemente de la renta que se obtiene de la inversión, ya que están íntimamente relacionadas. Una tasa alta no debe ir acompañada de una renta baja, ya que ello supondría la desaparición del negocio a largo plazo (Damodaran, 2002).

Debemos tener en cuenta que ésta debe cumplir dos objetivos fundamentales (Ruiz y Jiménez, 1999a): incluir el riesgo que supone dicha inversión e Incorporar el coste de oportunidad que tiene el inversor. El método que incluye de manera más eficiente estos dos factores es el establecido por el Capital Asset Pricing Model (CAPM), que debemos utilizar en el cálculo de los recursos propios (Damodaran, 2006).

Para la determinación del coste de los recursos propios por el CAPM es necesario determinar o estimar: el tipo de interés libre de riesgo en función de un valor o cartera de valores sin riesgo de impago; la prima de riesgo del mercado (Fernández, 2002), ésta representa la compensación adicional que los inversores esperan obtener por adquirir acciones de la empresa en lugar de un activo libre de riesgo. Se calcula por diferencia entre el promedio de los rendimientos de un índice representativo del mercado y el rendimiento de la inversión libre de riesgo (Brealey y Myers,2002).

## 2.5.5. Los Modelos de Valoración de Intangibles

Una de las cuestiones económicas que la sociedad del conocimiento se plantea es el notable cambio que se ha producido en la determinación de las causas del valor de las empresas. Antes, los activos tangibles eran los que determinaban el valor de una compañía de forma relevante y casi exclusiva; en la actualidad, existe un consenso en el mercado de considerar a los intangibles como los factores fundamentales para la fijación del precio de una empresa.

Sin embargo, este consenso se quiebra en el instante de intentar concretar, dentro de la realidad empresarial, cuáles son los activos y los recursos intangibles, y la dificultad se incrementa cuando se busca una metodología consensuada para la valoración de tales intangibles.

Después de una revisión bibliográfica exhaustiva, atendemos a la forma que tienen diversos autores, tanto nacionales y, fundamentalmente, extranjeros, de valorar genéricamente tales activos y recursos inmateriales generadores de valor.

Dentro de los métodos de valoración de intangibles, destacamos los siguientes enfoques:

En el enfoque de coste, el intangible (marca, patente, etc.) se valora teniendo en cuenta el coste de su desarrollo: adquisición, creación o mantenimiento del mismo durante cualquier etapa de desarrollo de lamisma (testeo, I+D, concepto del producto, etc.).

El enfoque de mercado tiene en cuenta las transacciones recientes (ventas, adquisiciones, licencias, etc.)en que se han visto involucradas intangibles similares (patentes, marcas) y para las que se dispone del precio de la operación.

El enfoque de ingresos/beneficios/flujos de caja se centra en la valoración de la capacidad de generaciónde beneficios o ingresos del intangible (marca, patente, etc.). Puede medirse estimando el valor presente de los beneficios o ingresos que se recibirán durante la vida del intangible. Por ello, requiere identificar los ingresos, beneficios o flujos de caja futuros o pasados atribuibles al intangible y actualizarlos o capitalizarlos a valor presente.

Por lo que respecta al *enfoque de Coste*, en la valoración de intangibles, encontramos los siguientes autores nacionales y extranjeros que tratan la materia: Murphy et al, 2012; Pérez y Salinas, 2008; Salinas, 2007; Reilly y Schweihs, 1998; Smith, 1997; Smith y Parr, 2005.

Los autores contemplados en nuestro estudio por el *enfoque de Mercado* son los siguientes: Murphy etal, 2012; Pérez y Salinas, 2008; Salinas, 2007; Reilly y Schweihs, 1999; Smith, 1997; Smith y Parr, 1994 y 2005.

Los autores nacionales y extranjeros, que han estudiado el *enfoque de Ingresos/Beneficios/Flujos decaja* en la valoración de intangibles, son los siguientes: Murphy et al, 2012; Jiménez y Escobar, 2007;Torres, 2002; Reilly y Schweihs, 1999; Pérez y Salinas, 2008;

Salinas, 2007; Smith y Parr, 2005; Smithy Parr, 1994; García, 2008; Parr, 2007; Boer, 1999; Smith, 1997; Razgaitis, 2003 y 2009; Bogdan yVilliger, 2007; Damodaran, 2006; Fernández, 2002 y 2009; Keegan, 2008; Copeland et al, 2000; Lamothey Aragón, 2003; Schwartz y Gorostiza, 2000; Schwartz y Moon, 2000 y 2001; Kellog y Charnes, 2000;Omar, 2005; Rubio, 2003; Lamothe y Rubio, 2004; Adserá, 2002; Mascareñas, 2012; Rubio y Lamothe, 2005; López-Cózar y Rubio, 2008.

### 2.5.6. Los Modelos de Creación de valor

Para Fernández (2000), cuando la rentabilidad obtenida por los accionistas sea superior a la rentabilidadexigida por las acciones, una empresa crea valor para los accionistas. Esto nos indica que una compañía crea valor en un período cuando se comporta mejor que las expectativas.

Pero este mismo autor, también hay que recalcar que cuando aumenta el valor para los accionistas nose produce creación de valor para éstos, tal y como hemos considerado en el primer párrafo visto anteriormente.

Por consiguiente, la creación de valor es el aumento del valor para los accionistas por encima de lasexpectativas, lo que se refleja esto en la rentabilidad exigida por los accionistas (Fernández, 2000). Irimia et al. (2003) recalcan que para que se produzca creación de valor para el accionista se precisa que la rentabilidad para los accionistas sea superior a la rentabilidad que los mismos exigen a sus acciones.

Estos mismos autores consideran a la rentabilidad para los accionistas como el aumento del valor de lasacciones en un año determinado dividido por la capitalización al inicio del mismo. Por otra parte, la rentabilidad exigida a las acciones es la tasa que esperan obtener los accionistas para sentirse suficientemente remunerados, comparándola con inversiones de riesgo similares. Cuando se habla de aumento del valor para el accionista los autores se refieren a la diferencia entre la riqueza que se dispone a final de un período y la que se poseía el año anterior.

En este trabajo de investigación vamos a considerar los siguientes métodos de creación de valor:

EVA, nos encontramos diversos autores, tanto nacionales como extranjeros: Stewart, 2000 y 2013; De la Torre y Jiménez, 2013 y 2014; Fernández, 2000 y 2002; Ruiz y Gil, 2004; Irimia et al., 2003; Damodaran, 2006; Amat, 1999; Copeland et al., 2010; Carenys, 2013; Revello de Toro, 2004; Rappaport, 2005; Stern et al, 2001; García y López Barajas, 1998; Niresh y Alfred, 2014; Henryani y Kusumastuti, 2013; Roztocki y Kim, L.N., 1999; Alam y Nizamuddin, 2012; Salehi et al., 2014; Huang y Wang, 2008; Vijayakumar, 2012; Erasmus y Lambrechts, 2006; Damodaran, 2009; Sanjurjo y Reinoso, 2003; Milla, 2010; Martínez y García, 2005; Titman y Martin, 2009; Kramer y Pushner, 1997; PriceWaterhouseCoopers, 1999.

Beneficio Económico, nos encontramos diversos autores nacionales y extranjeros: Ruizy Gil, 2004, Sanjurjo y Reinoso, 2003; Fernández, 2000 y 2002; Irimia et al., 2003; Taggart et al, 1994; Copeland et al., 2010; Milla, 2010; PriceWaterhouseCoopers, 1999.

MVA (Market Value Added), nos encontramos diversos autores, tanto nacionales como extranjeros: Ruiz y Gil, 2004; Niresh y Alfred, 2014; Vijayakumar, 2012; Fernández, 2000 y 2002; Irimia et al., 2003; Copeland et al., 2010; Reddy y Rao, 2013; Milla, 2010; Kramer y Pushner, 1997; PriceWaterhouseCoopers, 1999.

CVA (Cash Value Added), nos encontramos diversos autores, tanto nacionales como extranjeros: Ruizy Gil, 2004; Fernández, 2000 y 2002; Milla, 2010; Boston Consulting Group, 1996; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003.

CFROI (Cash Flow Return On Investment), nos encontramos diversos autores nacionales y extranjeros: Ruiz y Gil, 2004;Madden, 1999; Erasmus y Lambrechts, 2006; Fernández, 2000 y 2002; Irimia et al., 2003; Sennetti et al., 2004; Boston Consulting Group, 1996; Milla, 2010; PriceWaterhouseCoopers, 1999; Sanjurjo y Reinoso, 2003.

Por último, ciertos autores encuentran problemas en los cometidos de este tipo de métodos de creaciónde valor para el accionista, como es el caso de los estudios realizados por Fernández (2002), el cual considera que partiendo de la base de que el aumento de valor de una empresa, en un período determinado principalmente, se debe a los cambios de las expectativas en cuanto al crecimiento de los flujos de caja de la compañía y los cambios del riesgo traducibles en la tasa de descuento.

Por ello, dado que la contabilidad sólo refleja la historia de la empresa es imposible que medidas fundamentadas en la contabilidad (EVA, CVA y beneficio económico) puedan medir la creación de valor.

## 2.5.7. Los Modelos de Opciones reales

En la teoría de las Opciones Reales, debemos valorar la opción de tener que tomar un nuevo camino por no cumplirse los objetivos previamente previstos. De esta forma, las opciones matizan al alza el valor de la empresa en función de la elección entre distintas vías - demorar, ampliar, abandonar, etc.- que dicha sociedad decida tomar, solucionando el problema de la infravaloración.

Es decir, que, bajo este enfoque, el valor de la empresa será igual al valor tras aplicar el método de los flujos descontados, más el valor de las opciones que pueda presentar. De esta forma, las opciones reales incorporan la flexibilidad y las oportunidades de crecimiento como fuentes de valor.

A continuación, vamos a considerar los siguientes modelos de opciones reales:

De este modelo parten los tres métodos que vamos a contemplar en nuestra investigación y que van a ser desarrollados por diferentes autores, tanto nacionales como extranjeros, los cuales exponemos a continuación:

*Modelo de Black-Scholes*: Mascareñas, 2011; Ruiz y Gil, 2004; Lamothe y Méndez, 2013; De la Torre y Jiménez, 2012 y 2014; Jiménez et al., 2013; Ruiz y Jiménez, 2000; Jiménez y Escobar, 2007; Adserá y Viñolas, 2003; Martínez y García, 2005; Keegan, 2008; Amat, 2011; Rojo, 2007; Fundación de Estudios Bursátiles y Financieros, 2009; Fernández, 2002, 2013; Murphy et al., 2012; Boer, 1999; Razgaitis, 2003 y 2009; Copeland y Antikarov, 2001;Omar, 2005; García, 2008; Amram y Kulatilaka, 2000; García, 2001; Beaton, 2010; Damodaran, 2009, 2012, 2006; Tamayo, 2006; Bogdan y Villiger, 2007; MacMillan y Van Putten, 2005; Mascareñas et al., 2004; Lamothe y Aragón, 2003; Villiger y Bogdan, 2006; PriceWaterhouseCoopers, 1999.

*Modelo Binomial*: Mascareñas, 2011; Ruiz y Gil, 2004; De la Torre y Jiménez, 2012 y 2014; Lamothe y Méndez, 2013; Ruiz y Jiménez, 2000; Mascareñas, 2007 y 2012; Kester, 1991; Jiménez et al., 2013; Adserá y Viñolas, 2003; Martínez y García, 2005; Rojo, 2007; Keegan, 2008; ACCID, 2009; AECA, 2014; Fundación de Estudios Bursátiles y Financieros, 2009; Titman y

Martin, 2009; Fernández, 2002, 2013; Revello de Toro, 2013; Murphy et al., 2012; Boer, 1999; Nomen, 2005; Razgaitis, 2003 y 2009; Copeland y Antikarov, 2001; Omar, 2005; García, 2008; Amram y Kulatilaka, 2000; Lamothe y Aragón, 2003; García, 2001; Beaton, 2010; Damodaran, 2009, 2012, 2006; Tamayo, 2006; Bogdan y Villiger, 2007; Trigeorgis y Mason, 1991; Martín, 2004; Rubio y Lamothe, 2005 y 2006; Mascareñas et al., 2004; López- Cózar y Rubio, 2008; Rubio, 2003; Kellogg y Charnes, 2000; Borissiouk y Peli, 2001; Joos y Zhdanov, 2005; Lavoie, 2004; Villiger y Bogdan, 2006; Copeland et al., 2010; PriceWaterhouseCoopers, 1999.

*Modelo de Simulación Montecarlo*: Mascareñas, 2011; Ruiz y Gil, 2004; De la Torre y Jiménez, 2012 y 2014; Lamothe y Méndez, 2013; Jiménez et al., 2013; AECA, 2014; Jiménez y Escobar, 2007; Adserá y Viñolas, 2003; Martínez y García, 2005; Ruiz y Jiménez, 2000; Fundación de Estudios Bursátiles y Financieros, 2009; Murphy et al., 2012; Boer, 1999; Nomen, 2005; Razgaitis, 2003 y 2009; Copeland y Antikarov, 2001; Omar, 2005; García, 2008; García, 2001; MacMillan y Van Putten, 2005; Mascareñas et al., 2004; Lamothe y Aragón, 2003; Borissiouk y Peli, 2001; Mascareñas, 2007; Jiménez y Escobar,2007; Blasco y Ribal, 2009; Villani, 2013.

Para Fernández (2013), los principales problemas con los que nos encontramos al valorar opciones reales son: dificultad para definir los parámetros necesarios para identificar y valorar las opciones reales; dificultad para definir y cuantificar la volatilidad de las fuentes de incertidumbre; dificultad para calibrar la exclusividad de la opción.

## 2.6. CONSIDERACIONES FINALES

En la actualidad hay muchos modelos que intentan medir el efecto de los intangibles, pero muy pocos son los que intentan integrar éstos en la valoración de empresas y, por tanto, darle un valor determinado y ver como ellos contribuyen al valor y gestión de la empresa.

Esta dificultad se acrecienta cuando trabajamos en sectores de alta volatilidad y crecimiento como ocurre con las empresas con problemáticas relacionadas con la seguridad de la información con grandes exposiciones de información a ciberamenazas y vulnerabilidades, problemática que nos ocupa.

Cuando abordamos los principales métodos de valoración de empresas en internet, podemos referirnos: a los métodos de valoración cuantitativos donde se aplican técnicas como el descuento de flujos de caja, las compañías comparables y la metodología de las opciones reales; y a los métodos de valoración cualitativo donde se utilizan factores tales como el modelo de negocio, la tecnología o la percepción del mercado.

Algunas compañías sin beneficios son valoradas por encima de las llamadas compañías de la vieja economía. ¿Están justificadas estas valoraciones?, ¿Qué factores influyen en la valoración?, ¿Cómo valorar estas empresas?

Existen dos razones fundamentales por las cuales resulta difícil valorar las compañías de internet: En primer lugar, las industrias y las empresas que la componen son tan jóvenes que existe muy poca información financiera disponible mediante la cual poder predecir rentabilidades futuras; en segundo lugar, la industria se está desarrollando a una velocidad tan rápida que si existe información histórica es probable que sea de menor utilidad para evaluar estas empresas que para evaluar aquellas que pertenecen a industrias más establecidas, o, incluso, a aquellas que no pertenecen de alta tecnología.

Considerando esta situación, resulta complicado valorar estas compañías utilizando métodos tradicionales. A pesar de todo, la industria de internet ofrece una importante ventaja, la

disponibilidad de una gran cantidad de datos no financiero sobre el uso de internet, los cuales pueden ser utilizados por inversores en la predicción de ingresos futuros. Estos datos provienen directamente de las empresas, así como de compañías de rating independientes, tales como Media Metrix, PC Data, Nielsen/Netratings (http://www.nielsen-netratrings.com, OJD (http://www.ojd.es), e incluye entre otros números, estadísticas sobre páginas web vistas y visitantes.

Entre los factores que influyen en la valoración están (ciberconta.unizar.es/lección/valempint/inicio.html): Crecimiento esperado del negocio; mercado objetivo final de la empresa de internet; margen del beneficio en cuestión; beneficios.

Respecto al primer factor, si una compañía es capaz de incrementar sus ventas con mayor rapidez, o si el mercado bursátil percibe que el subsector en el que se encuentra la compañía de internet tendrá un fuerte crecimiento en el futuro, entonces el precio que se pagará por estas acciones será más alto. A modo de ejemplo, las empresas B2B (Business to Bussines) cotizan a precios mucho mayores comparativamente que las B2C (Business to Consumers) debido a las grandes expectativas de negocios que están generando las B2B.

Respecto al segundo factor, lo importante aquí no es la capacidad de la empresa de internet de multiplicar sus ventas en el siguiente año o dentro de dos años, sino a largo plazo cual es la población objetivo. Es el caso de Terra en el año 2000, debido a que el ámbito de actuación de Terra era el mercado iberoamericano, mientras que por ejemplo Tiscali.it sería sólo Italia.

Con referencia al Margen del Negocio en cuestión, por ejemplo, una empresa de subastas se limita a intermediar en compraventas de productos entre particulares y funciona a comisión, con lo que la comisión tiende a ser mayor que si lo comprara directamente al productor.

En el caso de los beneficios, si los inversores piensan que nos encontramos ante una revolución industrial, entonces, una empresa de internet que se dedicara a obtener beneficios para repartírselo entre los socios en lugar de conquistar el mundo, sería una empresa poco atractiva a los ojos del mercado secundario.

Actualmente, se disponen de tres tipos de instrumentos financieros que sirven para valorar las empresas de internet: el descuento de flujos de caja futuros; la utilización de las compañías comparables; la metodología de las opciones reales.

Con referencia al descuento de los flujos de caja futuros, esta metodología estima la cantidad de flujos positivos y negativos que una compañía generará en el futuro y descuenta el valor de esos flujos futuros al valor de hoy. Tradicionalmente, este método está basado en expectativas de ventas y tasas de descuentos futuras. Entre los inconvenientes de este modelo para el caso que nos ocupa estarías: necesidad de realizar una proyección financiera en detalle (ingresos, gastos, inversiones); dificultad de prever el futuro (ritmo de crecimiento, cambios en el modelo de negocio, competencia); dificultad de establecer la tasa de descuento (riesgo), el valor terminal. ¿Cómo se pueden calcular los ingresos futuros de una empresa que trabaja en un negocio completamente nuevo y en constante cambio?

El siguiente método que se puede aplicar es el de la utilización de compañías comparables, este método está basado en la investigación de otra compañía que cotice en el mercado de valores y que posea características similares en cuanto a: pertenencia al mismo sector, tamaño similar, evolución futura, adquisiciones recientes, etc. Con estos datos se obtienen unas ratios indicativas del valor de estas compañías tomadas como modelo y se aplican con el fin de

obtener el valor de la compañía que queremos valorar. Así se obtiene un valor aproximado al que el mercado asignaría si la empresa cotizase en el mismo y se comportase de una manera parecida a las del resto de su sector.

Entre los inconvenientes de este método están: la no existencia de dos empresas iguales; los múltiplos utilizados en un mercado de valores no tienen por qué ser idénticos a los de cualquier otro; la diferencia en el tamaño de las empresas de un sector junto con el número de acciones admitidas a cotización e, incluso, la pertenencia a un índice bursátil de referencia puede ser inútil la utilización de comparables; la gran volatilidad de las empresas de internet hace que el valor de los ratios de comparación varíen ampliamente de forma continuada; la diferencia de la implantación de internet entre distintos países obliga a extremar la precaución a la hora de establecer comparaciones entre compañías.

Los ratios y multiplicadores que pueden ser utilizados como elemento de comparación serían:

Múltiplo de los ingresos por ventas (valor de mercado de la empresa/ingresos por ventas), en este caso el valor teórico de una compañía se obtendría mediante el producto de este múltiplo por los ingresos dela compañía. Un aspecto que es necesario definires si el valor de la compañía en el mercado se refiere a su capitalización bursátil o el valor de mercado de sus activos.

Múltiplos de los visitantes únicos (valor de mercado de la empresa/visitantes únicos), así obtenemos una ratio que se denomina multiplicador de los visitantes únicos de la empresa. Si multiplicamos el valor del ratio por el número de visitantes únicos de la empresa obtendremos su valor de mercado (http://www.webmergers.com/calc.htm), el problema sería la dispersión de valores de los múltiplos de visitantes únicos que si es grande, la dispersión, dificultaría la valoración de las empresas.

Múltiplo de páginas vistas (valor de mercado de la empresa/páginas visitadas), esta ratio es una expresión del valor recibido por los inversores, basado en el número de personas que visitan la página web específica.

Multiplicador de suscriptores y usuarios registrados, se utiliza principalmente en la valoración de los proveedores de servicios online, los portales y los brokers online.

Multiplicador del EBITDA (beneficio operativo + amortizaciones + intereses+ impuesto. El motivo por el que se utiliza este tipo de beneficio a la valoración de las empresas de internet es porque al no tener recursos suficientes para hacer frente al servicio de la deuda, no van a tener beneficios, ni impuestos ni capacidad para amortizar sus activos fijos. Este método es utilizado para las empresas de telecomunicaciones que han alcanzado su madurez (TimeWarner o Disney), en el caso de empresa de reciente creación se utiliza EBITDA libre de gastos de marketing, debido al enorme volumen de dichos gastos al que tienen que hacer frente inicialmente dichas empresas.

PER normalizado, precio de mercado actual /valor actualizado del beneficio por acción. Muy útil para aquellas empresas que presentan pérdidas en la actualidad.

Otros múltiplos y relaciones: (Ingresos/costes del e marketing directo; ventas/empleados; Ingresos/coste del ancho de banda; Ingreso/alcance).

Metodología de las opciones reales. Este método está recomendado para compañías que presenten las siguientes características: sus mercados tengan un alto nivel de incertidumbre;

mantengan algún tipo de liderazgo en su sector y estén dirigidas por personas que comprenden las opciones y tienen una cierta habilidad para ejercitarlas.

Método propuesto por L. Lamothe (2000) (1) Precio= Beneficio por acción/K + VAOC (valor actual de las opciones de crecimiento de la compañía). K= tasa de descuento utilizada para actualizar los valores.

Dado que Precio P0= Dividendo/K-g (tasa de crecimiento)

PER= P0/BPA.

De aquí se deduce que PER= P0/BPA = 1/k (1 + VAOC/BPA)

Conclusiones:

A mayor VAOC, mayor será el precio de las acciones de las compañías tecnológicas.A mayor tasa de crecimiento g, obtenemos mayor Po (precio de la acción), y por tanto un mayor PER (es decir, en principio, tienen mayores posibilidades de crecimiento).

Como el valor actual de las opciones de crecimiento de las compañías de internet es muy alto y el beneficio por acción, si existe, es bajo, esto hace que se generen cifras de PER casi desconocidas hasta ahora.

Esto explica gran parte de por qué los inversores están actualmente más interesados en valorar las estrategias de la compañía, para valorar así su VAOC, que en los beneficios y dividendos presentes. Este crecimiento esperado es, por tanto, el pilar fundamental de la creación actual de valor para el accionista.

Método de valoración: Análisis cualitativo. Hanno Beck (2000).

Para poder llevar a cabo un análisis más profundo en la valoración de empresas de internet, es necesario completar el anterior análisis cuantitativo con la realización de un análisis cualitativo donde se tengan en cuenta aspectos tales como: importancia de ser el primero en entrar, el valor de la marca, la fortaleza del modelo de negocio, el valor del equipo de dirección, etc. Todos estos aspectos pueden ser recogidos.

Factores críticos de éxito:

Dirección/Gestión: experiencia, cualidades específicas del sector, capacidad de la dirección, creatividad.

Modelo de negocios: Barreras de entradas (culturales, costes de entrada, posibilidad de copia del negocio), amenaza de productos sustitutivos, fuentes de ingresos diversificadas, tamaño del mercado, poder de negociación de clientes y proveedores, tasa de crecimiento del mercado.

Tecnología: Innovación tecnológica, innovación de productos específicos, innovación de procesos específicos.Percepción del mercado: liquidez, ratio call / put

## 2.7. BIBLIOGRAFÍA

AAKER, D.A.; MASCAREÑAS, B. (1984): The need for strategic flexibility. Journal of Business Strategy, Vol. 5.

ABBOT, A.; BANERJI, K. (2003): Strategic flexibility and firm performance: the case of US based transnational corporations. Global Journal of Flexible Systems Management

ACCID (2009): Valoración de empresas. Valoración de marcas e intangibles. Fernández, P. Profit. Barcelona.

ALCOVER, S. (2009): Metodología del descuento de flujos de caja (DCF). Aplicación a una empresa de distribución minorista.---

FABREGAT, J. (2009): Introducción a los métodos de valoración de empresas--- Fernández, P. (2009): Valoración de marcas e intangibles.---

LABATUT, G. (2009): La valoración de la empresa mediante el método comparativo o por múltiplos.

ADSERÁ GEBELLÍ, X. (2002): La valoración de las empresas de nuevas tecnologías. Trabajo de investigación de doctorado. Universidad Complutense. Madrid. Septiembre.

ADSERÁ, X. Y VIÑOLAS, P. (2003): Principios de Valoración de Empresas. Ed. Deusto, Bilbao.

AECA Asociación Española de Contabilidad y Administración de Empresas (1997): Principios de Valoración de Empresas, Estudio de Aplicabilidad de los Diferentes Métodos de Valoración. Documento 5. Ed. Gráficas Ortega. Madrid.

AECA Asociación Española de Contabilidad y Administración de Empresas Concepto y uso del EBITDA como recurso generado en explotación. Opinión número 4 de la Comisión de Principios y Normas de Contabilidad de AECA, fecha: Diciembre de 2016

AECA Asociación Española de Contabilidad y Administración de Empresas (2014): Opciones Reales y Gestión de Empresas. La Importancia de la Flexibilidad y el Riesgo en la Valoración. Ponentes: Mascareñas, J. y Rodríguez, M. DocumentoAECA 12, valoración y financiación de empresas. Mayo.

AFUAH, A. (2004). Business models: A strategic management approach. McGraw-Hill/Irwin. New York.

AFUAH, A. y TUCCI, C. (2000). Internet business models and strategies: Text and cases. New York: McGraw-Hill Higher Education.

ALAM, P.; NIZAMUDDIN, M. (2012): Performance measures of Shareholders wealth: an application of economic value added (EVA). International Journal of Applied Financial Management Perspectives1.2. Oct/Dec 2012.

AMAT SALAS, O. (2011): Valoración de empresas: enfoques convencionales y nuestras tendencias. Harvard Deusto business review. Nº 203(Ejemplar dedicado a: Aspectos financieros clave para la dirección de la empresa).

AMAT, O. (1999): EVA. Un nuevo enfoque para optimizar la gestión, motivar y crear valor. Gestión 2000.Barcelona.

AMRAM, M. Y KULATILAKA, N.: (2000). Opciones Reales. Harvard Business School Press. Gestión 2000. Barcelona

ANCONA, D.G. (1990): Outward Bound: Strategies for Team Survival in an Organization. The Academy ofManagement Journal. Vol. 33. Nº 2. June.

ANCONA, D.G.; CALDWELL, D.F. (1992): Bridging the boundary: External activity and performance inorganizational teams. Administrative Science Quarterly, 37.

ANDREWS K.R. (1987): The Concept of Corporate Strategy. Richard D Irwin. Third Edition.

ANDRIESSEN, D. (2004): Making sense of intellectual capital: designing a method for the valuation of intangibles; Elsevier Butterworth-Heinemann; Oxford.

ANSOFF, H.I. (1965): Corporate strategy. McGraw Hill. Nueva York.

ANSOFF, H.I. (1980): Strategic issue management. Strategic Management Journal.April/June.

ARGYRIS, C. (1999): Sobre el aprendizaje organizacional. México: Oxford University Press.

ARGYRIS, C.; & SCHÖN, D. (1978): Organizational learning: A theory in action perspective. Reading, MA: Addison Wesley.

ARRUÑADA, BENITO (1990): Economía de la empresa: un enfoque contractual. Ed. Ariel Economía. Barcelona.

ASOCIACIÓN ESPAÑOLA DE CONTABILIDAD Y ADMINISTRACIÓN DE EMPRESAS. AECA (2006):Aplicabilidad del modelo de Ohlson para la valoración de acciones. Documentos AECA 8. Valoración de empresas. Madrid.

BANDURA, A. (2000): Cultivate self-efficacy for personal and organizational effectiveness. In E. A. Locke (Ed.), Handbook of principles of organization behavior. Oxford, UK: Blackwell.

BARNAY, A. Y CALBA, G. (1977): Como Valorar una Empresa. Ed. Francisco Casanovas. Barcelona.

BARNEY, J. (1991): Firm Resources and Sustained Competitive Advantage. Journal of Management, Vol. 17. Núm. 1.

BARNEY, J.B. (2007): Gaining and sustaining competitive advantage. Pearson Prentice Hall. Upper Saddle River. 3ª Ed.

BEATON, N.J. (2010): Valuing Early Stage and Venture Backed Companies; Ed. John Wiley & Sons.

BEER, M.; EISENSTADT, R.A.; SPECTOR, B. (1990): Why change programs don´t produce change. Harvard Business Review. November/December.

BELTRÁN, L. (1976): Historia de las doctrinas económicas. Ed Teide. Barcelona.

BENNIS, W. (1995): Cambio y liderazgo. Deusto. Barcelona.

BERNARD, V.L. (1995): The Feltham-Ohlson framework: implications for empiricist. Contemporary Accounting Research. Vol. 11.

BETTIS, R.A.; HITT, M.A. (1995): The new competitive landscape. Strategic Management Journal (1996-1998). Chichester: Summer. Vol. 16.

BLANCHARD, K.; JOHNSON, S. (2002): El ejecutivo al minuto. Grijalbo Mondadori. Barcelona.

BLASCO RUIZ, A. Y RIBAL SANCHIS, J (2009): El arte de valorar empresas. Simulación de escenarios a través de la técnica de simulación de Montecarlo, valoración de empresas y la teoría de opciones reales. Fundación de Estudios Bursátiles y Financieros. Ed Civitas. Thomson Reuters. Navarra.

BOER, F.P. (1999): The Valuation of technology. Ed. Jon Wiley & Sons. Estados Unidos.

BOGDAN, B. Y VILLIGER, R. (2007): Valuation in life sciences. Ed. Springer. Berlín. Alemania.

BONTIS, N. (1996): There's a price on your head: Managing intellectual capital strategically, Business Quaterly, Summer.

BONTIS, N. (1998): Intellectual capital: an exploraty study that develops measures and models. Management Decisión.BORISSIOUK, O.; PELI, J. (2001): Real option approach to R&D project valuation: Case study at SeronoInternational S.A.The Financier. Vol. 8. N º 1-4.

BOSTON CONSULTING GROUP (1996): Shareholder Value Metrics. Booklet 2.

LIBERTY, B.D.; BOULTON, R.E.S.; SAMEK, S.M.; (2001): Un modelo de negocio para la nueva economía. Harvard Deusto business review; Nº 101, págs. 68-77

BOYATZIS, R.; MCKEE, A. (2006): Liderazgo emocional. Deusto. Barcelona.

BREALEY, R.A. Y MYERS S.C. (2002): Fundamentos de financiación empresarial. Ed. McGraw-Hill/Interamericana de España

BREALEY, R.A. Y MYERS, S.C. (1999): Fundamentos de financiación empresarial. Ed. Mc Graw-Hill.

BRENNAN, N.; CONNELL, B. (2000): Intellectual Capital: Current Issues and Policy Implications. Journal of Intellectual Capital, Vol. 1, Núm. 3.

BRIGHAM, E.F. (1985): Financial management: theory and practice. Ed. The Dryden Press.

BRILMAN, J. Y MAIRE, C. (1990): Manual de Valoración de empresas. Ed Díaz de Santos. Madrid.

BRITO, E. (2000): Valoración de Empresas tecnológicas mediante la teoría de opciones. Revista de la Bolsa de Madrid, nº 88, pág. 13-17.

BROOKING, A. (1998): El Capital Intelectual. Ed. Paidós Empresa. Barcelona.BUENO CAMPOS, E. (1998): El capital intangible como clave estratégica en la competencia actual. Boletín de Estudios Económicos. Vol. LIII. Nº 164. Agosto.

BUENO CAMPOS, E. (DIRECTOR); ARRIEN, M; RODRÍGUEZ, O. (2003): Modelo Intellectus: medición y gestión del capital intelectual. Documentos Intellectus. Número 5. IADE-CIC. Junio.

BUENO CAMPOS, E. (director); CIC (2003): "Dirección estratégica por competencias básicas distintivas:Propuesta de un modelo". Documentos Intellectus núm. 5, IADE, Madrid.

BUENO CAMPOS, E.; (2000): Gestión del conocimientoy capital intelectual. Experiencias en España. Instituto Universitario Euroforum Escorial. Madrid.

BUENO CAMPOS, E. ASOCIACIÓN ESPAÑOLA DE CONTABILIDAD Y ADMINISTRACIÓN DE EMPRESAS, AECA, (2012): "El Capital Intelectual de las Organizaciones". Documento AECA núm.22, Madrid.

BUENO CAMPOS, E.; MORCILLO, P. (1997): Dirección estratégica por competencias básicas distintivas: Propuesta de un modelo. Documento IADE núm. 5, UAM, Madrid.

BUENO CAMPOS, E.; SALMADOR SÁNCHEZ, M.P. (2000): Perspectivas sobre dirección del conocimiento y capital intelectual. Instituto Universitario Euroforum Escorial. Madrid.

BUENOS CAMPOS, E. (1991): Dirección estratégica de la empresa: metodología, técnicas y casos. Ed. Pirámide. Madrid.

BUENO CAMPOS, E. (1982): Economía de la empresa: análisis de las decisiones empresariales; Ed. Pirámide; tercera edición; Madrid.

BURGELMAN, R.A. (1990): Strategy-making and organizational ecology: a conceptual integration, en SING, J. (ed): Organizational Evolution: New Directions. Sage Publications.

CABALLER, V. (1998): Métodos de Valoración de empresas. Ed. Pirámide, Madrid.

CABRERA, A.; RINCÓN, M. (2001): La Gestión del Conocimiento: Creando Competitividad en la Nueva Economía, ICE, Núm. 791, Abril-Mayo.

CAMPION, M. A., PAPPER, E. M., & MEDSKER, G. J (1996): Personnel Psychology Volume 49, Issue 2, June.

CAÑIBANO, L.; GARCÍA, M. Y SÁNCHEZ, M.P. (1999): La Relevancia de los Intangibles para la Valoración y la Gestión de las Empresas: Revisión de la literatura (I). Revista Española de Financiación y Contabilidad. Nº 100.

CAÑIBANO, L.; SÁNCHEZ, M.P.; GARCÍA-AYUSO, M.; CHAMINADE, C. (2002): Directrices para la Gestión y Difusión de la Información sobre Intangibles. Informe de Capital Intelectual. Proyecto MERITUM, Fundación Airtel Móvil.

CARENYS, J. (2013): Sistemas de incentivos y creación de valor: el EVA. Revista de contabilidad y dirección. Nº 17 (Ejemplar dedicado a: Retribución variable: nuevas tendencias).

CASADESUS-MASANELL, R. (2004): Dinámica competitiva y modelos de negocio. Universia business review actualidad económica-; Nº4; Cuarto trimestre.

CASADESUS-MASANELL, R. y RICART, J. (2007). Competing through business models. IESE Research Papers.

CASADESUS-MASANELL, R. y RICART, J. (2010). From strategy to business models and onto tactics. Long Range Planning, 43,

CASTRO CALVÍN, J.; GONZÁLEZ SIMÓN, M.; GUENAGA GARAY, G.; MIJANGOS DEL CAMPO, J.J. (2009). Universidad del País Vasco.

CATALANA d´iniciatives. Divisió Noves Tecnologies (1999): Hacia un método para valorar negocios en internet

CHANDLER, A. (1962): Strategy and structure: chapters in the history of the industrial enterprise. MIT Press, Cambridge.

CHEN, G.; BLIESE, P.D. (2002): The role of different levels of leadership in predicting self- and collective efficacy: Evidence for discontinuity. Journal of Applied Psychology. Vol 87(3), June.

CHESBROUGH, H. (2010). Business model innovation: Opportunities and barriers. Long Range. Planning, 43

CHESBROUGH, H. y ROSENBLOOM, R. (2002). The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies. Industrial and Corporate Change, 11.

CHIU, CH.-CH. (2013): The Free Cash Flow Rate on the Stock Return Rate. Journal of Accounting, Finance &Management Strategy, Vol. 8. No 1. June.

CHRISTENSEN, C., JOHNSON, M. y KAGERMANN, H. (2008). Reinventing Your Business Model. Harvard Business Review.

COHEN, W. Y LEVINTHAL, D. (1994): Fortune favors the prepared firms. Management Sciences, 40.

COLLINS, J. (2001): Empresas que sobresalen. Gestión 2000. Barcelona

COLLINS, JAMES C.; PORRAS, JERRY I. (1996): Empresas que perduran. Paidós empresa. Barcelona

COPELAND, T.; KOLLER, T.; MURRIN, J. (2000): Valuation Measuring and Managing the Value of Companies. Ed. John Wiley & Sons, Inc. New York.

COPELAND, T.; KOLLER, T.; MURRIN, J. (2010): Valuation Measuring and Managing the Value of Companies. Fifth edition. John Wiley & Sons. New York.

COPELAND, T; ANTIKAROV, V. (2001): Real Options. Texere. New York.

CORNELL, B. (1993): Corporate Valuation: Tools for Effective Appraisal and Decision-Making. Ed. McGraw-Hill.

COVEY, S. R. (2004): El liderazgo centrado en principios. Ed. Paidós. Barcelona.COVEY, S. R. (2014): Los 7 hábitos de la gente altamente efectiva: la revolución ética en la vida cotidiana y en la empresa. Ed. Paidós. Barcelona.

CROSSAN, M.; LANE, H.; WHITE, R. (1999): An organizational learning framework: From intuition to institution. Academy of Management Review. Vol. 24. Nº3.

CUERVO GARCÍA, A. (1979): Estudios sobre los objetivos de la empresa. Revista de Económicas y Empresariales. De UNED, CECA.

DAFT, R.L.; WEICK, K.E. (1984): Towards a model of organizations as interpretation systems. Academy of Management Review, 9.

DAMODARAN, A. (2002): Investment Valuation: Tools and Techniques for Determining the Value of Any Asset; Wiley; Second Edition; January 18.

DAMODARAN, A. (2006): Damodaran on Valuation: Security Analysis for Investment and Corporate Finance. John Wiley & Sons, Inc. New Jersey.

DAMODARAN, A. (2009): The Dark Side of Valuation: Valuing Young, Distressed, and Complex Businesses. Second edition. Pearson education. New Jersey.

DAMODARAN, A. (2012): Investment on Valuation. Third edition. Ed. Wiley Finance. New York. April.

DAVENPORT, T., LEIBOLD, M. y VOELPEL, S. (2006). Strategic Management in the Innovation Economy: Strategy Approaches and Tools for Dynamic Innovation Capabilities. Erlangen: Publicis Wiley.

DAY, D.V.; GRONN, P.; SALAS, E. (2004): Leadership capacity in teams. The Leadership Quarterly. Volume 15, Issue 6. December.

DAY, D.V.; GRONN, P.; SALAS, E. (2006): Leadership capacity in teams. The Leadership Quarterly. Volume 17, Issue 3. June.

DE LA TORRE GALLEGOS, A.; JIMÉNEZ NAHARRO, F. (2014): Valoración de empresas y análisis bursátil. Pirámide. Madrid. DE LA TORRE, A. Y JIMÉNEZ NAHARRO, F. (2012): Manual de valoración de empresas y análisis bursátil. Ed. Digital @tres. Sevilla.

DE LEEW, T.; VOLBERDA, H.W. (1996): On tue concept of flexibility: a dual control perspective. Omega International Journal of Management Science, Vol. 24, nº2.

DEMIL, B. y LECOCQ, X. (2010). Business Model Evolution: In Search of Dynamic Consistency. Long Range Planning, 43.

DIBELLA, A.J.; NEVIS, E.C.; GOULD, J.M. (1996): Understanding organizational learning capability. Journal of Management Studies. Vol. 33.

DIXIT, A.K.; NALEBUFF, B.J. (1991): Thinking Strategically: The Competitive Edge in Business, Politics, and Everyday Life. W.W. Norton. Nueva York.

DRATH, W. H., & PALUS, C. J. (1994): Making common sense: Leadership as meaning making in a SPACE community of practice. Greensboro, NC: Center for Creative Leadership.

DRUCKER, P. (1954): The practice of management. Harper & Row. Nueva York.

DRUCKER, P 1992): Managing for the future. The 1990s and Beyond. Truman Tallet Books, New York.

DRUCKER, P. (2000): El management del siglo XXI. Edhasa. Barcelona.

DURBÁN OLIVA, S. (1993): Introducción a las finanzas empresariales: la selección de inversiones y financiaciones. Ed. Universidad de Sevilla Secretariado de Publicaciones. Sevilla.

DURBÁN OLIVA, S. (2008): Dirección Financiera. Ed. McGraw-Hill. Madrid.DYER, L.; SHAFFER, R.A. (1999): From human resource strategy to organizational effectiveness: Lessons from research on organizational effectiveness. Research in Personnel and Human Resource Management. Ed. Pirámide. Madrid.

EDVINSSON, L.; MALONE, M. S. (1999): El Capital Intelectual, Ed.Gestión 2000, Barcelona.

EISENMANN, T. R., HALLOWELL, R. y TRIPSAS, M. (2001). Internet business models: texts and cases. New York, NY: McGraw-Hill, Inc.

ERASMUS, P D; LAMBRECHTS, I J. (2006): EVA and CFROI: A comparative analysis. Management Dynamics 15.1.

ESCUDERO CUEVAS, J. (2013): Modelos de negocio que funcionan. Revista Emprendedores: las claves de la economía y el éxito profesional. Nº 186.

EUROFORUM (1998): Medición del Capital Intelectual. Modelo Intelec, IUEE, San Lorenzo del Escorial. Diciembre. Madrid.

EVANS, J.S. (1982): Strategic flexibility in business. Research Report, Nº 678. SRI International, Business Intelligence Program, Menlo Park.

EVANS, J.S. (1991): Strategic flexibility fo High Technology Manoeuvres: A conceptual framework. Journal of Management Studies, Vol. 28 (January).

EVERED, R. (1983): So what is strategy? Long Range Planning 16, nº3, junio.

FABREGAT, J. (2009): Introducción a los métodos de valoración de empresas. Valoración de empresas, bases conceptuales y aplicaciones prácticas. ACCID. Ed. Profit. Barcelona.

FELTHAM, G.; OHLSON, J.A. (1995): Valuation and clean surplus accounting for operating and financial activities. Contemporary Accounting Research. Vol. 11. Nº 2. Spring.

FERNÁNDEZ PIRLA, J.M. (1974): Economía y gestión de la empresa. Biblioteca de Ciencias Empresariales. Ed. ICE.

FERNÁNDEZ RODRÍGUEZ, Z. (1987): Evolución del pensamiento estratégico. Economistas, nº 28, octubrenoviembre.

FERNÁNDEZ RODRÍGUEZ, Z. (1993): La organización interna como ventaja competitiva para la empresa. Papeles de Economía Española. Nº 56.

FERNÁNDEZ, P. (2000): Creación de valor para los accionistas. Ed. Gestión 2000. Barcelona.

FERNÁNDEZ, P. (2002): Valoración de Empresas. Segunda Edición. Ed. Gestión 2000. Barcelona.

FERNÁNDEZ, P. (2013): Valoración de opciones reales: dificultades, problemas y errors. SSRN:http://ssrn.com/abstract=1159045. Abril.

FERNÁNDEZ, P. (2014c): Valoración de Empresas por Descuento de Flujos: lo fundamental y las Complicaciones Innecesarias. SSRN: http://ssrn.com/abstract=2089397. Abril.

FERNÁNDEZ, P. (2014a): Métodos de valoración de empresas. SSRN: http://ssrn.com/abstract=1267987. Julio.

FERNÁNDEZ, P. (2014b): Valoración de empresas por descuento de flujos: 10 métodos y 7 teorías. SSRN: http://ssrn.com/abstract=1266623. Abril.

FERNÁNDEZ, P. (2015): Valoracion de Marcas e Intangibles (Brand Valuation); Junio 10; SSRN:http://ssrn.com/abstract=975471

FERNANDEZ, P.; CARABIAS, J. M. (2013): Utilidad y limitaciones de las valoraciones por múltiplos (Valuations with Multiples); Abril 15; SSRN: http://ssrn.com/abstract=918469

FESTEL, G.; WUERMSEHER, M.; CATTANEO, G. (2013): Valuation of Early Stage High-tech Start-up Companies. International Journal of Business. 18(3).FIOL, C.M.;

LYLES, M.A. (1985): Organizational learning. Academy of Management Review, Vol. 10.

FRAZER, R.W. (1985): Demand fluctuations, inventory and flexibility. Australian Economic Papers, June.

FREIJE Obregón, Inmaculada (2014): Innovación en modelos de negocio. Qué dejar en manos del cliente. Boletín de estudios económicos (Ejemplar dedicado a: Competitividad e innovación). Vol. 69. Nº 213.

FUNDACIÓN DE ESTUDIOS BURSÁTILES Y FINANCIEROS (2009): El arte de valorar empresas. Thomson Reuters. Navarra.---

BLASCO RUÍZ, A.; MOYA CLEMENTE, I.; RIBAL SANCHIS, J. (2009): Capítulo 12. Valoración de intangibles.---

BLASCO RUIZ, A.; RIBAL SANCHIS, J. (2009): Capítulo 5. Simulación de escenarios, a través de la técnica de simulación de Montecarlo, valoración de empresas y la teoría de opciones reales.---

DE ÁLAVA HORCAJO, P. (2009): Capítulo 9. Valoración de empresas en base a análisis sectoriales (II).---

DOMINGO FOLGADO, J. (2009): Capítulo 2. Introducción a los métodos de valoración.--- Milla

GUTIÉRREZ, A. (2009): Capítulo 11. Valoración y creación de valor. Estrategias y medición de la creación de valor para el accionista.---

TOMÁS CATALÁ, F.J. (2009): Capítulo 3. Método del descuento de flujos de caja.---

GINER INCHAUSTI, B.; ÍÑIGUEZ SÁNCHEZ, R.; REVERTE MAYA, C. (2009): Capítulo 4. Aplicación práctica del modelo de valoración de Ohlson.

FUNKE, G.J.; KNOTT, B.A. (2014): Team workload. A multilevel perspective. Organizational Psychology Review. Vol. 4. Nº. 2. May.

GALBRAITH, J.R. (1973): Designing complex organizations. Addison-Wesley Pub. Co. Boston.

GAMBARDELLA, A. y MCGAHAN, A. M. (2010). Business-model innovation: General-purpose technologies and their implications for industry structure. Long Range Planning, 43.

GARCÍA ALONSO, A.; LÓPEZ-BARAJAS DE LA PUERTA, A. (1998): El EVA y la creación de valor para el accionista. Bolsa de Madrid. Nº 62 (ENE).

GARCÍA- AYUSO, M.; MONTERREY MAYORAL, J. (1998): El modelo de valoración Edwards-Bell-Ohlson (EBO): Aspectos teóricos y evidencia empírica. Revista Española de Financiación y Contabilidad. Nº 96.

GARCÍA MACHADO, J.J. (2001): Opciones Reales. Ed. Pirámide. Madrid

GARCÍA VILLANUEVA, R. (2008): La incorporación de los activos intangibles en la valoración de empresas del sector hotelero. Tesis doctoral. Universidad de Sevilla. Departamento de Economía Financiera y Dirección de Operaciones.

GARVIN, D.A. (1993): Building a learning organization. Harvard Business Review, Julio-agosto.

GHEMAWAT, P. (1991). Commitment. Boston: Free Press.

GIBSON, C. B., RANDEL, A. P., & EARLEY, P. C. (2000): Understanding group efficacy: An empirical test of multiple assessment methods. Group and Organization Management, 25.

GIL CORRAL, A.M. (2009): El arte de valorar empresas. Introducción a los métodos de valoración. Fundación de Estudios Bursátiles y Financieros. Ed Civitas. Thomson Reuters. Navarra.

GOLEMAN, D. (2013): Liderazgo: el poder de la inteligencia emocional. Ediciones B.

GOLEMAN, D.; BOYATZIS, R.; MCKEE, A. (2007): El líder resonante crea más. Ed. Debolsillo. Barcelona.

GRANT, ROBERT M. (2002): Dirección Estratégica. Ed. Civitas. Madrid

GULLY, S. M.; JOSHI, A.; INCALCATERRA, K. A.; BEAUBIEN, J. M. (2002): Meta analysis of team-efficacy, potency, and performance: Interdependence and level of analysis as moderators of observed relationships. Journal of Applied Psychology, 87.

GUZZO, R.A., YOST, P.R., CAMPBELL, R.J., & SHEA, G.P. (1993): Potency in groups: Articulating a construct. British Journal of Social Psychology, 32.

HACKMAN, J.R.; BROUSSEAU, K.R.; WEISS, J.A. (1976): The interaction of task design and group performance strategies in determining group effectiveness. Organizational Behavior and Human Performance. Vol. 16.

HAMEL, G. (2000): Liderando la revolución. Gestión 2000. Barcelona.

HAMEL, G.; PRAHALAD, C.K. (1999): Compitiendo por el futuro. Ariel. BarcelonaHARMON, S. (1999): “The Metrics for Evaluating Internet Companies. The internet Stock Report.

HARRIGAN, K.R. (1982): Exit decisions in mature industries. Academy of Management Journal. Briarcliff Manor, December. Vol. 25, Nº4.

HARRIGAN, K.R. (1985): Strategic flexibility: A management guide for changing times. Lexington, M.A. Lexington Books.

HEIFETZ, R. A.; GRASHOW, A.; LINSKY, M. (2012): La práctica del liderazgo adaptativo: las herramientas y tácticas para cambiar su organización y el mundo. Paidós. Barcelona.

HELDAL, F; ANTONSEN, S. (2014): Team Leadership in a High-Risk Organization. The Role of Contextual Factors. Small Group Research. Vol. 45.Nº 4. August.

HELLELOID, D.; SIMONIN, B. (1994): Organizational learning and a firm´s core competence, en

HAMEL y HEENE(eds.): Competence Based Competition. John Wiley and Sons.

HEMPHILL, J. K.; COONS, A. E. (1957): Development of the leader behavior description questionnaire. In R. M. Stodgill and A. E. Coons (Eds.), Leader behavior: Its description and measurement. Columbus, Ohio: Bureau of Business Research, Ohio State University.

HENRYANI, F. F.; KUSUMASTUTI, R. (2013). Analysis Of Ownership Structure Effect On Economic Value Added. Bisnis & Birokrasi 20.3. Sep.

HEWETT, T. T. O'BRIEN , G. E. HORNIK , J. (1974). The effects of work organization, leadership style, and member compatibility upon the productivity of small groups working on a manipulative task. Organizational Behavior and Human Performance, 11.

HILL, C.W.L.; JONES, G.R. (2009): Administración estratégica. McGraw Hill. México. Octava edición.

HITT, M.A.; KEATS, B.W.; DEMARIE, S.M. (1998): Navigating in the new competitive landscape: building strategic flexibility and competitive advantage in the 21st century. The Academy of Management Executive. Vol. 12.

HORMIGA PÉREZ, E.; MARÍA BATISTA CANINO, R.; SÁNCHEZ MEDINA, A.J. (2008): El capital intelectual en las empresas de nueva creación: influencia de los activos intangibles en el éxito empresarial. Fundación FYDECajaCanarias.

HUANG, CH.; WANG, M.CH. (2008): The Effects of Economic Value Added and Intellectual Capital on the Market Value of Firms: An Empirical Study. International Journal of Management 25.4. Dec.

IÑIGUEZ SÁNCHEZ, R; GINER INCHAUSTI, B. (2006): Aplicación de los modelos Feltham-Ohlson a la valoración de activos en el mercado español. Revista de economía financiera. Nº 8, 2006.

IRIMIA, A.I.; JIMÉNEZ, J.L.; RUÍZ, R. (2003): La Creación De Valor Para el Accionista. Ed. Cie Dossat.

ITAMI, H. (1987). Mobilizing Invisible Assets. Harvard University Press. Boston.

ITAMI, H. y NISHINO, K. (2010). Killing Two Birds with One Stone: Profit for Now and Learning for the Future. Long Range Planning, 43.

JACOBS, T. O., & JAQUES, E. (1990). Military executive leadership. In K. E. Clark and M. B. Clark (Eds.), Measures of leadership. West Orange, New Jersey: Leadership Library of America.

JAENSCH, G. (1974): Valoración de la empresa. Ed. Ariel. Barcelona.

JIMÉNEZ NAHARRO, F.; SANTIAGO MORENO, I.; DE LA TORRE GALLEGOS, A. (2013): M2M Marketplace: el valor de lo intangible. Digital@tres. Sevilla.

JIMENEZ NAHARRO, F.; GUZMAN LÓPEZ, S.A.: “Valoración del sector de acceso a internet: en Micro y Pequeña empresa. 2012.

JIMÉNEZ, F.; ESCOBAR, B. (2007): Una propuesta para incluir el capital intelectual en el modelo de flujos descontados Partida Doble nº192.

JOOS, P.; ZHDANOV, A. (2005): Examining the Price-Earnings Relation in a Real Options Framework with Investor Learning. November 4. SSRN: http://ssrn.com/abstract=835524

KAPLAN, R. S.; NORTON D. P. (1997): El Cuadro de Mando Integral. Ed. Gestión 2000. Barcelona.

KAPLAN, R.S.; NORTON, D.P. (2001). Cómo utilizar el cuadro de mando integral. Ed.Gestión 2000. Barcelona

KAPLAN, R.S.; NORTON, D.P. (2002). Cuadro de mando integral. Ed. Gestión 2000. Barcelona

KAPLAN, R.S.; NORTON, D.P. (2004). Mapas estratégicos. Ed. Gestión 2000. BarcelonaKAPLAN, R.S.; NORTON, D.P. (2006). Alignment. Ed. Gestión 2000. Barcelona

KAPLAN, R.S.; NORTON, D.P. (2008). The execution premium. Ed. Deusto. BarcelonaKATZ, D. ;

KAHN, R. L. (1978): Social psychology of organizations. Segunda edición. New York: John Wiley.

KEEGAN, K.D. (2008): Biotechnology Valuation. An introductory guide. Ed. John Wiley & Sons. Estados Unidos.

KEISER, J.D.; FERRIS, G.R. (1997): Work forcé flexibility and human resource system. L.H. Peters. Youngblood, C.R. Greer (EDS.); The Blackwell Dictionary of Human Resources Management. Blackwell Publishers. Oxford.

KELLOGG, D.; CHARNES, J. M. (2000): Real-options valuation for a biotechnology company. Financial Analysts Journal. 56.3.May/Jun.

KESTER, W.C. (1991): Las opciones de hoy para el crecimiento futuro. Análisis financiero. Nº 54. Abril-Junio.

KIM, L. (1998): Crisis construction and organizational learning: Capability building in catching-up at Hyundai Motor. Organization Science, 9(4).

KIM, W. C.; MAUBORGNE, R. (2002): Dibuje el futuro estratégico de su empresa. Harvard Deusto business review. Nº 110.

KIM, W. C.; MAUBORGNE, R. (2005): La estrategia del océano azul. Granica. Barcelona. Septiembre.

KOGUT, B. (1985): Designing global strategies: profiting from operational flexibility. Sloan Management Review, Vol. 26.

KOGUT, B.; ZANDER, U. (1992): Knowledge of the firm, combinative capabilities and the replication of technology. Organization Science, Vol. 3.

KOTTER, JOHN P. (1990): El factor liderazgo. Ed. Díaz de Santos. Madrid.

KOTTER, JOHN P. (2000): Qué hacen los líderes. Ed. Gestión 2000 Barcelona.

KOTTER, JOHN P. (2007): Al frente del cambio. Ed. Urano. Barcelona.

KOTTER, JOHN P. (2015): Acelerar. Penguin Random House Grupo Editorial. Barcelona.

KRAMER, J.K. Y PUSHNER, G. (1997): An Empirical analysis of Economic Value Added as a proxy for Market Value Added. Financial Practice and Education. Spring/Summer.

KRIJNEN, H.G. (1979): The flexible firm. Long Range Planning.

KRIJNEN, H.G. (1985): The flexible firm. International Studies of Management & Organization. Vol. 14. Nº4. Winter.

KULATILAKA, N.; MARKS, S.G. (1988): The strategic value of flexibility: reducing the ability to compromiso. The American Economic Review. Nashville. Jun. Vol. 78.

LAMOTHE FERNÁNDEZ, P. Y RUBIO MARTÍN, G. (2004): Valoración de empresas nutracéuticas. Análisis Financiero. Nº 95. Segundo cuatrimestre. Instituto Español de Analistas Financieros. Madrid.

LAMOTHE, P. Y ARAGÓN, R. (2002): Valoración racional de acciones de Internet. El caso europeo. Comunicación presentada al X Foro de Finanzas, Sevilla, noviembre.

LAMOTHE, P.; ARAGÓN, R. (2003): Valoración de empresas asociadas a la nueva economía. Ed. Pirámide-IEAF. Madrid.

LAMOTHE, P.; MÉNDEZ, M. (2013): Opciones reales. Métodos de simulación y valoración; Ed. Ecobook; Ecobook Editorial del Economista; Madrid.

LAU, R.S.M. (1996): Strategic flexibility: a new reality for world class manufacturing. S.A.M. Advanced Management Journal: Vol. 61.

LAVOIE, B. F (2004): Real options and the management of R&D investment: An analysis of comparative advantage, market structure, and industry dynamics in biotechnology. The Ohio State University, ProQuest, UMI Dissertations Publishing.

LENCIONI, P. (2002): Las cuatro obsesiones de un ejecutivo: el reto del nuevo líder pasa por una excelente claridad organizacional. Ed. Empresa activa. Barcelona.

LEV B. (2001): Intangibles: Management, Measurement and reporting Ed. The Brookings Institution Press, Washington.

LEV, B. (2000): New Accounting for the New Economy. http://www.strn.edu.

LEV B. (2013): Ganar la confianza de los accionistas. Guia para fortalecer el valor de la empresa a traves de integrida; Ed. Profit. Barcelona.

LEVITT, B.; MARCH, J.G. (1988): Organizational learning. Annual Review of Sociology. Vol. 14.

LINTNER, J. (1965): Security Prices, Risk and Maximal Gains from Diversification. Ed. J. Financ. Diciembre.

LO, K.; LYS, T. (1999): The Ohlson model: contributions to valuation theory, limitations and empirical applications. Working Paper. University of British Columbia.

LÓPEZ- CÓZAR NAVARRO, C. Y RUBIO MARTÍN, G. (2008): Modelo de valoración económica para una patente: el caso del sector farmacéutico. Estrategia Financiera, nº 246. Enero.

LÓPEZ PÉREZ, R. (2012): Innovación del modelo de negocio: propuesta de un modelo holístico. Tesis doctoral. Directores: Bueno Campos, E.; Salmador Sánchez, M.P. Universidad Autónoma de Madrid. Departamento de organización de empresas.

LÓPEZ PÉREZ, R.; BUENO CAMPOS, E.; SALMADOR SÁNCHEZ, M.P. (2013): Dinamizar la PYME mediante la innovación del modelo de negocio. Economía industrial. Nº 388 (Ejemplar dedicado a: PYME y emprendimiento innovador).

LÓPEZ RUIZ, V.R.; NEVADO PEÑA, D. (2006): Gestione y controle el valor integral de su empresa. Análisis integral. Díaz de Santos. Madrid.

LÓPEZ SINTAS, J. (1996): Los recursos intangibles en la competitividad de las empresas. Un análisis desde la teoría de los recursos. Economía Industrial. Nº 307.

LORING, J. (1997): La gestión financiera. Ed. Deusto. Bilbao.

LOZANO GUTIÉRREZ, M.C.; FUENTES MARTIN, F.: El valor de la marca y el valor de la empresa de Internet". Investigaciones Europeas de Dirección y Economía de la Empresa. Vol. 10, nº 1, 2004, pp. 111-133, ISSN 1135-2523.

LUND R.; GJERDING, A.N. (1996): The flexible company innovation. Work Organization and Human Resource Management.

DRUID. Working Paper.LÜTOLF-CARROLL, C.; PIRNES, A.; WITHERS LLP (2009): From Innovation to Cash Flows: Value Creation by Structuring High Technology Alliances. Wiley. August

MACDUFFIE, J. (1995): Human resource bundles, manufacturing performance organizational logic, and flexible production system in the world auto industry. Industrial and Labour Relations Review. Vol. 48.

MACMILLAN, I.C.; VAN PUTTEN, A.B. (2005): Opciones reales que funcionan realmente. Harvard Deusto business review. Nº 134.MADDEN, B.J. (1999): CFROI Valuation. Butterworth-Heinemann. March 22.

MAGRETTA, J. (2002): La importancia de los modelos de negocio. Harvard Deusto Business Review. Nº 110.

MAHAVAN, R. (1996): Strategic flexibility and performance in the global steel industry: the role of interfirm linkages.University of Pittsburg.

MALONE, S.C. (1986): Strategic flexibility and form performance in a cyclical industry. Unpublished Dissertation.Temple University.

MARCH CHORDÀ, I.; SEOANE TRIGO, R. (2006): Los modelos de negocio en las empresas de biotecnologíaespañolas. Universia business review. Actualidad económica. Cuarto trimestre 2006.

MARCH CHORDÀ, I; SEOANE TRIGO, R; YAGÜE PERALES, R.M. (2007): Modelos de Negocio en las Empresasde Biotecnología: Análisis Comparativo entre España y los Países Líderes. Journal of Technology Management &Innovation. Vol. 2. Nº 1.

MARTÍN BERZAL, C. (2004): Valoración de empresas tecnológicas mediante opciones reales. IE Working Paper.WPE 05/04. Mafrid.

MARTÍN MARÍN, J.L. Y RUIZ MARTÍNEZ R.J. (1992): El inversor y el patrimonio financiero. Ed. Ariel. Barcelona.

MARTÍN, J.L. Y TRUJILLO, A. (2000): Manual de valoración de empresas. Ed. Ariel. Barcelona.

MARTÍNEZ ABASCAL, E. (2001): PER y valoración en bolsa. Ed. Pirámide. Madrid.

MARTÍNEZ ALONSO, R. (2013): El manual del estratega: Los cinco estilos de hacer estrategia. Gestión 2000.Abril. Barcelona.

MARTÍNEZ CONESA, I.; EMMA GARCÍA MECA, E. (2005): Valoración de empresas cotizadas. AsociaciónEspañola de Contabilidad y Administración de Empresas, AECA Monografías. Madrid.

MARTÍNEZ LEÓN, I. (2001): El aprendizaje en las organizaciones. Aplicación al sector agroalimentario. Directora:Ruíz Mercader, J. Tesis Doctoral. Universidad Politécnica de Cartagena. Departamento de Organización deEmpresas y Comercio.

MARTÍNEZ PEDRÓS, D.; MILLA GUTIÉRREZ, A. (2005): La elaboración del plan estratégico y su implantación através del cuadro de mando integral. Díaz de Santos.

MARTÍNEZ, I. Y GARCÍA, E. (2005): Valoración de Empresas Cotizadas. AECA, Madrid.

MARX, K. (1976): El Capital. Ed. Popular. México.

MASCARENHAS, B. (1982): Coping with uncertainty in the international business. Journal of International BusinessStudies. Vol. 1.

MASCAREÑAS, J. (2007): Opciones reales en la valoración de proyectos de inversión. Última versión. Julio.Monografías de Juan Mascareñas sobre Finanzas Corporativas. Universidad Complutense. Madrid.

MASCAREÑAS, J. (2011): Fusiones, adquisiones y valoración de empresas; Ecobook, editorial del economista;quinta edición; Madrid.

MASCAREÑAS, J. (2012): La valoración de un proyecto de inversión biotecnológico como una opción realcompuesta. Documentos de trabajo. Última versión. Marzo. Universidad Complutense/Autónoma. Madrid.

MASCAREÑAS, J.; LAMOTHE, P.; LÓPEZ LUBIÁN, F.J. Y DE LUNA, W. (2004): Opciones Reales y Valoraciónde Activos. Prentice Hall, Madrid.

MASCAREÑAS, J.: “Métodos de valoración de empresas de la Nueva Economía”. Revista de la Bolsa de Madrid, nº 88, pág. 6-12.MAURYA, A. (2014): Running Lean. UNIR. Logroño.

MAXWELL, JOHN C. (2007): Liderazgo, principios de oro: las lecciones que he aprendido a lo largo de una vidade liderazgo. Grupo Nelson.

MAYO, A.; LANK, E. (1994): The Power of Learning. Institute of personnel and development. London.

MCCRAE, M.; NILSSON, H. (2001): The Explanatory and Predictive Power of different specifications of the Ohlson(1995) valuation models. The European Accounting Review. Vol. 10. Nº 2.

MCGRATH, J.E. (1991): Time, Interaction, and Performance (TIP). A Theory of Groups. Small Group Research.Vol. 22. Nº 2. May.

MEHRA, A.; SMITH, B.R.; DIXON; A.L.; ROBERTSON, B. (2006): Distributed leadership in teams: The network ofleadership perceptions and team performance. The Leadership Quarterly. Vol. 17, Issue 3. June.

MÉNDEZ, J.S. (1996): Fundamentos de Economía. Ed. Mc Graw-Hill.MENGER, CARL (1996): Teoría del valor. Biblioteca Cinco Días. Confederación Española de Cajas de Ahorro(CECA).

MILLA GUTIÉRREZ, A. (2010): Creación de valor para el accionista. Díaz de Satos. Madrid.

MINZBERG, H. (1990): Strategy formation. Schools of thought, en J. W. Fredrickson (ed): Perspectives on strategicmanagement. Harper Business, Nueva York.

MORALES PLAZA, J.I. Y MARTÍNEZ DE OLCOZ, J.M. (2006): "Análisis y valoración sectorial". Ed. Ariel Economía.Barcelona.

NEWMAN; MORGERSTERN (1944): Theory of Games and Economic Behavior; Princeton University Press,Princeton; Nueva Jersey.

MOSSIM, J. (1968): Optimal Multiperiod Portfolio Policies. Ed. J. Bussi. Abril.

MOWERY, D. C., & OXLEY, J. E. (1995): Inward technology transfer and competitiveness: The role of nationalinnovation system. Cambridge Journal of Economics, 19(1).

MULLINS, J; KOMISAR, R. (2010): Mejorando el modelo de negocio. Ed. Profit. Barcelona.

MULVEY, P.W.; KLEIN, H.J. (1998): The Impact of Perceived Loafing and Collective Efficacy on Group GoalProcesses and Group Performance. Organizational behavior and human decision processes. Vol. 74, No 1. April.

MURPHY, W. J.; ORCUTT, J.L.; REMUS, P.C. (2012): Patent Valuation: Improving Decision Making throughAnalysis. Wiley Finance. New Jersey.

NANDAKUMAR, M.K.; JHARKHARIA, S; ABHILASH; NAIR, A.S.(2014): Organisational Flexibility andCompetitiveness. Flexible Systems Management. March.

NAVAS LÓPEZ, J.E.; GUERRAS MARTÍN, L.A. (2012): FUNDAMENTOS DE LA DIRECCIÓN ESTRATÉGICA DELA EMPRESA. CIVITAS-THOMPSON REUTERS. NAVARRA.

NEIL J. BEATON, N.J. (2010): Valuing Early Stage and Venture Backed Companies. Wiley Finance. New Jersey.March.

NELSON, R.; WINTER, S. (1982): An evolutionary theory of economic change. The Belknap Press of HarvardUniversity Press. Cambridge.

NEUMANN, J.V.; MORGENSTERN, O. (1944): Theory of games and economic behavior. Princeton UniversityPress. Princeton, Nueva Jersey

NEVADO PEÑA, D.; LÓPEZ RUIZ, V.R. (2002): El Capital intelectual: valoración y medición. Pearson Educación.Madrid.

NIRESH, A.J; ALFRED, M. (2014): The Association between Economic Value Added, Market Value Added andLeverage. International Journal of Business and Management 9.10.

NOMEN, E. (2005): Valor razonable de los actives intangibles: el efecto mariposa de la segunda deslocalización.Ed Deusto. Barcelona.

NONAKA, I.; TAKEUCHI, H. (1995): The Knowledge-Creating Company. Oxford University Press.

OHLSON, J.A. (1989): Accounting earnings, book value, and dividends: The theory of clean surplus equation.Working Paper. Lancaster University. September.

OHLSON, J.A. (1995): Earnings, Book Values and Dividends in Equity Valuation. Contemporary AccountingResearch. Vol. 11. Nº 2.

OHMAE, K. (2004): La mente del estratega. Mc Graw Hill. Madrid.

OMAR LÓPEZ, C. (2005): La incorporación del capital intelectual en la valoración de empresas: un estudio de casoen el sistema general de Seguridad Social en salud de Colombia. Tesis doctoral. Universidad de Sevilla.Departamento de Economía Financiera y Dirección de Operaciones.

ORDÓÑEZ DE PABLOS, P.; PARREÑO FERNÁNDEZ, J. (2005): Aprendizaje organizativo y gestión delconocimiento: un análisis dinámico del conocimiento de la empresa. Investigaciones Europeas de Dirección yEconomía de la Empresa. Vol. 11. Nº 1.

OSTERWALDER, A.; PIGNEUR, Y.; (2011): Generación de modelos de negocio. Deusto.

OSTERWALDER, A.; PIGNEUR, Y, SMITH, A.; BERNARDA, G. (2015): Diseñando la propuesta de valor. Deusto.

OSTERWALDER, A.; PIGNEUR, Y; CLARK, T. (2012): Tu modelo de negocio. Deusto.

OTA, K. (2000): A new improvement to the Ohlson (1995) model: empirical evidence from Japan. Working Paper.Kansai University Graduate School.

OTA, K. (2002): A test the Ohlson (1995) Model: Empirical Evidence from Japan. The International Journal ofAccounting. Vol. 37. Nº 2.

OVERHOLT, M.H. (1997): Flexible Organizations: Using Organizational Design as a Competitive Advantage.Human Resources Planning. Vol. 20. Nº1.

PAIK, Y. (1991): The Impact of Strategic Flexibility on Business Performance in the International BusinessEnvironment. Unpublished dissertation. University of Washington.

PALACIOS PRECIADO, MARIANA; DUQUE OLIVA, EDISON JAIR (2011) Modelos de negocio: propuesta de unmarco conceptual para centros de productividad. Administración & Desarrollo 39(53).PARR, R.L. (2007): Royalty rates for licensing intellectual property. Ed. John Wiley & Sons. Estados Unidos.

PEARCE III, J.A.; RAVLIN, E.C. (1987): The Design and Activation of Self-Regulating Work Groups. HumanRelations November. Vol. 40 nº11.

PEARCE, CRAIG L., GALLAGHER, C. A., & ENSLEY, M. D. (2002). Confidence at the group level of analysis: Alongitudinal investigation of the relationship between potency and team effectiveness. Journal of Occupational andOrganizational Psychology, 75.

PEDLER, M.; BOYDELL, T.; BURGOYNE, J. (1991): The Learning Company. McGraw-Hill. London.

PENMAN, S.H. (1996): The articulation of price-earning ratios and market to book ratios, and the evaluation ofgrowth. Journal of Accounting Research, vol 34, nº 2, pp. 235-259.

PÉREZ CASTRO, C. Y SALINAS, G. (2008): Valoración y evaluación de marcas. Ed. Deusto. Barcelona.

PÉREZ-CARBALLO VEIGA, J.F. (1998): Compitiendo por crear valor. Ed. ESIC. Colección Empresa.

PERROW, C. (1970): Organizational analysis: A sociological view. Belment. CA: Brooks-Cole.

PETRASH, G. (1996): Dow's Journey to a Knowledge Value Management Culture. European Management Journal.Vol. 14. No. 4.

PIORE, M.J.; SABEL, C.F. (1984): The second industrial divide: possibilities for prosperities. Basic Books. NewYork.

PODSAKOFF, P.M.; AHEARNE, M.; MACKENZIE, S.B. (1997): Organizational Citizenship Behavior and theQuantity and Quality of Work Group Performance. Journal of Applied Psychology, Vol. 82, No. 2.PORTER, M.E. (1982): Estrategia competitiva. CECSA. México

PORTER, M.E. (1987): Ventaja competitiva. CECSA. México

PORTER. M.E. (1991): Towards a Dynamic Theory of Strategic. Strategic Management Journal. 12. Númeroespecial. Invierno.

PRAHALAD, C.K.; HAMEL, G. (1990). The Core Comptences of the Corporation. Harvard Business Review. Mayojunio.

PRICEWATERHOUSECOOPERS (1999): Guía de valoración de empresas. Cuadernos Cinco Días.QUINN J.B. (1980): Strategies for Change: Logical Incrementalism. Irwin series in management and the behavioralsciences. December

RAPPAPORT, A. (2005): La Creación de Valor para el Accionista: una guía para inversores y directivos. Deusto,Barcelona.

RAUCH, C. F.; BEHLING, O. (1984): Functionalism: Basis for an alternate approach to the study of leadership. InJ. G. Hunt, D. M. Hosking, C. A.

RAZGAITIS, R. (2003): Valuation and pricing of technology-based intellectual property. Ed. Jon Wiley & Sons.Estados Unidos.

RAZGAITIS, R. (2009): Valuation and Dealmaking of Technology-Based Intellectual Property: Principles, Methodsand Tools. Wiley. New Jersey. Jul.

REDDY, NRV. R.; RAO, B.S. (2013): Financial analysis of Indian cement industry using market value addedapproach. International Journal of Trade & Global Business Perspectives 2.1. Jan/Mar.

REILLY, R.F. Y SCHWEIHS, R.P. (1999): Valuing intangible assets. Ed. McGraw-Hill. Estados Unidos.

REVELLO DE TORO CABELLO, J.M. (2004): La valoración de los negocios. Ariel Economía. Barcelona.

REVELLO DE TORO CABELLO, J.M. (Coordinador) (2013): Manual de Corporate Finance y Banca de Inversión.Delta Publicaciones. Madrid.

LÓPEZ PÉREZ, R. (2012): Innovación en el modelo de negocio: propuesta de un modelo holístico. UniversidadAutónoma de Madrid. Tesis doctoral.

LÓPEZ PÉREZ, R.; BUENO CAMPOS, E.; SALMADOR SÁNCHEZ, M.P. (2013): Dinamizar la PYME mediante lainnovación del modelo de negocio. Economía industrial. Nº 388 (Ejemplar dedicado a: PYME y emprendimientoinnovador).

RICARDO, D. (1997): Principios de Economía Política y Tributación. Fondo Cultura Económica. Segundaimpresión. Bogotá Colombia.RICHARDS, D., & ENGLE, S. (1986). After the vision: Suggestions to corporate visionaries and vision champions.In J. D. Adams (Ed.), Transforming leadership. Alexandria, VA: Miles River Press.

ROBINSON, J. (1986): La acumulación del capital. Ed. Fondo de cultura económica. Bogotá. Colombia.

RODRÍGUEZ ANTÓN, J.M. (COODINADOR); GARCÍA MORALES, V. (2004): Aprendizaje organizativo.Documentos Intellectus. Número 7. IADE-CIC. Noviembre.

ROJO RAMÍREZ, A. A. (2007): Valoración de empresas y gestión basada en valor.Thomson. Madrid.

ROJO, A. (1996): Valoración de Empresas y Partes de Empresas. Ed Instituto de Auditores Censores Jurados de Cuentas de España. Escuela de Auditoría. Madrid.

ROJO, A.A.; SIERRA, M. (2000): Los Activos Intangibles (Capital Intelectual) en Contabilidad Financiera. Accésit al IV Premio Carlos Cubillo Valverde, Convocatoria 2000.

RONDA, G.A.; GUERRAS, L.A. (2012): Dynamics of the evolution of the strategy concept 1962–2008: a co-word analysis; Strategic Management Journal 33; 162-188

Roos, G. (2005): Valuing Brands: a Presentation to The Brand Finance Forum. Londres. 19 de agosto.

ROOS, G.; PIKE, S.; FERNSTRÖM, L. (2006): Managing Intellectual Capital in Practice, Elsevier Butterworth- Heinemann. Oxford.

ROOS, G.; ROOS, J. (1997): “Measuring your company’s intellectual performance” en revista Long Range Planning. Vol. 30. Nº 3. June.

ROOS, J.; DRAGONETTI, N. C.; ROOS, G.; EDVINSSON, L. (2001): Capital Intelectual. Ed. Piadós. Barcelona.

ROSENBAUM, J; PEARL, J. (2013): Investment Banking: Valuation, Leveraged Buyouts, and Mergers &Acquisitions. Second edition. Wiley. New Jersey. May.

ROZTOCKI, N.; KIM, L.N. (1999): Integrating activity-based costing and economic value added in manufacturing. Engineering Management Journal 11.2. June.

RUBIO MARTÍN, G. (2003): Valoración de compañías biotecnológicas a través de opciones reales. Aplicación a Zeltia. Análisis Financiero. Nº 92. Tercer cuatrimestre. Instituto Español de Analistas Financieros. Madrid.

RUBIO MARTÍN, G; LAMOTHE FERNÁNDEZ, P.(2006): Real option in biotechnological firms valuation. An empirical analysis of European firms. Journal of Technology Management Innovation. Vol. 1. Nº 2, 2006.

RUBIO, G. Y LAMOTHE, P. (2005): Las opciones reales en la valoración de las empresas biotecnológicas. Un análisis empírico de empresas europeas. Documento de trabajo. Universidad Complutense/Autónoma. Madrid.

RUIZ MARTÍNEZ, R.J. Y GIL CORRAL, A.M. (2004): El valor de la empresa. Ed. Instituto Superior de Técnicas y Prácticas Bancarias. Madrid.

RUIZ, R.; JIMÉNEZ, F. (1999a): ¿Qué nos dejó el viejo Análisis Fundamental? Boletín de Estudios Económicos, Deusto. VOL. LIV. Abril.

RUIZ, R.; JIMÉNEZ, F. (1999b): Antes y después del Flujo Descontado de Fondos. Revista Profesional de Gestión Financiera Banca & Finanzas, nº 48.

RUIZ, R.; JIMÉNEZ, F. (2000): Opciones Reales sin Soluciones Ficticias. Revista Profesional de Gestión Financiera Banca & Finanzas, Nº 60. Madrid.

SAHOO, S; RAJIB, P. (2013): Comparable firm's P/E multiple and IPO valuation: an empirical investigation for Indian IPOs. Institute of Management Calcutta 2013. 16 November.

SAINT-ONGE, H. (1996): Tacit knowledge. The key to the strategic alignment of intellectual capital. Strategy &Leadership. Marzo/Abril.

SALAS FUMAS, V. (1996): Economía y gestión de los intangibles. Economía Industrial. Nº 307.

SALEHI, M.; ENAYATI, G.; JAVADI, P (2014): The Relationship between Intellectual Capital with Economic Value Added and Financial Performance. Iranian Journal of Management Studies7.2. Jul.

SALINAS, G. (2007): Valoración de marcas. Ed. Deusto. Barcelona.

SÁNCHEZ, R. (1993): Strategic flexibility, firm organization and managerial work in dynamic markets. Advances in Strategic Management. Vol. 9.

SÁNCHEZ, R. (1997): Preparing for an uncertain future: managing organizations for strategic flexibility. International Studies of Management & Organization; Nº27. Summer.

SANDULLI, F.D.; CHESBROUGH, H. (2009): Open Business Models: Las dos caras de los Modelos de Negocio Abiertos. Universia business review. Segundo trimestre.

SANJURJO ÁLVAREZ, M.; REINOSO CASADO, M.M. (2003): Guía de valoración de empresas.PricewaterhouseCoopers. Pearson Educación.

SANTANDREU, E. Y SANTANDREU, P. (1998): Valoración, venta y adquisición de empresas. Ed. Gestión 2000. Barcelona.

SCHEIN, EDGAR (1992): Organizational Culture and Leadership: A Dynamic View. San Francisco. CA: Jossey-Bass.

SCHELLING, T.C. (1980): The strategy of conflict, 2ª ed., Harvard University Press, Cambridge.

SCHMID, B., ALT, R., ZIMMERMANN, H. y BUCHET, B. (2001). Anniversary edition: business models. Electronic markets, 11.

SCHWARTZ, E.S. Y GOROSTIZA, C.Z. (2000): Valuation of Information Technology Investments as Real Options, American Finance Association Meeting, New Orleans.

SCHWARTZ, E.S. Y MOON, M. (2000): Rational Pricing of Internet Companies, Financial Analysts Journal, mayojunio.

SCHWARTZ, E.S. Y MOON, M. (2001): Rational Pricing of Internet Companies, Financial Review, Nº 36.

SCREPANTI, E. Y ZAMAGNI, S. (1997): Panorama de historia del pensamiento económico. Ed. Ariel Economía.

SCWANDT, D.; MARQUARDT, M. (2000): Organizational Learning: From World-class Theories to Global Best Practices. Boca Raton: St Lucie.

SELZNICK, P. (1957): Leadership in Administration: A Sociological Interpretation. Harper & Row. New York.

SENGE, P.M. (1999): La quinta disciplina en la práctica. Granica. Barcelona.

SENGE, P.M. (1993): La quinta disciplina: cómo impulsar el aprendizaje en la organización inteligente. Granica. Barcelona.

SENNETTI, J.T.; CHANG-SOO, K.; SELLANI, R. J. (2004): Measuring the Effect of Investment in Intellectual Capital. Journal of Applied Management and Entrepreneurship 9.2. April.

SHARPE. W.F. (1976): Teoría de cartera y del mercado de capitales. Ed. Deusto. Bilbao.

SHIMIZU, K.; HITT, M.A. (2004): Strategic flexibility: Organizational preparedness to reserve ineffetive strategic decisions. The Academy of Management Executive. Briarcliff Manor; nov. Vol. 18.

SKARZYNSKI, P. y GIBSON, R. (2008). Innovation to the core: a blueprint for transforming the way your company innovates. Boston, Massachusetts: Harvard Business Press.

SLATER, J.C.; NARVER, J.C. (1995): Market orientation and the learning organization. Journal of Marketing, 59, 3.

SMITH, A. (1997): Investigación sobre la naturaleza y causa de la riqueza de las naciones. Ed. Fondo cultura económica. Bogotá. Colombia.

SMITH, G.V. (1997): Trademark Valuation. Ed. John Wiley & Sons. Estados Unidos.

SMITH, G.V. Y PARR, R.L. (1994): Valuation of intellectual property and intangible assets. Ed. Jon Wiley & Sons. Estados Unidos.

SMITH, G.V. Y PARR, R.L. (2000): Valuation of intellectual property and intangible assets. Ed. Jon Wiley & Sons. Estados Unidos.

SMITH, G.V. Y PARR, R.L. (2005): Intellectual Property. Ed. John Wiley & Sons. Estados Unidos.

SAHOO, S.; RAJIB, P. (2013): Comparable firm's P/E multiple and IPO valuation: an empirical investigation for Indian IPOs; Indian Institute of Management Calcutta; 16 November.

SOTOMAYOR GONZÁLEZ, S. (2005): La relevancia valorativa de los intangibles y los valores tecnológicos europeos. Servicio de publicaciones Universidad de Cádiz.

SOTOMAYOR GONZÁLEZ, S. Y LARRÁN JORGE, M. (2005): La valoración de empresas y los intangibles. Partida Doble. Nº 166.

STATA, R. (1989): Organizational learning-The key to management innovation. Sloan Management Review. Sping.

STERN, J.M.; ROSS, I.; SHIELY, J.S. (2001): El reto del EVA: cómo implantar y gestionar el cambio de valor añadido en una organización. Gestión 2000.

STEWART, G.B. III (2000): En Busca del Valor. Gestión 2000. Barcelona.

STEWART, G.B. III (2013): Best-Practice EVA: The Definitive Guide to Measuring and Maximizing Shareholder Value. Wiley. March 18.

STEWART, T.A. (1997): La Nueva Riqueza de las Organizaciones: EL Capital Intelectual. Ed. Granica, Buenos Aires.

STOPFORD, J.M.; BADEN-FULEER, C. (1990): Flexible Strategies. The key to success in knitwear. Long Range Planning. Vol. 23.

SUÁREZ SUÁREZ, A.S. (1981): Decisiones óptimas de inversión y financiación. Ed. Pirámide. Madrid.

SUÁREZ SUÁREZ, A.S. (1988): Decisiones óptimas de inversión y financiación. Ed. Pirámide. Madrid.

SUÁREZ SUÁREZ, A.S. (1996): Decisiones óptimas de inversión y financiación.

SULLIVAN P.H. (2001): Rentabilizar el capital intelectual. Paidós, Barcelona.

SUNDSTROM, E., DE MEUSE, K. P., & FUTRELL, D. (1990): Work teams: Applications and effectiveness. American Psychologist, 45.

SVEIBY, K.E. (2000). Capital intelectual. La nueva riqueza de las empresas. Cómo medir y gestionar los activos intangibles para crear valor. Ed. Gestión 2000, París.

TAGGART, J.; KONTES, P.; MANKINS, M. (1994): The value imperative. Managing for superior shareholderreturns; The free press; New York.

TAMAYO TORRES, I. (2006): Flexibilidad estratégica y opciones reales en los procesos de cambio estratégico. Tesis doctoral. Director: Lloréns Montes, F.J. Universidad de Granada. Departamento de organización deempresas.

TEECE, D. J. (2010). Business models, business strategy and innovation. Long Range Planning, 43.

TEECE, D.J.; PISANO, G.; SHUEN, A. (1997): Dynamic capabilities and strategic management. Strategic Management Journal. Vol. 18.

TERMES, R. (1998): Inversión y Coste de Capital. Ed. Mc Graw Hill. Madrid.THOMSON, J.D. (1967): Organizations in action. McGraw-Hill. New York.

TIMMERS, P. (1998). Business models for electronic markets. Electronic markets, 8.

TITMAN, S.; MARTIN, J.D. (2009): Valoración. El arte y la ciencia de las decisiones de invesión corporativa. Pearson educación. Madrid.

TOBIN, J. (1978): Monetary policies and the economy: The transmisión mechanism. Southern Economic Journal, Abril.

TOBIN, J. (1969): A general equilibrium approach to monetary theory; Journal of money, credit and banking; 1.

TOLLINGTON, T. (1999): The Brand Accounting Side-show. The journal of product and brand management. Tomo 8. Nº3.

TORRES CORONAS, T. (2002): La valoración de marcas. Gestión 2000. Barcelona.

TREACY, M.; WIERSEMA, F. (2004): La disciplina de los líderes del mercado. Norma. Bogotá, Colombia

TRIGEORGIS, L.; MASON, S. (1991): Valoración de la flexibilidad futura en las decisiones de inversión. Análisis financiero. Nº 54. Abril-Junio.

TRUEMAN, B.; FRANCO WONG, M.H.; ZHANG, X. (2000): “The eyeballs have it: searching for the value in internet stocks. (http://www.ssrn.com)

UNIÓN EUROPEA DE EXPERTOS CONTABLES, ECONÓMICOS Y FINANCIEROS (UEC) (1962): Evaluación de empresas y partes de empresa: reglas formuladas por la Comisión Especial U.E.C. Deusto. Bilbao.

UPTON, D.M. (1994): The management of manufacturing flexibility. California Management Review; Winter.

VALHONDO, D. (2003): Gestión del conocimiento. Ed. Díaz de Santos. Madrid.

VÉLEZ-PAREJA, I. (2013): Valoración de intangibles. Publicado en Cuadernos Latinoamericanos de Administración. Volumen IX. Nº 17. Julio – Diciembre.

VENTURA VICTORIA, J.; ORDÓÑEZ DE PABLOS, P.; GARCÍA SUÁREZ, J.L.; ARIAS ÁLVAREZ, A.M. (2003): Capital intelectual y aprendizaje organizativo. Nuevos desafíos para la empresa. AENOR. Madrid.

VIJAYAKUMAR, A. (2012): Economic Value Added (EVA) and other accounting performance indicator: an empirical analysis of Indian automobile industry. International Journal of Marketing and Technology 2.3.

VILLANI, G. (2014): Valuation of R&D Investment Opportunities with the Threat of Competitors Entry in Real Option Analysis. Springer Science+Business Media New York.

VILLIGER, R.; BOGDAN, B. (2006): Pitfalls of valuation in biotech. Journal of Commercial Biotechnology 12.3. April.

VISCIO, A. y PATERNACK, B. (1996). Toward a new business model. Strategy y Business, 20.

VOLBERDA, H.W. (1996): Toward the flexible form: how to remain vital in hypercompetitive environments. Organization Science. Vol. 7.

VOLBERDA, H.W. (1997): Building flexible organizations for Fast-Moving Markets. Long Range Planning. Vol. 30. April.

WEICK, K.E. (1979): The social psychology of organizing. Addison Wesley.

WESTON, J.F.; COPELAND T. (1995): Finanzas en Administración. Ed. McGraw-Hill, México.

WHIPP, R.; ROSENFELD, R.; PETTIGREW, A. (1989): Managing Strategic Change in a mature business. Long Range Planning. Vol. 22. Nº 6.

WIEDERHOLD, G. (2014): Valuing Intellectual Capital: Multinationals and Taxhavens (Management for Professionals); Ed. Springer.

WIRTZ, H. (2012): Valuation of Intellectual Property: A Review of Approaches and Methods. International Journal of Business and Management. Vol. 7. Nº 9. May.

WOFFORD, J.C.; GOODWIN, V.L.(1994): A cognitive interpretation of transactional and transformational leadership theories. The Leadership Quarterly. Volume 5, Issue 2, Summer.

WOODWARD, C. (2003): Valuing Intangible Assets and Impairment Testing in the Pharmaceuticals Industry. Ed. Pricewaterhousecoopers.

WORD, C. O., ZANNA, M. P., COOPER, J. (1974): The nonverbal mediation of self-fulfilling prophecies in interracial interaction. Journal of Experimental Social Psychology, 10.

WRIGHT, P.M.; SNELL, S.A. (1998): Toward a unifying framework for exploring fit and flexibility in strategic humanresource management. Academy of management review. Vol. 23. Nº4.

VROOM, V.H.; YETTON, P.W. (1973): Leadership and Decision-Making; Jun 28; University of Pittsburgh Press; 1st edition

YOUNDT, M.A.; SNELL, S.A.; DEAN, J.W.J.; LEPAK, D.P. (1996): Human resource management, manufacturing strategy, and firm performance. Academy of management journal. Vol. 39. Nº4.

YUKL, G. (2008): Liderazgo en las organizaciones. Pearson Prentice Hall. Sexta edición. Madrid.

YUNUS, M., MOINGEON, B. y LEHMANN-ORTEGA, L. (2010). Building social business models: Lessons from theGrameen experience. Long Range Planning, 43.

ZACCAROA, S.J.; RITTMAN, A.L.; MARKS, M.A. (2001): Team leadership. The Leadership Quarterly. Volume 12, Issue 4, Winter 2001.

ZAHRA, S.; GEORGE, G. (2002): Absorptive capacity: A review, reconceptualization and extension. Academy of Management Review. Vol. 27. Nº2.

ZIMMERMAN, R.; KLEIN BÖLTING, U.; SANDER, B.; MURAD- AGA, T. (2002): Brand Equity evaluator. Vol2. BBDOGroup.Germany.

ZOOK, C.; ALLEN, J. (2012): Repetibilidad. LID Editorial empresarial.

ZOTT, C. y AMIT, R. (2010). Business Model Design: An Activity System Perspective. Long Range Planning, 43.

# CAPÍTULO 3: LA SEGURIDAD INFORMÁTICA Y LA SEGURIDAD DE LA INFORMACIÓN

## 3.1 INTRODUCCIÓN

"Datos masivos, riesgos masivos. Nuestro poderío tecnológico aumenta, pero los efectos secundarios y los riesgos potenciales también son cada día más elevados", Alvin Toffleren su obra "El Shock del Futuro". Otra de sus obras importantes "La Tercera Ola". Autor de algunas de las predicciones más lúcidas sobre el cambio tecnológico dela segunda mitad del siglo XX y la adaptación de las sociedades tecnológicas. Sus siete frases para entender el siglo XXI: "La primera, el conocimiento es la fuente más democrática de poder; segunda, formular la pregunta correcta es más importante que dar la respuesta correcta a una pregunta equivocada; tercera, tienes que pensar en cosas grandes mientras estés haciendo cosas pequeñas, de modo que todas las pequeñas cosas vayan en la misma dirección; cuarta, hay que clausurar las escuelas (refiriéndose al sistema inspirado en la era industrial); quinta, el futuro será para aquellos que desarrollen habilidades o técnicas de pensamiento crítico; sexta, la sociedad necesita todo tipos de habilidades que no son cognitivas, son emocionales, son afectivas (inteligencia emocional). No podemos montar la sociedad sobre los datos; séptima, los analfabetos del siglo XXI no serán aquellos que no sepan leer o escribir, sino aquellos que no puedan desaprender y reaprender.

Para Alvin Toffler en la obra "El Shock del Futuro": Una de las definiciones de la cordura es la capacidad de distinguir lo real de lo irreal. Pronto necesitaremos una nueva definición".

El fin de la privacidad, para David Petraeus, exdirector de la CIA: "los objetos de interés serán localizados, identificados, monitorizados y controlados de manera remota mediante tecnologías como la identificación de radiofrecuencias, redes de sensores, servidores diminutos incrustados y recolectores de energía, todos los cuales se conectarán a internet de la siguiente generación mediante una computación abundante, de bajo coste y alta potencia"

Hogar, pirateado hogar. Según Padmasree Warrior, directorde tecnologías, Cisco: "Calculamos que actualmente sólo el uno por ciento de las cosas que podrían tener una dirección IP la tienen; de ahí que nos guste afirmar que el noventa y nueve por ciento del mundo aún dormita. Sólo nuestra imaginación puede proyectar qué sucederá cuando ese noventa y nueve por ciento se despierte".

Siguiendo a Dave Evans, exjefe del departamento de Futurismo de Cisco: "La internet de las Cosas, también conocido como internet de los Objetos, lo cambiará todo…inclusive a nosotros".

Para Christof Paar, profesor e investigador de la seguridad incorporada: "la mayoría de las personas preferiría tener un software malicioso en su ordenador portátil que en el interior del sistema de frenado de su vehículo".

Sobre la cámara cándida, siguiendo a Howard Rheingold, crítico y ensayista: "Hoy por hoy, vayas donde vayas, debes dar por supuesto que no tienes privacidad, porque los métodos de vigilancia son cada vez más asequibles e invisibles"

Preet Bharara, fiscal del Distrito Sur de Nueva York, Estados Unidos: “Como fiscal de los Estados Unidos en Manhattan, pocas cosas me preocupan tanto como las ciberamenazas que se ciernen sobre nosotros”.

Terry Pratchett en “Pies de barro”: “Para hacer carrera entre delincuentes, hay que tener reputación de ser honrados”

Ben Kingsley, “The good guy”: “El mundo ya no está dominado por las armas, ni por la energía ni por el dinero. Está dominado por unos y ceros, por pequeños bits de datos. Todo está en los electrones. Ahí fuera se está librando una guerra, una guerra mundial. Pero ya no importa quién tiene más datos. Lo auténticamente relevante es quién controla la información: qué vemos, cómo trabajamos, qué pensamos. Lo importante es la información”.Sun Tzu en su obra “El Arte de la Guerra”: Toda guerra se basa en el engaño”. Dean Koontz (2015): “En un mundo que cada día se desconecta más de la verdad, cada vez más personas aceptan lo virtual frente a lo real, y todo lo virtual es también maleable”.

Albert Gore (2011) dijo que en “casi todos los países (…) la gente ha aceptado la violación de su privacidad a cambio de la comodidad de internet”. En un momento en el que se multiplican las redes sociales disponibles y en el que crece geométricamente su número de usuarios, la privacidad (derecho constitucional español de la intimidad) es un tema central y debe respetarse siempre.

Vinto Cerf, diseñador del protocolo TCP/IP: “el mayor beneficio que sacamos de internet es la información que otros deciden compartir”. Para Tim Berners-Lee, inventor del protocolo “www”, comenta que “la web incluye lo que está en el ordenador, pero que uno debe poder tener el control sobre dónde está y con quién lo comparte”.Una de las razones para usar esta herramienta es encontrar la verdad de la situación política, de la ciencia, etc.” Al Gore alentó en su día a “defender la libertad de internet” ante la “crisis climática y de democracia”. “Internet es una herramienta esencial para la democracia”. “Internet es una red de personas y no de máquinas”. “Debemos proteger esa idea central”. “Internet es la solución del cambio climático”, en su compromiso con el medio ambiente. Por otro lado, debemos contextualizar internet como una herramienta inscrita en el respeto a los valores y los derechos humanos en un mundo global: “El respeto a la Madre Tierra”, López Pérez, F. (2016) Conferencia sobre la Amazonía, Centro Padre Arrupe, Sevilla.

Al Gore en Marc Goodman (2015): “En la era digital, le privacidad debe ser una prioridad. ¿Me lo parece a mí o la vigilancia generalizada en secreto es una atrocidad y una obscenidad?”.

Para Omar N. Bradley en Marc Goodman (2015): “Si continuamos desarrollando tecnología sin sabiduría y prudencia, es posible que nuestro siervo acabe convirtiéndose en nuestro ejecutor”

“He leído y acepto los términos y condiciones de este servicio” es la mayor mentira de la Red. Terms of service: didn´t read, http//tosdr.Org.

David Mitchell en Marc Goodman (2015): “Vale, mi teléfono. Cuando aparecieron esas cosas, eran súper guays. Nos dimos cuenta demasiado tarde de que, de hecho, eran tan guays como los chips electrónicos que ponen a los reos en las prisiones preventivas”.

Eugeny Morozov en Marc Goodman (2015): “los teléfonos móviles son unos dispositivos más inseguros que hayan existido nunca, por lo cual resultan más fáciles de rastrear y de pinchar”.

Viver Wadhwa en Marc Goodman (2015), “un ingrediente básico de la innovación es la capacidad de desafiar a la autoridad y transgredir las reglas”.

Charles C. Mann, escritor, en Marc Goodman (2015), “Un Smartphone enlaza los ordenadores del paciente y el doctor, que a su vez están conectados a internet, que a su vez están conectados a otro Smartphone en otro lugar. Los nuevos dispositivos podrían colocar la gestión de los órganos internos en manos de cualquier hacker, timador online y vándalo digital sobre la faz de la tierra”.

“Si alguien te roba la contraseña puedes cambiarla…tantas veces como sea preciso. Pero no te puedes cambiar las huellas dactilares (dedos pirateados). Sólo tenemos diez y las dejamos en todo lo que tocamos”. Senador Al FranKen en Marc Goodman (2015).

Los derechos de los robots: legislación, ética y la privacidad, “Un hombre sin ética es una bestia salvaje soltada en este mundo”, Albert Camus.

Los ataques de los drones. “Los drones dan miedo. No se puede razonar con ellos”, Matt Groening, creador de los Simpson, en Marc Goldman (2015).

La relación de los hombres y las máquinas pueden transformar las relaciones entre humanos ampliamente acerca de cómo los esclavos pueden convertirse en los dueños.

Nos proponemos a partir de ahora orientar a nivel de empresa las actividades que debemos realizar para afrontar la problemática de la seguridad de la información.

Nuestro mundo está lleno de sistemas compuestos por máquinas y por programas, software, muchos sistemas formados por ordenadores, dispositivos de red, teléfonos inteligentes, tablets, etc., forman parte de redes, privadas o de empresa, públicas, grandes o pequeñas, interconectadas unas con otras y comunicándose entre sí, mediante otro gran sistema de hardware como cables o inalámbricos, gestionado a su vez por un conjunto de aplicaciones con diferentes objetivos, a los que se denominan protocolos de comunicaciones, siguiendo a Díaz y Orueta, G (2013) en su obra: “ Procesos y herramientas para la seguridad de redes”. “Internet, es un sumatorio complejo de redes y sistemas que ha modificado desde años todas las formas habituales de comunicación, cambiando radicalmente los hábitos de vida y formas de trabajar de todos los sectores de la sociedad, ha provocado cambios organizacionales a todos los niveles, robotización de las cadenas de producción, etc.”.

Los sistemas gozan de una serie de propiedades: son complejos y capaces de interactuar; otra propiedad curiosa es que muchos de ellos hacen cosas no esperadas, no pensadas ni diseñadas, no buscadas. Esta propiedad no buscada le llamamos “bug” que es una clase de fallo del sistema no previsto, esto no significa que el sistema no funcione correctamente. Está demostrado que cuanto más complejo y sofisticado sea el sistema, mayor es el número de “bugs” que contiene.

Algunos de estos bugs se pueden transformar en problemas de seguridad informática en los sistemas y protocolos. El sumatorio de tales bugs de seguridad y vulnerabilidades de seguridad originadas en un desarrollo incorrecto, precipitado, o ambas cosas a la vez, de las aplicaciones del software en general, provocan lo que conocemos como agujeros de seguridad. Si son aprovechados por alguien mal intencionado, los sistemas y las redes en los que están sufrirán ataques a su seguridad.

Todos estos bugs y vulnerabilidades hacen que sea difícil conseguir que un sistema, como puede ser, por ejemplo, la red de una universidad, o de una empresa, o, más aún, la red internet, sea seguro. Los sistemas seguros son difíciles de obtener. Los sistemas complejos seguros son aún más difíciles de construir.

Los ataques a la seguridad de sistemas y redes se aprovechan de esa complejidad de la que estamos considerando, ya sea para realizar ataques de obtención de información, (de contraseña de sistemas y aplicaciones o de datos), ataques de acceso no autorizado a sistemas, aplicaciones, etc., ataques de modificación de información o de borrado de información o ataques de negación de servicios, que tienen como consecuencia la inhabilitación de un servicio Web o de correo y, en general, no poder usar un recurso concreto. Este último tipo de ataques han llegado recientemente a inhabilitar internet en una parte del mundo.

Contra este tipo de problemas, se han desarrollado tecnologías informáticas que, como los cortafuegos o criptografías de comunicaciones, parecen impecables. Son necesarios, pero a su vez, están compuestos de sistemas que pueden (y, por desgracias, suelen) exhibir los mismos problemas citados.

Si nos dedicamos a investigar los ejemplos recientes de problemas de seguridad en sistemas y redes (una sencilla búsqueda en internet proporciona cientos de informes sobre incidencias de este tipo), comprobaremos que prácticamente todos (incluidos los que tienen que ver con problemas en sistemas de seguridad) están relacionados con esas propiedades de los sistemas citados anteriormente.

Ayudará bastante pensar, desde un principio, que con todos sus componentes hardware y software, etc.; la seguridad es un sistema dentro de sistemas mayores, más que un producto o un conjunto de ellos, más que una o varias tecnologías, la seguridad es un proceso, que hace intervenir todas las tecnologías, todos los productos, todas las herramientas y, especialmente, el sentido común de los seres humanos que la gestionan, ese mismo sentido común que es el menos común de los sentidos.

La seguridad de las redes, sistemas y datos usa nuevas herramientas y procedimientos, nuevas tecnologías, pero no será digna de uso si no utiliza las viejas técnicas de seguridad humana que se llevan usando (cuando se usan) miles de años en muy diversas circunstancias.

La seguridad informática debe tener muy en cuenta la prevención (cortafuegos, criptografía, etc.), pero está evolucionando en cuanto a las otras dos (detección y respuesta).

Se utilizan cada vez más herramientas de detección (como los sistemas de detección de intrusiones) y herramientas, procedimientos y sistemas (muchas veces humanos) de análisis y gestión de riesgos y auditorías de vulnerabilidades.

Debemos tratar las preguntas que nos tenemos que hacer para definir mejor el sistema que uno quiere asegurar, explorando alguna solución aparentemente perfecta, (pero sólo aparentemente), y proponiendo una solución imperfecta pero realista, basada en lo que se llamará política de seguridad del sistema, herramienta básica para la seguridad.

Una serie de preguntas nos ayudará a definir mejor el problema, el objetivo prioritario deseado es conseguir la seguridad más completa para los sistemas y redes de comunicación. Para ello, se va a delimitar más el problema usando una vieja táctica pedagógica: hacerse preguntas claves.

Nuestra primera pregunta clave, debe resultar evidente:

¿Qué es lo que se quiere tener protegido? Esta pregunta debería tener asociada la realización de un inventario de los activos de la organización, entendiendo como tales, los sistemas, redes,

aplicaciones, elementos de red, bases de datos, y, en general, cualquier tipo de activo, físico o no, que se quiera tener asegurado.

Por supuesto, no todos los activos tendrán el mismo valor y éste será un criterio muy importante a la hora de establecer una estrategia de cara a la seguridad. Ejemplo, supongamos una empresa con una base de datos con información de sus productos y que es accesible a los posibles clientes por internet. Supongamos que se tiene una copia de seguridad de la base de datos suficientemente buena y que se tiene un plan de recuperación de la base de datos en caso de pérdidas. Supongamos que el coste de tal recuperación se estima en cinco mil euros. ¿Tiene sentido poner en marcha un sistema de prevención de ataques que cueste cincuenta mil euros? La respuesta suele ser no, pero y si la empresa solo vende por internet, (¿en cuánto dañaría su imagen ese ataque y pérdida?). Esta situación hay que evaluarla con detalle haciendo un buen análisis de riesgos.

Otra pregunta que ayudará mucho a definir el problema es:

¿Contra quién se quiere proteger? O, expresado de otra forma, ¿En quién se puede confiar y en quién no?, ¿Quiénes son los posibles atacantes?

Como respuesta a esta pregunta suele desarrollarse un modelo de confianza. Con este análisis, se debe decidir qué empleados tienen acceso a qué activos y porqué, qué tipo de acceso se va a dar a cada persona de cada organización que colabore con la empresa, qué tipo de acceso (físico o lógico) van a tener, es decir, acceso de ordenadores, redes y datos. Así mismo, se deberá pensar en qué tipo de acceso van a tener los posibles clientes de la organización. La cosa se complica un poco (y suele hacerlo) si alguno de los clientes es, además, colaborador de la organización.

Además, se debe estudiar, con cuidado y detalle, quién y porqué querría atacar a la organización. Esto, que está muy ligado con lo anterior, hará incluir una categoría de individuos que no ha aparecido aún. Los malos. Podría parecer que son claves separadas, que estos últimos son de una categoría distinta a la de los empleados, compañeros, colaboradores o clientes; pero esto no suele ser así desgraciadamente.

Si estudiamos distintas problemáticas sobre pérdidas económicas debidas a ataques informáticos (por ejemplo, los que se pueden consultar en http://www.fbi.gov/, http://www.inteco.es, http://www.cert.org/, http.//www.sans.org) se observa una serie de característica comunes: Alrededor del 65% (el 55% en unas encuestas el 75% en otras) de los encuestados reconocen haber sido atacados (pérdidas de datos, pérdidas de información, inhabilitación de servidores o acceso a redes, cambio de información, robo, fraude, etc.); Alrededor del 60% de los encuestados reconocen que algunos de sus ataques fueron realizados desde el interior de sus organizaciones; alrededor del 60% de los encuestados reconocen que algunos de sus ataques fueron realizados mediante conexiones desde la red internet; prácticamente todos los encuestados reconocen haber sufrido más incidentes de este tipo que el año anterior.

Con esto concluimos que el perfil del posible atacante no hay que buscarlo solo en un usuario de la red internet, sino también dentro de la organización.

En cuanto a los tipos de atacantes, se debe comenzar hablando de hacker. Esta es una palabra que ha cambiado de significado con el tiempo. Al principio, lo hackers eran personas muy expertas en un sistema operativo, protocolo, etc., que, en el caso de encontrarse fallos de

seguridad de un sistema, lo notificaban al fabricante, incluso, a veces, facilitando, además, una posible solución. Tales personas existen todavía y, aunque sus hallazgos suelen ser muy interesantes, hay una polémica, hoy en día: si hacen bien o mal a la industria informática. Independientemente de esto último, hoy en día se le ha dado un sentido peyorativo a la palabra hacker, pensando en alguien que, por distintas motivaciones (venganza, ira, cuestiones religiosas, políticas o simplemente reto intelectual) ataca las redes o sistema de una organización), Chema Alonso (2017), directivo de Eleven Paths, entrevista en ABC sobre su respuesta ante la RAE (Real Academa de la Lengua), defendiendo la actitud profesional positiva de los hackers en las organizaciones.

Algunos ejemplos de tales motivaciones son: empleados que son despedidos injustamente y que dejan en los sistemas de la empresa sorpresas que destruyen datos de la organización o la dañan de muy diferentes maneras; empleados que creen ser injustamente pagados, a menudo en comparación con algún compañero suyo, y alteran los registros de personal propios, de los compañeros o de ambos; defensores de los derechos civiles que atacan a los servidores Web de organizaciones racistas y, por supuesto el caso contrario; hackers que roban mensajes de correo electrónico de unos políticos, para otros políticos; individuos que acceden a sitios Web muy conocidos (por ejemplo, el periódico New York Times) para cambiar su contenido, por razones de línea editorial u otras; todos los ejemplos de los últimos años relacionados con wikileaks.

Un caso especial es el de Anonymous, un seudónimo usado internacionalmente por diferentes grupos y/o individuos para realizar en su nombre acciones o publicaciones individuales o concertadas. Desde 2008, Anonymous se manifiesta en acciones de protesta a favor de la libertad de expresión, de la independencia de internet y en contra de diversas organizaciones.

Otro tipo de atacante es el amateur que juega (wannabes, término despectivo). El perfil suele ser una persona joven o muy joven, sin experiencia en sistemas ni en redes, que usa herramientas automatizadas contra sistemas de internet, para ver qué pasa.

Hay un tercer tipo de atacantes, cada vez más numeroso y más peligroso: el profesional, individuo que presta sus conocimientos (interesada o desinteresadamente) para atacar un objetivo concreto, que puede ser el robo, la alteración de la información con fines delictivos oel sabotaje. Lo que les caracteriza fundamentalmente es el modo profesional de atacar. Además, estos profesionales se alían en verdaderas organizaciones cibercriminales que aprovechan las múltiples vulnerabilidades existentes y las herramientas de ataques en continuo desarrollo (como los botnets) para crear un verdadero modelo de negocio en la red, basado en la oferta de diferentes servicios de ataque a cambio de una contraprestación económica. Todas las fuerzas de orden público internacionales siguen sus pasos en lo que puede catalogarse como guerra global contra el crimen organizado en internet. Muy relacionados con este tipo de situaciones son los continuos ataques entre servicios militares de diferentes países por internet, que ha dado lugar al término de ciberguerra que está poniendo en peligro desde la seguridad de las instalaciones civiles y militares en muchos países hasta por ejemplo misiones concretas de la OTAN en zonas de conflicto. Otra pregunta muy importante para caracterizar finalmente el problema es:

¿Cómo se quiere proteger? O, más concretamente, ¿Qué tecnologías, herramientas, sistemas concretos, procesos se van a utilizar para protegerlos?

Para contestar bien a esta pregunta se tienen que conocer dos temas complejos: lo primero, los distintos tipos de ataques posibles; las distintas defensas posibles.

Debemos de hacer el siguiente comentario: no será posible nunca conocer los distintos tipos de ataques. Es imposible que lo haga nadie, pues nadie puede abarcar todo lo hecho y todo lo que se puede estar haciendo ahora y se podrá hacer más adelante. Así, un buen profesional ha de conformarse con conocer el mayor número posible y estar bien informado sobre todos los nuevos que van apareciendo.

Los tipos más importantes son: ataques para obtener información. Son ataques no intrusivos que tienen como objetivos obtener información (como direcciones, IP de redes y sistemas, sistemas operativos de cada equipo, número de puertos abiertos, aplicaciones y sus versiones, contraseñas, etc.); ataques de accesos no autorizados son ataques de acceso de personas no autorizadas a los sistemas, suelen ser pruebas, sin mayor interés que demostrarse a sí mismo que pueden llegar a ese sistema, pueden ser peligrosos si el acceso se hace, además, a través de una cuenta privilegiada del sistema; ataques con revelación de información, una vez que se tiene el acceso anterior, se puede utilizar para acceder a información secreta, con la idea de aprovecharse de esa información, de borrarla o, peor aún, de modificarla de un fin no demasiado lícito; ataques de denegación de servicios, buscan dejar no disponible un sistema, un servicio, o una red, habitualmente agotando el recurso, sea este el ancho de la banda, espacio en disco, conexiones TCP, etc. Desafortunadamente, este tipo de ataques no suele necesitar ningún acceso previo a ningún sistema y en el caso de algunos, como los DDOS (Distributed Denial of Service) son prácticamente imparables.

Estos serían los más importantes, pero, además, hay que recordar que el atacante no tiene por qué cumplir fielmente con un tipo de ataque determinado. Cada vez más, los ataques suelen ser combinaciones de varios.

En cuanto a las defensas posibles, aspectos muy relacionados con lo anterior vamos a relacionar algunas de las más importantes:

Esquemas de seguridad de sistemas operativos, especialmente para el caso de servidores con información muy relevante y de dispositivo de gestión de red, se deben mantener unos buenos esquemas de seguridad de ficheros, usuarios y aplicaciones, así como de servicios de red controlados desde tales sistemas. Hoy en día, además, estos esquemas son fundamentales para todo tipo de dispositivos móviles.

Sistemas de identificación o autenticación seguros, hay muchos y muy razonables, desde las contraseñas hasta los sistemas biométricos, certificados digitales, tarjetas de identificación o distintas combinaciones. Se pueden usar tanto para acceso local a dispositivos como para acceso remoto.

Sistemas de cortafuegos o (firewalls), sistemas de control de la información en forma de mensajes que entran o salen de una red. Se han convertido en esenciales y los hay de muchos tipos distintos.

Sistemas criptográficos, son sistemas que permiten, de varias formas distintas mantener la integridad y autenticación de mensajes o datos, así como la privacidad o confidencialidad de los mismos. Se integran en protocolos y en parte de los distintos sistemas operativos y aplicaciones, que usan algoritmos criptográficos suficientemente probados.

Sistemas antivirus, son aplicaciones locales, o distribuidas, que permiten defenderse de los virus informáticos, nombre que reciben algunas aplicaciones utilizadas para cualquiera de los ataques citados.

Sistemas de análisis de vulnerabilidades. Son aplicaciones que permiten buscar en sistemas y aplicaciones instaladas distintos bugs o vulnerabilidades conocidas, para decidir si se corrigen (parchean), se cambian de versión o se dejan como están.

Sistemas de detección de intrusiones, son sistemas o aplicaciones que permiten, en tiempo real, detectar distintos tipos de ataques y alertar sobre ellos a la vez, en algunos casos, pueden pararlos.

Estándares para sistemas de gestión de seguridad, como el ISO/IEC 27.001 que se describe a lo largo de la tesis y que permite organizar los procesos y procedimientos de gestión de la seguridad de cualquier organización.

Una vez conocido los ataques y las posibles defensas se deberá decidir qué defensas se eligen frente a qué ataques. Aunque esto no podrá hacerse hasta haber contestado a la pregunta más comprometida de todas:

¿Cuánto dinero se puede gastar en implantar y mantener el proceso de seguridad?

La seguridad en las redes puede ser más o menos completa, pero siempre tiene un componente económico, como sucede para cualquier problema de seguridad.

Se debe tener en cuenta el dinero (o recursos de todo tipo) que van a ser empleados en cada una de las siguientes tareas:

- Adquisición de herramientas Hardware y Software, que implementen algunas de las defensas citadas.El tiempo empleado en configurarlas y educar a los usuarios en su uso.
- El tiempo empleado en la administración, mantenimiento y reconfiguración paras permitir nuevos servicios, auditar las herramientas, etc.
- El tiempo empleado en poner en marcha un sistema de gestión de seguridad con todos los procedimientos, roles y responsabilidades asociadas.
- El tiempo empleado, en muchos casos, en volver a una situación estable, después de la inconveniencia para los usuarios de alguno de los nuevos sistemas.

Resumiendo, para tratar de enfocar el problema con acierto se debe tener cuanto más conocimiento mejor de qué se puede perder, qué se quiere proteger, de quién se quiere proteger, quien puede querer atacar, cómo pueden ser los ataques, cuáles pueden ser las defensas y cuánto se puede invertir.

Se debería de tratar de resumir todo este conocimiento en un análisis de riesgos que, de manera condensada tendría cuatro puntos clave:

Valorar los activos.

Entender todas las posibles amenazas.

Monitorizar y conocer todas las debilidades y vulnerabilidades del sistema.

Tratar de poner en marcha todas las medidas posibles para disminuir la probabilidad de tener pérdidas.

Contra problemas tan complejos como los que hemos comentados anteriormente, podemos hacer una aproximación completa, en el sentido de tratarlos como problemas científicos,

estudiarlos de manera analítica, teniendo como objetivo que, en el sistema concreto, la probabilidad de sufrir un ataque sea lo más cercana a cero. A esta aproximación, que ahora se va a desarrollar, se le da el nombre de aproximación militar. Tal aproximación, que sería perfecta si lograra su objetivo- probabilidad de sufrir un ataque igual a cero- pasa por cumplir y hacer cumplir una serie de requisitos formalidades sobre todas las partes de la organización que va a ser asegurada y llevaría a adoptar una serie de decisiones de mucho peso, como:

La no aceptación de ningún código de aplicación no desarrollado siguiendo las propias normas de seguridad.

La no aceptación de ningún sistema operativo, de ningún dispositivo, suficientemente comprobado, lo que suele querer decir, tecnología menos moderna.

La no aceptación de ninguna actualización de ningún sistema operativo hasta que hubiera pasado un margen suficiente de exposición al mundo real como para estar tranquilos.

No conectarse a internet o, si ya se estuviese conectado, desconectarse de ella y constituir una red propia.

Durante años hubo organizaciones, como los ejércitos, algunos sistemas del transporte ferroviario japonés, proyectos de investigación de tecnología militar, etc., que intentaron poner en marcha esta solución perfecta, pero no es posible. Hoy en día, es imposible pensar en implementar con éxito las decisiones citadas en prácticamente cualquier organización.

Conviene recordar que la seguridad no es un producto, sino un proceso, en el que están implicados desde sistemas software, redes, aplicaciones, organizaciones y personas. La criptografía, por ejemplo, no ha sido nunca en su historia tan potente y nunca ha sido tan fácilmente burlada como hoy en día. Existen muchas herramientas, pero hay que saber usarlas, no solo en el sentido de configurarlas, sino en el sentido de dirigirlas en el sentido adecuado, con la estrategia válida, que, por supuesto, tiene que tener en cuenta todos los factores citados anteriormente; pero también el de no gastarse todo el presupuesto de la organización y de sus recursos, que debe seguir funcionando y cumpliendo sus objetivos, sean estos de negocios (telecomunicaciones, financieros, energéticos, etc.).

En este marco de esta aproximación se define lo que se denomina política de seguridad, como una serie de sentencias formales que deben cumplir todas las personas que tengan acceso a cualquier información y/o tecnología de una organización (IEFT Site Security Handbook).

El propósito principal de una política de seguridad debe ser informar a los usuarios, trabajadores y personal de dirección de los requisitos obligatorios para proteger los valores tecnológicos e información de la empresa. La política debería especificar los mecanismos a través de los cuales estos requisitos pueden ser conocidos. Otro objetivo de la política de seguridad debe ser proporcionar una base para adquirir, configurar y auditar todos los dispositivos y las redes. Por tanto, emplear un conjunto de herramientas de seguridad sin una política de seguridad implícita, no tendría mucho sentido.

Una buena política de seguridad debe cumplir una serie de normas generales, una vez más, de sentido común:

Debe poderse implantar. Como consecuencia de ella, se deben tener unas normas de comportamiento para los usuarios y administradores, unas políticas de uso aceptables.

Debe entenderse. Debería de explicarse a todo el personal de la organización el alcance de no cumplirla, así como el significado técnico y legal de una serie de conceptos como confidencialidad, integridad, identificación, autenticación, etc.

Debe cumplirse. Debe contemplar una serie de procedimientos de auditoría, para comprobar que no es un papel mojado, sino que está realmente cumpliéndose. Debe contemplar, igualmente, sanciones adecuadas a cada una de las posibles infracciones. En este sentido, es muy importante señalar que debe estar respaldada completamente por la dirección de la organización, sin tal apoyo nunca se puede llevar a cabo.

Debe definir responsabilidades. No puede ser igual el papel de un usuario que el de un administrador de una gran red, en el sentido de las distintas responsabilidades.

Debe permitir que siga realizándose el trabajo normal. Si no fuera así, se estaría en la aproximación militar: no se permite un nuevo servicio, hasta que no sea completamente seguro. Debe ofrecerse seguridad, pero al precio de que no funcione la organización. Debe implicar un análisis de riesgos, teniendo en cuenta el precio de la seguridad frente a la probabilidad de pérdidas.

Debe ser exhaustiva. Debe tener en cuenta todos los componentes del sistema, es decir, debe incluir como objetivos asegurar: componentes físicos; sistemas informáticos (ordenadores personales, portátiles, servidores, host, dispositivos móviles, etc.) y su software; aplicaciones en red de los sistemas; dispositivos de red (encaminadores, conmutadores, etc.) y su software; sistemas de gestión de red; organizaciones humanas, individuos, departamentos, divisiones, colaboradores externos, clientes, etc.).

Debe incluir mecanismos de respuestas. Habrá que tener en cuenta qué se debe hacer al sufrir un ataque, cómo pararlo, cómo identificar al atacante y cómo responder al ataque.

Debe tener mecanismos de actualización. Por el principio de que la seguridad es un proceso. Al descubrir mediante una auditoría un fallo en el sistema de seguridad no contemplado en la política, hay que poder hacer una nueva versión e implementarla.

Habrá que tener en cuenta muchos más detalles:

Contemplar el principio de privilegio mínimo necesario, principio de menor autoridad, consiste básicamente en minimizar el impacto de cualquier fallo, accidente o vulnerabilidad del sistema.

Contemplar el principio de defensa en profundidad o defensa elástica, con la existencia de más de un nivel de defensas.

Contemplar el principio de diversidad de defensa, con la existencia de defensas de distintos tipos.

Tener conocimiento permanente de los puntos débiles de la organización.Participación universal del personal de la organización.

Simplicidad de los mecanismos de seguridad

Todavía hay muchas empresas, en base a las encuestas que hemos citado anteriormente existe sobre un 30% de los encuestados sin política de seguridad y un 70% de los encuestados con una política de seguridad que reconocen que no se cumple ni se mantiene.

En el mundo actual, la mayor parte de las organizaciones cumplirán las leyes como la Ley Orgánica de Protección de Datos (LOPD), la Ley de Servicio de Sistemas de Información y Comercio Electrónico (LSSICE) o el Esquema Nacional de Seguridad. Todo esto está obligando a las empresas a poner en marcha una aproximación. La enumeración de dispositivos y herramientas no criptográficas utilizadas para hacer cumplir la política de seguridad no sería completa sin hacer referencia a lo que suele llamarse diseño seguro de redes. Esto hace referencia a la seguridad en un sentido distinto al que venimos comentando. En realidad, se estaría hablando de fiabilidad del sistema, de alta disponibilidad de la información. Los procedimientos y herramientas utilizadas para mantener tal fiabilidad no son criptográficos y contemplan, en su diseño, técnicas de tolerancia de fallos. Estas técnicas consisten en que el software o el hardware proporcionen una cierta redundancia frente a posibles eventos negativos que pueden ocurrir.

Se debe hacer referencia o resaltar aquí dentro de la LOPD los derechos ARCO, son la garantía que tienen los usuarios, consumidores o cualquier ente para poder tener el control sobre sus datos, cuando estos estén en mano de otras personas o empresas: derecho de acceso a la información; derecho de rectificación, derecho de cancelación, derecho de oposición (hppt://www.grupoiwi.com)

Estos derechos se caracterizan por ser personalísimos, solo pueden ser ejercidos por el titular de los datos o su representante legal; son independientes, es decir, que el ejercicio de uno no supone el ejercicio de los otros. El ejercicio de los derechos supone para los encargados del tratamiento o las empresas la obligación de contestar de acuerdo con lo establecido en la ley, y poner a disposición de los usuarios un procedimiento gratuito por escrito. En caso de que los responsables no cumplan adecuadamente con sus obligaciones respecto a los ejercientes de los derechos arco, estos podrán solicitar la tutela de la Agencia Española de Protección de Datos o bien la tutela de las agencias autonómicas (Agencia Vasca de Protección de Datos y Autoridad Catalana de Protección de datos, en los casos en que estas fueran competentes).

Medidas de Seguridad en el tratamiento de datos de carácter personal. Las medidas de seguridad exigibles a los ficheros y tratamientos se dividen, en función de la naturaleza de la información, en tres niveles acumulativos, es decir, a un fichero de nivel alto, le serán aplicados también las medidas de nivel básico y medio.

El nivel básico, aplicable a todos los ficheros o tratamiento de datos personales.

El nivel medio, es aplicado a los siguientes ficheros personales: aquellos relativos a la comisión de infracciones administrativas o penales; aquellos de los que sean responsables Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias; aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros; ficheros de las Entidades Gestoras y Servicios Comunes, de las mutuas de accidentes y enfermedades de la Seguridad Social y se relacionen con el ejercicio de sus competencias; aquellos que contengan un conjunto de datos de carácter personales que ofrezcan un definición de las características o de la personalidad de los ciudadanos y que permitan evaluar aspectos de su personalidad o de su comportamiento; aquellos relativo a solvencia patrimonial y crédito.

El nivel alto, se aplica a los siguientes ficheros o tratamientos de datos personales: aquellos que contengan datos de ideología, religión, creencias, origen racial o étnico, salud o vida sexual; aquellos que contengan datos recabados para fines policiales sin consentimiento de los afectados; aquellos que contengan datos derivados de actos de violencia de género.

Podemos a modo de ejemplo, significar en la LOPD la existencia de medidas de seguridad aplicables a los ficheros y tratamientos automatizados de nivel básico: funciones y obligaciones del personal estarán claramente definidas y documentadas en el documento de seguridad; registro de incidencias, se define como cualquier anomalía que afecte a pudiera afectar a la seguridad de los datos. Habrá que registrar el tipo de incidencia, el momento en el que se ha producido, la persona que realiza la notificación de la incidencia y a quién se la comunica, los efectos que se ha derivado de la misma y las medidas correctoras aplicadas; control de acceso, el personal tendrá acceso autorizado únicamente a los recursos que necesite para el desarrollo de sus funciones, debiendo el responsable del tratamiento establecer los mecanismos necesarios para evitar accesos no permitidos; gestión de soportes y documentos, con datos personales deberán estar identificado e inventariado y sólo accesible para el personal autorizado, su salida deberá ser autorizada por el responsable del fichero o encontrarse autorizada en el documento de seguridad; identificación y autenticación, el responsable del tratamiento deberá establecer una mecanismo que permita la identificación de forma inequívoca y personalizada de los usuarios y su autenticación al intentar acceder a los sistemas de información. Lo más habitual es la asignación de un código o nombre de usuario y una contraseña, esta deberá cambiarse al menos anual.

Medidas de seguridad aplicables a los ficheros de tratamientos no automatizados de nivel básico.

Medidas de seguridad aplicables a los ficheros y tratamientos automatizados y no automatizados de nivel medio. E igualmente existen medidas de seguridad aplicables a los ficheros y tratamientos automatizados y no automatizados de nivel alto.

Otro aspecto importante relacionado con la seguridad de la información es la Auditoría de la seguridad de la información.

El responsable del fichero o tratamiento deberá realizar una auditoría cuando disponga de ficheros o tratamientos a los que se apliquen medidas de seguridad de nivel medio o alto. La auditoría deberá realizarse cada dos años y con carácter extraordinario siempre que se realicen modificaciones sustanciales en el sistema de información que pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

La auditoría deberá dictaminar sobre la adecuación a la normativa vigente de las medidas y controles aplicados a los sistemas de información e instalaciones de tratamiento y almacenamiento, identificando en su caso las deficiencias y proponiendo las medidas correctoras o complementarias necesarias; deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas. La auditoría debe ser llevada a cabo por personal interno, perteneciente al responsable del fichero o tratamiento, o externo, contratado a tal efecto. El responsable de seguridad analizará el informe de auditoría y elevará a las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas. Dicho informe no ha de ser remitido a la AGPD, pero sí debe estar a su disposición.

Con respecto a las medidas de seguridad videovigilancia, las imágenes deben ser consideradas como un dato de carácter personal, siempre y cuando permitan identificar a las personas que aparecen en las mismas. El tratamiento de imágenes puede consistir en la grabación, captación, transmisión, conservación y almacenamiento de las mismas incluidas su reproducción o emisión en tiempo real; ahora bien, si se trata exclusivamente de su reproducción en tiempo real no se genera un fichero, por lo que en estos casos no existirá

obligación de inscribir un fichero ante la Agencia de Protección de Datos, sin bien ello no exime del deber de informar.

Informar sobre la existencia de cámaras, colocar al menos un dispositivo informativo en lugar suficientemente visible en las zonas videovigiladas, tanto en espacios abiertos como cerrados.

Tener a disposición de los interesados impresos en los que se detalle la existencia del fichero o tratamiento, la finalidad de la recogida de los datos los destinatarios de la información, la identidad y dirección del responsable del tratamiento y la posibilidad de ejercer los derechos ARCO.

Las imágenes serán canceladas en el plazo máximo de un mes desde su captación. El responsable del fichero o tratamiento deberá adoptar las medidas de índole técnica y organizativa que garanticen la seguridad de los datos, evitando su alteración, pérdida o acceso no autorizado.Las infracciones pueden ser leves, graves y muy graves.

Las infracciones leves serán sancionadas con multas de 900 a 40.000 euros. Considerándose infracciones leves: no remitir a la AGPD las notificaciones previstas en la LOPD o en sus disposiciones de desarrollo; no solicitar la inscripción de fichero de datos de carácter personal en el Registro General de Protección de Datos (RGPD); el incumplimiento del deber de información al afectado a cerca del tratamiento de sus datos de carácter personal, cuando los datos sean recabados del propio interesado; la transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en la LOPD.

Las infracciones graves, serán sancionadas con multas de 40.001 a 300.000 euros, se consideran infracciones graves entre otras: proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el BOE.

Infracciones muy graves, con multas de 300.001 a 600.000 euros. Se consideran grave entre otras las recogidas de datos en forma engañosa o fraudulenta; tratar o ceder los datos de carácter personal siguientes: ideología, afiliación sindical, religión y creencia, origen racial, a la salud y a la vida sexual como los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, salvo en los supuestos en la que la LOPD lo autorice.

Hemos utilizado definiciones y terminología científico técnica de artículos y capítulo de libros para desarrollar aspectos relacionados con “los procesos y herramientas para la seguridad en redes”, “seguridad de la información” y “valoración de empresas” que han sido publicados bajo una licencia libre por decisión de sus autores. No obstante, los autores consultados, en cada momento en esta tesis, han sido citados en la bibliografía e infografía correspondiente. El conocimiento científico tiene que circular libremente, financiado públicamente, motivo por el cual hemos utilizado alguna documentación en licencia libre. (GNU Free Documentation License).

A nivel internacional, los ataques cibernéticos son unas de las mayores amenazas en 2017. El desarrollo tecnológico trae consigo muchas ventajas, pero también muchas dificultades. La repercusión del desarrollo de las TICs (tecnologías de la información y comunicación) ha transformado la sociedad y la forma en que interactúan las personas, las empresas, las instituciones, de forma que se crean nuevas redes entre ellas, podríamos llamar a esto nuevo contexto, de una manera genérica, ecosistema digital. Igualmente, ha traído consigo importantes riesgos y dificultades. Los ataques cibernéticos han aumentado más que

exponencialmente en todo el mundo y se han convertido en uno de los principales riesgos de este año. Se necesitará implantar una nueva gobernanza y nuevas directivas para para garantizar la seguridad cibernética[22].En base al buen gobierno de las empresas hemos expresado en las hipótesis de partida que un riesgo importante para las empresas hoy es velar por la seguridad de la información. Este asunto debe estar presente, como un tema estratégico de máxima importancia, en los consejos de administración, cuyos miembros deben estar proactivamente preparados para el nuevo paradigma digital. Los informes de Buen Gobierno de las Empresas deben considerar la creación de una Comisión sobre gestión de la información y de los recursos humanos relacionados con esta problemática. Organismos internacionales americanos y europeos están preocupados por esta situación que viven no sólo las empresas sino también las instituciones. De aquí emerge la importancia de la privacidad de los particulares por su relación con las empresas y las instituciones.

Tomando como referencia el informe anterior, la tecnología digital y la "hiperconectividad cibernética" han pasado a ser una funcionalidad clave en los últimos diez años. Las empresas, la interacción social, el compromiso político, las decisiones económicas e incluso la actividad sanitaria están constantemente conectados a Internet y los vínculos entre todos ellos se han incrementado en gran medida. Es decir, la dependencia en la conectividad está aumentando exponencialmente, así como los vínculos entre las personas, las empresas y las instituciones. Esta situación ofrece enormes oportunidades sociales y económicas, pero también origina importantes dificultadesy la necesidad de desarrollar directivas y métodos de gobernanza nuevas, ya que el efecto de la tecnología ha transformado las operaciones de las empresas, las instituciones y la forma en que interactúa la sociedad.

El alza de la dependencia en el ciberespacio y los avances tecnológicos en los últimos diez años han abierto también una puerta a nuevas vulnerabilidades y amenazas que han provocado una preocupación por la seguridad. Tal es el caso de los ataques cibernéticos, que incluyen el espionaje, el crimen cibernético (principalmente), el hacktivismo y la guerra cibernética. En tan solo tres años, las amenazas que presentan los ataques cibernéticos ha aumentado de forma exponencial atacando drásticamente a los negocios en sectores cruciales como la banca, la energía, el transporte, la comunicación, el agua y la sanidad, y ponen en jaque al mundo entero, desde Estados Unidos hasta el Pacífico y el este asiático. Por tanto, los ataques cibernéticos han pasado a ser uno de los principales riesgos globalesconsiderándose entre los riesgos más probables y con mayores consecuencias de los últimos años, según el informe sobre riesgos globales para 2016 del Foro Económico Mundial´[23]

Cobertura mediática de la guerra cibernética, ataques cibernéticos, filtraciones de información y otros problemas informáticos relacionados con la seguridad online en todo el planeta. BBVA research y www.gdelt.or

Estamos inmersos en un nuevo paradigma digital, que conlleva una transformación, hoy se habla de digitalización de la empresa en compañías tan importantes como Banco Santander, BBVA, Inditex, Telefónica y otras del Ibex-35, empresas del Euro Stoxx 50, empresas del Fortune 500, etc.

En base al informe de las Tecnologías de la información emitido por la Fundación Telefónica, España es uno de los países más conectados a las TICs (Tecnologías de la Información y Comunicación), y esto lo podemos ver en el informe número dieciséis de la Fundación de

[22](https://www.bbvaresearch.com/wp-content/uploads/2016/03/Situacion_ED_Mar16.pdf)
[23](http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.)

Telefónica[24] titulado "La sociedad de la información en España", correspondiente al ejercicio 2015, presentado en abril de 2016.

España se posiciona como una sociedad avanzada en el ámbito de dispositivos y utilización de servicios. Según los resultados de un estudio realizado en diversos países en los que opera Telefónica (Reino Unido, Alemania, Argentina y Brasil), España es líder en penetración de dispositivos como el *smartphone*, la tableta, el libro electrónico, o el televisor inteligente. Además, España es el país que tiene un mayor número de internautas avanzados o *early adopters*, con un 16% de los internautas, frente al 14% de Reino Unido o el 11% de Alemania.

Por otro lado, el informe refleja la gran relevancia que los usuarios dan a su privacidad y seguridad en la Red, como muestra el hecho de que el 82,8% de los internautas consideran de gran importancia este tema, y además reclama el poder controlar sus datos. En este sentido, el 85,2% de los internautas reclama el poder identificar y borrar los datos personales, y casi dos de cada tres, el 62,2%, poder mover sus datos entre plataformas si lo desea.

El incesante incremento de la actividad online de los ciudadanos y el uso intensivo de Internet en los procesos de negocio empresariales está provocando una creciente preocupación por la seguridad en la red. Desde fraudes en el comercio electrónico hasta ciberguerras entre países enemigos, la ciberseguridad tiene un campo de acción muy destacado y va a despuntar como uno de los sectores más dinámicos de la economía digital en un corto espacio de tiempo.

También las nuevas tendencias corporativas como el BYOD (*Bring Your Own Device*), la movilidad o la utilización masiva de herramientas en la nube están intentando ser aprovechadas por los ciberdelincuentes para obtener rendimiento económico de las empresas y se presentan como nuevos desafíos para la seguridad online empresarial. Se estima que el coste del ciberdelito a nivel mundial se situó entre los 375.000 y los 575.000 millones de dólares en 2013. Estas cifras suponen que el ciberdelito extrae alrededor del 15-20% del valor generado por Internet. El 38% del coste del ciberdelito se debe a fraudes online, el 24% a las reparaciones necesarias en las infraestructuras para corregir las consecuencias de los ciberataques, el 21% a robos de información o dinerarios y el 17% restante a otras causas. Otras fuentes estiman que los incidentes de seguridad en Internet tendrán un coste de 2,1 billones de dólares en 2019. Estas cifras muestran claramente la magnitud del problema y la necesidad de reforzar la ciberseguridad para el crecimiento sostenible de la economía digital.

En España el 66,4% de los usuarios de Internet ha experimentado algún problema de seguridad online; los más comunes son la recepción de correos electrónicos no solicitados o deseados (85,3% de los usuarios que han experimentado algún problema de seguridad online) y la infección por virus informáticos o códigos maliciosos (31,7% de los usuarios que han sufrido problemas de seguridad online). El 48% de los usuarios también ha sufrido intentos de fraude. Únicamente un porcentaje muy limitado de estos intentos (7,6%) acaban suponiendo un perjuicio económico para la víctima, por lo común con un impacto económico por debajo de los 100 euros.

Tras analizar el impacto económico del cibercrimen es necesario también prestar atención a las oportunidades existentes en el ámbito de la ciberseguridad, ya que se trata de uno de los sectores ligados a la economía digital con mayor proyección. Se estima que en 2014 el gasto mundial en ciberseguridad alcanzó los 72.200 millones de dólares, mientras que en España se

[24](http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina item-publicaciones/itempubli/483/).

invirtieron 150 millones de euros. Otros analistas sitúan el mercado mundial de la ciberseguridad en los 87.000 millones de dólares en 2014.

La previsión de crecimiento para los próximos años de este sector se sitúa en una tasa media anual del 10,3% entre 2014 y 2019, año en el que se espera un mercado de 155.700 millones de dólares. La ciberseguridad no debe ser abordada exclusivamente desde el ámbito tecnológico, ya que también tienen un peso importante el ámbito jurídico y organizativo. Sin embargo, el componente tecnológico es el responsable de la mayor parte del mercado.

En este sentido, las herramientas de gestión de la identidad y control de acceso a los sistemas TI de las organizaciones, las herramientas antimalware y los sistemas de análisis de la actividad en los sistemas TI en tiempo real, que permiten identificar patrones de comportamiento anómalos que podrían indicar un ciberataque, así como las herramientas de continuidad del negocio y recuperación de desastres, son las más utilizadas por las empresas e instituciones.

El ciberdelito no solo tiene repercusiones económicas para los ciudadanos y las empresas, sino que también cuenta con una atención especial desde un punto de vista geoestratégico en la denominada ciberguerra. Por este motivo los Estados invierten cada vez más en mejorar la seguridad online de su información e infraestructuras críticas. Por ejemplo, Estados Unidos destinó en el presupuesto para el año 2015 cerca de 13.000 millones de dólares para mejorar la ciberseguridad en diferentes agencias federales. En Europa, Reino Unido ha desarrollado su Programa Nacional de Ciberseguridad 2011-2016, dotado con 860 millones de libras. Ambos ejemplos muestran como la ciberseguridad se ha convertido en un asunto estratégico en todas las agendas políticas de los gobiernos, dado el gran impacto que está cobrando el aprovechamiento de las redes de comunicaciones para llevar a cabo ataques contra intereses nacionales.

Para que el crecimiento del sector de la ciberseguridad se haga realidad y permita combatir de forma efectiva el ciberdelito es necesario contar con profesionales cualificados. La falta de estos profesionales es una de las principales barreras con las que se encuentra el sector**.** Nada menos que el 86% de los profesionales TIC asociados a ISACA[25] (más de 140.000 en 180 países), consideran que hay una escasez de profesionales cualificados en ciberseguridad. Y según CISCO[26], en 2014 faltaban ya un millón de profesionales de seguridad online en todo el mundo, lo que confirma de forma cuantitativa la percepción cualitativa del problema. Telefónica sigue acelerando en el mundo de la ciberseguridad. La compañía factura en este ámbito en todo el mundo cerca de 400 millones de euros anuales, incluidos los clientes del segmento corporativo y del área residencial.

En este sentido, la operadora espera alcanzar un volumen de negocio solo en el área de empresas de 100 millones de euros en España este año. La teleco ha mantenido crecimientos en el mercado español del 30% en los últimos ejercicios y prevé seguir con este ritmo en 2016.

Los retos en ciberseguridad – desde la escasez de personal cualificado a escala mundial al incremento de amenazas sofisticadas – están afectando actualmente y en gran medida a las empresas y fueron asuntos destacados en la conferencia europea sobre Auditoría, Control y Seguridad en Informática (CACS)[27] / Seguridad de la Información y Gestión de Riesgos (ISRM) que ISACA celebró en Barcelona, en octubre de 2014.

[25] https://m.isaca.org (asociación independiente relacionada con la seguridad de la información).
[26] www.cisco.com>es_es (Cisco en el NASDAQ: CSCO). Es la empresa líder en TI a nivel mundial,
[27] EuroCACS Conference-ISACA- isaca.org, Join US in Munich, Germany 30 May and Enhance Your Knowledge at EuroCACS!

¿Qué está sucediendo en este entorno de internet para que existan tantas ciberamenzas y ciberataques a todos los niveles, a lasgrandes, pequeñas y medianas empresas, administración e incluso la sanidad?

Como hemos visto en los distintos informes anteriores, Internet ha crecido en sofisticación y posibilidades de ingresos: aumento de sitios de comercio electrónico, servicios de pago y banca online, intercambio de información entre empresas, particulares, operadores de telefonía nacionales e internacionales, etc. La información bancaria y de las tarjetas de crédito de miles de millones de personas ha sido potencialmente accesible para aquellos que aprovechan vulnerabilidades.

Mientras que los objetivos de la ciberdelincuencia han crecido de manera exponencial, según el Informe del Ministerio del Interior con datos de 2014, también lo han hecho las habilidades de estos ciberdelincuentes. Las ventajas técnicas han permitido que los cibercriminales puedan actuar más fácilmente y esconder mejor su propia identidad. Para los usuarios de Internet, se están viviendo momentos emocionantes (fibra óptica, internet industrial, Mercado Único Digital), avances online que nos permiten comunicarnos, expresarnos y hacer negocio de forma nueva y distinta a lo conocido hasta entonces pero también ha sido una década de crecientes amenazas que ponen el dinero e identidad en peligro. Phising, Scam, Pharming, ataques de denegación de servicio, son algunos de los ejemplos de las técnicas que utilizan los cibercriminales para realizar fraudes, sabotajes, robo de bases de datos de clientes, etc.

Con este entorno digital, surgen nuevos riesgos a los que las empresas, independientemente de su tamaño, se enfrentan en cada instante. Queremos resaltar aquí que para mitigar el impacto de los ataques vamos a aludir a activos dentro del buen gobierno de las empresas como: el liderazgo, el conocimiento, la gestión de la información, el talento adecuado de los recursos humanos para afrontar estos riesgos, las aplicaciones informáticas de defensa ante ciberamenzas (ya sean propiedad industrial propia o adquirida a terceros), los ciberseguros que nos cubran ante riesgos de ciberataques, el control interno correcto en base a una estrategía correcta de defensa dentro del informe de buen gobierno de las empresas (comisión de ciberseguridad) y una contabilidad adecuada al entorno digital donde se dé información deslindada de las operaciones digitales respecto a las tradicionales. Todo lo anterior implicaría un mayor valor de la empresa en base a los activos intangibles anteriores.

Entendemos que una comisión de ciberseguridad con fuerza propia en colaboración con la comisión de auditoría interna con un diseño de mínimos deseables adecuados al control interno de la organización protegería y evitaría en gran parte los riesgos cibernéticos. Estos mínimos deseables nacerían de los resultados de una encuesta a las personas implicadas en la valoración de las empresas teniendo en cuenta la problemática actual de ciberseguridad.

Sobre las características de la Nueva Economía, tomamos como referencia a la máxima autoridad de la empresa española más internacional y más longeva en laConferencia-coloquio: “dirigir una empresa: una carrera de valores” con el Presidente de Telefónica, Universidad Pablo de Olavide, viernes 30 de enero 2017:

Vivimos en una era de disrupción tecnológica, desde la electromecánica en 1900 a los circuitos integrados en 2010;

El desarrollo social es exponencial:desde la sociedad agraria (4000 A.C. a 1763), el indicador clave era el consumo medio de proteínas per cápita; pasando por la sociedad industrial (1764-1970), el indicador clave era el consumo medio de electricidad per cápita; la sociedad de

internet (1971-2014), el indicador clave penetración de internet; sociedad de los datos después de 2015, el indicador clave es el consumo medio de información per cápita.

El tráfico de datos de móviles es exponencial: 2016, 8,5 Exabytes, 50% vídeo; siendo la previsión del tráfico de datos móviles para 2022 69 exabytes, 75% vídeo.

Información exponencial: en 1995, 200 terabytes; en el año 2000, 800 terabytes; año 2005, 2.400 petabytes; en el año 2010, 20 exabytes, año 2015, 80 exabytes; en el año 2020, se preve 800 exabytes Big Data.

Inteligencia exponencial: capacidad de procesado, algoritmos y sistema cognitivos.

La tecnología se expande cada vez más rápido, indicador "tiempo para llegar a 100 millones de usuarios en el mundo": el teléfono fijo tardó setenta y cinco años; el móvil dieciséis años; internet, siete años; I tunes, seis años y cinco meses; face-book, cuatro años y seis meses; whatsapp, tres años y cuatro meses; Instagram, dos años y cuatro meses; Apple store, dos años y dos meses; Candy Crush Saga, un año y tres meses; Pokémon go; veinticinco días.

Las plataformas digitales tienen un impacto instantáneo y masivo: Facebook, 1800 millones; twitter, 317 millones, equivalente a la población de los Estados Unidos de América; Instagran, 600 millones, equivalente a población de la Unión Europea; Linked in 467 millones.

Mueve a la opinión pública, Power Tools: twitter, Facebook, etc., caso de las recientes elecciones en Estados Unidos. Las elecciones presidenciales francesas el 7 de mayo de 2017 (pirateo de la campaña electoral)[28].

Un Smartphone es más potente que un ordenador de 1957,y, como su propio nombre indica mucho más pequeño; su capacidad de procesado es millones de veces mayor que la de la NASA en 1969; contiene una tecnología de 1991, en una pequeña herramienta llevamos al equivalente de muchas máquinas de entonces.

Un Selfie en el año 1929 era muy complicado hacerlo; hoy, lo podemos hacer con drones a cualquier distancia y con diferentes ángulos. Hasta Hacienda controla las piscinas piratas hechas al margen de la leycon las herramientas como los drones.

En el año 2030: youtube, Skype,Facebook, twitter nos parecerá anticuado.

La vida media de una empresa se reduce: en el año 1955, la vida media era de 61 años; el año 2015, 17 años de vida media.

El 52% de las compañías en S&P e 2000 han desaparecido.

Las fronteras entre el mundo físico y digital se difuminan: Uber, la mayor compañía de taxis del mundo no tiene ningún coche. Como operador cuenta con más coches que taxis en Estados Unidos; Facebook, el mayor dueño de contenidos del mundo no los genera; Alibaba.com, el minorista más valorado del mundo, no tiene inventarios; airbnb, el mayor proveedor de alojamientos no posee ninguna propiedad.

[28] "Un ciberataque contra Macron enrarece las cruciales elecciones de Francia". El País, 17 de mayo de 2017.

La disrupción en la mensajería, mensajes al día en miles de millones: los SMS, tuvieron su máximo hacia 2009, veinte mil millones de mensajes diarios, a partir de ahí descendió; whasapp, en 2015 llegó a cuarenta mil millones de mensajes al día.

Las cuotas de mercados de las compañías de móviles históricamente, unidades vendidas han evolucionado (Nokia, Symbian, Blackberry) e igualmente los sistemas operativos (window, IOS, Android).

En relación con los medios de comunicación, el consumo medio diario en % tiempo desde 2010-2014: las revistas papel han bajado un 19%; la prensa papel ha bajado un 26%; TV ha bajado un 6%; Internet ha subido un 84%.En relación con los ingresos en publicidad expresado en, US$ Miles de Millones, en el año 2000 los ingresos en prensa papel fue de 67 mil millones de dólares y en el 2010 bajó a 16,4 mil millones de dólares. Sin embargo, en Goole en esa misma fecha los ingresos por publicidad fueron 66 mil millones de dólares y facebook 17,9 mil millones de dólares.

Las ventas de vehículos de lujo en EE.UU en 2015:Tesla, Modelo S, subió un 51%; Mercedes Benz S bajó en un 13%; BMW, 7 series, bajo un 5%; BMW, 6 series, bajó un 6%; Audi, A7, bajó un 5%; Lexus, LS, bajó un 16%; Mercedes Benz, CLS, bajó un 12%; Audi, A8, bajó un 15%; Porche, Panamera, bajó un 13%; Jaguar XI, bajo con 17%.

Crecimiento asimétrico de las compañías en capitalización bursátil en miles de millones de dólares: En 2006, Exxon número 1, valor bursátil 446; General Electric número 2, valor bursátil 383; Total número 3, valor 327. En 2016, Appel número 1, valor bursátil 587; Alphabet, número 2, valor bursátil 529.

España lidera la adopción de fibra óptica: en el año 2008, estábamos en lugar 14 en el mundo; en 2009-2011, lugar número 9; en el año 2012, sexto lugar; en el año 2013, en el lugar número 3; a partir del año 2014, el número en cuanto a adopción de fibra óptica. En el caso de Andalucía, Telefónica impulsa la digitalización, invirtiendo más de mil millones de euros en los últimos cinco años, representando un 2,2% del PIB de Andalucía; 95% cobertura 4G, 50% cobertura FTTH[29].

En la nueva economía, se está trabajando en temas como la geolocalización, internet de las cosas, biotecnología y medicina, agricultura, impresión 3D, realidad virtual. The Time, publicó "The Hootest JOBS of the future". El 65% de las profesiones del futuro aún no existen: se necesitan: abogados digitales, economistas digitales, ingenieros digitales, etc.

La importancia del Software, de los intangibles, en la valoración de empresas.En el caso de Telefónica:

La innovación interna en I+D+i suponen 6.600 millones de euros (patentes, innovación en red, innovación en servicios).

Innovación abierta: Talento, más de 700 compañías invertidas, 17 países, 9 fondos, 380 millones de euros de compromiso de inversión más de 1500 start ups. Openfuture.org[30];

[29] Fiber To The Home. También conocida como fibra hasta la casa o fibra hasta el hogar, enmarcada dentro de las tecnologías FTTx (acceso de banda ancha sobre fibra óptica, con distintas modalidades)
[30] Telefonica Open Future (red de emprendimiento, espacio donde encontrar oportunidades para las start up. https://www.openfuture.org

amerigo[31] (navegador de internet, descarga archivos de internet la APP destacada), Crowd-working(espacio creado por Telefónica y diferentes gobiernos regionales (Crowdworking Galicia, Crowdworking El cubo de Andalucía, Crowdworking Extremadura, crowdworking Telefónica Open Future Chile, centro de emprendimiento) cuya misión es convertirse en un centro de conocimiento e innovación participativos y colaborativos, donde se pueda hacer crecer un proyecto o madurar una startup. En estos hubs (centros de actividad), los emprendedores que han sido seleccionados en cada reto, reciben formación y el mentoring necesario para hacer crecer su negocio digital con la ayuda de los expertos del ecosistema de Telefónica Open Future(online.openfuture.org), Wayra, Talentum, Think Big, Amérigo, Telefonica Ventures.

En el caso específico de Andalucía, openfuture, posee más de 450 proyectos presentados, 75 empresas aceleradas, 47% startups facturando. El Cubo en Sevilla, La Farola en Málaga y El Cable en Almería.

Dentro del paradigma de la nueva economía o economía digital, debemos tener en cuenta la ética ante futuros desarrollos de software como: ¿Hijos a la carta?, ¿influir en el comportamiento humano?, ¿Coches autónomos que discriminan tipos de obstáculos?

Para ello necesitamos nuevos valores para este nuevo mundo: planificación de objetivos, un objetivo sin ambición es solo un deseo; sacrificio y esfuerzo, el esfuerzo es el progreso; superar obstáculos, derriba muros y construye retos; fracaso como lección, “la derrota no es mi enemigo. Mi enemigo es el miedo a perder”. Rafa Nadal; ambición y superación, en una carrera contra ti mismo, sólo puede haber un ganador; disciplina y constancia, el éxito es la suma de pequeños esfuerzos repetidos; experiencia, la experiencia es cada kilómetro que superamos y que nos ayuda a alcanzar la meta.

Una vez que hemos pasado por las características fundamentales del nuevo paradigma digital o nueva economía, pasamos a desarrollar aspectos relacionados con la seguridad de la información. Para un mejor seguimiento de esta investigación, sería aconsejable usar el diccionario sobre glosario de seguridad como: (http://www.symantec.com); (http://www.sophos.com).

Terminología sobre ataques y vulnerabilidades:

Ataque informático, bluejacking (es un método de hacking que permite a una persona enviar mensajes anómimos a dispositivo compatibles con Bluetooth dentro de un radio determinado. Se basa en una técnica mediante la cual son enviados mensajes dañinos no deseados, es decir virus entre equipos que se comunican a través de una red Bluetooth, como son los teléfonos móviles, ordenadores portátiles, J Xu, T Zhang, D Lin, Y Mao, X liu (2013));

Ingeniería social (también se aplica al acto de manipulación cara a cara para obtener acceso a los sistemas informáticos, se trata de engañar a otra persona para obtener información de terceros, https://hackstory.net/ingenieria_social, JA Bertolin (2008), H Jara, FG Pacheco (2012), Jl Sánchez, MJ Ignoto (1991));

[31] www.desarrollapp.com

Exploits (es un programa o técnica que aprovecha una vulnerabilidad, dependede los sistemas operativos y sus configuraciones, de las configuraciones de los programas que se están ejecutando en un ordenador y de la LAN[32] donde están, James Newsome, Dawn Song (2005));

Ataque del día cero (es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que por lo general son desconocidas para la gente y fabricante del producto, J Newsome, D Song (2005), JS Guisado, JCT Rendón (2014), RC Naranjo Cuervo (2011), DVR Duque, EG Rogel (2015));

Hacking (normalmente se suele pensar en alguien con profundos conocimientos sobre máquinas que realizan funciones de cómputo, la cultura del hacking está distorsionada por la realidad y se ha ido perdiendo poco a poco la esencia de lo que significa la palabra Hacker, en el ámbito de la informática es una persona apasionada, curiosa, dedicada, libre, comprometida con el aprendizaje y con enormes deseos de mejorar sus habilidades, http://hacking-etico.com, http://www.nebrija.es>Modulo_0, profesor Constantino Malagón, S Harris, A Harper, C Eagle (2005)).

Ataque de denegación de servicio(en internet un ataque pordenegación de servicio, DDoS[33], es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación del servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos, GM Fernández, PG Teodoro (2007)).

Man in the middle (en criptografía, un ataque de intermedio es un ataque en el que se adquiere la capacidad de leer, insertar, modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado, F. Gutiérrez Benítez (2014), V. Delgado y R Palacios (2006), Bejtlich, R. (2005), Rando, E.; Alonso, C. (2012), Troncoso, R.; Ramírez, F.J. (2013), Intypedia, Information Security Encyclopedia).

Ataques de replay (también llamado ataque de playback, en español ataque de reproducción o ataque de reinyección, es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida, Garcia, J. (2014), Naharro, R. (2015)).

Ataques por fuerza bruta (en criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso).

SQL injection (es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos).

Cross-site scripting y cross site request Forgery, Spoofing (es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en la página web visitada por el usuario código JavaScript o en otro lenguaje similar, evitando medidas de control como la Política del mismo origen).

[32] Local Area Network, es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada. Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio. Otras modalidades de redes (MAN, WAN, WLAN, CAN, VLAN, SAN, WPAN).

[33] Distributed Denial of Service (ataque distribuido denegación de servicio). Se ataca al servidor desde muchos ordenadores para que deje de funcionar. Ataque masivo.

Desbordamiento de búfer (es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre el área de memoria reservada a tal efecto, buffer).

Terminología sobre defensas y protecciones: copias de seguridad, parche (conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento, también conocidos como actualizaciones);

Zona desmilitarizada (DMZ o red perimetral es una zona segura que se ubica entre la red interna de una organización y una red externa, internet).

Biometría (es el estudio automático para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos)

Firewall (es una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas);

IPsec[34] (es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet, IP (número que identifica a cada dispositivo dentro de una red), autenticando y cifrando cada paquete IP en el flujo de datos;

IPv6 (protocolo de internet versión 6 para reemplazar al 4 y se está implementando en la gran mayoría de dispositivo que acceden a internet), precauciones recomendables al usar el correo electrónico, red privada virtual o VPN (es una tecnología de red de computadoras que permite una extensión segura en la red de área local, LAN, sobre una red pública o no controlada por internet);

P2P (red de pares, es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes o proveedores fijos, sino una serie de nodos que se comportan como iguales entre sí);

Sistema de detección de intruso o IDS (es un programa de detección de accesos no autorizados a un computador o a una red), sistema de prevención de intruso o IPS es una aplicación que ejerce control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos).

Otra terminología relacionada: gestión de la continuidad, plan de continuidad del negocio;

BS 25999 (se trata de una norma certificable en el que se tiene como objeto la gestión del plan de continuidad del negocio fundamentalmente enfocado a la disponibilidad de la información, uno de los activos más importantes para cualquier organización;

Plan de contingencias (es un instrumento de gestión para el manejo de las tecnologías de la información y de la comunicación), plan de recuperación ante desastres (es un proceso de recuperación que cubre los datos, el hardware y el software crítico para que un negocio pueda comenzar de nuevo sus operaciones en caso de desastre natural o causado por humanos);ISO/IEC 27001;

Actores que amenazan la seguridad:

[34] Internet Protocol Security, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet, autenticando y/o cifrando cada paquete IP en el flujo de datos.

Un hacker es cualquier persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura". Su formación y las habilidades que poseen les convierte en un experto mayor que les permite acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

Un cracker, es aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.

Un lamer (falto de habilidades técnicas, sociabilidad o madurez), es una persona que alardea de pirata informático, cracker o hacker y solo intenta utilizar programas de fácil manejo realizados por auténticos hackers.

Un copyhacker' es una persona dedicada a falsificar y crackearhardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos los bucaneros. Los copyhackers se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.Un "bucanero" es un comerciante que depende exclusivamente de la red para su actividad.

Los "bucaneros" no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.

Un phreaker se caracteriza por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los teléfonos móviles, han tenido que entrar también en el mundo de la informática y del procesamiento de datos.

Un newbie o "novato de red" es un individuo que sin proponérselo tropieza con una página de hacking y descubre que en ella existen áreas de descarga de buenos programas de hackeo, baja todo lo que puede y empieza a trabajar con ellos.

Un script kiddie o skid kiddie, es un simple usuario de Internet, sin conocimientos sobre hackeo o crackeo que, aunque aficionado a estos tema, no los conoce en profundidad limitándose a recopilar información de la red y a buscar programas que luego ejecuta, infectando en algunos casos de virus a sus propios equipos.

Un tonto o descuidado, es un simple usuario de la información, con o sin conocimientos sobre hackeo o crackeo que accidentalmente borra daña o modifica la información, ya sea en un mantenimiento de rutina o supervision.

Las tecnologías referentes a la seguridad de la información e informática son:

Las principales tecnologías referentes a la seguridad de la información en informática son: cortafuegos, administración de cuentas de usuarios, detección y prevención de intrusos,

antivirus, infraestructura de llave publica, capas de Socket Segura (SSL), conexión única "Single Sign on- SSO", biométria, cifrado, cumplimiento de privacidad, acceso remoto, firma digital, intercambio electrónico de Datos "EDI" y Transferencia Electrónica de Fondos "EFT", redes Virtuales Privadas "VPNs", transferencia Electrónica Segura "SET", informática Forense, recuperación de datos, tecnologías de monitoreo.

Estándares de seguridad de la información: ISO/IEC 27000-series, ISO/IEC 27001, ISO/IEC 27002. Otros estándares relacionados: COBIT, ITIL, ISO/IEC 20000 — Tecnología de la información, Gestión del servicio. BSI fue pionera con el desarrollo de la BS 15000 en 2002, norma en la que se basó la ISO 20000

Certificaciones independientes en seguridad de la información: CISA- Certified Information Systems Auditor, ISACA; CISM- Certified Information Security Manager, ISACA; Lead Auditor ISO27001- Lead Auditor ISO 27001, BSI; CISSP - Certified Information Systems Security Professional, ISC2; SECURITY+, COMPTia - Computing Technology Industry Association; CEH - Certified Ethical Hacker; PCI DSS - PCI Data Security Standard.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

La seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación.

## 3.2 OBJETIVOS

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

La información: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

## 3.3 AMENAZAS

No sólo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias no informáticas que deben ser tomadas en cuenta. Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad.

Las amenazas pueden ser causadas por:

Usuarios: causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobredimensionados, no se les han restringido acciones innecesarias, etc.

Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica, un programa espía o *spyware*, en general conocidos como *malware*.

Errores de programación: la mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.

Intrusos: personas que consiguen acceder a los datos o programas a los cuales no están autorizados (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).

Un siniestro (robo, incendio, inundación): una mala manipulación o mala intención derivan en la pérdida del material o de los archivos.

Personal técnico interno: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.

Fallos electrónicos o lógicos de los sistemas informáticos en general.

Catástrofes naturales: rayos, terremotos, inundaciones, rayos cósmicos, etc.

## 3.3.1 INGENIERÍA SOCIAL

Existen diferentes tipos de ataques en Internet como virus, troyanos u otros; dichos ataques pueden ser contrarrestados o eliminados, pero hay un tipo de ataque, que no afecta directamente a los ordenadores, sino a sus usuarios, conocidos como “el eslabón más débil”.

Dicho ataque es capaz de conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos. Además, es un ataque más eficiente, debido a que es más complejo de calcular y prever. Se pueden utilizar infinidad de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

## 3.3.2 TIPOS DE AMENAZAS

Existen infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación. Por ejemplo, un caso de phishing puede llegar a robar la contraseña de un usuario de una red social y con ella realizar una suplantación de la identidad para un posterior acoso, o el robo de la contraseña puede usarse simplemente para cambiar la foto del perfil y dejarlo todo en una broma (sin que deje de ser delito en ambos casos, al menos en países con legislación para el caso, como lo es España).

Amenazas por el origen:

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella y hurtar información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco, aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

Amenazas internas: generalmente estas amenazas pueden ser más serias que las externas, por varias razones como:

Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además, tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite mínimos movimientos.

Los sistemas de prevención de intrusos o IPS[35], y firewalls son mecanismos no efectivos en amenazas internas por no estar, habitualmente, orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

[35] Intrusion Prevention System

Amenazas externas: Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

Amenazas por el efecto

El tipo de amenazas según el efecto que causan a quien recibe los ataques podría clasificarse en:

- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.
- Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.
- Robo de dinero, estafas,...

Amenazas por el medio utilizadoSe pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos: Phishing, Ingeniería social, Denegación de servicio, Spoofing: de DNS[36], de IP, de DHCP[37], etc.

### 3.3.3 EJEMPLOS DE ATAQUES INFORMÁTICOS

Según Valdivia; 2014, los ataques informáticos más usuales son los siguientes:

1) Ataques por repetición: ocurre cuando un pirata informático copia una secuencia de mensajes entre dos usuarios y envía tal secuencia a uno o más usuarios. A menos que esto sea minimizado, el sistema atacado procesa este comportamiento como mensajes legítimos y producen respuestas como pedidos redundantes.

2) Ataques de modificación de bits: se basan en las respuestas predecibles de las estaciones receptoras. El pirata modifica bits de un mensaje para enviar un mensaje cifrado erróneo a la estación receptora, y éste se puede comparar entonces contra la respuesta predecible para obtener la clave a través de múltiples repeticiones.

3) Ataques de denegación de servicio (DOS, Denial of Service): consiste en colapsar total o parcialmente a un servidor para que éste no pueda dar respuesta a los comandos (no para sacar de él información). En la red internet, esto puede lograrse saturando un solo servidor con múltiples solicitudes desde múltiples ordenadores. Como el servidor es incapaz de responder a

[36] Domain Name System, sistema de nombres de dominio. Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como internet o una red privada.
[37] Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host. Es un servidor que usa protocolo de res de tipo cliente/sefvidor en el que generalmente un servidor posee unas listasde direcciones IP dinámicas y las va asignando a los clientes.

todas las solicitudes, colapsa. En las redes inalámbricas, esto se logra también provocando ruido: se coloca un teléfono a 2,4 GHz cerca del punto de acceso e iniciar una llamada. La energía de radiofrecuencia provocada es suficiente para bloquear de manera efectiva gran parte del tráfico de datos en el punto de acceso.

4) Ataques de diccionario: en ciertos modelos de autenticación de datos, para ingresar al sistema la contraseña se mantiene en secreto, mientras que el nombre de usuario es enviado en forma de texto simple y es fácilmente interceptable. En este caso, el pirata informático obtiene distintos nombres de usuarios y con ellos, desde un ordenador, empieza a adivinar las contraseñas con base en palabras de diccionarios en distintos idiomas. Este ataque es exitoso en gran medida porque muchos usuarios utilizan contraseñas poco creativas.

## 3.3.4 AMENAZA INFORMÁTICA DEL FUTURO

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

Se puede afirmar que “la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas”.

Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas”, La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital”.

Obtención de perfiles de los usuarios por medios, en un principio, lícitos: seguimiento de las búsquedas realizadas, históricos de navegación, seguimiento con geoposicionamiento de los móviles, análisis de las imágenes digitales subidas a Internet, etc.

Para no ser presa de esta nueva ola de ataques más sutiles, se recomienda: mantener las soluciones activadas y actualizadas; evitar realizar operaciones comerciales en computadoras de uso público o en redes abiertas; verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.

## 3.4 ANÁLISIS DE RIESGOS

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, tecnología informática, finanzas, etcétera y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

Cada organización tiene una misión. En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben de ser conscientes de que la administración del riesgo informático juega un rol crítico.

La meta principal de la administración del riesgo informático debería ser "proteger a la organización y su habilidad de manejar su misión" no solamente la protección de los elementos informáticos. Además, el proceso no solo debe de ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización.

Es importante recordar que el riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia. Por lo que podemos decir a grandes rasgos que la administración de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable.

El análisis de riesgo informático es un elemento que forma parte del programa de gestión de continuidad de negocio (Business Continuity Management).

En el análisis de riesgo informático es necesario identificar si existen controles que ayudan a minimizar la probabilidad de ocurrencia de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado.

Dentro de la evaluación del riesgo es necesario realizar las siguientes acciones: Calcular el impacto en caso que la amenaza se presente, tanto a nivel de riesgo no controlado como el riesgo controlado y evaluar el riesgo de tal forma que se pueda priorizar, esto se realiza de forma cuantitativa (asignando pesos) ó de forma cualitativa (matriz de riesgos)

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

### 3.4.1 ELEMENTOS DE UN ANÁLISIS DE RIESGO

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo. En este documento se muestran los elementos identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgo es indispensable para lograr

una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización. Existen diferentes tipos de riesgos como el riesgo residual y riesgo total, así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras. La fórmula para determinar el riesgo total es:

RT (Riesgo Total) = Probabilidad x Impacto Promedio

A partir de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el riesgo residual.

Como se describe en el BS ISO/IEC 27001:2005, la evaluación del riesgo incluye las siguientes actividades y acciones: identificación de los activos; identificación de los requisitos legales y de negocio que son relevantes para la identificación de los activos; valoración de los activos identificados, teniendo en cuenta los requisitos legales y de negocio identificados anteriormente, y el impacto de una pérdida de confidencialidad, integridad y disponibilidad; identificación de las amenazas y vulnerabilidades importantes para los activos identificados; evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir; cálculo del riesgo; evaluación de los riesgos frente a una escala de riesgo preestablecidos.

Después de efectuar el análisis debemos determinar las acciones a tomar respecto a los riesgos residuales que se identificaron. Las acciones pueden ser: controlar el riesgo. Fortalecer los controles existentes y/o agregar nuevos controles; eliminar el riesgo (eliminar el activo relacionado y con ello se elimina el riesgo); compartir el riesgo (mediante acuerdos contractuales parte del riesgo se traspasa a un tercero); aceptar el riesgo (se determina que el nivel de exposición es adecuado y por lo tanto se acepta).

No se debe pasar por alto que en las empresas la seguridad comienza por dentro. Capacitando al personal, creando normas basadas en estándares, analizando brechas y puntos ciegos en la seguridad lógica y en la seguridad de sistemas de información.

Es fundamental la creación de escenarios de conflicto de forma continuada participando la gerencia de la empresa junto con un auditor en seguridad.

Los elementos relacionados son los siguientes:

Activo. Es un objeto o recurso de valor empleado en una empresa u organización

Amenaza. Es un evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.

Vulnerabilidad. Es una debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo.

Riesgo. Es un incidente o situación, que ocurre en un sitio concreto, en un intervalo de tiempo determinado, como consecuencia negativas o positivas que pueden afectar el cumplimiento de los objetivos

Análisis. Examinar o descomponer un todo detallando cada uno de los elementos que lo forman a fin de terminar la relación entre sus principios y elementos.

Control. Es un mecanismo de seguridad de prevención y corrección empleado para disminuir las vulnerabilidades

Este proceso administración de riesgo es un proceso continúo dado que es necesario evaluar periódicamente si los riesgos encontrados y si estos tienen una afectación, hay que hacer calculo en las diferentes etapas del riesgo.

Regulación y normas relacionadas con el riesgo.

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

## 3.4.2 ANÁLISIS DE IMPACTO AL NEGOCIO

La economía de la seguridad informática estudia los aspectos económicos de la privacidad y la seguridad en cómputo e información. La economía de seguridad informática busca comprender las decisiones y comportamientos individuales u organizacionales con respecto a la seguridad y la privacidad como decisiones de mercado.

El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver.

Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los valores para el sistema se pueden distinguir: confidencialidad de la información, la integridad (aplicaciones e información) y finalmente la disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor web público puede poseer la característica de confidencialidad baja (ya que toda la información es pública) pero necesita alta disponibilidad e integridad, para poder ser confiable.

## 3.4.3 PUESTA EN MARCHA DE UNA POLÍTICA DE SEGURIDAD

Definiremos primero lo que es un plan de contingencia.Un plan de contingencias es un buen instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el

mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante.

El plan de contingencias sigue el conocido ciclo de vida iterativo PDCA (plan-do-check-act, es decir, planificar-hacer-comprobar-actuar). Nace de un análisis de riesgo donde, entre muchas amenazas, se identifican aquellas que afectan a la continuidad del negocio.

Sobre dicha base se seleccionan las contramedidas más adecuadas entre diferentes alternativas, siendo plasmadas en el plan de contingencias junto con los recursos necesarios para ponerlo en marcha.

El plan debe ser revisado periódicamente. Generalmente, la revisión será consecuencia de un nuevo análisis de riesgo. En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.

Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa del fallo y proponer nuevas contramedidas.

Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos.

El plan de contingencias comprende tres subplanes. Cada plan determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza:

El plan de respaldo. Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

El plan de emergencia. Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es paliar los efectos adversos de la amenaza.

El plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Por otra parte, el plan de contingencias no debe limitarse a estas medidas organizativas. También debe expresar claramente: qué recursos materiales son necesarios; qué personas están implicadas en el cumplimiento del plan; cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan; qué protocolos de actuación deben seguir y cómo son.

Activos e interdependencias: Oficinas centrales → Centro de proceso de datos → Computadoras y almacenamiento → Información de pedidos y facturación → Proceso de negocio de ventas → Imagen corporativa

Este análisis demuestra que una amenaza materializada en las oficinas centrales podría llegar a afectar al proceso de negocio dedicado a la venta. Aunque esto no impida a la compañía seguir comercializando productos, supondría una interrupción temporal de las ventas. Además, afectaría negativamente a la imagen corporativa.

Actualmente, las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Por ejemplo, en España, la Ley Orgánica de

Protección de Datos de carácter personal o también llamada LOPD y su normativa de desarrollo, protege ese tipo de datos estipulando medidas básicas y necesidades que impidan la pérdida de calidad de la información o su robo. También el Esquema Nacional de Seguridad establece medidas tecnológicas para permitir que los sistemas informáticos que prestan servicios a los ciudadanos cumplan con unos requerimientos de seguridad acordes al tipo de disponibilidad de los servicios que se prestan.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene: elaborar reglas y procedimientos para cada servicio de la organización; definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión; sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

### 3.4.4 TÉCNICAS PARA ASEGURAR EL SISTEMA

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a las personas autorizadas para hacerlo.

Cada tipo de ataque y cada sistema requiere de un medio de protección o más (en la mayoría de los casos es una combinación de varios de ellos)

A continuación, se enumeran una serie de medidas que se consideran básicas para asegurar un sistema tipo, si bien para necesidades específicas se requieren medidas extraordinarias y de mayor profundidad:

Utilizar técnicas de desarrollo que cumplan con los criterios de seguridad al uso para todo el software que se implante en los sistemas, partiendo de estándares y de personal suficientemente capacitado y comprometido con la seguridad.

Implantar medidas de seguridad físicas: sistemas anti incendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.

Codificar la información: criptología, criptografía y criptociencia. Esto se debe realizar en todos aquellos trayectos por los que circule la información que se quiere proteger, no solo en

aquellos más vulnerables. Por ejemplo, si los datos de una base muy confidencial se han protegido con dos niveles de cortafuegos, se ha cifrado todo el trayecto entre los clientes y los servidores y entre los propios servidores, se utilizan certificados y sin embargo se dejan sin cifrar las impresiones enviadas a la impresora de red, tendríamos un punto de vulnerabilidad.

Contraseñas difíciles de averiguar que, por ejemplo, no puedan ser deducidas a partir de los datos personales del individuo o por comparación con un diccionario, y que se cambien con la suficiente periodicidad. Las contraseñas, además, deben tener la suficiente complejidad como para que un atacante no pueda deducirla por medio de programas informáticos. El uso de certificados digitales mejora la seguridad frente al simple uso de contraseñas.

Vigilancia de red. Las redes transportan toda la información, por lo que además de ser el medio habitual de acceso de los atacantes, también son un buen lugar para obtener la información sin tener que acceder a las fuentes de la misma. Por la red no solo circula la información de ficheros informáticos como tal, también se transportan por ella: correo electrónico, conversaciones telefónicas, mensajería instantánea, navegación por Internet, lecturas y escrituras a bases de datos, etc. Por todo ello, proteger la red es una de las principales tareas para evitar robo de información. Existen medidas que abarcan desde la seguridad física de los puntos de entrada hasta el control de equipos conectados. En el caso de redes inalámbricas la posibilidad de vulnerar la seguridad es mayor y deben adoptarse medidas adicionales.

Redes perimetrales de seguridad, permiten generar reglas de acceso fuertes entre los usuarios y servidores no públicos y los equipos publicados. De esta forma, las reglas más débiles solo permiten el acceso a ciertos equipos y nunca a los datos, que quedarán tras dos niveles de seguridad.

Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc.

Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Copias de seguridad e, incluso, sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona.

Controlar el acceso a la información por medio de permisos centralizados y mantenidos (tipo Active Directory, LDAP, listas de control de acceso, etc.). Los medios para conseguirlo son:

Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.

Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.

Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro y que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.

Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo, como se ha indicado más arriba, e incluso utilizando programa que ayuden a los usuarios a la gestión de la gran cantidad de contraseñas que tienen gestionar en los entornos actuales, conocidos habitualmente como gestores de identidad.

Redundancia y descentralización.

Candado Inteligente: USB inalámbrico utilizado para brindarle seguridad a la computadora. La misma se bloquea cuando el usuario que tiene este aparato se aleja más de tres metros. El kit contiene un USB inalámbrico y un software para instalar que detecta cuando el usuario está lejos y cuando está más cerca de los tres metros, habilitando nuevamente la computadora.

## 3.4.5 RESPALDO DE INFORMACIÓN

Una "copia de seguridad", "copia de respaldo" o también llamado "backup" (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc.

El proceso de copia de seguridad se complementa con otro conocido como restauración de los datos (en inglés restore), que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como hurtos, incendios, fallas de disco, virus y otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups. Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (solo se copian los ficheros creados o modificados desde la última copia de seguridad). Es vital para las empresas elaborar un plan de copia de seguridad en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

Continuo: el respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.

Seguro: muchos *softwares* de respaldo incluyen cifrado de datos, lo cual debe ser hecho localmente en el equipo antes del envío de la información.

Remoto: los datos deben quedar alojados en dependencias alejadas de la empresa.

Mantenimiento de versiones anteriores de los datos: se debe contar con un sistema que permita la recuperación de, por ejemplo, versiones diarias, semanales y mensuales de los datos.

Hoy en día los sistemas de respaldo de información online, servicio de backup remoto, están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información derivando la necesidad del crecimiento de la copia de respaldo a proveedor del servicio.

## 3.4.6 PROTECCIÓN CONTRA VIRUS

Los virus son uno de los medios más tradicionales de ataque a los sistemas y a la información que sostienen. Para poder evitar su contagio se deben vigilar los equipos y los medios de acceso a ellos, principalmente la red.

### 3.4.6.1 CONTROL DEL SOFTWARE INSTALADO

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Asímismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

### 3.4.6.2 CONTROL DE LA RED

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red solo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

## 3.4.7 PROTECCIÓN FÍSICA DE ACCESO A LAS REDES

Independientemente de las medidas que se adopten para proteger los equipos de una red de área local y el software que reside en ellos, se deben tomar medidas que impidan que usuarios no autorizados puedan acceder. Las medidas habituales dependen del medio físico a proteger.

A continuación, se enumeran algunos de los métodos, sin entrar al tema de la protección de la red frente a ataques o intentos de intrusión desde redes externas, tales como Internet.

### 3.4.7.1 REDES CABLEADAS

Las rosetas de conexión de los edificios deben estar protegidas y vigiladas. Una medida básica es evitar tener puntos de red conectados a los switches. Aun así siempre puede ser sustituido un equipo por otro no autorizado con lo que hacen falta medidas adicionales: norma de acceso 802.1x (es una norma de IEEE para el control de acceso a red basada en puertos. Es una parte del grupo de protocolos IEEE 802), listas de control de acceso por MAC[38] addresses, servidores de DHCP por asignación reservada, etc.

### 3.4.7.2 REDES INALÁMBRICAS

En este caso el control físico se hace más difícil, si bien se pueden tomar medidas de contención de la emisión electromagnética para circunscribirla a aquellos lugares que consideremos apropiados y seguros. Además, se consideran medidas de calidad el uso del cifrado ( WPA[39], WPA v.2[40], uso de certificados digitales, etc.), contraseñas compartidas y, también en este caso, los filtros de direcciones MAC, son varias de las medidas habituales que cuando se aplican conjuntamente aumentan la seguridad de forma considerable frente al uso de un único método.

### 3.4.7.3 SANITIZACIÓN

Proceso lógico y/o físico mediante el cual se elimina información considerada sensible o confidencial de un medio ya sea físico o magnético, sea con el objeto de desclasificarlo, reutilizar el medio o destruir el medio en el cual se encuentra.

## 3.5 ALGUNOS COMENTARIOS O CONSIDERACIONES ACERCA DE LA SEGURIDAD

Dado que los métodos de contagio se realizan por medio de programas automáticos, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto, abrir sistemas y dejarlos sin claves es facilitar la vida a los virus y de posibles atacantes. Otra consideración es que muchos ataques no tienen otro fin que el destruir por destruir sin evaluar la importancia.

¿No abrir los archivos que no conozco es bueno? Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas, si bien la medida es en sí acertada y recomendable.

[38] Lista de Control de Acceso (filtrado MAC). Esta funcionalidad, conocida como dirección MAC filtrado permite al administrador de red para denegar el acceso a cualquier dirección MAC que no esté especialmente permitido en la red. Esto exige que cada nuevo dispositivo de la red tiene su dirección MAC, entró en la base de datos como un dispositivo autorizado. MAC (Media Access Control).
[39] WPA (Wifi Protected Access) es un sistema para proteger las redes inalámbricas Wi-Fi, creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy).
[40] WPA2 (Wi-Fi Protected Acess II).

¿Si tengo antivirus estoy protegido? En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer[41] que hacen que la seguridad del sistema operativo se vea más afectada aún, aunque se considera como una de las medidas preventivas indispensables.

¿Si dispongo de firewall, no existe posibilidad de contagio? Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra técnicas de suplantación de identidad (spoofing). En todo caso, el uso de cortafuegos del equipo y de la red se considera altamente recomendable.

¿Si tengo un servidor web con sistema operativo Unix[42] actualizado hasta este momento, eso es seguridad plena? Puede que esté protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etc.) está desactualizada, un ataque sobre algún *script*[43] de dicha aplicación puede permitir que el atacante abra una shell y por ende ejecutar comandos en el unix. También hay que recordar que un sistema actualizado no está libre de vulnerabilidades, sino que no se tiene ninguna de las descubiertas hasta el momento.

## 3.6 ORGANISMOS OFICIALES DE SEGURIDAD INFORMÁTICA

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el Computer Emergency Response Team Coordination Center del Software Engineering Institute de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

### 3.6.1 En el caso de España

El Instituto Nacional de Ciberseguridad (INCIBE)[44] es un organismo dependiente de Red.es[45]y del Ministerio de Industria, Energía y Turismo de España[46].

### 3.6.2 En el caso de la Unión Europea

La Comisión Europea ha decidido crear el Centro Europeo de Ciberdelincuencia el EC3 abrió efectivamente el 1 de enero de 2013 y será el punto central de la lucha de la UE contra la delincuencia cibernética, contribuyendo a una reacción más rápida a los delitos en línea. Se

[41] Búffer es un espacio de la memoria en un disco o en un instrumento digital reservado para el almacenamiento temporal de información digital.
[42] Unix es un sistema operativo portable, multitarea y multiusuario.
[43] Script es un archivo de órdenes, archivo de procesamiento por lotes. Guión es un programa simple, interactuar con el sistema operativo o con el usuario.
[44] www.incibe.es
[45] www.osi.es
[46] www.certsi.es

prestará apoyo a los Estados miembros y las instituciones de la UE en la construcción de una capacidad operacional y analítico para la investigación, así como la cooperación con los socios internacionales.[47]

### 3.6.3 En el caso de Alemania

El 16 de junio de 2011, el ministro alemán del Interior, inauguró oficialmente el nuevo Centro Nacional de Defensa Cibernética (NCAZ, o Nationales Cyber- Abwehrzentrum) que se encuentra en Bonn. El NCAZ coopera estrechamente con la Oficina Federal para la Seguridad de la Información (Bundesamt für Sicherheit in der Informationstechnik, o BSI); la Oficina Federal de Investigación Criminal (Bundeskriminalamt, BKA); el Servicio Federal de Inteligencia (Bundesnachrichtendienst, o BND); el Servicio de Inteligencia Militar (Amt für den Militärischen Abschirmdienst, o MAD) y otras organizaciones nacionales en Alemania. Según el Ministro la tarea primordial de la nueva organización fundada el 23 de febrero de 2011, es detectar y prevenir los ataques contra la infraestructura nacional.

### 3.6.4 En el caso de los Estados Unidos

El 1 de julio de 2009, el senador Jay Rockefeller (D -WV) introdujo la "Ley de Seguridad Cibernética de 2009 - S. 773 " (texto completo) en el Senado, el proyecto de ley, co - escrito con los senadores Evan Bayh (D- IL), Barbara Mikulski (D -MD), Bill Nelson (D -FL ) y Olympia Snowe (R -ME ), se remitió a la Comisión de Comercio, Ciencia y Transporte , que aprobó una versión revisada del mismo proyecto de ley (el "Ley de ciberseguridad de 2010 ") el 24 de marzo de 2010. el proyecto de ley busca aumentar la colaboración entre el sector público y el sector privado en temas de ciberseguridad, en especial las entidades privadas que poseen las infraestructuras que son fundamentales para los intereses de seguridad nacionales (las comillas cuenta John Brennan, el Asistente del Presidente para la seguridad Nacional y Contraterrorismo : "la seguridad de nuestra nación y la prosperidad económica depende de la seguridad, la estabilidad y la integridad de las comunicaciones y la infraestructura de información que son en gran parte privados que operan a nivel mundial" y habla de la respuesta del país a un "ciber - Katrina".), aumentar la conciencia pública sobre las cuestiones de seguridad cibernética, y fomentar la investigación y la ciberseguridad fondo. Algunos de los puntos más controvertidos del proyecto de ley incluyen el párrafo 315, que otorga al Presidente el derecho a "solicitar la limitación o el cierre del tráfico de Internet hacia y desde el Gobierno Federal comprometido o sistema de información de Estados Unidos o de las infraestructuras críticas de la red". La Electronic Frontier Foundation, una defensa de los derechos digitales sin fines de lucro y la organización legal con sede en los Estados Unidos, que se caracteriza el proyecto de ley como la promoción de un "enfoque potencialmente peligroso que favorece la dramática sobre la respuesta sobria ".

La Union Internacional de Teldecomunicaciones, evalúa el compromiso con la ciberseguridad de las naciones, Global Cybersecurity Index[48].

### 3.6.5 México

[47] http://www.enisa.europa.eu/activities/Resilence-and-CIIP/national-cuber-security-strategies-ncss/national-cyber-security-strategies-in-the-world
[48] http://www.itu.int/en/ITU-D/cybersecurity/Pages/GCI.aspx

La UNAM CERT es un grupo de profesionales que se encargan de evaluar las vulnerabilidades de los sistemas de Información en México[49].Otros documentos relacionados[50].

## 3.7 LOS NUEVOS DELITOS INFORMÁTICOS EN LA REFORMA DEL CÓDIGO PENAL TRAS LA LEY ORGÁNICA 1/2015 DE 30 DE MARZO.

El día uno de julio de 2015 entrabaen vigor en España el nuevo, y también polémico, Código Penal, en virtud de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Se trata de una de las mayores y más duras reformas en materia penal llevadas a cabo en nuestro país. En total, se eliminan 32 artículos de este cuerpo legal mientras que otros 252 artículos son modificados. Como ya se puede suponer, todos estos cambios afectan a aspectos muy diferentes en materia penal, incluidos los llamados delitos informáticos algo que, en la sociedad actual de la información y la comunicación, en la que gran parte de nuestra información más privada y personal se encuentra automatizada y almacena en bases de datos, resulta especialmente relevante.

Así, en el ámbito de las nuevas tecnologías, esta reforma ha agregado al Código Penal el artículo 197 bis relativo al acceso no autorizado a sistemas informáticos:

1. El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Del mismo modo, también se introduce el artículo 197 que castiga con “con una pena de prisión de seis meses a dos años” la producción, adquisición, importación o entrega a terceros de datos de acceso (usuarios y contraseñas) o software desarrollado o adaptado básicamente para cometer cualquiera de los delitos antes citados

El nuevo Código Penal también recoge delitos informáticos relativos a la propiedad intelectual e industrial a través de la nueva redacción del artículo 270 y el uso de expresiones tales como “cualquier tipo de soporte” o “a través de cualquier medio”, no dejando así oportunidad a delinquir respecto a esta materia sea cual sea el medio empleado para ello, aún cuando en el momento de la redacción de este texto no existiese.

Así, dicho artículo en su apartado primero establece una “pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses” a todo aquel que, teniendo la intención de obtener un beneficio económico y perjudicando a otros, “reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación,

[49] http://www.oas.org/cyber/documents/resolution.pdf
[50]http://www.oas.org/cyber/documents/Declaration.pdf

interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios".

Pero aún más interesante resulta el apartado siguiente de este mismo artículo que castiga a quien facilite el acceso a contenidos (links o enlaces de descarga) de cuyos derechos de propiedad intelectual o industrial no es el titular, también con la clara intención de obtener un beneficio económico en perjuicio de tercero:

La misma pena se impondrá a quien (…) facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".

La protección de los derechos de la propiedad intelectual e industrial es un claro y evidente objetivo en el nuevo Código Penal. Prueba de ello es no sólo lo que acabamos de analizar, sino también el artículo 270.6 que castiga con una "pena de prisión de seis meses a tres años" la fabricación, comercialización y uso de cualquier medio especialmente destinado a anular las medidas de protección contra copia que en la actualidad incorporan gran parte de programas de ordenador, cd´s, dvd´s, libros en formato digital, etcétera.

Y, por supuesto, también la fabricación, producción, importación, almacenamiento, ofrecimiento, distribución y comercialización, tanto al por mayor como al por menor, de "productos que incorporen un signo distintivo idéntico o confundiste" al original, serán castigados con penas "de uno a cuatro años de prisión y multa de doce a veinticuatro meses" o de "seis meses a tres años de prisión" respectivamente.

Otros delitos informáticos:

Las muestras de delitos informáticos las encontramos a lo largo de todo el Código Penal ya que este hace referencia al medio utilizado para la comisión de un delito. En este sentido, otros delitos de este tipo que se encuentran regulados son:

La producción, venta, distribución, exhibición, o su facilitamiento, e incluso su posesión, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces (art. 189).

La inducción a la prostitución de menores por cualquier medio (art. 187).

Las amenazas (arts. 169 y siguientes), así como las calumnias e injurias (arts. 205 y siguientes) efectuadas y difundidas a través de cualquier medio de comunicación.

Los fraudes informáticos para cuya consecución se manipulen datos o programas (art. 248).

El sabotaje informático, es decir, la alteración o destrucción de datos, documentos, software que se encuentran almacenados en sistemas o redes informáticas (art. 263).

La posesión de software informático destinado a cometer delitos de falsedad, por ejemplo, falsificar contratos, el DNI, etcétera.

Delito de descubrimiento y revelación de secretos a través del acceso y difusión sin consentimiento de sus respectivos titulares de datos registrados en ficheros o soportes informáticos (arts. 197 a 201)

## 3.8 EL CIBERSEGURO

En este apartado se hace referencia a la historia del ciberseguro, a su negocio, a su cadena de valor. La base de este apartado está en consonancia con el publicado por "Thiber[51]: The cybersecurity Think Tank"del que tomamos algunos apartados para sacar nuestras propias conclusiones. "La transferencia del ciberriesgo en España", patrocinado por AIG, K2Intelligence, Marsh, Minsalt by Indra, Telefónica, Partner Académico: IE Business School.

Aunque es difícil establecer una fecha exacta, las primeras estrategias contemporáneas de transferencia de riesgos tecnológicos vieron la luz en Estados Unidos a mediados de los noventa.

Sin embargo, no fue hasta finales de la década cuando estos seguros comenzaron a comercializarse de una manera más regular al albor de cuatro acontecimientos de especial relevancia:

1.- La llegada del efecto 2000, conocido también como por el numerónimo Y2K, y los potenciales impactos catastróficos que conllevaría el cambio de milenio sobre los sistemas informáticos que sustentaban un entorno empresarial cada vez más dependiente de las tecnologías de la información.

2.- Explosión de las puntocom, empresas que aprovechando la exuberante financiación de los fondos de capital riesgo y una corriente especulativa favorable, explotaron el auge de internet y del comercio electrónico para establecer nuevas formas de negocio digitales. Empresas como Amazon, Yahoo, Ebay, Altavista y Google, se convirtieron en clientes potenciales de estos productos de seguro que pretendían cubrir su negocio ante un panorama de amenazas digitales creciente.

3.- La profesionalización del cibercrimen, pasando de una práctica desarrollada por aficionados a una vertiente criminal susceptible de ser enseñada, aprendida y mejorada. En pocos años se ha producido un importante proceso de profesionalización: actualmente los cibercriminales actúan perfectamente coordinados mediante estructuras jerarquizadas y ejecutando campañas de forma descentralizada en distintos países de forma simultánea.

4.- La promulgación en California el día uno de julio de 2003 de la SB1386 la primera ley a nivel mundial que obligaba a que cualquier agencia estatal, persona o empresa que lleve a efecto negocios en el Estado de California y que pose u opere datos informatizados con información de carácter personal, deberá comunicar cualquier brecha de seguridad que implique una fuga de datos, esta norma sentaba las bases del denominado "Data Breach Notification", es decir, la obligatoriedad de notificar al regulador ciertos incidentes de ciberseguridad asociadas a una fuga de datos digitales.

Este último aspecto es, sin duda alguna, uno delos factores catalizadores decisivos que han supuesto un espaldarazo comercial a la proliferación de las pólizas de ciberriesgos. La SB1386 fue la precursora en Estados Unidos de una oleada legislativa a la que en poco tiempo se sumaron otros cuarenta y cinco estados y que a día de hoy vive un momento muy activo a

[51] www.thiber.org

nivel internacional con el futuro nuevo Reglamento Europeo de Protección de Datos y la Directiva Europea 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Esos primeros productos de transferencia del riesgo tecnológico eran concebidos como productos financieros centrados en cubrir las pérdidas económicas asociadas a un incidente de seguridad. No obstante, dado que estos productos tenían un origen estrechamente vinculado con la normativa relativa a la notificación de fugas de información, sus coberturas eran limitadas y focalizadas en la responsabilidad civil asociada a los gastos de reclamación y responsabilidad ante terceros derivada de un fallo de seguridad de los sistemas informáticos del asegurado HERNÁNDEZ, A.; FOJÓN, E. (2016),

La propia naturaleza del riesgo a asegurar ha actuado, junto a otros factores, como inhibidores a la hora de favorecer el crecimiento masivo de las ciberpólizas.

Entre ellas, tenemos la falta de datos históricos de ciberincidentes, su impacto, provocado por el oscurantismo reinante y la reticencia en el sector empresarial a notificar y compartir datos sobre incidentes y amenazas.

Ello redundó en la imposibilidad de los departamentos actuariales de las aseguradoras de disponer de datos fiables para elaborar los modelos estadísticos y matemáticos necesarios para la evaluación de los ciberriesgos.

Falta de concienciación del nivel de exposición y del impacto asociado a las ciberamenazas entre las empresas como tomadores de seguros. Ello contribuyó a que la demanda de estos productos fuera limitada.

Las entidades interesadas en contratar estas pólizas de seguro debían – y en algunos casos todavía deben hacerlo – someterse a un conjunto de procedimientos de evaluación de su madurez en seguridad informática a menudo invasiva. Ello implicaba revelar el estado de sus infraestructuras tecnológicas y sus políticas o procedimientos de gestión de las tecnologías de la información. Al mismo tiempo al complementar los formularios de contratación aportados por las aseguradoras, se suele subestimar el riesgo por parte del asegurado siendo además respondidos por el área de Tecnologías de la Información y no intervienen las áreas de la empresa que son sensibles a la información como activo.

La naturaleza ubicua del ciberriesgo posibilita que una compañía aseguradora pueda sufrir pérdidas muy elevadas de un gran número de clientes repartidos en diferentes zonas geográficas del mundo como resultado de un mismo incidente. Este efecto, denominado agregación de riesgo, puede provocar que una misma compañía aseguradora o reaseguradora no pueda hacer frente al pago de las reclamaciones resultantes de un evento catastrófico.

De este modo, el mercado de los ciberseguros no logró prosperar a la velocidad esperada en sus etapas iniciales y se mantuvo como un mercado de nicho. Los pronósticos más conservadores en el año 2002 preveían un mercado mundial de ciberseguros de unos 2.500 millones dólares para el año 2005. Sin embargo, el ejercicio prospectivo era demasiado optimista, ya que tan sólo tres años después, en 2008, la previsión del año 2002 seguía siendo cinco veces superior que el tamaño del mercado ese año.

Situación actual:

Fenómenos como el cibercrimen, el Traiga Su Dispositivo Propio (BYOD), el consumo de las tecnologías de la información o la explosión de la economía digital han transformado la vertebración y desarrollo del sector. Hoy en día, el mercado de los ciberseguros es un mercado cada vez más establecido, con un número creciente de proveedores y una cadena de valor cada vez más madura, formado por aseguradoras, reaseguradoras, brokers y empresas de servicios. El aumento de oferta y de la competencia en el sector está, a su vez, reduciendo los precios de las pólizas. Además, existe un buen número de mercados primarios disponibles para colocar los grandes riesgos, y empresas de todos los tamaños están contratando cada vez más este tipo de productos como una compra obligatoria y no como una acción discrecional.

Según datos de Marsh and McLennan y Chertoff Group[52] (2014), el mercado de los ciberseguros generó en Estados Unidos 1.000 millones de dólares en 2013, cantidad que se duplicó en 2014. El mercado europeo de ciberseguros es aún pequeño comparado con Estados Unidos, pero crece también a buen ritmo. En cualquier caso, es indiscutible que los ciberseguros son uno de los productos de más rápido crecimiento en el mercado asegurador. A medio plazo, éste alcanzará los 7.500 millones en ventas anuales en 2020.

En el caso español, este tipo de productos han sido trasladados desde los mercados norteamericano y británico principalmente. En dicha génesis nacional, los productos presentaban coberturas y estructuración similar a sus homólogos extranjeros para, paulatínamente, ir adaptándose a la realidad de las empresas españolas. Las compañías internacionales de seguros, así como los grandes brokers, debido al profundo conocimiento de estos productos, están liderando esta adaptación a las necesidades nacionales. Adicionalmente, la crisis económica en España, ha obligado a muchas empresas a internacionalizarse y a operar en otros mercados para sobrevivir, enfrentándose muchas con la necesidad de adquirir este tipo de seguros a consecuencia de cumplir con las normativas de seguridad exigidas en los mismos.

Hoy en día ya no es una cuestión de si las ciberamenazas pueden o no afectar a una empresa con independencia de su tamaño, sector o ubicación. La pregunta a realizarse es, simplemente, cuándo sucederá y si la organización contará con los mecanismos adecuados para afrontar el incidente.

A finales de la década de 1990 se comenzaron a abordar los problemas de seguridad desdeuna forma metodológica y procedimentada mediante técnicas de análisis de riesgos.

La gestión de riesgos tecnológicos, de seguridad de la información o de ciberseguridad ha servido de marco sobre el cual se ha acomodado la definición de portfolios[53] comerciales de servicios de ciberseguridad. Más concretamente, en el mercado privado de la ciberseguridad nacional es posible hallar la siguiente cadena de valor: Fabricantes de software y hardware, mayoristas y distribuidores actuando como canal de los fabricantes, proveedores locales de servicios especializados, consultoras, integradores de tecnologías de seguridad, proveedores de servicios de seguridad gestionada.

Dichos proveedores han establecido una carta de servicios y de productos que generalmente se suelen clasificar en soluciones o servicios de tipo de detección, prevención y reacción. Así pues, los ciberseguros quedarían incluidos entre los servicios reactivos, orientados a la gestión directa de incidentes de ciberseguridad, cuyo objetivo es mitigar el impacto.

[52] www.mmc.com

[53] Conjunto de inversiones, o combinación de activos financieros que constituyen el patrimono de una persona o entidad.

Pasamos a la definición de ciberpólizas, para poder definir las pólizas de ciberriesgos es necesario acotar de forma previa qué es un ciberriesgo. Éste puede ser definido como el riesgo de pérdida financiera, de interrupción del negocio u otros daños (como el daño por reputación) de una organización que se deriva del uso de sistemas informáticos y redes de comunicación y operación; de la información almacenada y gestionada por los sistemas de dicha organización y de su presencia en medios digitales. Sin embargo, esta definición no abarca la totalidad de riesgos asociados al ciberespacio, puesto que sus efectos pueden ir más allá de las meras pérdidas financieras – como pueden ser daños materiales o lesiones personales – y afectando no sólo a las organizaciones y empresas, sino también a los usuarios.

Generalmente éstos no están cubiertos en los productos aseguradores clásicos de daños o de responsabilidad general, puesto que estos riesgos solían ser tipificados como una exclusión en las pólizas tradicionales. Así pues, de forma general, los ciberseguros o pólizas de ciberriesgos son productos aseguradores cuyo objetivo es proveer protección ante una amplia gama de incidentes derivados de los riesgos en el ciberespacio, el uso de infraestructuras tecnológicas y las actividades desarrolladas en este entorno, siguiendo a Tridib Bandyopadhyay: "Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management – A Modelling Approach", Proceedings of the Southern Association for Information Systems Conference, Atlanta, 2012, pp. 23-29.

Un contrato de seguro ante ciberriesgos vincula y obliga legalmente a una compañía aseguradora ante la ocurrencia de determinados eventos ciber definidos contractualmente que conlleven pérdidas, pagando una cantidad especificada (reclamación/siniestro) al asegurado. En contraprestación, el tomador del seguro paga una suma fija (prima) a la compañía aseguradora.

El contrato es firmado por ésta y el asegurado e incluye aspectos como los tipos de coberturas, límites y sublímites, exclusiones, definiciones y, en algunos casos, cómo se va a proceder a evaluar el nivel de seguridad del asegurado. Los apartados a tener en cuenta serían: Indentificación del asegurador y asegurado; fecha de emisión de la póliza y período de vigencia; descripción del seguro, los riesgos cubiertos y las sumas aseguradas, la designación y el estado de los bienes que son asegurados, la especificación de la prima, forma y el lugar de pago; las causas de la resolución del contrato; el procedimiento para reclamar la indemnización en caso de siniestro; definiciones, exclusiones y triggers[54], condiciones generales, particulares y especiales.

Sobre la base de los puntos anteriores se fijará el valor neto de la prima a pagar. Como cabe imaginar, su valor es altamente dependiente fundamentalmente del valor de los activos bajo amenaza del tipo de negocio, tamaño de la compañía, nivel de exposición digital, volumen de datos digitales a salvaguardar y nivel de seguridad de la organización. La falta de consenso en la definición del producto se pone de manifiesto en la heterogeneidad de denominaciones que adquieren estos productos entre la propia industria aseguradora.

Así aparecen referencias en lengua inglesa a Cyberrisk, Network Risk, Privacy Protection, Network Liability, Security & Privacy Liability, Professional Liability Privacy, Media Liability, Technology & Privacy Professional Liability o Data Privacy & Network Security con sus respectivas traduccionesa nuestro idioma.

[54] Eventos que se asocian con la posible aparición inminente de un riesgo u oportunidad. Ejemplos: riesgs: lluvias por encima del promediodurante la ejecución del proyecto. Disparador (triggers): incremento de la temperatura del mar.

Ello pone de manifiesto la gran diversidad de la oferta, ya que cada asegurador ha desarrollado el producto de seguro bajo la premisa de su comprensión de qué es lo que necesitan las empresas para mitigar los ciberriesgos, lo que implica también muy diversa terminología en cuanto a las garantías y al alcance de los riesgos cubiertos.

En consecuencia, se pueden hallar seguros enfocados a responsabilidad frente a terceros por vulneración de datos personales o violaciones de seguridad, riesgos regulatorios y gastos diversos, y otros que incorporan coberturas de daños propios y que, por lo tanto, dan cobertura a pérdida de beneficios o lucro cesante, robo y otros gastos y pérdidas relacionadas.

No obstante, debe señalarse que el fallo de seguridad no es la única causa de riesgo. Existen otros factores, como puede ser el riesgo de errores humanos, fallos técnicos o de programación, riesgos de difamación o usurpación negligente de propiedad intelectual de terceros o fallo en la cadena de suministro, que pueden ocasionar un perjuicio financiero, interrupción del negocio o un daño de reputación.

Estas coberturas no suelen ser ofrecidas de forma estándar y hay que negociar normalmente de forma expresa su inclusión en el cuadro del seguro. Deliberadamente se han excluido otras causas de riesgo como pueden ser los riesgos naturales o el riesgo de incendio y explosión, que también dan lugar a los mismos perjuicios financieros, de interrupción o de daño reputacional. Este conjunto de riesgos suele estar contemplado en seguros tradicionales, pero el enfoque frente al riesgo de cada organización es muy distinto y no siempre está asegurado. Y también son muy distintas las necesidades de cobertura de las organizaciones.

Bajo estas líneas se analizan las principales coberturas ante ciberriesgos ofrecidas en el mercado, si bien su redacción y las definiciones y exclusiones variarán entre los diversos productos.

Coberturas básicas:

Responsabilidades frente a terceros por privacidad de datos y seguridad de redes: se da cobertura frente areclamaciones de terceros (indemnización ygastos de defensa) por perjucios causados adichos terceros como consecuencia de un falloen la privacidad de datos de carácter personalo información corporativa de terceros,o por un fallo en la seguridad (como porejemplo, transmisión de códigos maliciosos,participación en ataques de denegación deservicios o por un impedimiento de acceso adatos y sistemas como consecuencia de unvirus o intrusión, entre otros).

Procedimientos regulatorios:se da cobertura de gastos de asesoramiento legal frente a un procedimiento administrativo iniciado por un organismo regulador por un incumplimiento de la normativa de protección de datos de carácter personal y eventualmente – siempre que no exista legislación en contra – se abona asimismo la potencial sanción administrativa.

Gastos de gestión de incidentes: siempre que se incurra en estos gastos mediante contratación de servicios externos:

a) Gastos forenses para analizar la causa y alcance del incidente/datos comprometidos y eventualmente terminar la causa del incidente.

b) Gastos de asesoramiento legal para analizar consecuencias legales frente a afectados, reguladores y asesoramiento en actuaciones como notificación, custodia de pruebas, etc.

c) Gastos de comunicación y/o gestión del riesgo por reputación, que incluye tanto el asesoramiento durante la notificación como a la propia la realización de campañas de comunicación.

d) Gastos de servicios prestados a los afectados: comprende gastos tales como la contratación de servicios de atención de llamadas (call centers), gastos de servicios de prevención de fraude y robo de identidad, pagos de primas de seguros en caso de robo de identidad, etc.

Garantías opcionales o complementarias:

Deben estar expresamente indicadas como cubiertas en las condiciones particulares del contrato e implican una prima mayor).

Pérdidas pecuniarias propias:

a) la pérdida de ingresos derivada de una interrupción de sistemas o redes por las causas indicadas en póliza (la cobertura estándar se limita a fallo de seguridad) incluyendo los gastos extraordinarios para mitigar la pérdida de beneficios, los costes de reposición de activos ditigitales (costes de reconstrucción de datos y software)

b) las pérdidas pecuniarias propias por amenazas de extorsión a sistemas (gastos de consultoría, recompensas y eventualmente, rescates).

Responsabilidad Civil de Medios Digitales:da cobertura frente a reclamaciones de terceros (indemnización y gastos de defensa) por perjucios causados por la difusión y publicación de contenidos en los sitios web de la empresa. Estos perjucios pueden ocasionarse por muy diversos motivos, desde invasión de privacidad, calumnia y difamación a terceros hasta la vulneración de propiedad intelectual o marcas cuando se publican contenidos que pueden estar protegidos por derechos de propiedad intelectual de dichos terceros.

Existen otras posibles garantías que pueden contratarse como parte de la cobertura. Es muy común para empresas que gestionan un volumen elevado de pagos por tarjeta de crédito y almacenan dichos datos. En consecuencia, una quiebra de datos o un fallo de seguridad pueden dar lugar a penalizaciones con los medios de pago, cuyo importe puede quedar cubierto bajo la cobertura. También hay aseguradores que otorgan – con sublímites o cantidades limitadas – la pérdida económica del asegurado por transferencia fraudulenta de fondos. En consecuencia, las diferencias entre pólizas son muy diversas. Las principales radican por supuesto, en el alcance de la cobertura que va más allá de la contratación de las garantías opcionales.

Coberturas de un producto típico de ciberriesgos. Fuente AON[55]. A modo de ejemplo podemos citar también la información en el Confidencial (2016) “CaixaBank se blinda con American International Group (AIG), la mejor aseguradora de ciberriesgo con quince años de experiencia, de los hackers con una póliza ciberriesgo ante los ataques masivos. Con tres grandes preocupaciones en la banca: los bajos tipos de interés que erosionan su negocio día a día; la presión de los supervisores para aumentar sus colchones de capital para evitar otra crisis sistémica; ataques cada vez constantes de los hackers a sus servidores, donde guardan los datos de sus millones de clientes. Otro Banco español en manos de AIG es BBVA, Banco de Santander con Zurich Insurance. Para el mismo periódico en noviembre de 2016, el Banco de Santander sufrió un ataque a sus servidores de su filial de tasación inmobiliaria, donde se

[55] www.thiber.org>ciberseguros

guardan las bases de datos con la información hipotecaria de sus clientes. Una documentación vital para la entidad que ahora está en mano de unos hackers.

Responsabilidades y procedimientos regulatorios. Defensa + Perjuicios + Multas regulatorias: Fallo seguridad redes; protección indebida de la información/Revelado no autorizado de información confidencial (datos personales e información corporativa); investigaciones autoridades regulatorias (privacidad/seguridad); cometidos por un proveedor de datos/IT; infracción en contenido multimedia (propiedad intelectual)/contenido difamatorio).

Daños propios Pérdida económica del asegurado. Pérdida de beneficios derivada de la interrupción en redes por fallo de seguridad; extracostes; pérdidas de beneficios derivadas de fallos de sistemas en función del asegurador/negociación; pérdidas de beneficios contingente; daños a activos intangibles; amenazas a sistemas y datos (extorsión).

Servicios de crisis, gastos pagados a expertos. Gastos de gestión de crisis/publicidad; gastos de asesoramiento legal; gastos de investigación forense; gasto de notificación a afectados; gastos de respuesta a afectados (líneas calientes, monitorización de crédito, control de identidad; seguros de robo de identidad); paneles de servicios pre-acordados gestión de siniestros (consultores de IT, asesores legales; asesores de comunicación, consultores de crisis).

Las garantías First Partyde las pólizas varían entre productos: gastos forenses, gastos de publicidad u otros gastos incurridos para minimizar la pérdida del asegurado o de los afectados. Una mera sospecha de una intrusión no autorizada en los sistemas puede activar la cobertura de gastos forenses. Otros gastos, tales como la monitorización de crédito, van a estar ligados seguramente a una reclamación, un proceso regulatorio o tras activar los gastos asociados a los servicios forenses, si la brecha de seguridad es real e implica una fuga de datos.

En cuanto a pérdida de ingresos, la interrupción de los sistemas está vinculado normalmente a fallo de seguridad en sistemas propios, aunque como se ha mencionado, existen coberturas de pérdida de beneficios contingente (por fallo en la cadena de proveedores de servicios tecnológicos, por ejemplo) o por otras causas (como fallo de sistemas y errores humanos). La interrupción o el fallo debe ocurrir durante el periodo de seguro y la cobertura está sometida a un periodo máximo de indemnización (que varía entre 90 y 120 días), a una franquicia medida en horas de parada.

Por otra parte, en relación a la pérdida de beneficios existe la problemática asociada a las dos aproximaciones predominantes: el enfoque americano (calcular la pérdida de beneficios hasta que se reinician las operaciones) y el enfoque de pólizas de londinenses o europeo (hasta el restablecimiento de la producción al nivel normal), así como las dificultades que normalmente encuentran las empresas para separar y cuantificar los factores que inciden en una reducción o aumento de los beneficios esperados que están directamente relacionados con el siniestro.

Pero también hay otras distinciones que son relevantes a la hora de seleccionar un producto frente a otro, como pueden ser la prestación de servicios de consultoría pre-siniestro o los servicios vinculados con la gestión de siniestros. Los servicios pre-siniestro están muy poco extendidos en España. Ello obedece a varios factores, entre los que se hallan la escasa percepción del valor que pueden aportar estos servicios a las empresas de tamaño medio o grande y, quizá también en vista del escaso interés que suscitan estos servicios, la oferta se limita de forma general a unas horas gratuitas de expertos en materia de seguridad tecnológica y algún dispositivo que combina herramientas de información de amenazas con herramientas de información. Estos servicios,sin embargo, pueden ser de gran valor en el sector de pequeña y mediana empresa. De hecho, los pocos productos aseguradores que están

viéndose en el mercado español para este sector presentan una aproximación técnica previa para mitigar el riesgo, además de una asistencia técnica especializada cuando ocurre el siniestro. En cualquier caso, la oferta de esta naturaleza es aún muy modesta y el valor de los servicios ofrecidos, lógicamente, muy ajustado.

Los servicios de gestión de siniestros son más habituales. Los aseguradores que prestan estos servicios ya han negociado con expertos forenses, legales y de comunicación y crisis (pudiéndose extender al establecimiento de servicios adicionales de respuesta a afectados) con proveedores de prestigio y experiencia tarifas exclusivas y los ofrecen como "paneles" dentro de las pólizas. La principal ventaja – siempre que los proveedores respondan en los plazos establecidos – radica en que una empresa que carezca de planes de contingencia o de gestión crisis ante incidentes de esta naturaleza pueda delegar en estos expertos la gestión de la crisis paso a paso.

No obstante, el asegurado continúa manteniendo el derecho de gestionar el siniestro por sí mismo y con sus propios expertos, pero tiene que tener en cuenta que debe solicitar aprobación previa al asegurador – y en teoría antes de incurrir en cualquier gasto – para que el asegurador acepte el reembolso del gasto.

Volviendo al entorno de las pequeñas y medianas empresas, aunque los productos pueden presentar prácticamente las mismas coberturas, su contrapartida radica en que su coste es todavía elevado. Otras pólizas contemplan costes inferiores, pero son más limitadas al cubrir básicamente garantizas responsabilidades frente a terceros por fallo de privacidad (defensa e indemnizaciones) y los gastos se limitan a asistencia forense y reconstrucción de datos.

Exclusiones principales:

Actos deshonestos y fraudulentos y deliberados del asegurado: hay que delimitar claramente cómo afecta esta exclusión a actos de empleados, cuando éstos son asegurados bajo la póliza.

Daños personales y materiales:

Responsabilidades asumidas por contrato o acuerdo: las pólizas de responsabilidad civil asumen principalmente responsabilidad extracontractual y sólo responden si existiera responsabilidad en ausencia de dicho contrato o acuerdo.

Reclamaciones previas y litigios previos e incidentes que hubieran ocurrido y fueran conocidos con anterioridad a la fecha de efecto del contrato.

Infracción de secretos comerciales y patentes:

Guerra y terrorismo, a pesar de que a día de hoy existen coberturas afirmativas o expresas relacionadas con ataques ciberterroristas.

Existe otra exclusión – que puede estar incluida como tal o formar parte de las condiciones generales del contrato y pasar más desapercibida – y es la relativa a datos no declarados o mantenimiento de datos y seguridad por debajo de lo declarado al asegurador durante el proceso de suscripción.

Aunque esta exclusión o condición causa mucha controversia, los asegurados deben tener en cuenta que la información y cuestionarios de riesgo se consideran parte inseparable del contrato, y existen pólizas en las que pueden incluso invalidar la cobertura. En consecuencia,

es necesario analizar esta cláusula, proponer medidas que suavicen dicha exclusión otorgando cobertura, pero, sobre todo, ser conscientes que cualquier cambio en el riesgo debe ser declarado, ya que el asegurador también tiene derechos contractuales de analizar el riesgo durante el ciclo de vida completo de la póliza, proponiendo cambios que se ajusten al estado de riesgo en cada momento.

Para finalizar, merecen una mención independiente los riesgos asociados a las infraestructuras críticas, y,sobre todo, los sistemas de control industrial. Determinadas industrias, como la energética, tienen altamente automatizado la generación y distribución de energía o la producción a través de controladores de lógica programable (PLC), sistemas de control distribuido (DCS) o sistemas de supervisión, control y adquisición de datos (SCADA).

Estos sistemas tienen que interactuar con nuevas soluciones tecnológicas y aplicaciones interconectadas y, en algunos casos, con acceso a Internet. Una incidencia en uno de esos sistemas podría conllevar daños físicos, materiales, adicionalmente a los meramente financieros.

La oferta aseguradora para este tipo de riesgo es muy limitada. Existen productos en el mercado que incorporan coberturas de daños materiales y personales, bien con diferentes condiciones respecto a los seguros tradicionales o bien asegurando la pérdida no cubierta. Sin embargo, ninguno de estos productos puede cubrir la pérdida de ingresos por paralización de actividad: asumiendo que la capacidad máxima del mercado asegurador se estima en 150/200 millones de euros por riesgo, esta cantidad puede ser claramente insuficiente en muchos casos donde se produzca la paralización de una infraestructura crítica con el consiguiente corte de suministro afectando a miles de usuarios.

En definitiva, el problema es doble: por un lado, los asegurados no han realizado aún un análisis de riesgos exhaustivo y les es difícil trasladar la información de forma adecuada al mercado asegurador. Y, por otra parte, esta falta de información, junto a la falta de conocimiento de las amenazas, siniestralidad e impactos por parte de las aseguradoras hace que dicho mercado opte por una posición conservadora, otorgando coberturas de daños materiales y responsabilidad civil, siendo reticente a proponer productos y capacidad.

A quienes van dirigidos:

Hasta ahora el mercado asegurador se había centrado en productos dirigidos a aquellas empresas más expuestas al riesgo cibernético, siendo normalmente grandes corporaciones multinacionales y que, por tanto, necesitan mayores niveles de protección. No obstante, cada vez hay más aseguradoras que dirigen su mirada al sector de la pequeña y mediana empresa y están intentando adaptar su oferta a su realidad y necesidades. La dificultad para asegurados, aseguradores y mediadores radica en la necesidad de adaptar los productos al perfil de riesgo y la cobertura que necesitan, no tanto al tamaño de la compañía.

Una característica diferenciadora que presenta el mercado español es el gran tejido de pequeñas y medianas empresas existente, hecho que las aseguradoras han identificado como una oportunidad de negocio diseñando y adaptando los productos a este sector.

El gran reto para llegar a este mercado es el escepticismo del pequeño empresario, que no encuentra necesario adquirir este tipo de seguros, porque considera que los ciberataques son consustanciales a las grandes empresas.

Sin embargo, las pequeñas y medianas empresas son ahora los objetivos comunes de los ciberdelincuentes, no porque sean lucrativas de forma individual, sino porque la

automatización hace que sea fácil de atacar en masa siendo víctimas fáciles. Así pues, se puede afirmar que:

Las pequeñas y medianas empresas se enfrentan a las mismas ciberamenazas que las grandes empresas, pero con una fracción del presupuesto para hacerlas frente.

La inversión en seguridad es impulsada por la necesidad de cumplir con el marco regulatorio, como Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS)[56], Ley Orgánica de Protección de Datos (LOPD), etc.

Las organizaciones más pequeñas carecen de la experiencia interna para gestionar sus ciberriesgos.

Aunque la seguridad plena no existe, si es posible reducir la exposición al riesgo digital. Y es que todas las empresas, con independencia de su tamaño o sector de actividad, tienen algún componente de riesgo cibernético ya que:

Dado que recopilan, mantienen, ceden o almacenan información privada de carácter personal o confidencial.

Dependen en mayor o menor grado de sistemas informáticos o redes que pueden ser interconectados entre ellos o con otras redes o sistemas de terceros.

Proveen servicios y productos a través de internet y otros medios electrónicos.

Contratan con proveedores de servicios tecnológicos desde, mantenimiento, seguridad, gestión de infraestructuras u otros servicios. O con otros proveedores y contratistas independientes para el almacenamiento o tratamiento de la información.

Pueden estar sujetos a normativa sectorial reguladora de su actividad en cuanto a seguridad de datos o comunicación electrónica que implique mayores medidas de seguridad adicionales y por tanto un mayor riesgo de investigaciones y sanciones a las que establece la LOPD.

Pueden tener obligaciones que cumplir en materia de seguridad frente a la industria de medios de pago.

Los empleados constituyen el eslabón más débil de la cadena de seguridad de la información.

Poseen secretos comerciales en formato digital de los que depende su negocio.

Proporcionan algún servicio o producto a terceros que pueden, en caso de ataques maliciosos, constituir los verdaderos objetivos de criminales y atacantes.

Aunque cada sector empresarial posee sus propios componentes, riesgos y exposición, existen sectores más sensibles que representan un mayor riesgo desde el punto de vista del análisis asegurador, a saber: Instituciones financieras (incluyendo las aseguradoras), sector sanitario, tanto por el tipo de datos que manejan, así como el volumen de los mismos. No obstante, el

[56] El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCIDSS fue desarrollado por un comité conformado por las compañías de tarjetas (crédito y débito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standars Council). Esta validación se hace por auditores autorizados Qualified Security Assessor (QSAs).

sector financiero suele presentar un nivel de madurez de seguridad mayor; Telecomunicaciones y proveedores de servicios tecnológicos, tanto por la información gestionada, así como por los datos de terceros procesados; Sector energético y utilities en general, por el impacto de una potencial pérdida y quizá los que están en clara desventaja desde el punto de vista de medidas de seguridad preventivas en los sistemas industriales.

Necesidades del asegurado:

Las necesidades del asegurado en el ámbito de la ciberseguridad no vienen solo motivadas por el mayor uso de las tecnologías y una mayor conectividad, sino también por las obligaciones legales impuestas por los órganos regulatorios. Es el caso de las obligaciones impuestas a todos aquellos proveedores de servicios de telecomunicaciones o redes electrónicas. Desde la Directiva Marco 2002/21/CE, relativa a un marco regulador común de las redes y de los servicios de comunicaciones electrónicas, en España traspuso a través de la ley 9/2014, ley general de Telecomunicaciones.

Los gestores de riesgos, los responsables de seguridad de la información y en definitiva los directivos de las compañías, afrontan determinadas necesidades en las que los ciberseguros presentan coberturas de especial utilidad y relevancia:

Esta norma exige a los operadores de redes públicas o de servicios de comunicaciones electrónicas a informar a los abonados de todos aquellos riesgos de fuga de datos que puedan existir y de las medidas a adoptar, así como comunicar de eventuales incidente a la AgenciaEspañola de Protección de Datos, al Ministerio de Industria, Energía y Turismo y a los abonados afectados.

El nuevo Reglamento Europeo de Protección de Datos indica también que tan pronto como el responsable del tratamiento de datos tenga conocimiento de que se ha producido una violación de seguridad, debe notificarla a la autoridad de control sin retraso injustificado y, cuando sea posible, en el plazo de 24 horas. Los costes asociados a dichas notificaciones y actuaciones son una de las coberturas básicas ofrecidas en las pólizas.

Adicionalmente, el procesamiento, almacenamiento o transmisión de datos de tarjeta de crédito por parte de las organizaciones obliga al cumplimiento del estándar de seguridad de los datos de tarjeta, PCI-DSS versión 3, entre cuyos requisitos se encuentra la notificación a los titulares de tarjeta en caso de fuga de datos relativos a los mismos.

Los riesgos cibernéticos que pueden cernirse sobre las empresas pueden ser:

De carácter directo, destacando el robo de datos personales, de contraseñas o de *know-how*[57]; la utilización indebida de información privilegiada, el sabotaje a sistemas o programas informáticos de la compañía; abusos en el acceso a correos e internet; accesos no autorizados; redes de equipos infectados remotamente; daños físicos de los equipos; captura de contraseñas; extorsiones; explotación de servidores y navegadores; hurtos y robos de ordenadores o dispositivos móviles6 entre otros.

De carácter indirecto, incluyendo la paralización de la actividad y/o suspensión de la prestación del servicio a terceros, con el consiguiente incumplimiento contractual; pérdida de beneficios (*loss of profit* – LOP); pérdida de mercado o pérdida de confianza en el sector; imposición de sanciones regulatorias; perjuicios causados a terceros; responsabilidad civil, penal o

[57] Conjunto de conocimientos técnicos y administrativos que son imprescindibles para llevar a cabo un proceso comercial y que no estén protegidos por patentes.

administrativa; incremento del coste para resolver o minimizar los daños así como el derivado de tener que asumir el pago de las indemnizaciones que se determinen a favor de los posibles afectados.

Como elemento principal, relacionado con los riesgos indirectos a los que puede enfrentarse un potencial asegurado, destaca la responsabilidad derivada del desarrollo de su actividad en el ciberespacio. Un único incidente de ciberseguridad puede provocar varios tipos de responsabilidad de forma que algunas de sus consecuencias queden cubiertas en las pólizas:

Responsabilidad civil frente a terceros, clientes y/o usuarios:

Responsabilidad laboral frente a los trabajadores de la compañía que se han visto afectados por el ciberincidente.

Responsabilidad penal de la compañía y/o sus administradores o directivos surgida, como consecuencia de la actuación en el ciberespacio de un tercero (ajeno a la compañía o no), o de la propia compañía por actuaciones poco diligentes.

Responsabilidad administrativa que pudiera derivarse frente a organismos regulatorios por el incumplimiento de obligaciones legales tendentes a garantizar un determinado nivel de seguridad.

Responsabilidad contractual en caso de que se produzca la paralización de la actividad y la imposibilidad de prestar servicio a los clientes y usuarios.

Responsabilidad extracontractual en caso de que haya terceros, ajenos a la prestación del servicio, afectados por el ciberincidente. Finalmente, en relación a las medidas a adoptar por los potenciales asegurados, es preciso comentar que, con el objeto de que los proveedores de ciberseguros acepten dar cobertura a las compañías en el ámbito de la ciberseguridad, es imprescindible que los interesados acrediten primero que ejercen un determinado nivel de monitorización, control y supervisión de las herramientas utilizadas para el desarrollo de su actividad (software y hardware) y que implementan y actualizan los procedimientos de control y fomentan una mayor concienciación de los trabajadores de la compañía en el ámbito de la ciberseguridad, así como demostrar un nivel de cumplimiento determinado ante el marco regulatorio y normativo de aplicación en cada caso (LOPD, PCI-DSS, etc).

Por otro lado, y respecto a la obligación de informar a las autoridades de cualquier vulneración de seguridad sufrida, se consolida la tendencia dirigida a que las autoridades incentiven a las compañías eventualmente afectadas, de manera que éstas no teman represalias o la imposición de sanciones elevadas por haber sufrido una vulneración de sus sistemas de seguridad.

Es importante que estén decididas a informar (e informen) a las autoridades sobre cualquier violación de seguridad que sufran. Es conveniente que la colaboración entre el sector privado y público sea continua y transparente, de forma que las compañías favorezcan el intercambio de información sobre incidentes que afronten.

Es conveniente que el asegurado adopte con carácter preventivo y proactivo en el diseño, adopción e implementación de todas esas medidas, antes de suscribir un ciberseguro. De lo contrario, puede encontrarse con que el asegurador o bien no acepte inicialmente suscribirle un seguro específico o bien, una vez suscrito, no otorgue cobertura al incidente en concreto por falta de cumplimentación de lo antes mencionado. El resultado, en cualquiera de los casos,

es que el interesado no habrá transferido los ciberriesgos de manera eficiente, y no verá cubiertas sus necesidades en el ámbito de la ciberseguridad en caso de sufrir un ciberincidente. “El hecho de que se adquiera un seguro, no significa que se pueda ignorar la seguridad tecnológica. Los aspectos tecnológicos, operacionales y del seguro van de la mano”.

Recomendaciones para realizar la contratación:

Las pólizas de ciberriesgos, como cualquier otro producto asegurador, presentan definiciones, coberturas, términos y exclusiones.Entender de forma adecuada los factores limitantes es el primer paso para contratar la póliza que mejor se adecue a las necesidades de cualquier empresa, evitando tanto el sobredimensionamiento como un alcance insuficiente de las mismas. A continuación, se listan los elementos más relevantes a considerar:

Identificar correctamente el alcance necesario de la cobertura a contratar:

a) Sujetos asegurados: la propia persona jurídica y si, fuese necesario – en el caso de un grupo empresarial – sus filiales, asícomo cualquier persona física que sea o haya sido un empleado, Administrador o Directivo, así como cualquier autónomo o persona subcontratada, siempre y cuando trabaje bajo la dirección y supervisión del Tomador. Asimismo, pueden negociarse coberturas específicas para proteger cargos concretos como el responsable de seguridad, el director de cumplimiento normativo o el director de asesoría jurídica.

También es recomendable que la póliza incluya extensión de cobertura al ProveedorExternos de Servicios Informáticos, de manera que, si se produce una brecha de seguridad en sus sistemas afectando al Asegurado, su póliza actúe como si dicha brecha la hubiese sufrido el propio Asegurado.

b) Ámbito temporal: es necesario verificar la que aplica en el contrato. Es habitual que las pólizas otorguen cobertura a incidentes producidos con anterioridad a la entrada en vigor del seguro. Teniendo en cuenta que el tiempo medio de detección de un incidente oscila entre 100 y 200 días es importante negociar una retroactividad ilimitada en las pólizas para amparar hechos descubiertos, o reclamados por primera vez, por un tercero perjudicado, durante la vigencia del contrato, pero sucedidos con anterioridad al mismo. No obstante, es preciso tener en cuenta que todas las pólizas aplican una exclusión específica de hechos conocidos a la fecha de contratación del seguro. Es decir, no podrá asegurarse aquello de lo que ya se tiene conocimiento a la fecha de contratación.

c) Ámbito territorial: en el contexto empresarial es habitual la existencia de serviciosTIC en la nube u otros servicios externalizados ubicados en otros territorios; por lo que es importante acotar el ámbito geográfico de aplicación de la póliza a contratar.

Conocer el negocio, los procesos y sus riesgos. Aunque no es necesario disponer de conocimientos avanzados en la gestión de riesgos de ciberseguridad, es importante entender e identificar el tipo de ciberamenazas asociadas al sector de actividad y a la exposición al mundo digital. Los brokers, las aseguradoras y determinadas empresas de ciberseguridad son actores habilitados para asesorar en la priorización y cuantificación de dichos riesgos.

La selección de los límites de indemnización, franquicias y coberturas más adecuadas debería estar basada en el análisis de posibles escenarios derivados de la identificación de estas amenazas y sus riesgos.

Entender las coberturas contratadas. Es importante comprender qué tipo de coberturas deben contratarse en función del análisis de riesgo comentado en el punto anterior. Del mismo

modo, es recomendable efectuar una auditoría del programa de seguros de la empresa, ya que algunas coberturas ciber podrían estar aseguradas bajo otras pólizas de seguros corporativas contratadas.

Contratar las coberturas en base a las necesidades del negocio. El elenco de coberturas y servicios proporcionados por las pólizas cada vez es mayor, por lo que el análisis de riesgo y el asesoramiento de los *brokers* especialistas en ciberseguros pueden contribuir a contratar las garantías adecuadas para proteger la empresa y, sobre todo, gestionar el evento cuando suceda.

Estructuración del panel de proveedores de servicios. Cada vez son más las pólizas que ofrecen la garantía de Primera Respuesta.

Este servicio permite una actuación urgente para cerrar la brecha cuanto antes y controlar la situación desde el inicio, consiguiendo con ello reducir la pérdida económica derivada del siniestro. Consiste en un panel preaprobado compuesto comúnmente por proveedores expertos en (i) informática forense, (ii) asesoramiento legal especializados en materia de Protección de Datos de Carácter Personal y (iii) especialistas en comunicación, siendo éstos últimos empleados para minimizar el daño ocasionado a la imagen del Asegurado en caso de que tal evento saltase a los medios de comunicación.

Las pólizas que tienen panel preaprobado también suelen admitir la libre designación de expertos por parte del Asegurado, de manera que éste siempre podrá elegir entre un experto establecido en la póliza, o bien, elegir otro que él estime conveniente. Por otro lado, aquellos productos que no incluyen panel preaprobado asumirán los honorarios de aquellos expertos que designe el Asegurado en el momento de producirse el siniestro. Adicionalmente es interesante comprobar en los paneles preabroados si (i) existen tiempos de respuesta establecidos para cada uno de los servicios (ii) existe la opción de elegir más de un proveedor de cada tipo.

Definir de forma adecuada límites y sublímites. Este punto es, con toda probabilidad, uno de los aspectos más delicados e importantes al contratar la póliza. Incluso ahora, los ejercicios prospectivos para tratar de determinar el impacto económico directo e indirecto de un ciberincidente es un ejercicio arduo y complicado. Ello, unido a la falta de datos históricos detallados, hace especialmente relevante la selección de límites, para no caer en un error de percepción *versus* realidad. Ante estas circunstancias, es aconsejable efectuar un análisis de posibles escenarios derivados de la identificación de las amenazas y los riesgos cibernéticos que permitirá plantear varios escenarios de pérdidas económicas ayudando a elegir el límite de indemnización y franquicia a asumir por el Asegurado más adecuado o conveniente.

Adicionalmente, la mayoría de las pólizas de ciberseguros sublimitan algunas coberturas. Es importante analizar estos sublímites para que mantengan una coherencia respecto al límite de indemnización general contratado en la póliza. Sublimitando algunas coberturas (como sanciones administrativas, servicio de control e identidad/monitorización del crédito, etc.), puede quedarse sin límite económico antes de finalizar la gestión total del siniestro en cuestión. Estos aspectos suelen ser negociables y están directamente relacionados con el coste económico de la póliza. Bajo estas líneas se muestran datos referenciales sobre el coste medio por evento o siniestro, así como el coste medio asociado a algunas de las coberturas más habituales.

Atención con las definiciones y las exclusiones. La amplitud del ámbito de cobertura va a depender también del clausulado de la póliza y en especial, de las definiciones y exclusiones empleadas. En este sentido, es importante contar con el asesoramiento de un *bróker* especialista en ciberriesgos que negocie un redactado *ad hoc* o incluya las matizaciones y aclaraciones que sean necesarias, tanto en las definiciones como en las exclusiones, para que el clausulado se ajuste a las necesidades y particularidades del Asegurado.

Definir y comprender los disparadores *(triggers)*. Es preciso entender los sucesos que activarían la cobertura de la póliza de ciberriesgos contratada, es decir, las causas del daño, ya que hay pólizas que sólo se activan ante una brecha de seguridad en los sistemas informáticos, y otras más amplias, admiten también causas de índole técnica como la sobrecarga de la tensión eléctrica, daños al sistema derivados de Incendio o Inundación afectando a los ficheros electrónicos, o eventos como el robo o pérdida de un dispositivo móvil cuando éstos contienen datos de carácter personal.

Igualmente, también debe tenerse en cuenta que algunas pólizas ejecutan la cobertura en la fecha en la que ocurrió el evento *(occurrence)*, mientras que otras se activan en la fecha en la que se recibe una reclamación de terceros contra el Asegurado como consecuencia, por ejemplo, de una fuga de datos *(claims made)*.

Ciberseguros como elemento de mejora de la seguridad:

Las aseguradoras suelen preocuparse por la percepción sobre la seguridad de sus asegurados, ya que éstos tienden a relajar la implantación de controles, sabiendo que el riesgo de pérdida se ha transferido a un tercero. Obviamente, ello redunda en una mayor probabilidad de afección ante una ciberamenaza y, por extensión, en un uso potencialmente mayor de las coberturas de una póliza.

En consecuencia, las aseguradoras juegan un papel clave para mejorar la madurez de ciberseguridad del mercado, ya que pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como condición *sine qua non* para la contratación de las pólizas incluyendo, entre éstas, la adopción demostrada (auditada) de un marco de buenas prácticas de seguridad, ya sea a través de modelos de gestión internacionales como la *ISO 27001* o bien mediante el desarrollo de un modelo de gobierno de seguridad específico desarrollado, por ejemplo, para la industria española.

Pueden ofrecer descuentos en las primas a aquellas entidades que demuestren un nivel adecuado de madurez en seguridad de forma que reduzcan los riesgos de pérdidas a transferir a la aseguradora. A mayor madurez en seguridad, menor número potencial de incidentes y, por lo tanto, menor coste de la póliza.

Las aseguradoras pueden poner en práctica los procedimientos de gestión de ciberincidentes en nombre del asegurado de forma inmediatamente posterior al mismo, mejorando la respuesta coordinada al mismo a través de paneles de coberturas preaprobados. La principal ventaja es que, generalmente, en este tipo de aproximaciones, la aseguradora establece tiempos de respuesta contractuales (a través de acuerdos de nivel de servicio) a los proveedores del panel para que respondan en los plazos establecidos, por lo que una empresa que carezca de planes de contingencia o de gestión crisis pueda delegar en estos expertos la gestión de la crisis paso a paso.

Dado que las aseguradoras necesitan datos fiables para que sus departamentos de suscripción cuantifiquen de manera adecuada las coberturas y las políticas de precios, el crecimiento del

mercado de los ciberseguros podría conducir a una mejor comprensión de los patrones de las amenazas y la mejora de intercambio de información entre el gobierno y las empresas aseguradas respecto a ciberincidentes y coste (impactos) derivados de los mismos.

Las propias aseguradoras desplegarán mecanismos de monitorización del estado de ciberriesgo de los mercados de sus clientes, jugando un papel importante en alerta temprana ante incidentes. Es factible imaginarse, como ya sucede en otras ramas de seguro, como por ejemplo el seguro de automóvil que presenta un coste reducido para aquellos conductores que autoricen la instalación de un GPS en su vehículo, una aproximación en la cual el asegurado autorice la instalación de sondas en sus sistemas informáticos de forma que tanto la aseguradora, como el propio asegurado, disponga de una visión del riesgo informático en tiempo real, combinado con estrategias de monitorización de internet y fuentes abiertas para detectar amenazas externas. De este modo, los precios de las pólizas podrán ser totalmente ajustados a lo largo del ciclo de vida del producto al nivel de riesgo del asegurado.

En definitiva, la adopción de este tipo de productos supone una mejora significativa del nivel de seguridad de las compañías bajo dos ópticas temporales diversas:

A corto plazo para los sujetos asegurados, ya que permite una gestión más efectiva de forma directa (transferencia de riesgo) e indirecta (mejora de los controles preventivos) de los impactos asociados a un ciberincidente.

A medio/largo plazo, para toda la industria, gracias a la visión agregada de los ciberriesgos, otorgando una comprensión detallada e incluso sectorial de las amenazas que atenazan el tejido empresarial español.

El papel de las ciberaseguradoras en España:

El papel clásico de las aseguradoras ha consistido en una labor reactiva, más que proactiva, actuando como depositarias de los fondos que sus clientes destinan a la cobertura de ciertas contingencias consustanciales al desarrollo de su actividad, para el caso de que alguna o todas ellas se materialicen.

La traslación del contenido de la mayoría de la vida comercial y profesional de las sociedades modernas desde el papel al ciberespacio ha cambiado radicalmente este escenario. La mentalidad y el enfoque con el que las aseguradoras deben diseñar y comercializar sus productos en este entorno habrá de tener también un enfoque global, transversal y multidimensional, sin limitarse a la actividad que el asegurado realiza en el ciberespacio, sino contemplando todas las interrelaciones que existen hoy (y serán cada vez más en el futuro inmediato) entre este entorno y dicha actividad.

En suma, nuestro país está asistiendo a un verdadero cambio de paradigma en el sector del seguro, donde se ha convenido que el primer supuesto de ciberseguro, considerado y denominado como tal, datos del año 2006, con la comercialización por una conocida firma multinacional con presencia en España del primer seguro que cubría los ataques de virus y las actividades dañinas piratas informáticos.

Hasta hace escasos años, la práctica totalidad de las aseguradoras en España, tanto nacionales como extranjeras, sólo protegían los equipos informáticos cuando éstos resultaban dañados por un siniestro con efecto primario y directo sobre el hardware (incendio, inundación, etc.), dejando de lado todos aquellos riesgos derivados de o relacionados con el software y/o, sobre todo, con la conexión de los equipos informáticos a Internet.

En muchos ámbitos específicos, como por ejemplo el del transporte marítimo, ha sido costumbre, en la mayoría de los casos, excluir de cobertura cualquier pérdida, daño o responsabilidad y gasto causado o relacionado, directa o indirectamente, con el uso de equipos o programas informáticos.

Algunos de los principales operadores del mercado nacional del seguro han reaccionado, adaptando sus productos durante los últimos años a los riesgos derivados del ciberespacio, abriendo incluso nuevas líneas de negocio, mediante el diseño de pólizas ad hocpara cubrir múltiples ciberriesgos (tanto los derivados de ciberataques, como de la existencia de una arquitectura informática o red obsoleta, o el uso incorrecto de las herramientas informáticas, entre otros).

Este cambio de mentalidad en el mercado de seguro en España es una realidad palpable, pero todavía incipiente, tanto por el lado de las aseguradoras entre quienes las ciberpólizas constituyen hoy un valor añadido y diferencial (y no una commodity como pudiera ser el seguro de daños a terceros), como por el lado de los asegurados, donde aproximadamente el 40% del tejido industrial y empresarial español (y dentro de este porcentaje, sólo las grandes compañías y superficies) se encuentra cubierto, en mayor o menor grado, frente a algún tipo de ciberriesgo.

Lo relativamente reciente del enfoque del seguro cibernético es que éste afecta a un elemento nuclear de la relación aseguradora el histórico de ciberincedentes sobre los que se hacen los cálculos actuariales y estadísticos que han de permitir una tarificación con una sólida base técnica. No existe en España, como es lógico, un track recordo histórico lo suficientemente amplio y variado de ciberriesgos, con el detalle de su periodicidad, alcance e impacto, que permita a los actuarios españoles hacer estimaciones precisas que permitan ajustar las primas de las ciberpólizas, optimizar y rentabilizar sus correlativos procesos de contratación y comercialización.

En esta línea, el mercado del ciberseguro en España debe dar el siguiente paso en su evolución hacia la madurez, mediante la implementación de cinco elementos básicos:

La concienciación del cliente respecto del alcance de su propia exposición a los ciberriesgos.

La gestión integral de todas las fases y sujetos relacionados con este tipo de riesgos y su aseguramiento.

La colaboración entre agentes: Administración Pública y organismos oficiales, empresas del sector asegurador (asociaciones, aseguradoras, brokers, proveedores de servicios) y los asegurados.

La retroalimentación.

El aprendizaje continuo.

Hace falta, pues, una importante labor de concienciación y en ello las aseguradoras pueden jugar un importante papel a través de su ejemplo, publicidad, conferencias, programas de formación y relación de contacto continuo entre la aseguradora y su cliente, superando la tradicional relación basada solo en los hitos de contratación, atención al siniestro (si es que se éste produce eventualmente) y renovación (o en su caso cancelación) de la póliza.

Es también vital que las aseguradoras superen su concepción del ciberseguro como algo centrado en reducir la exposición del asegurado y/o la probabilidad de que ocurra o se

materialicen las ciberamenazas. Se ha de pasar a una gestión integral de todas las fases y sujetos relacionados con este tipo de riesgos y su aseguramiento en una relación pre y post siniestro.

Esencial es, igualmente, que exista una colaboración fluida entre toda la cadena de valor de los ciberseguros, que ayude a superar en este ámbito las reservas que tradicionalmente existen en España (a diferencia de otros países) por parte de los afectados, a reportar con la deseada asiduidad y detalle los siniestros sufridos.

Una mayor fluidez y transparencia en este tipo de comunicación ayudaría a los ya citados actuarios a realizar mejor su trabajo, contribuyendo con ello a la obtención de un mayor experto en materia de ciberseguros y, a la postre, a la maduración del sector. De la mano de lo anterior va la conveniencia y/o necesidad de que exista una retroalimentación entre aseguradoras, asegurados, Administración, instituciones o gobiernos.

En este sentido, los condicionados que comienzan a manejarse en las ciberpólizas de las mayores aseguradoras proveedoras de estos productos prevén específicamente coberturas consistentes en servicios especializados de análisis continuo de la situación real del asegurado, de constatación o auditoría casi continua del nivel de actualización de los sistemas del asegurado, de compartición de *know-how* específico de las aseguradoras con los clientes y de un apoyo y asistencia casi en tiempo real tan pronto se detecta una posible incidencia cibernética.

No es exagerado identificar una tendencia a que los centros de gestión de incidentes o crisis de las aseguradoras actúen casi como una extensión de los departamentos de tecnología de la información de los asegurados, en los supuestos de compañías de cierto tamaño.

Según el Instituto Nacional de la Ciberseguridad (INCIBE), el mercado del ciberseguro en España mueve unos 500 millones de euros anuales, con ritmo de crecimiento anual estimado entorno al 12%. Este crecimiento va parejo al de la frecuencia e impacto de los ciberincidentes. El Instituto de Comercio Exterior (ICEX)[58] apunta que las compañías españolas pueden estar perdiendo más de 13.000 millones de euros anuales como consecuencia de ciberincidentes.

La antes comentada transición, desde el tradicional ámbito de relación entre aseguradora y asegurado (contratación, pago de la prima, pago de potencial siniestro y renovación o cancelación de la póliza), a un nuevo escenario en que la aseguradora se convierte en proveedor de servicios técnicos y de auditoría continua de los sistemas del asegurado, supone, obviamente, una ampliación de las posibilidades de oferta de tales aseguradoras.

Al mismo tiempo, teniendo en cuenta que la propia Administración Pública española posee un nutrido ecosistema de proveedores de tecnología de la información, se recomienda que actúe como eje vertebrador para aumentar el nivel de resiliencia de todos sus proveedores en términos de ciberseguridad y, por extensión, de un alto porcentaje del tejido empresarial nacional. Para ello deberá solicitar como criterio básico obligatorio de contratación para con la Administración el disponer de pólizas de seguro de ciberriesgo con un alcance de coberturas relevante para el servicio prestado y cuya cuantía no sea excesiva en relación con el objeto del contrato. Como ya sucediera con los seguros de responsabilidad civil, esta medida supondría un claro habilitador de estos productos aseguradores en el mercado español a la par que una mejora de control financiero de los ciberriesgos asociados a la cadena de suministro.

[58] ICEX España Exportación e Inversiones. www.icex.es

El Estado puede favorecer el establecimiento de unos criterios comunes de seguridad a través de un marco de controles de seguridad de referencia cuya observancia y cumplimiento por parte de las empresas facilitase al sector asegurador la suscripción de seguros de ciberriesgos. Las administraciones públicas tienen una doble función, como proveedores de servicios críticos a la sociedad y como reguladores del mercado y de la economía. Esta doble responsabilidad les ofrece también la capacidad de fijar los requisitos mínimos que deben cumplir no sólo sus servicios y proveedores TIC; sino también aquellos considerados críticos para la sociedad siguiendo el ejemplo de la Directiva Europea de Servicios de Confianza.

Esta regulación tiene una doble función:

Definir los límites por encima de los cuales deben situarse los planes de seguridad de las empresas.

Ayudar a los responsables de seguridad a conseguir los recursos necesarios para implantar los mecanismos mínimos de seguridad requeridos en la regulación.La acreditación de capacidades de las empresas que optan a ofrecer servicios a la Administración Pública ha sido siempre objeto de polémica, ya que no siempre son uniformes o están armonizados con los de otras administraciones europeas.

Es por esto que la definición de unos criterios de selección basados en normas y buenas prácticas reconocidas internacionalmente incentivaría su aplicación, ya que facilitaría la acreditación de capacidades para optar a la provisión de servicios a cualquier Administración Pública europea.

De hecho, éste es uno de los objetivos de la Comisión Europea para conseguir el mercado único y eliminar las barreras administrativas.

Además, la Administración Española podría mantener un listado de compañías que demostrasen su alineamiento con este marco de control. Mediante la constitución de una lista pública de empresas certificadas, países como el Reino Unido o Australia han dado respuesta a la necesidad de regular un mercado creciente con unas garantías de profesionalidad y calidad.

Estas listas centralizadas actuarían como punto de referencia público en el mercado aportando:

Un impacto positivo comercial y reputaciónentre las empresas.

Un nivel demostrable de seguridad de los procesos y procedimientos y validación de competencias técnicas de las organizaciones miembros.

Orientación, normas y oportunidades para compartir y mejorar los conocimientos.CIONAL

Medio ágil de inserción en el mercado de competencias, servicios y tecnologías de ciberseguridad.

Herramienta útil para las aseguradoras ya que contarían con una validación por parte un agente externo a la propia empresa privada sobre el nivel de madurez de sus controles de seguridad alineados con un marco de control definido.

## 3.9 ACTIVOS DE INFORMACIÓN PARA INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD)

Un activo de información es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser bases de datos con usuarios, contraseñas, números de cuentas, etc., siguiendo a Camilo Angel´s Blog[59]

Siguiendo al mismo autor anterior, sería crítico que a una entidad que maneja alta información confidencial, los intrusos pudieran acceder a ella afectando así la confidencialidad, la disponibilidad y la integridad de dicha información, por eso algunas entidades adoptan un plan de seguridad para los activos de información y así no tener la desgracia de que los datos se fuguen, se modifiquen o se pierdan.

En general, es toda la información que la entidad posee dentro de un activo informático tales como servidores, switch, etc.

Entre los términos y definiciones a tener en cuenta cuando hablamos de los activos de información tenemos: activos de información, seguridad de la información. La ISO 27002:2013 define activo como "*cualquier cosa que tiene valor para la organización*", y recomienda los siguientes tipos de activos de información: Datos o información, software, hardware, servicios, personas, conocimiento.

Para Álvarez[60], C. (2014), un activo de información es aquel elemento que contiene o manipula información, ejemplos: bases de datos, computadoras, servidores. Documentos archivados, correos electrónicos, tasas, contratos, información de empleados, licencias, entre muchas cosas. El dueño del activo de información es aquella persona que responde por la razonabilidad del sistema de información o proceso a su cargo y por ende define quién puede tener acceso a la información. Es quien puede autorizar cualquier modificación a datos que se encuentran en ambiente de producción, previa evaluación y justificación de dicho cambio.

En relación con los tipos de clasificación de la información: Información pública es aquella que puede ser accedida por cualquier persona, incluso por personas o entidades externas a la compañía, con o sin vínculos laborales, comerciales, legales, entre otros (elementos publicitarios, folletos ya publicados, comunicados públicos, horarios de atención de las oficinas, información de carácter pública y que puede ser descargada desde internet y que no hubiese sido procesada por la empresa, información de sociedades matrices); Información uso interno, es aquella que puede ser accedida por cualquier persona de la compañía, con o sin consentimiento del dueño del activo de información (directorios internos de teléfonos, políticas, intranet, metodologías, proyectos y procedimientos de gestión tácticos o estratégicos); Información confidencial es de uso y consumo exclusivo de los empleados de las empresa y de proveedores especiales que hayan firmado un acuerdo de confidencialidad. En algunos casos, por razones legales esta información deberá tener la debida autorización del autor, la divulgación a un tercero debe tener el aval del dueño de proceso o de la alta dirección (datos personales de clientes, transacciones, beneficiarios, datos demográficos, información amparada por reserva bancaria, campaña de mercadeo antes de su lanzamiento, actas de junta directivas y asambleas); Información restringida es aquella que es de uso exclusivo de una persona o un pequeño grupo. Su circulación está restringida y no debe ser compartida con

[59](https://camiloangel.wordpress.com).
[60]https://www.prezi.com),

personas externas al grupo de distribución y su divulgación a un tercero debe tener el aval de la alta dirección (claves caja fuertes, claves de acceso a sistemas de información, información enviada a entes de control, UIAF[61], juzgados, fiscalía);

Para INSTITUTO NACIONAL DE CIBERSEGURIDAD, anteriormente INTECO (2014) https://www.incibe.es), los activos de seguridad de la información. Las organizaciones poseen información que deben proteger frente a riesgos.

Roles frente a los activos de la información:

Propietario/responsable: define el criterio de clasificación de la información, indica qué se puede hacer con el activo, autoriza privilegios y define el ciclo de vida.

Custodio: encargado de resguardar la información, debe seguir las líneas definidas por el dueño de la información para su protección.

Usuario: quién usa la información, responsable de su buena utilización (gerente administrativo, director de riesgos, secretaría general, auditor de cuentas, gerente de operaciones, gerente TICs, etc.).

Cómo vamos a realizar el proceso de clasificación de los activos dentro de la compañía:

Elaborar el inventario de información; identificar qué información generamos en nuestro proceso, de la que somos dueños; identificar qué información usamos, generadas por otras áreas; identificar cuál es el uso que le dan otras áreas a la información que generamos en nuestro proceso; definir la clasificación de cada activo de información; definir el mecanismo de protección de acuerdo a la clasificación; mantener actualizado el inventario de activos de información.

Entre las preguntas que nos ayudan a elaborar el inventario de activos de información están:

¿Qué tipo de activo es? (información, software, hardware, servicios); usuarios (quienes deben tener derecho de acceso); ¿La información está en medio físico o electrónico?; ¿Es activo de información de terceros o de clientes?, ¿Qué debe protegerse?; ¿El activo de información debe ser restringido a un número limitado de empleados?; ¿El activo de información debe ser restringido a personas externas?; ¿El activo de información puede ser alterado o comprometido para fraudes o corrupción?; ¿Es crítico para las operaciones interna?; ¿Es crítico para el servicio hacia terceros o clientes?; ¿Ha sido declarado público/confidencial por parte del dueño?; ¿Ha sido declarado público o confidencial por alguna autoridad?; ¿Ha sido declarado público o confidencial por alguna norma jurídica?; ¿Se tiene autorización para suministro a terceros?

Elaborar un inventario de activos de información y su clasificación es fundamental desde el punto de vista de la responsabilidad de la empresa y sus consecuencias en las cuentas anuales y en el informe anual, de igual manera para el informe de buen gobierno, responsabilidad social corporativa; memoria de reputación, en el informe de gestión, en el informe de auditoría. La seguridad de los activos de información es fundamental y está relacionado con el objeto social, cadena de valor, estrategia empresarial, activo intangible, capital intelectual. Al mismo tiempo el inmovilizado intangible está relacionado con las ventas en el análisis de los

[61] Unidad de Información y Análisis financiero, unidad que tiene como objetivo esclarecer como oentra el dinero procedente de los sobornos.

estados financieros, rentabilidad económica y financiera vinculada al inmovilizado intangible. La importancia del principio de empresa en funcionamiento.

En base a la ISO 27001, los activos son los recursos del Sistema de Seguridad de la información, necesario para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección. Los activos se encuentran relacionados, directa o indirectamente, con las demás entidades.

Características de los activos:

Cada activo tiene sus características, que difieren en el estado, en materia de seguridad, en los niveles de los subestados, confidencialidad, integridad y disponibilidad. Vamos a definir los diferentes subestados que nos podemos encontrar:

Subestado A (Autenticación): tiene la característica de ofrecer y reconocer la autenticidad de los activos de información e identificar los actores o la autorización necesaria ofrecida por parte de las personas con poder, además de verificar las tres cuestiones anteriores.

Subestado C (Confidencialidad): presenta la característica de prevenir la divulgación o no autorizada de los activos de información, a menos se relaciona con la intimidad cuando esta información se refiere a personas físicas, es decir, la Ley Orgánica de Protección de Datos, de carácter personal.

Subestado I (Integridad): tiene la característica que proteger sobre la modificación o destrucción no autorizada de activos del dominio, lo que vincula la fiabilidad de los Sistemas de Seguridad de la Información ISO 27001 y se refiere a los activos de tipo información, por ejemplo, problemas de integridad por culpa de virus alojados en los datos almacenados en un PC.

Subestado D (Disponibilidad): protege contra la negación de acceso no autorizado a los activos y se encuentra asociado con la fiabilidad técnica de los componentes del Sistema de Información.

Tipos de activos:

podemos considerar cinco grandes tipos de activos de información, que son:

El entorno del Sistema de Seguridad de la Información basado en ISO 27001, que comprende a los activos y que se precisan para garantizar los siguientes niveles.

El sistema de información en sí.

La misma información generada por la aplicación del Sistema de Seguridad de la Información.

Las funcionalidades de la organización, en las que se justifican las exigencias de los Sistemas de Información anteriores y les generan la finalidad deseada.

Otros activos, ya que el tratamiento realizado a los activos es un método de evaluación de riesgos que tienen que permitir la inclusión de cualquier otro activo, sea cual sea su naturaleza.

Estos cinco tipos de activos implican la tipificación según la naturaleza intrínseca. Durante los tres primeros tipos se constituye el dominio estricto de todo proyecto de Seguridad de Sistema de Información ISO 27001, los otros dos son extrínsecos del Sistema de Información propiamente dicho, aunque no están exentos de consecuencias desde el punto de vista de seguridad. El proyecto de seguridad articula los cinco tipos como diferentes capas. Los fallos que se producen en los activos del entorno son:

Provocar fallos en los Sistemas de Información

Provocar fallos en la información

Soportar funcionalidades de la organización

Condicionantes de otros activos

Atributos de un activo

Cada activo o grupo de activos conlleva diferentes tipos de indicadores de valoración que ofrecen una orientación con lo que poder calibrar el impacto que materializa la amenaza que puede provocar.

Valorar intrínsecamente el activo considerado, ya que tiene dos aspectos diferenciados:

Un atributo cuantitativo, es decir, el valor del cambio que se puede emplear en ciertos tipos de activo y su utilidad.

Un atributo cualitativo, es decir, soporta la clasificación de los tipos de activos por su naturaleza.

Se valora de forma específica el estado en el que se encuentra la seguridad del activo de información que sea considerado, es por esto que se puede concretar la cuatro subestado mencionado anteriormente, A-C-I-D: Autentificar, Confidencial, Integridad y Disponibilidad.

Métrica de los activos de seguridad:

Las personas responsables de proteger los activos tienen que identificar, definir y valorar todos sus activos. Las métricas de valoración intrínseca se apoyan en:

Los activos que se encuentran inventariados tienen una parte en activos relacionados con el entorno y otra parte con los sistemas de información, que seguirán las clasificaciones de estos inventarios.

Otros activos que pueden estar o no inventariados, suelen estarlo con las aplicaciones existentes que cubren la obtención de información.

Muchos otros activos no pueden ser inventariados en el sentido contable del término. Por eso no deja de tener un valor de uso para la empresa, lo que se suele apreciar de forma cualitativa por su carencia.

Llevar a cabo las métricas de valoración del estado de seguridad del activo que se tiene en cuenta permite estimar los valores de los cuatro subestados, mencionados anteriormente, A-C-I-D (autenticación, confidencialidad, integridad y disponibilidad).

Clasificación de los activos de seguridad de la información:

Según INTECO (Instituto Nacional de Tecnologías de la Comunicación), los activos de seguridad de la información nacen como consecuencia de que las organizaciones poseen información que deben proteger a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio (el término seguridad de la información está muy relacionado con el objeto social y con el principio contable de empresa en funcionamiento). Este tipo de información es imprescindible para las empresas, es lo que denominamos Activo de Seguridad de la Información.

Su protección es el objeto de todo sistema de seguridad de la información.

Los activos de seguridad de la información se clasifican siguiendo la metodología de Magerit en Eterovic, E. (2011).

1.- El proceso de negocio de la organización, los servicios que ofrece con carácter externo y con carácter interno como es el caso de la elaboración, gestión de la nómina de los empleados.

2.- Datos e información que se manipula dentro de la organización, suele ser el núcleo del sistema, mientras que el resto de los activos suelen darle soporte de almacenamiento.

3.- Aplicaciones de software.

4.- Equipos informáticos.

5.- Personal es el activo principal, incluye personal interno, subcontratado, de los clientes, etc.

6.- Redes de comunicaciones que dan soporte a la organización para el movimiento de la información. Pueden ser redes propias o subcontratadas a terceros.

7.- Los soportes informáticos que permiten el almacenamiento de la información durante un largo período de tiempo.

8.- Equipamiento auxiliar que da soporte a los sistemas de información y que son activos que no se han incluido en ningún otro grupo, como por ejemplo equipos de destrucción de documentación o climatización.

9.- Instalaciones.

10.- Intangibles.

Para proteger los activos de información es necesario conocerlos, identificarlos dentro de la organización. Para ello se debe elaborar un inventario que los identifique y clasifique. Cada activo del inventario debe incluir al menos: su descripción, su localización y propiedad.

El propietario del activo debe ser quien define el grado de seguridad que requiere o debe ser el usuario. El propietario no tiene necesariamente que ser quien va a gestionar el activo o ser usuario. Por ejemplo, las bases de datos de clientes pueden pertenecer al Director Comercial de una empresa, su gestión puede estar encargada al área de sistemas y sus usuarios pueden ser los comerciales.

## 3.10 LAS FUNCIONES DE LA COMISIÓN DE AUDITORÍA INTERNA EN EL NUEVO CÓDIGO DE BUEN GOBIERNO EN ESPAÑA. LA PROBLEMÁTICA DE CIBERAMENAZAS Y VULNERABILIDADES.

Según Borja Guinea[62] (2015), resulta cada vez más evidente que aplicar buenas prácticas de gobierno corporativo aporta valor a largo plazo a las empresas, con beneficios en competitividad, transparencia y reputación. Los cambios recientes en el marco de gobierno corporativo se han completado con la aprobación por parte de la CNMV del nuevo Código de Buen Gobierno Corporativo, con el objetivo de mejorar la eficacia, transparencia y responsabilidad en la gestión de las sociedades cotizadas.

Uno de los pilares de estos cambios –primero en la Ley de Sociedades de Capital y ahora del propio Código- reside en la adecuada supervisión y control de la empresa, tarea que el consejo de administración delega en la denominada comisión de auditoría y cuya función resulta clave para los accionistas, inversores, y otros grupos de interés. Entre las competencias mínimas de la comisión de auditoría se incluyen supervisar la eficacia del control interno de la sociedad; los sistemas de gestión de riesgos, incluidos los de ciberseguridad; fiscales; el proceso de elaboración y presentación de la información financiera; la labor de la auditoría interna, así como establecer las relaciones oportunas con el auditor externo y la discusión de las debilidades de control interno significativas.

Ahora el nuevo Código va más allá de los requisitos legales e incluye recomendaciones dirigidas a ampliar las competencias de la comisión de auditoría, establecer criterios adicionales sobre su composición, reforzar la función de auditoría interna y crear una unidad de control y gestión de riesgos.

Además, recomienda que esta comisión de auditoría o, en su caso, otra especializada supervise el cumplimiento de las reglas de gobierno corporativo, de los códigos internos de conducta y de la política de responsabilidad social corporativa. También se aconseja que la comisión de auditoría elabore una serie de informes como el de independencia del auditor, el de funcionamiento de la propia comisión, el de operaciones vinculadas o el de aplicación de la política de responsabilidad social corporativa y que se deben publicar en la página web corporativa al tiempo de la convocatoria de la junta general ordinaria. Junto a este mayor protagonismo de la comisión, la CNMV recomienda que todos los miembros de esta comisión, y especialmente su presidente, se designen teniendo en cuenta sus conocimientos y experiencia en contabilidad, auditoría o gestión de riesgos, y que la mayoría sean consejeros independientes.

Esta recomendación supone un paso más a la norma fijada por la Ley de Sociedades de Capital de que esté compuesta exclusivamente por consejeros no ejecutivos, dos de los cuales como mínimo deban ser independientes y uno de ellos con conocimientos y experiencia en contabilidad o auditoría.

Otro aspecto relevante del nuevo marco es que han asumido que el control y gestión de riesgos en las empresas es un aspecto determinante para el mercado. De hecho, se ha elevado a rango legal que entre las facultades indelegables del consejo de administración se encuentre la aprobación de una política de control y gestión de riesgos, y el que la comisión de auditoría debe supervisar la auditoría interna, eliminando la coletilla “si existe”, por lo que las sociedades deben disponer de esta unidad en su estructura.

[62] https://assets.kpmg.com/content/dam/kpmg/pdf/2015/06/El-nuevo-gobierno-corporativo-2015.pdf

En este sentido, el nuevo Código aconseja que, bajo la supervisión de la comisión de auditoría, se disponga de una función de auditoría interna que vele por el buen funcionamiento de los sistemas de información y control interno y que funcionalmente dependa del presidente no ejecutivo del consejo o del de la comisión de auditoría. El responsable de la unidad deberá presentar su plan anual de trabajo y un informe anual de actividades, así como informarla directamente de las incidencias detectadas. Además, se avanza otro paso al recomendar que las sociedades cotizadas cuenten con una unidad de control y gestión de riesgos, esencial en un mundo tan interdependiente y complejo, con mención a las funciones que debe tener atribuidas. En definitiva, cambios relevantes que exigen a las comisiones de auditoría seguir avanzando en el objetivo de guiar a las empresas a las máximas cotas de transparencia y confianza.

Para desarrollar este apartado tomamos como referencia el nuevo Código de Buen Gobierno aprobado recientemente y también el reglamento de la comisión de tecnología y ciberseguridad en el Informe Anual de BBVA[63], publicado en 2016.

La Comisión de Tecnología y Ciberseguridad tiene como objeto asistir al Consejo en: la comprensión y conocimiento de los riesgos asociados a la tecnología y los sistemas de la información relacionados con la actividad del Grupo y la supervisión de su gestión y control, en especial en lo relativo a la estrategia de ciberseguridad; el conocimiento y supervisión de las infraestructuras y estrategia tecnológica del Grupo y de cómo ésta se integra en el desarrollo de su estrategia general; asegurarse que la Entidad tiene definidos los planes y políticas, y cuenta con los medios adecuados, para la gestión de las anteriores materias; así como en todas aquellas otras cuestiones y responsabilidades que le puedan ser atribuidas por el Consejo en cada momento en este ámbito.

Asimismo, la Comisión podrá contar con los asesoramientos externos que fueren necesarios para formar criterio sobre las cuestiones de su competencia, lo que se cursará a través de la Secretaría del Consejo.

En lo demás, su régimen de convocatoria, quórum de constitución, adopción de acuerdos, actas y demás extremos de su régimen de funcionamiento, se estará a lo dispuesto en el Reglamento del Consejo de Administración para este órgano, en lo que resulte aplicable.

Dentro del objeto establecido en el apartado correspondiente de este Reglamento, la Comisión de Tecnología y Ciberseguridad ejercerá las siguientes funciones:

Supervisión del riesgo tecnológico y gestión de la ciberseguridad

Revisar las exposiciones a los principales riesgos tecnológicos del Banco, incluidos los riesgos sobre seguridad de la información y ciberseguridad, así como los procedimientos adoptados por el área ejecutiva para el seguimiento y control de estas exposiciones.

Revisar las políticas y sistemas de evaluación, control y gestión de los riesgos e infraestructuras tecnológicas del Grupo, incluyendo los planes de respuesta y recuperación frente a ciberataques.

Ser informada sobre los planes de continuidad del negocio en lo que respecta a cuestiones de tecnología e infraestructuras tecnológicas.

[63]https://accionistaseinversores.bbva.com/TLBB/fbinir/mult/Reglamento_Comision_IT_tcm926-592287.pdf´

Ser informada, según corresponda, sobre: los riesgos de cumplimiento asociados a las tecnologías de la información; los procedimientos establecidos para identificar, valorar, supervisar, gestionar y mitigar estos riesgos.

Asimismo, la Comisión será informada de los eventos relevantes que se hubieran producido en materia de ciberseguridad, entendiendo por tales aquellos que, aisladamente o en su conjunto, puedan tener un impacto o daño significativo en el patrimonio, resultados o reputación del Grupo. En todo caso estos eventos serán comunicados, en cuanto se conozcan, al Presidente de la Comisión.

Estar informado sobre la Estrategia Tecnológica:

Ser informada, según corresponda, sobre la estrategia y tendencias tecnológicas que puedan afectar a los planes estratégicos del Banco, incluyendo el seguimiento de las tendencias generales del sector.

Ser informada, según corresponda, sobre las métricas establecidas por el Grupo para la gestión y control en el ámbito tecnológico; incluyendo la evolución de los desarrollos e inversiones que el Grupo lleve a cabo en este ámbito.

Ser informada, según corresponda, sobre las cuestiones relacionadas con las nuevas tecnologías, aplicaciones, sistemas de información y mejores prácticas que afecten a la estrategia o a los planes tecnológicos del Grupo.

Ser informada, según corresponda, sobre las principales políticas, proyectos estratégicos y planes definidos por el Área de Ingeniería.

Informar al Consejo de Administración y, en su caso a la Comisión Delegada Permanente, en los asuntos relacionados con las tecnologías de la información que sean de su competencia.

Para el mejor ejercicio de sus funciones se establecerán los sistemas de coordinación adecuados entre las Comisiones de Tecnología y Ciberseguridad y la de Auditoría y Cumplimiento, para facilitar:

Que la Comisión de Tecnología y Ciberseguridad pueda conocer las conclusiones de los trabajos que desarrolle el Departamento de Auditoría Interna en materias de tecnología y ciberseguridad.

Que la Comisión de Auditoría y Cumplimiento sea informada sobre los sistemas y procesos relacionados con las tecnologías de la información que tengan relación o afecten a los sistemas de control interno del Banco y otras cuestiones de su competencia.

Asimismo, se establecerán los sistemas de coordinación adecuados entre la Comisión de Tecnología y Ciberseguridad y la Comisión de Riesgos para facilitar el seguimiento por esta última del impacto de los riesgos tecnológicos en el ámbito de Riesgo Operacional y demás cuestiones de su competencia.

## 3.11 NORMATIVA BÁSICA EN ESPAÑA SOBRE LA SEGURIDAD DE LA INFORMACIÓN

Siguiendo a Warren, S.; Brandeis, L. (1995), en Volpato, S. (2016): La prensa está traspasando, en todos los ámbitos, los límites de la propiedad y de la decencia. El chismorreo ha dejado de

ser ocupación de gente ociosa y depravada, para convertirse en una mercancía, buscada con ahínco e, incluso, con descaro. Los más íntimos detalles de las relaciones sexuales se divulgan en las columnas de los periódicos, para satisfacción de la curiosidad lasciva. Con el fin de entretener al indolente, columna tras columna se llenan de chismes insustanciales, obtenidos, únicamente, mediante la intromisión en el ámbito privado. La intensidad y la complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales".

Es una evidencia que no necesita demostración que internet ha generado profundos cambios en la dinámica de la sociedad actual y en el comportamiento de las personas. Hoy, las nuevas tecnologías de la información y comunicación están incrustadas en la sociedad. Esta es la sociedad de la información, la sucesora de la sociedad industrial, con una cultura globalizada y conectada en red.La sociedad actual es la sociedad nacida de la revolución tecnológica de internet. Diríamos que la nueva sociedad, y por ende las empresas, están en red, provocando cambios sociales y cambios organizacionales tanto institucionales como empresariales.

Todos estos cambios en la historia de la humanidad exigen unarespuesta por parte de los sistemas que los gobiernan. De la misma manera que el sistema jurídico en los que se sustentan debe ser dinámico para acompañar estos cambios y cumplir con su función social.

El cumplimiento de una normativa básica nos protegerá de amenazas externas y nos permitirá respetar los derechos de nuestros clientes, proveedores, evitando infracciones involuntarias y por tanto costes innecesarios:

1.- Ley Orgánica de Protección de Datos de Carácter Personal conocida con las siglas LOPD. Esta ley tiene por objetivo proteger todos los datos de carácter personal, para que no sean utilizados de manera inadecuada, ni tratados, ni cedidos a terceros sin autorización del titular.

2.- Ley 34/2002 de servicios de la Sociedad de la Información y de Comercio Electrónico cuyas siglas son LSSI. La finalidad de esta ley es regular el funcionamiento de prestadores de servicios de la sociedad de la información. Empresas que realizan comercio electrónico, y aquellas que hacen publicidad por vía electrónica, como correo electrónico o SMS.

3.- Ley 32/2003, General de Telecomunicaciones, el objeto de esta ley es la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas. Entre otros objetivos, esta ley fomenta la competencia efectiva de los mercados de las telecomunicaciones, promueve el desarrollo del sector y defiende los intereses de los ciudadanos.

Ley 59/2003 de firma electrónica, esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. La firma electrónica es un conjunto de datos asociados que sirve para identificar a una persona en sus transacciones electrónicas y permite conocer si el contenido del mensaje ha sido manipulado de alguna manera.

Real Decreto Legislativo1/1996 Ley de Propiedad Intelectual, según esta ley la propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación. El autor tiene derecho exclusivo a la explotación de la obra. La ley protege las

creaciones originales expresadas en cualquier medio, incluidos programas de ordenador o bases de datos.

Ley 17/2001 de Propiedad Industrial, para la protección de signos distintivos de las organizaciones se concederán los derechos de propiedad industrial de marcas y nombres comerciales. De acuerdo con esta ley, el uso de un nombre comercial en redes telemáticas, en nombre de dominios, y en metadatos y palabras claves en páginas webs, sin autorización previa por parte de su titular, habilita a éste a prohibirle su autorización.

Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, esta ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. Además, regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa en las relaciones entre las Administraciones Pública, así como en las relaciones de los ciudadanos con las mismas.

Algunos sectores, como el agrario, poseen legislación propia sobre seguridad de la información. Otros, como la banca disponen de una normativa internacional que contiene recomendaciones al respecto.

La legislación anterior se ha desarrollado para proteger a todos los actores que utilizamos las nuevas tecnologías ante el aumento de delitos informáticos.

En un sentido muy amplio, delito informático es todo aquel que implique la utilización de cualquier medio de tecnología informática.

Estándares de gestión de la seguridad de la información:

Para poder estar preparados ante cualquier imprevisto y actuar con rapidez y eficacia es necesario implantar un Sistema de Gestión de Seguridad de la Información, en un contexto global coexistiendo con otros sistemas como la contabilidad (considerada como sistema de información útil para la toma de decisiones de los usuarios), sistema de calidad, medioambiente, etc.

Gracias a este sistema se podría analizar los posibles riesgos, establecer las medidas de seguridad necesarias y disponer de controles que nos permitan evaluar la eficacia de esas medidas. De este modo nos anticiparíamos a los posibles problemas y estar preparados en caso de contingencias. Esta actitud debe venir de la alta dirección y en concreto de la comisión de auditoría interna y comisión específica de tecnología de la información.

Para llevar a cabo este proceso, necesitamos lasnormas internacionales ISO (Organización Internacional de Normalización)/IEC (Comisión Electrónica Internacional) 27000. En los últimos años, ISO e IEC han trabajado mucho con normas relacionadas con las nuevas tecnologías como la telefonía móvil o la seguridad de la información. Se han elaborado también normas de gestión como las conocidas ISO 9001 e ISO 14001. Las normas son de carácter voluntario, sin embargo, su uso por millones de empresas facilita el entendimiento entre países y organizaciones. Las normas también contribuyen a mejorar la seguridad y la calidad de los productos y servicios que utilizamos todos los días.

La ISO 27.000, recoge los términos y definiciones empleados en el resto de las normas de la serie, con ello se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de las mismas y una introducción al SGSI (Sistema de Gestión de Seguridad de la Información) y una descripción del ciclo de mejora continua.

La norma más importante de la serie es la ISO 27001, se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y su actividad. Las normas contienen los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permiten evidenciar el buen funcionamiento del sistema. Igualmente, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización.

En España, esta norma ha sido publicada como UNE-ISO/IEC 27001 y puede adquirirse a través de la página web de AENOR[64], el organismo español de normalización, la versión inglesa (www.iso.Org). Esta es la norma de esta serie con la que serán certificados los Sistemas de Gestión de Seguridad de la Información de las empresas u organizaciones que lo deseen.

La ISO 27002 es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización. Para ello describe 11 áreas de actuación. 39 objetivos de control o aspectos a asegurar en cada área. Ente las áreas más importantes: Política de seguridad, análisis y gestión del riesgo, estructura organizativa para la seguridad, seguridad del personal, control de accesos, gestión de incidencias.

En relación con la implantación de un Sistema de Gestión de la Seguridad de la Información, se trata de una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada por la alta dirección. Su diseño dependerá de los objetivos, necesidades de la empresa y estructura organizacional. La empresa debe contar con estructura organizativa, así como recursos necesarios (Plan, Do, Act, Check).

Se utilizan cuatro tipos de documentos: políticas, que sientan las bases de la seguridad, indican las bases para conseguir los objetivos que se proponen; procedimientos desarrollan los objetivos marcados por las políticas; las instrucciones que desarrollan los procedimientos; registro, indicadores que evidencian la implantación del sistema.

La primera fase del modelo PDCA es la fase planificación, realizándose un estudio de la situación de la organización desde el punto de vista de la seguridad. Es importante realizar un análisis de riesgo que valore los activos de información y vulnerabilidades a los que están expuestos. En la fase de ejecución se establecen unos controles técnicos y documentación necesaria que permitan reducir los riesgos, para ello se necesita mucha concienciación y preparación del personal vinculado a estas tareas. En la fase de seguimiento se evalúa la eficacia y el éxito de los controles implantados. Por último, la mejora del sistema.

En relación con la política de seguridad, organización de la misma y formación del personal, la empresa debe determinar cuáles son los procesos críticos para su organización, decidiendo qué es lo se quiere proteger, saber la ubicación física en la que van a verse involucradas, estimación de los recursos económicos y el personal capacitado para esta tarea.

También, se deben establecer las pautas de actuación en caso de incidentes y definir responsabilidades e identificar los riesgos a los que se ve sometida la organización, debe ser aprobada por la alta dirección y publicitarla dentro de la organización implicada. Debe ser referencia para la resolución de conflictos en caso de incidentes en la seguridad de la organización.

[64] www.aenor.es

## 3.12 CONSIDERACIONES FINALES

Habida cuenta de que el software es el motor que mueve la economía mundial y que todas nuestras infraestructuras críticas, desde el tendido eléctrico hasta el sistema de telecomunicaciones, están ligadas a softwares específicos, no hay tiempo que perder en considerar que necesitamos programas de mayor calidad, dado que la tecnología que nos rodea funciona a duras penas, en muchos casos el software es una basura. Todos los bugs o errores y fallos de seguridad tienen un efecto acumulativo en la red de información mundial, lo cual explica que un alto porcentaje de nuestros sistemas pueden vulnerarse en cuestión de segundos.

La complejidad de algunos programas informáticos, combinada con una honda actitud relajada por lo que respecta a los errores de software ha llevado a Dan Kaminsky, un investigador en materia de seguridad informática a observar que hoy en día gracias al Código, vivimos inmersos en la era de la Cólera. Cuando se les increpa por el lamentable estado del software que circula por el mundo, muchos programadores replican: “somos humanos. El software perfecto no existe”.

Los consumidores demandan softwares llenos de funciones y potentes. Para ello es imperativo apuesten mucho más fuerte y coloquen el diseño de seguridad entre sus máximas prioridades, de manera que se convierta en un elemento clave de la computación fiable.

## 3.13. BIBLIOGRAFIA

ACEITUNO CANAL, V. (2004): “Seguridad de la Información: Expectativas, riesgos y técnicas de protección: incluye ejemplos de normativas de seguridad y referencias”. 2004.

AGENCIA ESPAÑOLA DE PROTECCIÓN, DATOS, URL: http://www.agpd.es

ALBERT GORE (2015): “Los delitos del futuro”, editorial Ariel. En Marc Goodman.

ALONSO, CHEMA (2017): “Cómo saltarse el control de cuentas de usuario en Window 7/10 con Hijacking Ole32.dll y .Net, 1 de febrero de 2017.

ALONSO, CHEMA (2017): “La tecnología tiene que ser el ADN de tu compañía, si no no vas a subsistir en el nuevo mundo”. @chemaalonso. Ow.ly/LzD1308xciQ. Elevan Paths.

ALONSO, CHEMA (2017): “No hay que parar la innovación, pero sí dotarla de valores”. Entrevista en ABC, 30 de enero de 2017.ÁLVAREZ, C.(2014): http://prezi.com>clasificacion-de-activo

ANDREASSON, O. (2006): “IPTables Tutorial (version 1.2.2)”. Descargable desde AON CIBERRIESGOS: http://www.aon.com>productos_servicios

AREITIO BERTOLIN, J. (2008): “Seguridad de la información: redes, informática y sistemas de información”.2008.

BBVA(2015):(https://accionistaseinversores.bbva.com/TLBB/fbinir/mult/Reglamento_Comision_IT_tcm926-592287.pdf´) BEJTLICH, R. (2005): “The Tao of Network Security Monitoring”. Ed. Addison Wesley

BEJTLICH, R. (2005): “The Tao of Network Security Monitoring”. Ed. Addison Wesley

BEN KINGSLEY (2015): "The good guy"en "Los delitos del futuro", editorial Ariel. En Marc Goodman.

BERTOLIN, J.A. (2008): "Seguridad de la información. Redes informática y sistemas de información"- Books Google.com

BORJA GUINEA (2015): (https://assets.kpmg.com/content/dam/kpmg/pdf/2015/06/El-nuevo-gobierno-corporativo-2015.pdf).

CAMUS, A. (2015): "genesyrobots.blogspot.com"

CAYÓN PEÑA, J.; GARCÍA SEGURA, L. (2015): "Hacia un nuevo enfoque del conflicto ciber en el ámbito empresarial ", Diario La Ley. 2015 (8577):2-2

CHESWICK, W.R.; BELLOVIN, S.; RUBINA, A. (2003): "Firewalls and Internet Security; Repelling the Wily Hacker". 2ª. edición. Addison-Wesley Professional.

CHRISTOF PARA (2015): "Los delitos del futuro", editorial Ariel. En Marc Goodman.CISCO SYSTEMS (2010): "Cisco VPN Administrator Guide, Release 5.0" Ed. Cisco Systems. http://www.cisco.com/en/US/docs/security/vpn-client/cisco_vpn_client/vpn_client500_501/administration/5vcA.pdf

CISCO SYSTEMS, sitio web official de Cisco Systems. http://www.cisco.com

CRIPTONOMICON (seguridad en el comercio electrónico), servicio ofrecido por el Instituto de Física Aplicada del CSIC (Consejo superior de investigaciones científicas) URL: www.iec.csic.es/criptonomicon

DAVE EVANS (2015): "Los delitos del futuro", editorial Ariel. En Marc Goodman.

DAVID PETROEUS (2012): "Director de la Cia dice que espiará a la población a través de aparatos electrónicos del hogar". verdadahora.cl

DEAN KOONTZ (2015): "Los delitos del futuro", editorial Ariel. En Marc Goodman.

DELGADO, V.; PALACIOS, R. (2006): "Aplicaciones prácticas de la criptografía", anales de mecánica y electricidad/marzo-abril 2006.

DUQUE, D.; ROGEL, E.G. (2015): "Vulnerabilidad en redes de datos. Propuestas para analizar e identificar riesgos". Eumed.net

ELLISON, C. y SCHENEIDER, B. (2000): "Ten risks of PKI: what you´re not being told about Public Key Infrastructure". Computer Security Journal, Volume XVI, Number 1.ESQUEMA NACIONAL DE SEGURIDAD, URL: http://www.ccncert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es

ETEROVIC, J.E.; PAGLIARI, G.A.(2011): "Metodología de Análisis de Riesgos Informáticos". Técnica Administrativa, ISSN-e 1666-1680, Vol. 10, Nº. 45, 2011- Dialnet.

FÉRNANDEZ, J.M.; TEODORO, P.G. (2007): "Ataques de denegación de servicio a laja tasa contra servidores" -2007- 0-hera.ugr.es.adrastea.ugr.esFIREWALL, BUILDER, sitio web del

creador de FWBuilder, herramienta gráfica de configuración de cortafuegos IPTables. URL: http://www.fwbuilder.org/

FRAHIM, J. (2010): Cisco ASA. “All in one firewall, IPS, anti-X and VPN Adaptative Security Appliance. Ed. Cisco Press.

GARCÍA ALFARO, J. (2014): “Simulaciones software para el estudio de amenazas contra sistemas SCADA. Actas de la XIII Reunión Española sobre Criptografía y Seguridad de la Información: celebrado del 5 al 8 de septiembre 2014, Alicante. Pp. 151-156.

GARFINKEL, S.; SHELAT, A. (2003): “Remembrance of Data Passed: A Study of Disk Sanization Practices”. IEEE Security & Privacy, publicado por IEEE Computer Society.

GARFINKEL, S.; SPAFFORD, G.; SCHWARTZ, A. (2003): “Practical UNIX and Internet Security”. 3ª edición. O´Reilly Media.

GERG, C. Y KERRY J. (2004): “Managin Security with Snort and IDS Tools”. Ed. O´Reilly.

GÓMEZ CORONA, E.; SAMIRA VOLPATO (2016): “El derecho a la intimidad y las nuevas tecnologías de información”

GÓMEZ FERNÁNDEZ, L.; ANDRÉS ÁLVAREZ, A. (2012): “Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes”. Asociación Española de Normalización y Certificación, 2ª ed. (ampl. con el esquema Nacional de Seguridad).

GÓMEZ-BRAVO, F.; JIMÉNEZ NAHARRO, R.; MEDINA GARCÍA, J.A.; GÓMEZ GALÁN, M.; SÁNCHEZ RAYA, M. (2015): “Sobre la Vulnerabilidad de los Robots Móviles frente a los ataques de Hardware”. Actas de la XXXVI Jornadas de Automática, 2-4 de septiembre de 2015. Bilbao.

GONZÁLEZ CUSSAC, J.L.; CUERDA ARNAU, M.L. (2013): “Nuevas amenazas a la Seguridad Nacional : terrorismo, criminalidad organizada y tecnologías de la información y la comunicación”. Tirant lo Blanch

GORDON FYODOR LYON (2009): “Nmap Network Scanning: The official Nmap Project Guide to Network Discovery and Security Scanning”. Ed. Nmap Project

GRAWLEY, D.R. (2012): “Cisco Router Step-by-Step Configuration Guide (Volume 1)”. Ed. Soundtraining.net

GUISADO, J.S.; RENDÓN, J.C. (2014): “Detección y mitigación de vulnerabilidades día cero”, Cuaderno Activa, 2014- ojs.tdea.edu.co

GUTIÉRREZ BENITO, F. (2014): “Laboratorio Virtualizado de Seguridad Informática con Kali Linux”, Universidad de Valladolid. Escuela Universitaria Informática. http://uvadoc.uva.es/handle/10324/5792.

HARRIS, S.; HARPER, A.; EAGLE, C. (2005), Hacking ético, Dialnet.unirioja.es

HERNÁNDEZ, A.; FOJÓN, E. (2016): “Ciberseguros : la última línea de defensa”Revista SIC: ciberseguridad, seguridad de la información y privacidad. 2016 25(. 120):98-100

HOWARD RHEINGOLD (2015): “Los delitos del futuro”, editorial Ariel. En Marc Goodman.

http://hacking-etico.com

http://it-os.mx/index.php/2014-09-01-08-00-

http://www.frozentux.net/documents/iptables-tutorial/

http://www.nebrija.es>Modulo_0. Profesor Constantino Malagón.

https://camiloangel.wordpress.comhttps://hackstory.net/ingenieria_socialIEEE Official site, URL: http://standard.ieee.org/about/get/802/802.11.html

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE): (https://www.incibe.es)INTECO, INSTITUTO DE TECNOLOGÍAS DE LA COMUNICACIÓN, en su página web dedica un artículo a presentar las medidas recomendables para asegurar una red inalámbrica. URL://cert.inteco.es/Proteccion/Configuraciones_seguras/WiFi/

INTERNAUTAS.ORG (SEGURIDAD EN LA RED). URL: http://www.internautas.org/seguridad/INTYPEDIA, INFORMATION SECURITY ENCYCLOPEDIA, enciclopedia gratuita en video sobre seguridad informática, accesible en http://www.criptored.upm.es/intypedia.

INTYPEDIA, INFORMATION SECURITY ENCYCLOPEDIA, enciclopedia gratuita en video, que dedica la lección 12 a la seguridad de las redes inalámbricas, con la garantía de la red CRIPTORED y la Universidad Politécnica de Madrid, descargable desde http://www.intypedia.comISO 20000 CERTIFICACION, URL: http://www.isoiec20000certification.com/ISO 27000 DIRECTORY, URL: http://www.27000.org/index.htm

ITSMF ESPAÑA, URL:http://www.itsmf.es

J. XU, T. ZHANG, D. LIN, MAO, X.L. (2013): "Pairing and Authemtication Security Techonologies in Low-Power Bluetooth"

JARA, H.; PACHECO, F.G. (2012): "Ethical Hacking 2.0"- Books Google.comKRIPTOPOLIS (seguridad del comercio electrónico). URL: http://www.kriptopolis.comLa Protección de datos personales, soluciones en entornos Microsoft, V2.0, libro gratuito, descargable desde URL: hppt://download.microsoft.com/download/C/2/6/C2689C05-2B67-4D11-BD2A-43CF9DBCE59E/Libro_LOPD_V2_Alta.pdfLAMBERT Academic Publishing, 2010.

LIOTINE, M. (2003) "Mission critical network planning". Ed. Artech HouseLIOTINE, M. (2003): "Mission-Critical Network Planning". Ed. Artech House Publishers

LOPEZ PÉREZ, F. (2016): "Conferencia sobre la Amazonia". www.loyolaandnews.es

MARSH AND MCLENNAN Y CHERTOFF GROUP (2014): "A Cybersecurity call to Action"

MERINO BADA, C.; CAÑIZARES SALES, R.(2011): "Implantación de un sistema de gestión de seguridad de la información según ISO 27001: Un enfoque práctico. FC editorial. 2011.

MIGUEL PÉREZ, J.C. (2015): "Protección de datos y seguridad de la información: guía práctica para ciudadanos y empresas. Ra-Ma, 2015.

MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN PRODUCTIVA (2009): "libro blanco de la Prospectiva TIC 2020", Ministerio de Ciencia, Tecnología e Innovación Productiva, 2009.

MOLINA MATEOS, J.M. (2000): "Seguridad de la información: criptología". El Cid Editor, 2000.

NARANJO CUERVO, R.C. (2011): "Caso de estudio: Construcción de la herramienta MVPS para la verificación de políticas de seguridad en comercio electrónico B2C utilizando componentes XPCOM. Gerencia Tecnológica informática. 2010, Vol. 9 Issue 25, p 13-25, 13p.

NETFILTER, sitio web de la organización Netfilter, creador del proyecto de software libre IPTables. URL: http://www.netfilter.otg/projects/iptables/index.html

NEWSOME, J.; DAWN SONG (2005): "Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software", Carnegie Institute of Technology, Departament of Electrical and Computer Engineering.

PADMASREE WARRIOR (2015): "Los delitos del futuro", editorial Ariel. En Marc Goodman.

PASTOR, J.; SARASA, M.A.; SALAZAR, J.L. (2010): "Criptografía digital. Fundamentos y Aplicaciones". Ed. Prensas de la Universidad de Zaragoza.

PESO NAVARRO, E.; RAMOS GONZÁLEZ, M.A.(1994): "Confidencialidad y Seguridad de la Información: La LORTAD y sus implicaciones socioeconómicas.

PREET BHARARA (2015): "Los delitos del futuro", editorial Ariel. En Marc Goodman.

PROVOS, N.; THORSTEN, H. (2007): "Virtual Honeypots: From Botnet Tracking to Intrusion Detection". Addison Wesley Professional.

PURDY, G.N. (2004): "Linux iptables Pocket Reference". Ed. O´Reilly Media.

RAMOS ALVAREZ, B.; RIBAGORDA GARNACHO…(et al.) (2004): "Avances en criptología y seguridad de la información". Ediciones Díaz de Santos. 2004.

RANDO, E.; ALONSO, C. (2012): "Hacking de Aplicaciones Web: SQL Injection.

SÁNCHEZ, J.L.; IGNOTO, M.L. (1991): "La seguridad informática", iit.Comillas.eduSCHNEIER, B. (1996): "Applied Cryptography". 2ª. Edidicón. Ed. Wiley.SGUIL, sitio web del proyecto de software libre Sguil. URL: http://sguil.sourceforge.net/

SHARIF, l. Y AHMED, M. (2010): "IPSec: A Practical Approach: Network Security. Ed. LAP SINGH, S. (1999): "The code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography". Ed. Doubleday. Existe una version "ligera" descargable gratuitamente, y en formato interactivo con ejercicios, desde http://simonsingh.net/cryptography-cd-rom/SNORT, sitio web del Proyecto de software libre Snort. URL: http://www.snort.org

STEINBERG, J, (2005): "Understanding SSL VPN. Ed. Packt Publishing

SUN TZU (1972): "El arte de la Guerra"

T.Al-Tayeb (2013): "Al-Kindi, Cryptography, Code Breaking and Cyphers", http://www.muslimheritage.com/topics/default.cfm? ArticleID=372. Agosto 2013.

TERRY PRATCHETT (2015): “Pies de barro”. www.lectulandia.comTHIBER: The cybersecurity Think Tank” (www.thiber.com)TIM BERNERS-LEE (2015): “Los delitos del futuro”, editorial Ariel. En Marc Goodman.

TOFFLER, ALVIN (1970): “Future Shock”,TOFFLER, ALVIN (1990): “War and Anti-War”

TOFFLER, ALVIN AND HEIDI (2006): La Revolución de la Riqueza”

TOFLLER, ALVIN (1980): “La Tercera Ola”

TRIDIB BANDYOPADHYAY (2012): “Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management – A Modelling Approach”, Proceedings of the Southern Association for Information Systems Conference, Atlanta, 2012, pp. 23-29.

TRONCOSO, R.; RAMÍREZ, F.J. (2013): “Microhistorias: anécdotas y curiosidades de la informática. Edición Informática 64.UN INFORMÁTICO EN EL LADO DEL MAL, blog sobre seguridad informática de Chema Alonso, reputado consultor de seguridad, en el que se pueden encontrar gran cantidad de artículos de divulgación sobre seguridad informática, descargable desde http://www.elladodelmal.com/

VACA, J.R. (2017): “Cloud computing security: foundations and challenges”.

VILAMOWSKY, B.; IRWIN J.D. (eds.) (2011): “Industrial Communications Systems”. Ed. CRC Press.

VILLALON HUERTA, A. (2012): “Seguridad en Unix y redes Versión 2.1”, Julio, 2012. Descargable desde http://www.rediris.es/cert/doc/

VINTO CERF (2015): “Los delitos del futuro”, editorial Ariel. En Marc Goodman.

VOLPATO SAMIRA (2016): “El derecho a la intimidad y las nuevas tecnologías de la información”. Tesis Doctoral, septiembre de 2016, Universidad de Sevilla. (Samuel Warren y LOUIS BRANDEIS*. El derecho a La intimidad.* Edición a cargo de Benigno Pendás y Pilar Baselga, Civitas, Madrid: 1995, p.26)

WRIGHTSON, W. (2012): “Wireless Network Security. A Beginner´s Guide.” Ed. MacGraw Hill.

YOUNG CARL S. (2016): “Information security science : measuring the vulnerability to data compromises”

ZURICH CIBERRIESGOS: http://www.zurich.es>seguros>mas

# CAPITULO 4: LOS ACTIVOS INTAGIBLES Y SU IMPORTANCIA ESTRATEGICA EN LA EMPRESA, LIGADOS AL LOGRO DE LAS VENTAJAS COMPETITIVAS. LA SEGURIDAD DE LA INFORMACIÓN, NUEVA VENTAJA COMPETITIVA EN LAS ORGANIZACIONES

## 4.1 INTRODUCCIÓN

En este capítulo se pretende resaltar la importancia estratégica de los inmovilizados intangibles en un entorno económico relacionado con problemas de seguridad de la información que apuntan directamente a la línea de flotación del negocio y al principio de empresa en funcionamiento. Toda empresa que decide invertir recursos en estrategia, emprende un camino. La meta es la consecución de los objetivos estratégicos y los beneficios que estos nos aportan a la organización. Este itinerario ha de pasar por la ejecución de la estrategia, y, lógicamente, tiene su comienzo en la definición y planificación de la estrategia. Es decir, trazando el mapa del camino que vamos a recorrer.

En la nueva economía, basada en internet, el talento y el liderazgo junto a otros intangibles como la propuesta de un sistema de gestión para la seguridad de la información basado en unos mínimos deseables por encima de los mínimos normativos, giran alrededor del inmovilizado intangible I+D+i, añaden valor a la organización y son las claves para la obtención de esos mínimos deseables que se proponen en esta tesis.

Las empresas basadas en internet cada día son más fuertes y su negocio online es el verdadero motor de las mismas. Existen noticias de prensa económica como la siguiente: Facebook y Amazon desplazan a Berkshire Hathaway y a ExxonMobil de los primeros puestos.

El poderío de las compañías tecnológicas en los mercados y en los negocios ha alterado radicalmente la clasificación de las mayores empresas de Estados Unidos por valor en Bolsa.

La red social Facebook y el gigante de comercio electrónico Amazon han desplazado a las veteranas ExxonMobil[65] y Berkshire Hathaway[66] de la clasificación, y, por tanto, han conseguido que los cinco primeros puestos del ránking estén ya en manos de compañías tecnológicas: Apple, Google, Microsoft, Facebook y Amazon.

Esta situación es absolutamente inédita y da continuidad a los profundos cambios que se han producido en los últimos meses y que, sobre todo, han estado protagonizados por el salto de Facebook y Amazon. A esto se han unido los problemas que están experimentando grupos tradicionales como la petrolera ExxonMobil, a la que la fiscalía de Nueva York acaba de abrir una investigación por presuntas irregularidades contables. A Berkshire, por su parte, le está afectando su exposición a Wells Fargo, en la que controla un 9,5%.

Nueve de los diez primeros puestos de la lista pertenecen ya al sector tecnológico y de telecomunicaciones, después de que la operadora AT&T arrebatara a Wells Fargo la décima posición hace apenas tres meses. El banco, tradicionalmente el mayor de Estados Unidos por

[65] Corporate.exxonmobil.com, es una empresa petrolera estadounidense, antigua Standard Oil Company (1870).

[66] www.berkshirethathaway.com, es una sociedad tenedora de origen estadounidense, dueña de acciones de varios grupos internacionales.

valor en Bolsa, se encuentra en el ojo del huracán por una investigación sobre la apertura de cuentas falsas durante años, lo que ha hecho que JPMorgan le haya superado en capitalización.

Nueve de los diez primeros puestos de la lista pertenecen ya al sector tecnológico y de telecomunicaciones

El protagonismo tecnológico se explica, según los analistas, por la capacidad de las empresas de captar talento y de introducirse en industrias tradicionales, y por su abultada liquidez. Estas características refuerzan el gancho del sector por parte de los inversores, en un momento en el que los principales índices bursátiles de Estados Unidos se sitúan en niveles récord.

Facebook y Amazon son las grandes favoritas del mercado. La primera, que desplazó hace apenas un año a la cadena de supermercados Wal Mart de la clasificación de las diez mayores, ha subido un 35% en Bolsa en los últimos doces meses y ya vale cerca de trescientos setenta mil millones de dólares.

El impulso de Amazon es aún más acusado. La compañía que fundó Jeff Bezos en 1944 se ha revalorizado un 44% en un año y, con una capitalización de más de trescientos sesenta y siete mil millones de dólares, rivaliza con Facebook por el cuarto puesto de la lista. El año pasado, ni siquiera figuraba entre los diez primeros.

Apple, Google y Microsoft encabezan el ránking. Después de semanas de parálisis, Apple está experimentando una fuerte recuperación en Bolsa tras el lanzamiento del nuevo iPhone 7, que salió a la venta y del que ya se han agotado varios modelos. Apple ha vuelto a superar los seiscientos mil millones de dólares de capitalización.

Google, por su parte, se mantiene en el segundo puesto de la clasificación tras lograr el hito de adelantar a Apple en la primera posición en varias ocasiones durante este ejercicio. La tercera mayor compañía de Estados Unidos es Microsoft. Detrás de las tecnológicas, figuran Berkshire, ExxonMobil, el gigante industrial General Electric, la farmacéutica Johnson & Johnson y AT&T.

Con respecto a los activos intangibles, debemos decir, desde el punto de vista de la seguridad de la información, que sólo debemos proteger aquellos activos intelectuales que produzcan o puedan producir beneficios a la empresa o cuyo riesgo de pérdidas sea alto unido al perjuicio que podría causar su conocimiento o copia por la competencia.

## 4.2 LA TEORÍA DE LOS RECURSOS Y DE LAS CAPACIDADES. ASPECTOS GENERALES

Después de la introducción y las características actuales de los activos intangibles, en este apartado nos proponemos adentrarnos en el poder estratégico de los inmovilizados intangibles.

La teoría de recursos y capacidades propone que las organizaciones son diferentes entre sí en función de los recursos y capacidades que poseen en un momento determinado, así como por las diferentes características de la misma y que dichos recursos y capacidades no estén disponibles para todas las empresas en las mismas condiciones. Esta teoría nos permite encaminar el análisis interno hacia los aspectos más relevantes del interior social de la organización, en relación con el análisis externo realizado y como base para el planteamiento estratégico general y de recursos humanos posterior. También es una herramienta que permite determinar las fortalezas y debilidades internas de la organización. Y según esta teoría

la única forma de conseguir ventajas competitivas sostenibles es a través del desarrollo de capacidades distintivas.

Según Wernerfelt (1984) “la eficiencia adquirida por una empresa es función de los recursos y capacidades distintivas que la misma controla, los cuales son fuente de sinergia y de ventajas competitivas porque provienen del aprendizaje colectivo y exclusivo de la organización que compite en mercados imperfectos” Barney en 1991 argumentó que “los recursos de la empresa incluyen todos los activos, capacidades, procesos organizativos, características de la empresa, información, conocimientos,…que son controlados por ella y que le permiten concebir y desarrollar estrategias para aumentar su eficacia y eficiencia”

Siguiendo a Peteraf (1993) deben caracterizarse por su heterogeneidad, por la existencia de límites ex-ante y ex-post a la competencia y por su imperfecta inmovilidad, esto significa que los recursos no están disponibles para todas las empresas en las mismas condiciones (movilidad imperfecta) y por ello las empresas son diferentes por los activos que poseen (heterogeneidad).

Posteriormente en 2001 Barney puntualizó “los recursos son los activos tangibles e intangibles que una empresa emplea para formular e implantar sus estrategias”.

Los recursos productivos de la empresa se clasifican en físicos, intangibles, capital humano y de capital organizacional, los cuales se integran en procesos y rutinas operativas y administrativas denominadas capacidades.

Los recursos físicos que hacen referencia a tecnología física, planta y equipo, localización geográfica, acceso a materia prima, infraestructura en lotes y construcciones y otros factores que afectan el costo de producción. También se consideran en este grupo los recursos financieros, considerados como fuentes para financiar las inversiones de la empresa, y provenientes de los fondos que se genera internamente, o de afuera, como son los aportes de capital de los dueños y los otorgados por terceros en forma de créditos Weston y Brigham(1994).

Los recursos intangibles tienen mayor relevancia cuando se integran en capacidades empresariales; sin embargo, pocas organizaciones los identifican y valoran adecuadamente, porque contablemente, las inversiones de esta clase de activos que generan impacto en los resultados de la empresa en el largo plazo, se registran como gastos, tal como sucede con los gastos en investigación y desarrollo, formación del recurso humano, publicidad y posicionamiento de marca, desarrollo de software, entre otros. Entre los activos intangibles se tiene la marca, como valor y como potencial de ampliar los ingresos por los ámbitos de productos o mercados; la reputación, con relación a las relaciones con el cliente, la calidad de los productos, las relaciones con los proveedores y con otros entes; las patentes y propiedad intelectual en la que se apoya la protección legal del conocimiento y la generación de mayores ingresos, entre otros Barney y Arikan (2001); Grant, (2006).

Como recursos de capital humano, se cuenta con las personas que ejercen los distintos cargos de la compañía y sus competencias, entre otros: su grado capacitación, la experiencia, la forma de razonar y de tomar decisiones, el potencial de aprendizaje, la apertura al cambio, la capacidad de adaptación, habilidad de trabajo en equipo, las relaciones personales, el liderazgo, el espíritu emprendedor, así como aspectos sicológicos y sociológicos Barney, (1991); Grant, (2006).

Entre los recursos de capital organizacional, pueden incluirse la estructura organizacional, líneas de autoridad, forma de reportes, la planeación formal e informal, el control, la coordinación de sistemas; la forma como los empleados integran sus esfuerzos y habilidades, depende no sólo de sus habilidades personales, sino también del contexto organizativo. La cultura organizacional se relaciona también con los valores, tradiciones y normas sociales de la organización, y es considerado un recurso intangible clave y fuente fundamental de ventajas competitivas sostenibles Barney, (1991); Grant, (2006).

Las capacidades operativas y administrativas se consideran las formas en que los recursos interactúan, están integrados, organizados y se complementan en rutinas organizativas, compuestas por acciones secuenciales, estrechamente coordinadas sin necesidad de una especial dirección o comunicación verbal, Nelson y Winter (1982).

Grant (1991) define la capacidad como la actitud o habilidad de un grupo de recursos para realizar alguna tarea o actividad.

Amit y Schoemaker (1993) afirman que las capacidades se refieren a la competencia de una empresa para desplegar los recursos, normalmente en combinación, por medio de procesos organizativos para lograr el fin deseado.

Respecto a las capacidades, se debe advertir de lo siguiente:

Capacidades operativas: implica la realización de una actividad mediante un conjunto de rutinas que coordinan y ejecutan la variedad de tareas necesarias para su consecución.

Las capacidades dinámicas construyen, integran o reconfiguran capacidades operativas. Las capacidades dinámicas no afectan directamente al output, sino indirectamente a través de su impacto en las capacidades operativas.

La teoría de las capacidades dinámicas establece que la empresa podrá incrementar su potencial de generación de beneficios, si logra formas distintivas para desarrollar recursos y capacidades, configurar estrategias, acelerar la discontinuidad de las mismas y dirigir las estrategias de una manera contingente Mintzberg (1994), Peteraf, (1993); Hamel y Prahalad (1994); Teece et al., (1997); Grant(2006).

Respecto a la diferencia entre recurso y capacidad:

Una capacidad es específica de la empresa, ya que se encuentra integrada en la organización y sus procesos, mientras que el recurso no suele alcanzar un nivel de integración tan alto.

La propiedad de una capacidad no suele ser transferida de una organización a otra sin transferir la propiedad de la organización en conjunto.

El principal fin de una capacidad es mejorar la productividad de los otros recursos que la empresa posee.

Respecto al concepto de competencia, se debe significar lo siguiente:

Son el conjunto de capacidades de la empresa que poseen mayor potencial para generar una ventaja competitiva y competencias nucleares a aquellas que son clave en la estrategia competitiva de la empresa.

La heterogeneidad de recursos es una condición empresarial para sostener ventajas competitivas Barney, (1991); Peteraf, (1993). Barney, (1991), postula cuatro indicadores o cualidades empíricas del potencial de recursos de la empresa para generar ventaja competitiva sustentable, los cuales son: Valiosos, porque ayudan a aprovechar oportunidades y a neutralizar amenazas en el ambiente, así mismo permite a la empresa concebir que mejoren su eficiencia y efectividad. Raros, o poco comunes entre los competidores, el número de empresas que poseen un recurso particular valioso es menor al número de empresas necesarias para generar la dinámica de la competencia perfecta en una industria, por lo que ese recurso puede generar una ventaja competitiva. Inimitable, ya sea porque la habilidad de la empresa para poder obtener los recursos, depende de una situación histórica única, porque la relación entre recursos y ventaja competitiva es tan ambigua que nadie sabe cómo duplicarla o porque puede ser un fenómeno social muy complejo más allá de la habilidad de las empresas para dirigirlo o confluirlo sistemáticamente. Insustituible, es decir, que no hay equivalentes.

Es necesario disponer de recursos distintivos, que sean estratégicos o esenciales, es decir que cumplan los criterios de ser valiosos, escasos y difíciles de imitar o de sustituir, como la reputación de la firma, las patentes y conocimientos únicos y las tecnologías especializadas, entre otros; con ellos la empresa podrá obtener una ventaja competitiva sostenible y generar el potencial de beneficios. El cumplimiento de dichos criterios dificulta que otras firmas puedan replicar e implementar la estrategia explotando las oportunidades del entorno de la misma forma Barney(1991); Peteraf(1993); Teece et al. (1997); Grant(2006).

Para la empresa, es necesario poseer recursos superiores y lograr de ellos una eficiencia para mejorar la productividad y competitividad, lo que sucede cuando se usa el mínimo de recursos para un nivel de operación determinado, o se obtiene el máximo de resultados de un nivel dado de recursos. Igualmente, se debe buscar la posibilidad de emplear los recursos existentes en usos más rentables Peteraf (1993); Grant (2006).

Respecto a la teoría de los recursos y capacidades y su influencia en la dirección estratégica.

Esta teoría tiene gran influencia en la dirección estratégica ya que representa un marco conceptual, una forma de ver y entender la empresa. Además, la elaboración de estrategias para la empresa se hace teniendo en cuenta sus recursos y capacidades.

Según el modelo expresado por Grant (2006), la empresa interacciona los elementos que integran la estrategia –sus objetivos y valores, los recursos y capacidades y la estructura y sistemas-, con el entorno competitivo, conformándose un nexo que se concreta en la necesidad de realizar ajustes estratégicos continuos.

Quinn (1980) define que “Una estrategia es el modelo o plan que integra en un todo coherente los principales objetivos, políticas y secuencias de acción de una organización. Una estrategia bien formulada ayuda a ordenar y asignar los recursos de una organización de una forma única y viable, basada en las competencias y carencias internas relativas a ésta, los cambios previsibles del entorno y las eventuales maniobras de adversarios inteligentes”, más tarde referenciado por Grant en 2006.

En el enfoque que busca las fuentes de las ventajas competitivas no externamente, sino al interior de la organización, se destaca la relevancia de los recursos y capacidades para crear, mantener y apropiarse de los beneficios potenciales que generan las ventajas competitivas sostenibles, Penrose(1959); Wernerfelt(1984); Barney(1991); Peteraf(1993); Teece et al.(1997); Grant(2004).

Las líneas del pensamiento sobre estrategia convergen a la perspectiva de su configuración y de las capacidades dinámicas teniendo en cuenta los permanentes cambios del entorno, las condiciones competitivas, la capacidad proactiva y de innovación empresarial, así como generando recursos y capacidades únicos y heterogéneos y ventajas competitivas sostenibles Minztberg (1994); Teece et al. (1997).

El establecimiento de la ventaja competitiva a través del desarrollo y despliegue de los recursos y capacidades, más allá de suponer una protección contra la tormenta competitiva, se ha convertido en el objetivo principal de la estrategia Grant (2006). Siguiendo a este mismo autor, Ante la pregunta recurrente de investigación, acerca del porqué unas empresas triunfan y otras no, el campo de conocimiento de la gestión y en particular de la estrategia, ha generado conceptos y marcos teóricos para tratar de avanzar en su respuesta, la cual sigue en evolución, dada la complejidad y la acelerada turbulencia en la que se mueven los mercados (Grant, 2006).

El autor refiere que el origen de la estrategia se remonta a más de 2000 años, con los aportes a la estrategia militar de Sun Tzu e interpretada por R.L. Wing (1988) a la estrategia empresarial. Sin embargo, es a partir de mediados del siglo XX, donde se inicia una evolución acelerada de la disciplina de la estrategia.

Los aspectos que inciden en la estrategia de éxito son la definición del propósito y de los objetivos empresariales, el conocimiento profundo del entorno competitivo y la valoración objetiva de recursos, proceso que puede ser también implementado a nivel personal Grant, (2006).

Los dos grandes campos en que se ha desarrollo el estudio de la estrategia como búsqueda de fuentes de la rentabilidad empresarial, son, de un lado, la provenientes del entorno competitivo, cuyo análisis y estrategias se han derivado del modelo de las cinco fuerzas competitivas de Porter (1980) y de los factores claves de éxito; en segundo lugar, la que corresponde a la organización misma y a los recursos y capacidades en los que se basa el logro de ventajas competitivas, sostenibles de largo plazo, conocida como la teoría de la visión de la empresa basada en recursos ó Resource Based View- RBV, siguiendo a Armando Cardona (2011).

Se pretende resaltar con esta teoría en esta tesis, identificar cuáles son los principales criterios que la teoría de la estrategia ha desarrollado y que suelen utilizarse para evaluar el potencial de generación de beneficios de los recursos y capacidades de la empresa, como ya hemos comentado anteriormente. Para lograrse, los recursos estratégicos de la empresa deben ser heterogéneos y cumplir con las propiedades de ser valiosos, escasos y difíciles de imitar o de sustituir, criterios que se relacionan con el desarrollo y la sostenibilidad de las ventajas competitivas, Barney (1991; Peteraf(1993).

Comenzamos con la definición de estrategia, más tarde con teoría de la visión de la empresa basada en recursos; posteriormente se analizan las características de los recursos estratégicos y el proceso para identificar y valorar su potencial de generación de beneficios y de lograr ventajas competitivas sostenibles, mostrándose la relación de los recursos y capacidades con los activos intangibles de la empresa; seguidamente se integran los recursos y capacidades definidos por la empresa en un proceso de planeación financiera, el cual debe asegurar los recursos financieros para la ejecución de la estrategia.Para analizar el papel de los recursos y capacidades y su impacto a la generación de beneficios empresariales, es necesario remitirse al concepto de estrategia, dado que este es su objetivo, ligado a logro de ventajas competitivas sostenibles**.**

Grant, (2006) establece que la estrategia empresarial se enfoca en la búsqueda de beneficios, lo que implica planificar para alcanzarán sus objetivos, en un proceso aplicable tanto para un individuo como para una organización y para esta última, consistente en lograr ventajas competitivas, asegurar la supervivencia y la prosperidad.

El término estrategia se asocia con plan, no siempre esta ha seguido un proceso sistemático y detallado para el logro de los objetivos por parte de los agentes económicos; sin embargo, se ha reconocido que el conocimiento del sector, la experiencia, la intuición, la creatividad, la racionalidad, el compromiso y el liderazgo, juegan un papel fundamental en la forma como se estructuran las acciones empresariales implementadas para la obtención de beneficios Mintzberg, (1994) y conducir al logro de los mejores beneficios Simon y March, (1956).

Alfred Chandler (1962), define la estrategia como: las metas y los objetivos de una empresa y la adopción de acciones y la asignación de los recursos necesarios para la consecución de estos objetivos.

Con respecto al diseño de la estrategia, hay dos escuelas: la escuela de diseño, que define el proceso como racional, deliberado y planificado por la alta dirección, según Andrews, (1977); Ansoff, (1991), que sigue un proceso de negociación y compromiso de los directivos y es comunicada a toda la organización para ganar la adhesión y el compromiso con respecto a los objetivos trazados; la segunda, la escuela de la configuración o de estrategias emergentes, Mintzberg (1994), Teece et al.,(1997), que contempla decisiones resultantes de un proceso complejo, en el que los directivos traducen la estrategia deliberada y la adaptan a las circunstancias cambiantes del entorno de la organización. Luego es más democrática la escuela de diseño que la de configuración.

Los planes de acción diseñados por la alta dirección se comunican y posibilitan el intercambio de puntos de vista, la búsqueda de consenso y el compromiso de toda la organización en su implementación, sometidos a continua revisión y a la mejora continua Grant, (2006).

Para Quinn (1980), Grant (2006): “Una estrategia es el modelo o plan que integra en un todo coherente los principales objetivos, políticas y secuencias de acción de una organización. Una estrategia bien formulada ayuda a ordenar y asignar los recursos de una organización de una forma única y viable, basada en las competencias y carencias internas relativas a ésta, los cambios previsibles del entorno y las eventuales maniobras de adversarios inteligentes”.

Es importante señalar los resultados de los estudios de Henry Minstzberg (1978) y referenciados por Grant (2006), los cuales resaltan que las acciones empresariales o estrategias realmente realizadas materializan sólo entre un 10 y 30 por ciento de la estrategia deliberada y originada en la alta dirección.

Grant (2006) explica que contablemente se entiende por beneficio la diferencia entre los ingresos por ventas de bienes y servicios y los costes y gastos en los que se incurre para ofrecerlos; adicionalmente, presenta otras medidas de beneficios que se usan para medir el impacto de la estrategia en el objetivo básico financiero de la empresa, el cual consiste en aumentar el valor de la empresa y la riqueza de accionistas (Weston y Brigham, 1994).

Además del beneficio contable, entre otras, las medidas presentadas por Grant (2006), se tienen: el beneficio económico, el valor económico agregado- EVA[67] y los flujos de caja libre, siendo esta última técnica la de mayor relevancia para medir el valor de la compañía y evaluar decisiones de inversión y presupuestos de capital. Para lograr beneficio económico, la empresa

[67] Estado de Valor Añadido

debe alcanzar una rentabilidad superior a su coste de capital o coste promedio ponderado de los recursos que usa (deudas y fondos propios), Weston y Brigham (1994).

Respecto a la evolución del concepto estrategia, podemos citar a Andrews, (1971), aspectos conceptuales; Wing (1988), referenciado por Grant (2006) y Roger Evered (1983), término estrategia asimilado al arte de dirigir la guerra.

Los estudiosos de la estrategia han sido muchos. No obstante, resaltamos a los más importantes desde la década de los años cincuenta del siglo pasado, Penrose 1959; Andrews, 1977; Wernerfelt, 1984; Barney, 1991; Porter, 1980; Ansoff, 1991; Mintzberg, 1994; Teece et al.,1997; Grant, 2006; entre otros.

Desde la óptica de un análisis transversal, al desarrollo de la teoría de la estrategia se le han incorporado otros estudios que hacen de ella un cuerpo conceptual más estructurado; entre otras, se tienen la planificación corporativa, la evaluación de decisiones de inversión por medio de la técnica de flujos de caja, los conceptos microeconómicos, las previsiones econométricas, la teoría de juegos, las opciones reales, las teorías de la complejidad y del caos, la organización industrial, la teoría RBV[68], las organizacionales, las evolucionistas, las de contingencia, los costes de transacción y otras (Fernández, 1999; Robbins, 1999; Rialp, 2003; Short et al., 2008).

En base a la transversalidad, varias disciplinas convergen para tratar de entender la complejidad de las causas de los resultados empresariales, entre ellas la Administración, la Psicología, la Sociología, la Antropología, la Psicología Social, la Economía, las Finanzas y la Ciencia Política Menguzzato y Renau, 1991; Fernández, 1999.

El estudio de la estrategia, tiene dos enfoques: el de los factores externos o determinantes de la industria o las fuerzas competitivas (Porter, 1980, 1991); el de los aspectos correspondientes a la misma organización, a sus recursos y capacidades únicos y heterogéneos, los cuales deben orientarse según la estrategia a implementar, en un proceso de ajuste permanente, dadas la turbulencia del mercado y la competencia del sector (Penrose, 1959; Wernerfelt, 1984; Barney, 1991; Peteraf, 1993; Teece et al., 1997; Grant, 2006).

Según Hoskisson et al. (1999), el paradigma del enfoque externo o de las fuerzas competitivas presenta limitaciones, por no considerar suficientemente la inestabilidad del entorno y de la industria. Además, se ha criticado lo estático del modelo de las cinco fuerzas de Porter (1980). También se cuestiona por no considerarse el impacto en los bienes y servicios complementarios en el valor de un producto y la creación de redes de valor entre los competidores, en el fenómeno conocido como la co-opetencia[69] (Branderburger y Nalebuff, 1996; Baldwin et al., 2003; Grant, 2006).

Cada vez más trabajos han comprobado una mayor importancia a las estrategias empresariales (Demsetz, 1973; Schmalensee, 1985; Hill, 1988; Rumelt, 1991; González y Ventura, 2002; Spanos y Lioukas, 2004).

En el enfoque que busca las fuentes de las ventajas competitivas no externamente, sino al interior de la organización, se destaca la relevancia de los recursos y capacidades para crear,

[68] Esta teoría trata al conocimiento como un recurso genérico, en lugar de tener características especiales. Las tecnologías de la información pueden jugar un papel importante en la visión basada en el conocimiento de la empresa en los que los sistemas de información se utilizan para sintetizar, mejorar y acelerar a gran escala la gestión del conocimiento intra e inter empresa.

[69] Es la colaboración oportunista entre diferentes actores económicos que son además competidores (compartir más competir).

mantener y apropiarse de los beneficios potenciales que generan las ventajas competitivas sostenibles (Penrose, 1959; Wernerfelt, 1984; Barney, 1991; Peteraf, 1993; Teece et al., 1997; Grant, 2004).

Cada vez más autores comprueban una mayor importancia de las estrategias empresariales (Demsetz, 1973; González y Ventura, 2002; Rumelt, 1984; Schmalensee, 1985; Spanos y Lioukas, 2001). Entre esas estrategias se destacan dos: en primer lugar, el liderazgo en costes, buscando mayor productividad y eficiencia, para llegar al mercado con menores precios y/o maximizar los beneficios; de otro lado, la diferenciación en todas sus formas: por productos, nichos de mercado, publicidad, reputación de la firma, marcas, calidad, distinción tecnológica, investigación y desarrollo.

Las empresas pueden seguir varias estrategias y presentar estructuras híbridas y pueden incluir la diferenciación y su combinación con las de liderazgo en costes o enfoque, cuando el posicionamiento de la empresa, su capacidad de innovación y los volúmenes de la demanda justifiquen emplear tecnologías y economías de escala (Hill, 1988).

Es de amplia aceptación que, ante la mayor competencia global, la inestabilidad del entorno de los negocios y el acelerado desarrollo tecnológico, se hacen necesarios ajustes más rápidos en los recursos y capacidades de las organizaciones, para lograr procesos y productos más innovadores, así como alcanzar, mantener y apropiarse de los beneficios potenciales derivados de las ventajas competitivas (Penrose, 1959; Wernerfelt, 1984; Barney, 1991; Peteraf, 1993).

En las dos últimas décadas, las líneas del pensamiento sobre estrategia convergen a la perspectiva de su configuración y de las capacidades dinámicas teniendo en cuenta los permanentes cambios del entorno, las condiciones competitivas, la capacidad proactiva y de innovación empresarial, así como generando recursos y capacidades únicos y heterogéneos y ventajas competitivas sostenibles (Minztberg, 1994; Teece et al., 1997).

A nivel estratégico, los recursos productivos de la empresa se clasifican en físicos, financieros, tecnológicos, humanos y de capital organizacional, los cuales se integran en procesos y rutinas operativas y administrativas denominadas capacidades.

El término recurso fue utilizado inicialmente por Wernerfelt (1984), pero Edith Penrose (1959) fue pionera en el desarrollo de la teoría al establecer: Que una organización es más que una unidad administrativa, es también una colección de recursos productivos dispuestos entre los diversos usuarios y en un cierto plazo, dada una decisión administrativa. Cuando miramos el proceso de negocio de la empresa desde este punto de vista, el tamaño de la unidad económica es mejor calibrado a través de la medición de los recursos productivos que emplea.

Los recursos físicos que hacen referencia a tecnología física, planta y equipo, localización geográfica, acceso a materia prima, infraestructura en lotes y construcciones y otros factores que afectan el costo de producción. Los recursos financieros, considerados como fuentes para financiar las inversiones de la empresa, y provenientes de los fondos que se genera internamente, o de afuera, como el capital de los propietarios y los otorgados por terceros en forma de créditos (Weston y Brigham, 1994).

Entre los activos intangibles se tiene la marca, como valor y como potencial de ampliar los ingresos por los ámbitos de productos o mercados; la reputación, con relación a las relaciones con el cliente, la calidad de los productos, las relaciones con los proveedores y con otros entes; las patentes y propiedad intelectual en la que se apoya la protección legal del conocimiento y la generación de mayores ingresos, entre otros (Barney y Arikan, 2001; Grant, 2006).

Como recursos de capital humano, se cuenta con las personas que ejercen los distintos cargos de la compañía y sus competencias, entre otros: su grado capacitación, la experiencia, la forma de razonar y de tomar decisiones, el potencial de aprendizaje, la apertura al cambio, la capacidad de adaptación, habilidad de trabajo en equipo, las relaciones personales, el liderazgo, el espíritu emprendedor, así como aspectos sicológicos y sociológicos (Barney, 1991; Grant, 2006).

Este recurso, el capital humano, ha sido puesto en evidencia, al destacarse la importancia del capital humano genérico y específico del fundador y su impacto en el crecimiento de las PYMES, por Becker (1975), Colombo y Grilli, (2005), autores referenciados por Capelleras y Rabetino (2008).

La contribución de los recursos humanos de la empresa es difícil de valorar y tampoco aparece en sus balances; sin embargo, el desarrollo del sistema de competencias ha contribuido en parte a superar este problema, desarrollado por David McClelland, profesor de la Universidad de Harvard, según referencia de Grant (2006), por medio de la definición de los perfiles que debe cumplir un cargo específico.

Entre los recursos de capital organizacional, pueden incluirse la estructura organizacional, líneas de autoridad, los sistemas de información, la organización formal e informal, el control, la coordinación de sistemas; la forma como los empleados integran sus esfuerzos y habilidades, depende no sólo de sus habilidades personales, sino también del contexto organizativo. La cultura organizacional se relaciona también con los valores, tradiciones y normas sociales de la organización, y es considerado un recurso intangible clave y fuente fundamental de ventajas competitivas sostenibles (Barney, 1991; Grant, 2006).

Siguiendo a Burns y Stalker (1961), así como para Harrison (1987) y Rialp (2003), la estructura organizacional en la que se apoya la empresa para lograr las ventajas competitivas, debe ser de carácter orgánico-contingente, es decir, flexible para ofrecer los productos que se ajusten a los requerimientos de los ambientes dinámicos, con estructuras horizontales, altamente participativas, que motiven la creatividad, la innovación continua y la actitud proactiva corporativa; contraria a una estructura rígida, jerarquizada, altamente rutinaria, poco participativa y que no estimule el emprendimiento.

Respecto al concepto de capaciad, se debe advertir que los recursos aislados, no generan ventajas competitivas ni son productivos; como capacidades operativas y administrativas se consideran las formas en que los recursos interactúan, están integrados, organizados y se complementan en rutinas organizativas, compuestas por acciones secuenciales, estrechamente coordinadas sin necesidad de una especial dirección o comunicación verbal. (Nelson y Winter (1982). La rutinización, por tanto, es un proceso esencial en la transformación de propósitos y prácticas operativas y administrativas, incluso de alta dirección, en capacidades (Grant, 2006).

Las capacidades organizativas también se denominan competencias distintivas o esenciales o *Core Competences*, según el término usado por Hamel y Prahalad (1990). Para comprender la estructura y determinantes de las capacidades, así como su identificación, se pueden usar dos criterios: de un lado, el de capacidades funcionales, por las distintas áreas funcionales; en segundo lugar, el de las actividades de la cadena del valor, integrando actividades secuenciales, clasificadas a su vez en primarias (transformación de materias primas y relación con los clientes) y en actividades de apoyo. El análisis de capacidades se puede hacer en forma general o especializada y desagregada en niveles menores, generándose mayor dificultad

cuando se evalúan capacidades de más alto nivel y que requieren de la integración del conocimiento de los especialistas funcionales (Grant, 2006).

La estructura organizacional en la que se apoya la empresa para lograr las ventajas competitivas debe ser de carácter orgánico-contingente, es decir, flexible, para ofrecer productos que se ajusten a los requerimientos de los ambientes dinámicos, con estructuras horizontales, altamente participativas y con una comunicación abierta y clara que motive la creatividad y la innovación continuas; contraria a una de carácter mecánico, caracterizada por estructura rígida, jerarquizada, altamente rutinaria y poco participativa (Harrison, 1987).

## 4.3 RECURSOS Y CAPACIDADES COMO ACTIVOS INTANGIBLES Y SU IMPACTO EN EL VALOR DE LA EMPRESA.

Partiendo de la diferenciación y conceptualización de los activos intangibles, se explica su relación con los recursos y capacidades estratégicas que le generan ventajas competitivas a la empresa, dejando claro porqué éstos han tenido una importancia particular

Existen trabajos de investigación que han revelado que la valorización de numerosas compañías en el mercado bursátil, obedece a la habilidad que tienen de gestionar recursos fundamentales para la empresa, como los activos intangibles, los cuales se crean con la generación y estructuración de conocimientos tecnológicos, de mercado, administrativos, así como de derechos y propiedad intelectual, marcas, patentes, licencias, franquicias y otros (Carmeli y Tishler, 2004; García y Martínez, 2007; Flatt y Kowalczyk, 2008; Dedman et al., 2009) en la economía actual y en el análisis financiero.

Existe un gran seguimiento en la problemática de los intangibles desde el punto de vista contable y financiero por parte de investigadores, siendo la relacionada con el mercado de capitales la de mayor crecimiento en la última década (Giner, 2001; Moya et al., 2009); pero también se encuentra en la actualidad basta literatura, tanto teórica como proveniente de trabajos empíricos, en la que se señalan las deficiencias en los sistemas de contabilidad tradicionales y a los indicadores financieros resultantes en su análisis.

Un tema importante también es la incapacidad para considerar variables como el coste de oportunidad, el valor del dinero en el tiempo, el riesgo, el hecho de no considerar el coste de los recursos propios, así como el no disponerse de técnicas apropiadas para valorar los activos intangibles (Stickey y Weil, 1994; Amir y Lev, 1996; Aboody y Lev, 1998; Cañibano et al., 1999).

Existen trabajos importantes en valoración de activos intangibles que han dado sus frutos, debido a la importancia que los mercados de capitales le asignan al adecuado registro y revelación de éstos y del fondo de comercio. Debido a ello, a principios del siglo XXI ya se cuenta con la revisión de los Principios de Contabilidad Generalmente Aceptados- GAAP, produciéndose nuevas reglamentaciones plasmadas a nivel internacional y también para España (Giner y Pardo, 2007; Zeef, 2007).

En una nueva economía donde se ha evolucionado mucho, los sistemas contables también tienen que hacerlo, entendidos como conjunto de normas, principios generalmente aceptados y códigos de comunicación, son imprescindibles para las relaciones entre los usuarios externos e internos de la información que provee (Giner y Pardo, 2007; Zeff, 2007).

La medición del valor del Fondo de Comercio, los activos intangibles por separado, bajo diversas perspectivas presentadas por Lev (2001) y evaluar el impacto que tienen su registro y revelación, en los resultados empresariales, en el valor del mercado de la empresa, en el coste

de capital (Amir y Lev 1996; Aboody y Lev, 1998; Banham, 2005; García y Martínez, 2007; Jones, 2007).

La generación de valor en las empresas cotizadas por encima del valor de la contabilidad es una evidencia, la contabilidad que se emplea en las empresas registraban las actividades relacionadas con la creación de los activos intangibles, no como activos, sino como gastos o costes en las que incurren las mismas o a veces la contabilidad, deja a discreción de la administración y del conservadurismo que puede afectar la forma de registro y de invertir (Belkaoui, 1992; Goldfinger, 1997; Lev y Zarowin,1998; Lev, 2001).

## 4.4 LOS CRITERIOS PARA IMPLEMENTAR UNA ESTRATEGIA

Partimos de la heterogeneidad de recursos es una condición empresarial para sostener ventajas competitivas (Barney, 1991; Peteraf, 1993). Es necesario disponer de recursos distintivos, que sean estratégicos o esenciales, es decir que cumplan los criterios de ser valiosos, escasos y difíciles de imitar o de sustituir, como la reputación de la firma, las patentes y conocimientos únicos y las tecnologías especializadas, entre otros; con ellos la empresa podrá obtener una ventaja competitiva sostenible y generar el potencial de beneficios.

La implicación de la alta dirección con estos criterios dificulta que otras empresas puedan replicar e implementar la estrategia explotando las oportunidades del entorno de la misma forma (Barney, 1991; Peteraf, 1993; Teece et al., 1997; Grant, 2006). Para la empresa, es necesario poseer recursos superiores y lograr de ellos una eficiencia para mejorar la productividad y competitividad, lo que sucede cuando se usa el mínimo de recursos para un nivel de operación determinado, o se obtiene el máximo de resultados de un nivel dado de recursos. Igualmente, se debe buscar la posibilidad de emplear los recursos existentes en usos más rentables (Peteraf, 1993; Grant, 2006).

Ante el objetivo de generar potencial de beneficios, se requiere que los recursos sean escasos, que no abunden en el sector o sean fácilmente adquiribles. Pero no se trata sólo de que estén disponibles, sino también que no estén al acceso de todas las organizaciones que los requieren. Relevantes, es decir que se relaciones con los factores claves de éxito explicados con anterioridad.

El termino competitividad puede ser entendido como la capacidad de una empresa para integrarse de manera permanente a procesos de cambio e innovación, considerando en su quehacer empresarial, aspectos sociales y ambientales; logrando con ello mantenerse y sobresalir en un mercado global, a través de un desarrollo sustentable, mediante la creación de productos de valor. (Sarmiento, Sánchez y Cruz, 2009).

Siguiendo a Sáez de Viteri (2000) la ventaja competitiva se identifica con la capacidad de responder a la demanda e incrementar los niveles de rentabilidad, y que asentándose en competencias individuales, sea capaz de provocar mercados de competencia imperfecta a largo plazo, convirtiéndola así en una ventaja competitiva sostenida, logrando con ello que la empresa realice una estrategia de creación de valor que no esté siendo implementada por ninguno de sus competidores actuales o potenciales y que estos sean incapaces de imitarla. López y Pontet, (2011) afirman que “la ventaja competitiva sostenible deberá combinar los factores basados individualmente entre recursos propios e institucionales en él, y como empresas la relación entre estas y el entorno institucional” explicado como el resultado de la correlación entre gestión, y acumulación de recursos, e impacto de las estrategias implementadas en el sector y el mercado; capacidad de personalización; capacidad de configuración.

Una empresa no genera una mayor ventaja competitiva al tener más recursos, más bien se relaciona con la calidad de estos, en otro enfoque se puede decir que no todos los recursos son fuente de ventaja competitiva ni crean un valor adicional. Un recurso valioso debe ser demandado por los clientes, debe ser de oferta limitada; sin embargo, aunque "las fuentes de ventaja competitiva radican en los recursos, si esto no es traducido en la realización de mejores actividades nunca se logrará desarrollar una ventaja competitiva". Las ventajas competitivas percibida se ven influenciadas en función de las capacidades de personalización masiva y las capacidades de reconfiguración, ya que es lo que permitirá la implementación eficiente de las actividades producidas Maynes et al.(2013).

De durabilidad en el tiempo, acorde a los avances tecnológicos, lo cual muchas veces acorta el ciclo de vida de los recursos; también se prolonga, como puede ser el aumento de la reputación de la empresa, mientras no suceda algo no normal que la afecte, como una defraudación, problemas masivos de calidad, impactos negativos ambientales, seguridad de la información, entre otros.

Que no sean fáciles de adquirir en el mercado o de transferirse entre empresas, porque se pierden las ventajas. Los siguientes aspectos fortalecen el cumplimiento de este criterio: la inmovilidad geográfica; la información imperfecta respecto a la calidad y productividad de los recursos, ante lo cual sus oferentes tienen mayores ventajas que los demandantes; la complementariedad entre ellos; el tratarse de capacidades organizativas, menos transferibles que los recursos individuales, por la integración de rutinas y procesos en que están estructuradas.

Difícil copia por parte de la competencia, cuando no pueden adquirirse, o si lo hacen, mantener la ventaja en eficiencia y en costes, por las curvas de aprendizaje que le dan una fortaleza a la empresa que los posee o desarrolla inicialmente.

Identificar los recursos que son relevantes y distintivos a los de la competencia. Realizar su valoración, en función de los factores claves de éxito, diagnosticando sus fortalezas claves y debilidades claves, así como los que no son tan relevantes. No se trata sólo de hacer clasificaciones, se requiere el análisis profundo de los criterios señalados, el intercambio de distintos puntos de vista y realizar procesos de benchmarketing[70], para tener referencias de mejores prácticas.

Reproducir recursos y capacidades para el desarrollo de otros productos o mercados, adquirirlos, desarrollarlos y en casos en los que se detectan debilidades claves, potencializar la generación de beneficios con base en ellos o abandonarlos. La subcontratación de actividades en las que no se es eficiente o no son *core* del negocio, las alianzas, fusiones, adquisiciones, la incubación interna, mejoras incrementales, entre otras, son alternativas para avanzar en este proceso, el cual requiere de horizontes de largo plazo para concretar resultados.

Ajuste permanente de los recursos y capacidades, de acuerdo a las oportunidades del mercado y los cambios del entorno.

Estimación de los recursos y capacidades y su cuantificación, por medio de un proceso adecuado de planeación financiera, necesario para la implementación y puesta en marcha de la estrategia, el cual se describe a continuación (Cardona, 2010).

[70] El benchmarking implica aprender de lo que está haciendo el otro y adaptar sus propias prácticas según lo aprendido, realizando los cambios necesarios.

En relación con la planificación financiera, una de las definiciones más ajustadas a su significado la brinda Ortega (2008): "Es un proceso virtual del cual se proyectan y se fijan las bases de las actividades financieras con el objeto de minimizar el riesgo y aprovechar las oportunidades y los recursos". Cada vez más, en el entorno empresarial, ha ganado relevancia el conocimiento de las teorías de las finanzas corporativas relacionadas con la planificación financiera de la empresa, la realización de los presupuestos y las proyecciones de los estados financieros (estados contables previsionales), para un horizonte similar al que se tiene en cuenta a la hora de definir la planificación estratégica, los recursos y las capacidades para alcanzar los objetivos propuestos; éstos son el estado de ingresos y gastos o estado de resultados, el balance general y los flujos de caja (Ortega, 2008; Ramírez, 2002; Vélez, 2004).

El flujo de caja se ha convertido en una herramienta fundamental para la medición del objetivo financiero. En la mayoría de textos financieros se define como "incrementar la riqueza de los accionistas o el valor de la compañía" (Weston y Brigham, 1994).

Para Ramírez (2002), la planificación financiera consiste en el proceso de estimación de los distintos recursos necesarios, de las inversiones o el presupuesto de capital, de las proyecciones de las ventas, costos y gastos, la cuantificación de los flujos de financiación y el reparto de dividendos; se parte de la visualización que la empresa debe hacer de los objetivos organizacionales y los recursos necesarios a corto, mediano y largo plazo.

Los proyectos son las ideas que pretenden implementarse, lo que involucra los procesos de innovación en todas sus formas, denominadas como destrucción creativa por Schumpeter (1934), entre otras: tecnologías, materias primas, procesos, bienes de capital, bienes y servicios, mercados, estrategias organizacionales, etc.

El crecimiento de una compañía y su capacidad de permanecer competitiva depende de la cantidad de ideas que al implementarse agreguen valor y generen una rentabilidad adecuada, Brigham y Houstom, (2005).

La teoría financiera dispone de indicadores, uno de ellos es la estimación del valor presente neto (VPN) que debe ser positivo, lo que significa que los flujos de caja resultantes, después de descontados o traídos al presente, recuperan la inversión y agregan valor Brealey y Myers, (2006).

Los pasivos, junto con el coste de las fuentes después de impuestos y de los recursos propios, dada la participación de ambos en el total del activo, determinan el coste de capital de la empresa. Explícitamente, el costo de capital se define como el costo promedio ponderado de las fuentes que financian el activo de la compañía (CPPC En inglés, Weight Average Capital Cost (WACC), siguiendo a Weston y Copeland(1995).

Al unir la planificación estratégica con la elaboración presupuestaria de la compañía, a corto, mediano y largo plazo, las decisiones financieras se reflejarán en los estados financieros previsionales y en especial del estado de flujo de efectivo Ortega, (2008); Ramírez (2002).

La publicación del trabajo de Wernerfelt (1984) y de Barney (1991), fueron pioneros, más tardes aparecieron otros con otros enfoques en la teoría de recursos y competencias, *core competences*, capacidades dinámicas, teoría organizacional contingente, gestión humana, calidad total, capital intelectual, capacidades de innovación, entre otras, Lockett et al., (2008); Acedo et al., (2006); a su vez, la gestión del conocimiento, y las condiciones para convertir el conocimiento tácito a explícito, tienen un alto impacto en el desarrollo de capacidades superiores, Nonaka y Takeuchi, (1999).

La globalización, el acelerado desarrollo tecnológico, la acumulación de conocimientos en todas las áreas del saber, los cambios sociales, hacen que las organizaciones y los individuos enfrenten los nuevos retos de generar y gestionar el conocimiento para crear nuevos bienes y servicios, producir con nuevas tecnologías, de aceptación en el mercado y que puedan ser explotados comercialmente, Nelson y Winter (1982).

La teoría de las capacidades dinámicas establece que la empresa podrá incrementar su potencial de generación de beneficios, si logra formas distintivas para desarrollar recursos y capacidades, configurar estrategias, acelerar la discontinuidad de las mismas y dirigir las estrategias de una manera contingente, Mintzberg (1994), Peteraf(1993); Hamel y Prahalad(1994); Teece et al., (1997); Grant(2006). A esto se le incorpora que se integre un proceso de planeación financiera, para disponer de recursos financieros para implementarlas, al menor costo posible, Ortega (2008); Cardona(2010).

Los estudios de los impactos de la estrategia en las organizaciones deben realizarse en forma transversal, incorporado otras disciplinas en el análisis y haciendo del campo de estudio un cuerpo conceptual más estructurado; La planificación corporativa, la evaluación de decisiones de inversión, la teoría de los recursos y capacidades, las teorías organizacionales evolucionistas y de contingencia, los costos de transacción, los conceptos microeconómicos, las previsiones econométricas, la teoría de juegos, las opciones reales, la valoración de activos intangibles, la organización industrial y otras, Fernández (1999); Robbins (1999); Rialp(2003); Short et al.(2008).

## 4.5 ENFOQUE ESTRUCTURAL Y TEORÍA DE LOS RECURSOS Y CAPACIDADES

El enfoque estructural se enmarca en las formulaciones teóricas elaboradas alrededor de la Teoría de la Organización Industrial sintetizadas en el paradigma clásico *Estructura-Comportamiento-Resultados*, las cuales en la década de los ochenta del siglo pasado cobran gran impulso a partir de la amplia divulgación de la obra de Porter: C*ompetitiveStrategy*.

El autor sugiere que las diferencias de beneficios entre las empresas se explican fundamentalmente en función de cinco factores externos de naturaleza sectorial relacionados con las distintas estructuras en que compiten las industrias: la intensidad de la rivalidad entre los competidores actuales, la presión de productos o servicios sustitutos, el poder de negociación de los compradores, el poder de negociación de los proveedores y la amenaza de ingreso de nuevos competidores, Porter(1985). O sea, que en esta perspectiva se considera que las acciones estratégicas de las empresas están condicionadas en mucha mayor medida por el entorno externo que por las elecciones que los administradores pueden hacer basándose en el potencial de los recursos y capacidades internos de la organización.

Este enfoque de la Teoría de la Organización Industrial se fundamenta, entre otros aspectos, en las siguientes suposiciones subyacentes: El ambiente externo ejerce presiones e impone limitaciones que inciden en forma decisiva en la configuración de las estrategias empresariales; Las fuerzas competitivas predominantes son las que determinan la rentabilidad empresarial; La mayor parte de las empresas que compiten en un sector en particular, o en uno de sus segmentos, controlan recursos estratégicamente relevantes similares y siguen, con base en ellos, estrategias parecidas.

La movilidad de los recursos entre las empresas permite que cualquier diferencia existente entre las compañías sea breve. Se considera que quienes toman las decisiones lo hacen racionalmente y están comprometidos a actuar en beneficio de la organización, como lo

demuestran sus conductas dirigidas a maximizar utilidades. Por consiguiente, en primera instancia el desafío de La firma se centra en encontrar la industria más atractiva en la que va a competir, con potencial de beneficios más elevado para poner en práctica la estrategia que responda a las características del entorno en que se desenvuelve.

Sin embargo, en los últimos años de la década de los ochenta y principios de los noventa del siglo pasado, en trabajos como los de Cubbin y Geroski (1987), Jacobsen (1988), Hansen y Wernerfelt (1989) y Rumelt (1991) en la práctica se observó que aún en el caso de empresas situadas en el mismo entorno competitivo, en las que la influencia de los factores externos era muy similar, y por tanto con iguales expectativas de rentabilidad, los resultados económicos diferían sustancialmente. Por lo tanto, consideraron que la respuesta a estas diferencias residía en los aspectos propiamente empresariales.

En este contexto, paulatinamente resurgió nuevamente en la literatura sobre dirección estratégica un especial interés en el examen de los factores internos para explicar el origen de los distintos niveles de rendimientos alcanzados por las empresas en el largo plazo, dando lugar a una renovada perspectiva a la que se le denominó Teoría de Recursos y Capacidades y en la que se plantea que la principal fuente de ventaja competitiva se deriva del potencial de los recursos y capacidades internos. Luego, si los recursos y capacidades son la clave para competir con éxito en el mercado, entonces lo relevante no es *dónde* se compite, sino *cómo se compite*.

La Teoría de Recursos y Capacidades considera que cada organización se constituye por un amplio y diferente conjunto de recursos y capacidades tanto físicos como intangibles, no existiendo por consiguiente dos compañías idénticas, por no ser posible que a lo largo de su historia dos empresas hayan acumulado las mismas experiencias, adquirido recursos semejantes, desarrollado iguales habilidades y construido la misma cultura organizacional. Desde esta perspectiva, son los recursos y capacidades internos los que van a permitir a las firmas disfrutar de una ventaja competitiva, y, en consecuencia, de corrientes de rentas sostenidas en el largo plazo.

Con una perspectiva diametralmente opuesta al enfoque estructural, la Teoría de Recursos y Capacidades esencialmente se sustenta en las siguientes cuatro hipótesis: Los recursos y capacidades de la empresa proporcionan la dirección básica de su estrategia; Los recursos y capacidades constituyen la fuente primaria del beneficio empresarial (Grant, 1991); Las empresas de una industria pueden ser heterogéneas con respecto a los recursos y capacidades que poseen y controlan.

Esta hipótesis implica el considerar que cada empresa es una colección de activos única debido a su historia particular que la ha llevado a implementar combinaciones de recursos diferentes a las utilizadas por Los recursos de la empresa pueden no ser perfectamente móviles (imperfecta movilidad) a través de las empresas por lo que esta heterogeneidad pude ser duradera en el tiempo, Barney(1991). Ello posibilita el sostenimiento de las ventajas diferenciales y, por consiguiente, de los mayores beneficios obtenidos. Lo anterior implica aceptar que el mercado es ineficiente asignando los recursos de la economía. Si éste funcionara perfectamente, la imitación competitiva conduciría a la homogenización en las dotaciones de activos de las empresas en el largo plazo.

En sentido amplio los recursos se identifican con el stock disponible de factores productivos, no necesariamente tangibles, que la empresa posee o controla, independientemente de que tenga sobre ellos derechos de propiedad. En cambio, las capacidades se refieren a las

habilidades de una empresa para el despliegue coordinado de recursos para el logro del fin deseado.

O bien, a las habilidades en *saber hacer* y los conocimientos idiosincrásicos y tácitos que poseen la organización y sus miembros para el despliegue coordinado de recursos que encierran aptitudes especiales para desarrollar sistemática y eficazmente actividades (entendidas como categorías de problemas dados) que permiten la consecución de ciertos objetivos, Camisón(2002). Ahora bien, aunque en la literatura sobre el tema suele distinguirse entre los recursos propiamente dichos y las capacidades, con frecuencia ambos conceptos suelen emplearse indistintamente o bien, se utilizan los términos "recursos" o "activos" como nociones genéricas para referirse a ambos. Incluso, algunos autores consideran como irrelevante esta separación.

## 4.6 ACTIVOS TANGIBLES E INTANGIBLES.

Bajo la perspectiva de la Teoría de Recursos y Capacidades, se considera que no todos los activos de la organización, los cuales suelen clasificarse en tangibles e intangibles, tienen igual potencial para generar rentas sustentables. Son primordialmente los activos intangibles los impulsores clave del proceso de creación de valor.

Con el concepto de activos tangibles se identifica a los que tienen una expresión material en forma de elementos productivos de la empresa en los cuales podemos distinguir el capital físico: terrenos, edificaciones, maquinaria, equipo, materias primas, etc., y el capital financiero: el dinero, valores, créditos y cuentas por cobrar, entre otros. Estos activos son perfectamente identificables ya que aparecen en el balance contable de cualquier organización.

Evidentemente, el papel de los activos tangibles es relevante para el desarrollo de cualquier actividad productiva y cada negocio procurará dotarse de ellos en grado suficiente tanto en calidad como en cantidad. Pero, el hecho de que parte de ellos se deprecien conforme se utilizan y el que por su naturaleza material la competencia los pueda identificar, cuantificar y replicar con mayor facilidad, hace que no contribuyan plenamente a la creación y sostenibilidad de ventajas si pensamos en términos de competitividad y futuro de la organización. Sin embargo, pese a la superioridad atribuida en este enfoque a los intangibles como fuente de ventajas competitivas sostenibles, tampoco se pretende afirmar que los activos tangibles carecen de importancia o de efectos sobre la competitividad empresarial puesto que la inversión en intangibles no se transformará en productiva a no ser que vaya acompañada por una inversión en recursos físicos.

Por otra parte, la división entre tangibles e intangibles permite reflejar el hecho de que éstos últimos representan en cierta medida la diferencia entre el valor estrictamente contable de la empresa, es decir el valor de sus inversiones o propiedades, y el valor de mercado de la misma (Asset Equity Company, destacada empresa norteamericana dedicada a la consultoría en inversiones, señala que en 1985 el valor en libros de los activos tangibles representaba en promedio un 50% del valor de mercado de las empresas. En el año 2000, quince años después, este porcentaje había descendido a un 20%. El 80% restante era atribuido a los activos intangibles de las compañías. Igualmente, D. J. Skyrme (1997), investigador y consultor en gestión del conocimiento, estimó que en junio de 1997 la relación del valor de mercado al valor en libros para todas las empresas en el Dow Jones Industrial fue de 5.3. En cambio, en varias compañías intensivas en conocimiento (por ejemplo,Microsoft y empresas farmacéuticas) la relación alcanzó un valor de 10.0.

Los activos intangibles comprenden el conjunto de activos de una organización que, no obstante, al no encontrarse la mayoría de ellos reflejados en los estados financieros tradicionales, están generando valor en la actualidad o tienen el potencial para crearlo en el futuro, Osorio(2007). Son el resultado de la incorporación a los procesos operativos internos de la empresa de la información y el conocimiento y del despliegue de la red de relaciones con el exterior y de las capacidades organizativas y de innovación. Entre las cualidades relevantes que los caracterizan se encuentran las siguientes: Los activos intangibles, principalmente las capacidades, se construyen y acumulan a lo largo del tiempo, a partir de la experiencia de la empresa; A diferencia de los activos físicos que se deprecian por razones de obsolescencia o por su empleo, los activos intangibles son factores factibles de utilizarse sin merma de su valor, e incluso, algunos de ellos incrementan su nivel de dotación.

La clave de esta variación está en su carácter intrínseco de "learning by doing", es decir, su receptividad a procesos de aprendizaje mediante la repetición y la experimentación; Son activos de adquisición compleja poco asequibles en el mercado. Su alto grado de especialización e individualidad (si el intangible es humano) alcanzado como resultado de paulatinos y prolongados periodos de acumulación y su explotación conjunta con diversos recursos e interconexión con diferentes áreas de la empresa dificultan su transferencia, comercialización y sustituibilidad por otros activos alternativos. Constituyen en algún grado un factor de supresión de la concurrencia al originarse al interior de la empresa y al limitar su uso a terceros; Generan relevantes externalidades y sinergias.

La creación de valor sustentada en los activos intangibles difiere en diversos aspectos de la generación de valor basada en la gestión de activos tangibles físicos y financieros, Kaplan y Norton (2004): La *creación de valor es indirecta*. Por lo general, los activos intangibles no inciden directamente en los resultados financieros como mayores ingresos y utilidades y menores costes. El desarrollo de activos intangibles influye en los resultados financieros a través de las relaciones causa-efecto; El *valor es contextual.* El valor de un activo intangible depende de su alineación con la estrategia; El *valor tiene un carácter potencial*. El costo de invertir en un activo intangible no es representativo de su valor para la organización; Los *activos están asociados.* Los activos intangibles rara vez producen valor por sí mismos, no poseen un valor que se pueda disociar del contexto y la estrategia de la organización. Sólo en combinaciones eficientes con otros activos, tanto tangibles como intangibles, surge este valor.

A este conjunto de activos intangibles, no incluidos normalmente en los estados financieros de la empresa en forma separada, que no cumplen con los criterios de reconocimiento establecidos por las normas contables, pero con capacidad para generar beneficios económicos suele identificarse con el término genérico de "capital intelectual". Término que no siempre tiene el mismo significado para todos los estudiosos del tema así como en lo relativo a las categorías de activos intangibles comprendidas en esteConcepto Capital intelectual como sinónimo de capital humano, de capital de conocimiento, de activos ocultos, de fondo de comercio, de competencias básicas distintivas de naturaleza intangible, siguiendo a Monserrat y Rojo(2003) con el cual se pretende resaltar la esencia de su naturaleza, en especial de aquellos que se consideran clave para la obtención de rendimientos superiores al promedio.

## 4.7 LA GESTIÓN DEL CAPITAL INTELECTUAL

El proceso de dirección estratégica comprende, en términos generales, las fases de definición de la visión y la misión que constituyen el marco empresarial en el cual el sistema de objetivos se desarrollará, el análisis interno y externo, los objetivos estratégicos, la determinación de las acciones estratégicas, su implantación y la medición y evaluación de resultados.

Bajo la perspectiva de la Teoría de Recursos y Capacidades y a partir de los objetivos estratégicos fijados, los cuales constituyen la plataforma base para la configuración de las estrategias, se requiere precisar, además de los tradicionales indicadores financieros de resultados, los intangibles críticos cuyo mantenimiento, desarrollo, adquisición, medición y control es fundamental para el logro de los objetivos estratégicos dado que son los impulsores clave del proceso de creación de valor. Lo anterior, para estar en condiciones de derivar las actividades intangibles y los indicadores específicos que se utilizarán en la medición de cada intangible.

Habitualmente, las actividades de identificación, medición y seguimiento de intangibles conforman lo que se denomina "gestión del capital intelectual" o "gestión de activos intangibles", las cuales se detallan a continuación.

Primero, identificación de los intangibles:

Esta fase comprende el identificar los intangibles vinculado con los objetivos estratégicos. Como resultado de esta etapa, la organización deberá contar con una idea clara de los *intangibles críticos* que pueden ayudar a la empresa a mantener o aumentar su ventaja competitiva y, consiguientemente, a alcanzar sus objetivos estratégicos, de las acciones o actividades intangibles que implican la asignación de recursos destinados a adquirir o desarrollar nuevos activos intangibles, mejorar o aumentar el valor de los ya existentes y evaluar y controlar tales acciones. Por ejemplo, las actividades intangibles de formación de personal para mejorar el capital humano, las inversiones en I+D dirigidos a fortalecer las capacidades tecnológicas dentro del capital estructural o las tareas específicas de marketing para fidelizar a los clientes y perfeccionar el capital relacional.

La última hipótesis del armazón conceptual de la Teoría de Recursos y Capacidades mencionada en páginas anteriores, y referida a las posibilidades de mantenimiento de la heterogeneidad entre las empresas en el largo plazo, constituye una condición necesaria para responder a la pregunta relativa a qué características deben tener los activos con mejor potencial de generación de rentas sustentables, pues no todos son igualmente estratégicos para la consecución del éxito. A partir de las aportaciones de Barney(1991), Amit y Schoemaker (1993) y Grant (1995) se establece que los recursos de la empresa que soportan su ventaja competitiva deberán reunir ciertos atributos para considerarlos estratégicos o competencias distintivas, como el ser valiosos, escasos, imperfectamente imitables e imperfectamente sustituibles.

Los activos valiosos son aquellos que permiten a una firma generar, implementar y ejecutar estrategias que mejoren su eficiencia o eficacia. En cuanto a su escasez ésta pude venir propiciada por dos motivos: a) que se trate de recursos con una oferta fija, en cuyo caso generarían rentas ricardianas[71], o con una oferta cuasi fija en el sentido de que su oferta no puede expandirse en el corto plazo y a los cuales solamente tienen acceso unos cuantos de los competidores actuales o potenciales; y b) que se trate de recursos con una oferta deliberadamente limitada que generarían rentas de monopolio.

Para que las rentas sean sustentables en el tiempo se requiere que haya límites a la competencia, límites que se concretan por medio de dos mecanismos: la imitabilidad

[71] Es un modelo económico relacionado con el comercio internacional, introducido por David Ricardo para explicar el patrón y las ganancias del comercio en términos de ventaja comparativa, supone una competencia perfecta y un único factor de producción, generalmentela mano de obra. Otro estudio sobre los modelos relacionados con la economía internacional, lo tenemos en el teorema de Heckscher y Ohlin. El contexto teórico es muy distinto al que estamos analizando en este tema.

imperfecta y la sustituibilidad imperfecta. Las dificultades de imitación se pueden derivar de su carácter único por encontrase fuera del alcance de los competidores como una localización excepcional o ser resultante de trayectorias históricas y desarrollos de mediano y largo plazo como pueden ser reputación, imagen, contratos y relaciones exclusivos, las patentes debidamente protegidas, marcas registradas, el dominio de una tecnología, la acumulación a lo largo del tiempo del conocimiento individual y colectivo mediante un proceso de aprender haciendo y el aprendizaje organizativo, Thompson y Strickland (2004).

Asimismo, la disuasión económica supone enviar claras señales amenazadoras a los competidores que les hagan pensar que una estrategia de imitación no les será beneficiosa. La disuasión pude tener buenos resultados especialmente cuando la empresa tiene una reputación en el mercado avalada por su historia, Fernández, (1999). O bien, por la ambigüedad causal, cuyo término se emplea para reflejar el desconocimiento que tienen los agentes económicos sobre las causas que conducen a la obtención de una ventaja competitiva sostenible. Las empresas, a medida que usan sus capacidades, éstas se fortalecen y adquieren una superior complejidad, acrecentando el nivel de ambigüedad causal y dificultando a los competidores su comprensión e imitación.

En la medida en la que la ventaja competitiva de una firma tenga más dimensiones y cada una de ellas tenga su base en capacidades complejas, será arduo para un agente económico definir los determinantes del éxito, González y Nieto(2005). La ambigüedad causal no solo impide la imitación externa, también explica por qué algunas compañías tienen dificultades para identificar los mecanismos y recursos que sostienen una determinada posición competitiva con la consecuente inhibición de la difusión de rutinas en el interior de la organización, Fernández(1999).

En lo relativo a la sustituibilidad imperfecta implica que no existan activos estratégicamente equivalentes, entendiéndose por equivalentes aquellos que permiten a los competidores implementar las mismas estrategias, aunque de una forma distinta, utilizando para ello recursos o capacidades diferentes.

En segundo lugar, respecto a la medición: los sistemas tradicionales de medición del rendimiento, basados en la contabilidad financiera, dominan tanto la evaluación externa de las empresas como las evaluaciones internas de directivos y unidades de negocio. El problema de tales mediciones reside en el hecho de que estas herramientas no capturan el valor del capital intelectual.

La literatura sobre el tema ha sugerido una serie de alternativas para su medición como son las de tipo genérico que valoran el capital intelectual mediante la estimación de la diferencia entre el valor de mercado y el valor en libros de una empresa (fondo de comercio). O bien, utilizando una serie de indicadores vinculados con los objetivos estratégicos que permitan hacer un seguimiento de las variaciones en los diferentes elementos constitutivos del capital intelectual. Con relación a ello, uno de los retos más importantes a los que se continúa enfrentando este enfoque de competitividad es la construcción de procedimientos adecuados de medición de intangibles, de sistemas de valoración constituido por indicadores relevantes, significativos, comprensibles, comparables, flexibles y dinámicos.

Un indicador es relevante cuando proporciona información que permita modificar o confirmar las expectativas de quienes toman las decisiones. Significativo si la información que suministra está vinculada con los intangibles críticos, a las características de la empresa que ayuden a entender su proceso de creación de valor. Comprensible si está calculado y formulado de forma tal que puede ser fácilmente entendido por sus usuarios potenciales. Comparable si está

preparado y expuesto siguiendo criterios homogéneos internos en forma tal que sus usuarios estén en condiciones de efectuar las comparaciones necesarias. Flexible y dinámico si refleja los cambios y los efectos en el aprendizaje de la organización.

Entre los principales actores interesados en la medición de los activos intangibles se pueden distinguir dos grupos: el primero constituido por el personal de la empresa a cargo de la formulación ejecución y control de los procesos de dirección estratégica, en este caso evaluando cómo influyen los *intangibles críticos* en los resultados empresariales. El segundo, por los llamados *steakeholders*: accionistas, inversionistas, clientes, proveedores, gobierno, opinión pública en general, etcétera. Para ellos, cada vez un mayor número de empresas elaboran informes anuales de capital intelectual con la finalidad de transmitir una imagen de mayor transparencia en la magnitud de su patrimonio real y en los resultados logrados y para proporcionar una visión ampliada del conjunto de intangibles con que cuenta. Vinculando éstos esfuerzos con el concepto de capital intelectual, lo que se busca con tales informes es aumentar el denominado capital relacional.

En tercer lugar, respecto al seguimiento y acción,esta fase constituye la consolidación del sistema de gestión de los intangibles y su integración con las rutinas empresariales. Comprende la evaluación de la situación del capital intelectual, de los resultados logrados y los efectos de las distintas actividades realizadas para el desarrollo, adquisición y aumento de valor de los intangibles. Se podría afirmar que en la medida en la cual, las tareas de seguimiento y acción estén más integrados en las rutinas de la organización, más fortalecido estará el proceso de gestión de los intangibles.

Los modelos de capital intelectual son instrumentos empleados para la medición y gestión de activos intangibles de la empresa. Dado que estos modelos se han desarrollado asociados a la estrategia corporativa de la organización que lo implementó y, consecuentemente se ajustan a una realidad concreta en la cual se concederá distinta importancia a los diferentes elementos que contemple, no existen modelos normalizados y universales de capital intelectual equiparables a los modelos contables que pudiesen ser aplicados a todas las empresas (Sánchez, 2006). Por tal razón existen y continúan desarrollándose un significativo número de modelos para la medición y gestión del capital intelectual entre los que destacan el *Navegador de Skandia*, el *Monitorde Activos Intangible,* los Modelos *Intellectus* y Technology Broker y el *Cuadro de Mando Integral* (*Balanced Scorecard).*

La multinacional sueca Skandia, dedicada a los seguros y servicios financieros, dio a conocer en 1995, a través de su Informe Anual, los significativos avances en la investigación del capital intelectual. Desde 1991, bajo la dirección de Lieff Edvinsson, esta compañía ha venido realizando estudios sobre los componentes del capital intelectual con la idea de que el verdadero valor del rendimiento de una firma está en su capacidad para crear valor sostenible.

Como punto de partida el equipo de investigación de Skandia consideró como un absurdo el que inversiones realizadas que le habían permitido elevar su nivel de competitividad como es la formación de recursos humanos y los servicios al cliente, en el corto plazo incidían desfavorablemente en su estado de pérdidas y ganancias, lo cual a la vez reducía el valor del balance, y, por ende, el valor en libros de la empresa. Esto se vio reforzado por la creciente diferencia que normalmente se produce entre el valor de mercado de una compañía y su valor en libros.

En función de lo anterior, el enfoque de Skandia tiene como origen el considerar que el valor de mercado de una empresa se integra por el capital financiero y unos valores ocultos que, en su conjunto, denominó capital intelectual conformado por los capitales humano y estructural

marco que sirve de base para la delimitación de las áreas fundamentales sobre las cuales dirigir la identificación de indicadores y su medición.

Además, con el modelo de Skandia se propone un sistema de gestión denominado *Navegador* con la idea de incorporar en el proceso la variable "tiempo". Navegador que se integra por cinco áreas de enfoque: enfoque financiero, de clientes, de procesos, de renovación y desarrollo y humano con sus correspondientes indicadores de medición; en las que la empresa concentra su atención y de las cuales proviene el valor del capital intelectual dentro de su entorno competitivo. Modelo que no obstante referirse al sector de servicios financieros y de seguros puede servir de punto de partida para empresas de otras actividades económicas (CIDEC, 2007).

Valor de mercado= (Capital financiero+Capital intelectual)

Capital Intelectual= (Capital humano+Capital Estructural)

Capital Estructural= (Capital Clientela + Capital Organizacional)

Capital Organizacional= (Capital Innovación+ Capital Proceso)

En el modelo Skandia se resalta la importancia de enriquecer el capital intelectual con información financiera tradicional mediante indicadores significativos para captar los activos realmente valiosos. En consecuencia, desde el enfoque financiero se pretende realizar diversos análisis y generar indicadores de capital financiero, válidos, precisos y de amplio alcance que sirvan para evaluar la marcha de la empresa.

## 4.8 LA SEGURIDAD DE LA INFORMACIÓN UNA VENTAJA COMPETITIVA

Enlazando con el apartado anterior, en este apartado se aporta una visión general de los aspectos más significativos de la seguridad de la información que incide en la importancia de su aplicación en la empresa, para proteger la información como activo estratégico, como activo intangible crítico de la misma. Los sistemas de gestión de seguridad de la información son activos intangibles críticos que afectan al personal de la empresa y a los stakeholders, donde se pone de manifiesto la teoría de los recursos y capacidad que hemos relacionado a lo largo de este capítulo y que están vinculados al capital intelectual.

En un entorno competitivo y cambiante como el actual, toda empresa con visión de futuro sabe que ha de valorar y proteger sus activos más importantes, como son sus trabajadores cualificados, implicados en la capacidad interna, su know-how, su tecnología, sus bienes e inversiones, sus clientes y proveedores, y por supuesto, su información, esencial para mantener su competitividad, rentabilidad e imagen en el mercado, según San Martín, J.M. (2004).

Por ello, que se puede afirmar que aquellas empresas que protegen la información de forma adecuada disponen de una ventaja competitiva clara frente a otras que no lo hacen.

En la Norma de Seguridad de la Información UNE-ISO/IEC 17799, "La Información es un activo que, como otros activos importantes del negocio, tiene valor para la empresa y requiere, en consecuencia, una protección adecuada. La seguridad de la información protege a ésta de amenazas, para asegurar la continuidad del negocio, minimizar los daños a la empresa y maximizar el retorno de las inversiones y las oportunidades del negocio".

Actualmente, todos somos conscientes de que Internet ha cambiado el mundo. Existen en nuestro entorno de negocios una serie de factores que están influyendo en la aparición de nuevos hábitos empresariales. Así, el enorme desarrollo de los sistemas de información y de las comunicaciones, y sobre todo, la gran proliferación del uso de la banda ancha en Internet como medio gratuito y de acceso universal por excelencia, pero a la vez inseguro, unido al aumento de la movilidad y dispersión de usuarios y empleados, obligan a las empresas a adoptar nuevas prácticas de negocio, comunicándose cada vez en mayor medida internamente (empleados, oficinas, delegaciones…) y externamente (clientes, proveedores, medios de comunicación, administración pública…) por medios electrónicos.

Todos estos factores suponen la existencia de una nueva realidad para las empresas, que han de enfrentarse a nuevos riesgos y amenazas, inexistentes hace muy pocos años, procedentes de distintas fuentes, como fraude informático, espionaje, sabotaje, vandalismo, incendios, catástrofes físicas, etc., siendo las vulnerabilidades cada vez más comunes y sofisticadas, como virus informáticos, ataques de intrusión, hackers, accesos no deseados o denegación de servicios.

Tampoco hay que olvidar la existencia de riesgos de tipo interno, pero no por ello menos peligrosos para la empresa, como la falta de políticas y procedimientos (ej. la falta de un responsable de seguridad), el incumplimiento de la legislación vigente, o la existencia de personal subcontratado y empleados desleales o descuidados dentro de la organización.De hecho, este tipo de amenazas son en la práctica la principal fuente de problemas en materia de Seguridad en la empresa.

La dependencia cada vez mayor de sus sistemas y servicios informáticos, unido a la imparable evolución de la tecnología, hace a las empresas más vulnerables que nunca antes ante las amenazas. El creciente uso de las telecomunicaciones y la interconexión de redes públicas y privadas facilita enormemente a los usuarios compartir los recursos de la información, pero a la vez dificulta el control de su seguridad.

Además, la mayoría de los sistemas informáticos implantados en las empresas no son seguros, bien porque no fueron diseñados para ser seguros, bien porque no cuentan con los medios técnicos necesarios. No obstante, la seguridad no se consigue solo con medios técnicos. Para lograr un adecuado nivel de seguridad en la empresa, es fundamental disponer de una gestión y unos procedimientos adecuados, mediante los cuales se planifiquen los sistemas de protección y control necesarios. En definitiva, se necesita implantar un sistema de gestión de seguridad que abarque y tenga en cuenta a toda la organización, desde sus directivos y empleados, a sus clientes, proveedores, e incluso accionistas, así como sus procesos y recursos productivos.

Dentro de la empresa, la información adopta distintas formas; impresa en papel, almacenada electrónicamente, trasmitida por correo ordinario o por medios electrónicos, hablada de boca en boca, etc. Cualquiera que sea su forma, la información debe ser protegida convenientemente.

Proteger la información en la empresa consiste básicamente en garantizar en todo momento sus tres atributos fundamentales: confidencialidad, para asegurar que solo puedan acceder a la información quienes estén autorizados, integridad, para asegurar que la información sea en todo momento exacta, completa y fiable, disponibilidad, para asegurar que los usuarios autorizados tengan acceso a la Información cuando lo requieran.

Para lograr el objetivo de proteger la Información de la empresa, es necesario implantar un sistema de gestión de seguridad que incluya un conjunto de medidas de control a todos los niveles de la empresa, como políticas de seguridad, procedimientos organizativos, funciones, dispositivos hardware y software, etc.

La implantación de un sistema de gestión de seguridad de la información eficaz en la empresa debe incluir, como para cualquier otro proceso que se implante en la empresa, las siguientes fases: analizar y establecer el contexto de aplicación de la seguridad y los riesgos potenciales, en función de las características y necesidades concretas de cada empresa; Implantar y operar el sistema adecuado de controles técnicos y organizativos de seguridad; comprobar que el sistema funciona según los objetivos establecidos, mediante auditorias periódicas; adaptar de forma continua el sistema a las necesidades del negocio, reajustando los controles a las situaciones cambiantes del entorno.

Es recomendable comenzar por implantar un sistema de gestión de seguridad de partida que abarque un número de controles esenciales básicos y personalizados. Estos deben ser de tipo, tanto operativo (documento de seguridad, medidas técnicas…), como legal (cumplimiento de las leyes vigentes ley orgánica de protección de datos, ley de servicios de la sociedad de la información y de comercio electrónico, etc.).

Debido al enorme auge de las tecnologías de la información experimentado en los últimos años, existen en la actualidad multitud de soluciones técnicas disponibles para realizar una gestión de la seguridad de la Información de forma satisfactoria.

Los beneficios que proporciona un sistema de gestión de la seguridad de la información en la empresa son: mejorar la imagen, confianza y la reputación en general ante todos los stakeholers; cumplir la normativa en esta materia evita a la empresa riesgos, esfuerzos y costes innecesarios; incrementa la rentabilidad, debido a un mejor retorno a la inversión de los sistemas de información y al menor impacto de riesgos internos y externos; aumenta la calidad de los procesos de negocio, lo que permite una mejora continua en la gestión global de la empresa. En definitiva, podemos concluir que todos estos beneficios suponen una nueva ventaja competitiva para la empresa, que contribuyen a la viabilidad de la misma a largo plazo.

Es necesario implantar un sistema de gestión de la seguridad de la información que incluya un conjunto de controles de seguridad que pueden ser controles de tipo legislativo: protección de carácter personal y de la intimidad de las personas, contribuyendo al cumplimiento de la legislación vigente por parte de la empresa, entre ellos resultan esenciales como la ley orgánica de protección de datos y la ley de servicios de la sociedad de la información; protección de los registros esenciales de la empresa, evitando su pérdida, destrucción o falsificación, custodiándolos de forma segura como datos contables, bases de datos, registros de transacciones, auditorias, procesos y operaciones, firmas digitales…; protección de la propiedad intelectual regulando los derechos de copia de material protegido, diseños y marcas registradas, propios o de terceros; controles de tipo organizativo, se derivan de buena práctica interna en la empresa en materia de seguridad.

Estos controles se componen habitualmente de una conjunción de procedimientos internos (políticas, normas, funciones, recursos…) y de soluciones técnicas de seguridad (dispositivos hardware y software), entre los primeros podemos citar: la política de seguridad de la información de la empresa, elaborando el documento de seguridad, que contenga la definición, objetivos, alcance y responsabilidades de la seguridad en la organización; asignación de responsabilidades de seguridad para la protección de la información mediante la

identificación de los activos y procesos de seguridad, designación del responsable de la seguridad y propietarios de los activos y definición de los niveles de autorización.

Formación de usuarios propios y externos en los procedimientos de seguridad y el uso de los controles y recursos existentes para proteger la información (responsabilidades legales, uso de contraseñas de acceso a los ordenadores, normas de uso de Internet, utilización de software no deseado, copias de Seguridad…).

Registro de las incidencias de seguridad mediante un procedimiento de comunicación interno, estableciendo a la vez un procedimiento disciplinario para los empleados que cometan infracciones.

Gestión de la continuidad del negocio implantando procesos para reducir el impacto de grandes fallos o desastres naturales, accidentales o deliberados, consistentes en la combinación de controles preventivos y correctivos. En cuanto a las soluciones de tipo técnico, debido al crecimiento que ha experimentado en pocos años el mercado de la seguridad informática, existen todo tipo de fabricantes especializados en múltiples disciplinas, que disponen de una enorme oferta, para todas las necesidades y presupuestos.

En función del tipo de seguridad que ofrecen, es posible clasificar las soluciones existentes en los siguientes grupos:

Seguridad perimetral:

Detección y prevención de intrusiones, protección ante ataques de denegación de servicio y gestión de accesos externos mediante firewalls, sistemas IDS…

Redes privadas virtuales VPN, redes virtuales locales VLAN, redes seguras inalámbricas, wireless LAN, wi-fi… para garantizar y proteger las comunicaciones internas y externas a través de Internet

Seguridad de identidad:

Control de acceso de usuarios mediante sistemas de autentificación basados en contraseñas, claves PKI[72], firma digital, tarjetas inteligentes, tokens, lectores biométricos (huellas dactilares, sistemas oculares…).

Seguridad de contenidos:

Implantación de sistemas antivirus personales o corporativos para la protección ante virus, troyanos, gusanos, etc.

Herramientas de monitorización de red para proteger los sistemas contra sniffers, códigos maliciosos desconocidos, etc. (cookies, javaScripts, Actives…).

Inspectores de contenidos para proteger y limitar a los usuarios el uso indebido de Internet mediante herramientas antispam, filtrado de URLs…

Seguridad del puesto de trabajo:

[72] En criptografía, una infraestructura de clave pública (Public Key Infraestructure), es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, firma digital o el no repudio de transacciones.

Gestión de Copias de Seguridad local o remota para backup y recuperación de datos.

Soluciones de Seguridad para alta criticidad, como encriptación de discos, servidores en alta disponibilidad, balanceo de cargas, redundancia de electrónica de red y arquitecturas de red seguras.

Ante la gran cantidad de soluciones y proveedores existentes, es aconsejable contar con la ayuda de empresas especializadas, que ofrezcan servicios de asesoramiento específicos en Seguridad, con el fin de obtener las soluciones más adecuadas a cada necesidad y de acuerdo al presupuesto de cada empresa.

La norma española UNE-ISO/IEC 17799, publicada por AENOR en noviembre de 2002, constituye un "Código de buenas prácticas para la Gestión de la Seguridad de la Información", e incluye una extensa relación de controles de tipo organizativo.

De forma teórica, todos estos controles pueden aplicarse a cualquier empresa, pero en la práctica, debe hacerse siempre en función de sus, características (actividad, tamaño, situación económica, infraestructura informática…) y necesidades de seguridad (actividad, riesgos potenciales, etc.). Por ello, a la hora de implantar un sistema de gestión de seguridad hay que comenzar analizando, tal como se ha mencionado anteriormente, el contexto de aplicación de la seguridad, para de este modo elegir las soluciones más adecuadas y asignar los recursos técnicos, humanos y económicos al proyecto.

## 4.9 LOS ACTIVOS DE INFORMACIÓN COMO BASE DE LA VENTAJA COMPETITIVA: LAS BASES DE DATOS.

Una de las herramientas más importantes para poder llevar a cabo estrategias de marketing directo, son las bases de datos. Una base de datos bien organizada, actualizada y entendible puede representar un alto porcentaje de efectividad a la hora de hacer una campaña de e-mail marketing.

Las bases de datos han permitido a las empresas que hace campañas de marketing directo, seleccionar los mejores prospectos para cualquier producto que deseen vender. Cada vez más empresas que venden a negocios están recurriendo al correo directo y telemarketing como respuesta a los elevados y crecientes costes de emplear de emplear la fuerza de venta. Quienes implementan como estrategia el marketing directo, pueden comprar una lista de correos y datos con cientos de nombres de casi cualquier grupo, por lo cual pueden personalizar sus mensajes.

Una empresa puede determinar con mucha mayor precisión sus mercados, meta, a través de unas organizadas bases de datos para llevar a cabo un marketing directo, en lugar de un marketing masivo, marketing de segmentos o marketing de nichos. La empresa puede identificar grupos pequeños de clientes que reciben oferta y comunicaciones de marketing.

Las empresas utilizan sus bases de datos de cuatro diferentes maneras: una, para identificar prospectos. Muchas empresas generan prospectos de ventas anunciando su producto u oferta. Los anuncios generalmente contienen una función de respuesta, como una tarjeta de respuesta comercial o un número telefónico sin cargo. La base de datos se construye en base a estas respuestas; segunda, para decidir qué clientes deberán recibir una oferta dada, las empresas establecen criterios que describen el cliente meta ideal para una oferta. Luego se buscan en la base de datos las personas que más se parecen al tipo ideal. Al tomar dato de las tasas de respuestas, la empresa puede mejorar la precisión de sus objetivos con el tiempo.

Después de una venta, la empresa puede iniciar una serie automática de actividades; tres, para hacer más profunda la lealtad de los clientes, a través de obsequios, descuentos o material acorde a su interés; cuatro, para reactivar las compresas de los clientes, las empresas pueden instalar programas de envío automático de correo que envían tarjeta, recordatorio o promociones.

El rol estratégico de las bases de datos, requiere una inversión considerable. Las empresas deben invertir en hardware, software de bases de datos, programas analíticos, enlaces de comunicación y personal capacitado. El sistema de bases de datos debe ser amigable con el usuario.

## 4.10 EL PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS COMO VENTAJA COMPETITIVA. ESQUEMA DE MÍNIMOS INFORMATIVOS.

El plan director de seguridad tiene por misión el establecimiento de políticas y controles en el contexto de la organización. Este se basa en un conjunto de documentos y herramientas que demuestran y ayudan a realizar la gestión de la seguridad como son la ISO 27001 y la metodología para el análisis y gestión de riesgos de los sistemas de información MAGERIT.

El plan director de seguridad se compone de las siguientes fases:

Definición del ámbito o alcance: Donde se define y se delimita las áreas de aplicabilidad de sistema de gestión.

Análisis Gap*:* Fase donde se chequea y se realiza un balance de los fallos que presenta la organización en cuanto a seguridad

Identificación de los activos de información: fase que se encarga de definir e identificar todo aquello que genera un valor para la organización el sistema de información.

La valorización de los activos de información*:* en esta fase se define cuanto valor representa el activo para la organización basado en los criterios de disponibilidad, integridad y confidencialidad

Análisis de riesgo: etapa donde se valora el impacto y los riegos de las amenazas latentes en la organización.

Definición de políticas: es la definición de los lineamientos específicos para gestionar la seguridad de la información

Selección de controles: son los mecanismos utilizados para ejecutar las políticas de seguridad.

Definición de la estructura documentaria: donde se definen y establecen los documentos que apoyaran los controles de seguridad.

Requerimientos normativos:

Para la realización del Plan director de seguridad informática se tendrá en cuenta el estándar internacional ISO/IEC 27001 y la guía de buenas prácticas ISO 27002:2005, este estándar se

basa en la gestión de riesgos y subministra las pautas necesarias a considerar para la implementación de controles y la creación de políticas de seguridad bajo el foque PHVA[73], tomando elementos que puedan estructurarlo de forma adecuada.

Un sistema de gestión de esta índole está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

La fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad.

La fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.

La fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI (Sistema de Gestión de la Seguridad de la Información) mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.

La fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

La norma ISO 27001 requiere los siguientes documentos:Alcance del SGSI y Política del SGSI; Procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas;todos los demás documentos, según los controles aplicables; Metodología de evaluación de riesgos; Informe de evaluación de riesgos; Declaración de aplicabilidad; Plan de tratamiento del riesgo; Registros.

Documentos de ISO 27002:

Desde el 1 de Julio de 2000, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

Directrices:

ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a laInformación), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso

[73] El ciclo PHVA es una herramienta de la mejora continua, presentada por Deming a parti del año 1950, la cual se basa en un ciclo de cuatro pasos: Planificar (plan), Hacer (Do), Verificar (Check) y Actuar (do). Está considerado uno de los mejores sistemas para lograr la mejora continua de las organizaciones.

a la información y a sus activos asociados cuando lo requieran)".La versión de 2005 del estándar incluye las siguientes secciones principales:introducción, conceptos generales de seguridad de la información y SGSI (sistema de gestión de la seguridad de la información); campo de aplicación, se especifica el objetivo de la norm, términos y definiciones, breve descripción de los términos más usados en la norma; estructura del estándar, descripción de la estructura de la norma; evaluación y tratamiento del riesgo, indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información; política de seguridad, documento de política de seguridad y su gestión; aspectos organizativos, organización interna, organización externa; gestión de activos, responsabilidad sobre los activos; clasificación de la información; recursos humanos, anterior al empleo, durante el empleo,finalización o cambio de empleo; física y ambiental, areas seguras, seguridad de los equipos.

Comunicaciones y Operaciones: Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.

Control Accesos: requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

Adquisición, desarrollo y mantenimiento de sistemas: requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.

Gestión de incidentes: comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.

Gestión Continuidad de negocio: aspectos de la seguridad de la información en la gestión de continuidad del negocio.

Cumplimiento legal: con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

La norma ISO/IEC 27001, contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información. Esta norma recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización.

Con esta norma serán certificados los Sistemas de Gestión de Seguridad de la Información en la institución. El estándar aplica para cualquier organización sin importar el tamaño y a su vez define los siguientes dominios de controlque cubren por completo la Gestión de la Seguridad de la Información:Política de seguridad;Organización de la información de

seguridad;Administración de recursos;Seguridad de los recursos humanos;Seguridad física y del entorno;Administración de las comunicaciones y operaciones; Control de accesos; Adquisición de sistemas de información, desarrollo y Mantenimiento; Administración de los incidentes de seguridad; Administración de la continuidad de negocioCumplimientos (legales, de estándares, técnicas y auditorias), esta información se pueden encontrar en INCIBE[74] con aspectos teóricos y prácticos.

Para realizar el análisis de riesgos se hará uso de MARGERIT[75], es una metodología que brinda las pautas, las técnicas y los métodos necesarios para auditar sistemas de información que manejan medios electrónicos, informáticos, telemáticos, e información mecanizada en sus operaciones.MARGERIT[76] es un método de compuesto por tres fases para implementar una solución de SGSI como lo son:

Planificación:En esta parte se identifican y se definen los objetivos, la pertinencia, los requerimientos y las consideraciones necesarias para realizar el proyecto.

Análisis de riesgos:En esta fase se identifican todos y cada uno de los activos a tratar en la organización, sus dependencias y las amenazas a las que están expuestos. Igualmente se tiene en cuenta el impacto, la degradación y la frecuencia que tienen cada una de estas amenazas en el activo, analizando las salvaguardas existentes para mitigar este efecto.

Gestión de riesgos:Se buscan los mecanismos y las salvaguardas apropiadas y oportunas para mitigar el impacto y el riesgo de cada una de las amenazas a niveles aceptables través del diseño de un plan de seguridad.

Analisis diferencial ISO 27001:

Se realiza un análisis del nivel de seguridad con respecto a la ISO27001+ISO27002

1.- Políticas de Seguridad.Existencia de políticas de seguridad, medios para proteger la información y controles regulares para verificar la efectividad de las mismas.

2.- Seguridad de la Información.Mecanismos y procedimientos estructurados con responsabilidades y obligaciones detalladas contra hechos que afecten la seguridad organizacional, programas de formación en seguridad para los empleados.

3.- Clasificación del control de activos de información. Clasificar y etiquetar la información y gran variedad de activos. Inventario actualizado, organizado en forma eficiente.

4.- Seguridad física y del entorno: Perímetros de seguridad física conforme a las normas establecidas. Protección eficaz contra fallos en la alimentación eléctrica y los mecanismos para asegurar la disponibilidad e integridad de todos los equipos.

[74] www.incibe.es

[75] Ciberconta.unizar.es (auditoría informática)

[76] Regulación internacional sobre auditoría de sistemas de información: ISACA (Information Systems Audit and Control Foundation) propone metodología COBIT (Control Objectives for Information and related Technology); COSO (Committee of Sponsoring Organizations of the Treadway Commission´s Internal Control-Integrated Framework); AICPA-SAS (The American Institute of Certified Public Accountants´), IFAC (federación Internacional de Contables)-NIA (Normas Internacionales de Auditoría), SAC (Institute of Internal Aditors Researc Foundation´s Systems Auditability an Control ), MARGERIT (Metodologa de análisis y Gestión de Riesgos de los sistemas de información), EDP (auditors Foundation)

5.- Seguridad del personal. Procedimientos, responsabilidades y roles de seguridad a seguir en caso de incidente. Claridad a efectos de seguridad en cuanto a la selección y baja del personal.

6.- Gestión de comunicaciones y operaciones. Claridad a la hora determinar las responsabilidades pertinentes para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad. De la misma forma las medidas para proteger la confidencialidad e integridad de información, como también los controles para realizar la gestión de los medios.

7.- Control de accesos. Políticas de control de accesos, para la restricción y asignación de privilegios en entornos multi-usuario.

8.- Desarrollo y mantenimiento de sistemas. Medidas para controlar las vulnerabilidades de los equipos, los sistemas operativos y los ficheros del sistema. Medidas de seguridad en el proceso de desarrollo, testing y soporte.

9.- Comunicación de eventos. Existencia de registros, mecanismos para comunicar los eventos eincidentes de seguridad. Definición de las responsabilidadesante un incidente y el procedimiento formal de respuestas.

10.- Gestión de la continuidad del negocio Pruebas y procedimientos para el mantenimiento y reevaluación de los planes de continuidad del negocio. Procesos para la gestión del análisis de impacto de incidentes y amenazas.

11.-Conformidad. Procedimientos para la revisión de las políticas de seguridad y las conformidades técnicas.

Esquemadocumental:

Política de Seguridad. Esta Política de Seguridad de la Información del SGSI se ha desarrollado para garantizar la confidencialidad, integridad y disponibilidad de la información y de los de los procesos, Al implementar esta política las personas involucradas, tanto empleados como proveedores, deben garantizar la protección de los procesos, la reputación y la mejora continua.

Gestión de Roles y Responsabilidades. El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.

Fases del proyecto. El desarrollo del plan director se ha organizado en cuatro fases que se describen en sus principales actividades: definición de la metodología, desarrollo de la herramienta, análisis de riesgos, gestión de riesgos.

Metodología de análisis de riesgos. Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

La identificación de los tipos de activos puede definirse como la información de tipo documental de todos aquellos elementos del sistema de información o relacionados con este, que generan un valor para la empresa, para su buen funcionamiento y cumplimiento de los objetivos propuestos. Se deben tener en cuenta los diagramas de dependencia de activos y la

tabla de dependencia entre los distintos activos de información que nos permitirán tener una imagen global de la dependencia de un activo en relación con todos los activos identificados en la empresa.

Valorización de los activos:son las características o atributos que hacen valioso un activo. Estos se valoran por medio de dimensiones o facetas lo cual conlleva a que la valoración que recibe un activo en cierta dimensión es la medida del perjuicio del activo.

Las dimensiones son las siguientes: disponibilidad, los usuarios autorizados tienen acceso cuando lo requieran a la información y a sus activos asociados. Un activo tiene un gran valor desde el punto de vista de disponibilidad si una amenaza afectara a su disponibilidad, las consecuencias serían graves. Un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño; Integridad de los datos**,** garantía de la exactitud y completo de la información y los métodos de su procesamiento, los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna; Confidencialidad de los datos,seguridad de que la información es accesible sólo para aquellos autorizados a tener acceso; los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

Autenticidad de los usuarios del servicio,aseguramiento de la identidad u origen. La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio. Un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la empresa. Un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

Autenticidad del origen de los datosseguridad de la identidad u origen. Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.Los criterios de valoración de los activos se realizan generalmente utilizando una escala, en función del nivel de daño (muy grave, grave, importante, menor o irrelevante) a la empresa

Amenazas de los activos**,** se entiende por amenaza a la posible ocurrencia todo hecho que puede causar daños a los diferentes tipos de activos de la organización: desastres naturales, daños por agua, fuego, averías de origen físico o lógico, inadecuadas humedades o temperaturas, errores o fallos no intencionados, errores del administrador, errores de configuración, difusión de software dañino, errores de direccionamiento de la información, escapes de información, alteración de la información, introducción de información incorrecta, degradación de la información, destrucción de la información, divulgación de la información, errores de mantenimiento y actualización de hardware, errores de mantenimiento y actualización de software, caída del sistema por agotamiento de recursos, indisponibilidad del personal, manipulación de la configuración, suplantación de la identidad del usuario, abusos de privilegios de acceso, alteración de secuencias, acceso no autorizado, interceptación de información o escuchas, modificación de la información, introducción de falsa información,

corrupción de la información, destrucción de la información, divulgación de la información, manipulación de programas, denegación de servicios, robo,

Entre los activos de información, a modo de ejemplo, podemos destacar los siguientes:

Equipo auxiliar: equipo que funciona de soporte a los sistemas de información sin estar relacionado directamente con los datos: sistemas de alimentación, generadores eléctricos, equipos de climatización, cableado, armario archivador;

Redes de comunicaciones**:** Infraestructura para que los datos se trasladen de un lugar a otro, vía lógica, red telefónica, red inalámbrica, microondas, red local.

Soporte de Información:Se consideran los dispositivos físicos que permiten almacenar información de forma permanente, o al menos durante largos periodos de tiempo: Cd-Rom, dispositivos USB, cinta magnética, discos duros, material impreso.

Equipos Informáticos:Son aquellos que sirven de herramienta para el almacenamiento, procesamiento y transporte de los datos lógicos y físicos en la empresa: servidores, informática personal, medios de impresión, conmutadores, routers, consola de descargas y video conferencia, Access point, scanner, armarios (ejemplos: racks, switch, routers, patch panel, modem de fibra etc.)

Personal: personas relacionadas con los sistemas de información.Podemos hablar de usuarios internos (administradores de sistemas, administradores de comunicaciones, administradores de bases de datos, desarrolladores, auditores internos, talento humano, etc.

Aplicaciones:en esta clasificación se encuentran los activos con denominaciones concernientes a programas de desarrollo propio como adquiridos al exterior o subcontratados o estándares (sistemas operativos, antivirus, lenguaje de programación, editores para el diseño y programación de páginas webs, sistemas de gestión de bases de datos, lenguaje o plataforma de programación, navegador web, servicio de correos, ofimática) aplicaciones y desarrollos, para las tareas o procesos que han sido automatizadas. Su desempeño o utilización se realizará a través de un equipo informático, en miras a gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios.

Datos/información**:** informe anual, cuentas anuales consolidadas, informe de buen gobierno, informe responsabilidad social corporativa, información presupuestaria y otros. Los datos pueden ser: reservados, confidenciales, datos sin clasificar, datos personales, las contraseñas de servidores, licencia del software, backup y contraseñas personales, datos de administración de página web, código fuente de la página web, consultas a bases de datos, datos de nómina, prestaciones sociales.

Servicios**:** los activos de tipo servicios pueden definirse como aquellos activos que con su función o ejecución pueden satisfacer una necesidad de los usuarios (clientes que utilizan el servicio) tanto a usuarios internos como externos. Entre los servicios públicos en general, estarían los relacionados con su actividad corporativa, información en el portal web, servicios internos como sería los relacionados con compras o contratación, servicios externos como los de mantenimiento de planta y equipo, internet. Servicio de funcionamiento de la red interna y soporte técnico para el manejo y administración de la página web, soporte técnico para el funcionamiento de equipos informáticos.

## 4.11 CONSIDERACIONES FINALES

Robert F. Kennedy[77]: "Que a nadie le desaliente la idea de que no hay nada que podamos hacer frente a las enfermedades, la miseria, la ignorancia y la violencia que pueblan nuestro mundo. Pocos tendrán la grandeza de cambiar el rumbo de la historia, pero cada uno de nosotros puede aportar puede aportar su pequeño grano de arena para cambiar el curso de los acontecimientos. Y, en total, la suma de esos granos será la historia escrita de esta generación".

Tanto en los campos de lo virtual, la robótica, la inteligencia artificial y la biología sintética hay cambios trascendentales y dichos cambios nos han conducido a un punto de inflexión de una curva exponencial, la cual, como ya hemos podido observar en la introducción del tema anterior, registrará un crecimiento explosivo en los próximos años. Hemos observado a lo largo de estas tesis la existencia de delincuentes, terroristas, piratas informáticos y gobiernos corruptos que subvierten la tecnología y la emplean en perjuicios de otros. Esto no quiere decir que la tecnología sea mala.

El fuego, la primera tecnología servía para dar calor, para cocinar alimentos y también para incendiar y reducir a cenizas el pueblo vecino. Y tanto un cirujano como un asesino pueden blandir un cuchillo. En manos de personas con buenas intenciones, las tecnologías, que evolucionan rápidamente, aportarán una abundancia sensacional al mundo.

Como en este capítulo hemos hablado de ventaja competitiva como consecuencia del valor estratégico de los inmovilizados intangibles. La mejor estrategia en busca de una ventaja competitiva para salir de los problemas de la ciberseguridad es la educación de todos los stakeholders de la organización, especialmente en valores.

## 4.12 BIBLIOGRAFÍA

ABOODY, D.; LEV, B. (1998)."The Value Relevance of Intangibles: The Case of Software Capitalization". Journal of Accounting Research, Vol. 36, Pp.161 – 191.

ACEDO, F; BARROSO, C; CASILLAS, J; GALAN, J. (2006). The resource-based theory: dissemination and main trends. Strategic Management Journal, Vol. 9, No. 4, Pp.327–353.

AMIR, E.; LEV, B. (1996). "Value- relevance of nonfinancial information: The wireless"

AMIT, R, SCHMOAKER, P. (1993). "Strategic Assets and Organizational Rent. Strategic" Management JOURNAL, 14(1): 33 – 46.

ANDREWS, K.R. (1977). "El concepto de estrategia de la empresa". Pamplona: Ediciones Universidad de Navarra, S.A. Capítulo 2, 47-71.

ANSOFF H. I. (1991). Critique of Henry Mintzberg's The Design School: Reconstructing the Basic Premises of Strategic Management. Strategic Management Journal, Vol 12, Pp. 449-461.

ARMANDO CARDONA, RAÚL (2011) "Estrategia basada en los recursos y capacidades, criterios de evaluación y el proceso que desarrolla". Revista electrónica Forum Doctoral No. 4 Pp. 113-147.

[77] www.history.com

BALDWIN, C; O´MAHONY S; QUINN, J. (2003). IBM and Linux (A), Harvard Business School, 903-083.

BANHAM, R. (2005). “Valuing IP Post-Sarbanes-Oxley”. Journal of Accountancy.200 Vol. 5, Pp. 72-78.

BARNEY, J; ARIKAN, A. (2001). Resource-based view: origins and implications. The Blackwell Handbook of Strategic Management, Hitt M, Freeman R, Harrison J (eds). Blackwell: Malden, MA., 124–188.

BARNEY, JAY B. (1991). “Firm resources and sustained competitive advantage”. Journal of Management, Vol.17, Pp. 99–120.

BELKAOUI, A., (1992). “Accounting Theory.” London: Academic press.

BRANDERBURGER, A.; NALEBUFF, B. (1996). “Co-opeticion”. Nueva York: Doubleday.

BREALEY, R.; MYERS, S.; ALLEN, F. (2006). “Principios de finanzas corporativas”. Madrid, España: Ed. Mc Graw Hill,1136 p.

BRIGHAM, E.; HOUSTON, J. (2005). “Fundamentos de administración financiera”. México: Ed. Thompson, 838 p.

BURNS, T; STALKER, GM. (1961). “The management of innovation”. London: Tavistock. Campbell-Hunt, C., 200.

CAÑIBANO, L.; GARCÍA, M.; COVARSÍ, A.; SÁNCHEZ, M. P. (1999). “La Relevancia de los Intangibles para la Valoración y la Gestión de Empresas: Revisión de la Literatura (1)”. Revista Española de Financiación y Contabilidad, 17-88.

CAPELLERAS, J.L.; RABETINO, R. (2008). “Individual, organizational and environmental determinants of new firm employment growth. Evidence from Latin America”. International Entrepreneurship and Management Journal, Vol. 4, No.1, Pp. 79-99.

CARDONA, R.A. (2011). “Estrategia basada en los recursos y capacidades. Criterios de evaluación y el proceso de desarrollo”. Revista electrónica Forum-Doctoral nº 4. Mayo-julio 2011. ISSN: 2027-2146

CARDONA, RAÚL A. (2010). “Planificación financiera en las pymes exportadoras. Caso de Antioquia, Colombia”. Revista Administer, Universidad EAFIT, Medellín, Colombia. No.16, 50-74.

CARMELI, A.; TISHLER, A. (2004). “The relationship between intangible and organizational elements and organizational performance”. Strategic Management Journal, Vol. 25.

CHANDLER, A. (1962). “Strategy and Structure”. Cambridge, MA: Massachuttes Istitut of Technology, First MIT Press -1969, Pp11-13. CÓDIGO DE COMERCIO, APARTADO 4 DEL ARTÍCULO 39.

DEDMAN , E.; MOUSELLI, S; YUN, S.; ANDREW, S. (2009). “Accounting, Intangible Assets, Stock Market Activity, and Measurement and Disclosure Policy—Views From the U.K. A Journal of Acconting”, Finance and Business Studies, Vol.45 - No. 3, Pp312-341.

DEMSETZ, H. (1973). "Industry structure, market rivalry, and public policy". *Journal of Law and Economics*, Vol. 16, No.1-10. DISPOSICIÓN FINAL DECIMOTERCERA DE LA LEY 22/2015

FERNÁNDEZ, Z. (1999). "El Estudio de las Organizaciones (La Jungla Dominada)". Papeles de Economía Española, Pp. 56-77. FLATT, S.;

KOWALCZYK S. (2008). "Creating competitive advantage through intangible assets: the direct and indirect effects of corporate culture and reputation". Advances in Competitiveness Research,Pp*. 13-30*

GARCÍA, E; MARTÍNEZ, I. (2007). "The use of intellectual capital information in investment decisions. An empirical study using analyst reports". The International Journal of Accounting, Vol. 42, Pp. 57–81

GARCÍA, O. (1999). "Administración financiera. Fundamentos y aplicaciones". Cali: Prensa Moderna Impresores.

GINER, B; PARDO, F. (2007). "La relevancia del fondo de comercio y su amortización en el mercado de capitales: Una perspectiva europea". Revista Española de Financiación y Contabilidad,Vol. 134, Pp. 389-419.

GINER, BEGOÑA. (2001). "La utilidad de la información contable desde la perspectiva del mercado: ¿Evolución en la investigación?". Revista de contabilidad, ISSN 1138-4891, Vol. 4, No. 7, Pp. 21-52.

GONZÁLEZ, E; VENTURA, J. (2002). "How much do strategic groups matter?". Review of Industrial Organization, Vol. 21, Pp. 55-71.

GRANT, R.M. (2006). "Dirección Estratégica: Conceptos, Técnicas y Aplicaciones". Madrid: Civitas, (5ª ed.). HAMEL, G; PRAHALAD C. (1994). "Competing for the future". Harvard Business Review. Vol. 72, No. 4, Pp. 112-128.

HAMEL, G; PRAHALAD, C. (1990). "The Core Competences of the Corporation". Harvard Business Review, 68, 79-91.

HARRISON, MI. (1987). "Diagnosing Organizations. Methods, Models, and Processes". Sage Publications, Newburry Park.

HERNÁNDEZ G.J; DOMÍNGUEZ H., M. Y ITA C.D.(2008) "Ventaja competitiva sostenible en pequeñas y medianas empresas hoteleras del sur de México". Pensamiento y Gestión No.25 Universidad del Norte, pp. 161-177.

HILL, CWL. (1988). "Differentiation versus low cost or differentiation and low cost: a contingency framework". Academy of Management Review, Vol. 13, No. 3, Pp. 401-412.

HOSKISSON, R; HITT, M; WAN, W; YIU, D. (1999). "Theory and Research in Strategic Management: Swings of a Pendulum." Journal of Management, Vol. 25, No. 3, Pp.417-456.http://auditoriauc20102mivi.wikispaces.com/file/view/NTCAS436020101700422184.pdfhttp://blog.s21sec.com/2007/12/por-qu-un-plan-director-de-seguridad.htmlhttp://iso27002.wiki.zoho.com/00-Cl%C3%A1usulas-ISO-27002.htmlhttp://www.expansion.com/empresas/tecnologia/2016/09/20/57e004b2e2704e72288b4581.html

http://www.innotecsystem.com/plandirectorseguridad.htmhttp://www.iso27000.es/download/doc_iso27000_all.pdfhttp://www.iso27000.es/iso27000.html#section3bhttp://www.iso27001standard.com/es/que-es-la-norma-iso-27001http://www.rediris.es/difusion/eventos/foros-seguridad/fs2010/pres/viiiforoseguridadRI2.http://www.sia.es/img/Plan_director_Cepsa-Sia.pdf

JONES, D.A. 2007. "Voluntary Disclosures in R&D-Intensive Industries". Contemporary Accounting Research Vol.24, No. 2, Pp. 489-522.

LEV, B., (2001). "Intangibles: Management, Measurement and Reporting". Brooking Institution Press.

LEV, B., ZAROWIN, P., (1998): "The boundaries of financial reporting and how to extend them". New York University.

LEY 22/2015, DE 20 DE JULIO, DE AUDITORÍA DE CUENTAS. LEY 27/2014, DEROGACIÓN DEL APARTADO 3 DEL ARTÍCULO 13 Y SE MODIFICA EL APARTADO 2 DEL ARTÍCULO 12.LEY DE SOCIEDADES DE CAPITAL, APARTADO 4, ARTÍCULO 273.

LOCKETT, A.; O'SHEA, R; WRIGHT, M. (2008). "The Development of the Resource-based View: Reflections from Birger Wernerfelt 1". Organization StudiesNo. 29, Pp.1125.

LÓPEZ, C. Y PONTET U., N. (2011) "ventajas competitivas sustentables a través del capital intelectual integrando las complementariedades entre la teoría institucional y la teoría de recursos". Revista del Instituto Internacional de Costos, No.8 enero junio, ISSN 1646-6896

MENGUZZATO, M; RENAU, J. (1991). "La Dirección Estratégica de la Empresa: Un Enfoque Innovador del Management".Barcelona: Ariel. (2ª. ed).

MINTZBERG H. (1994). "The Rise and Fall of Strategic Planning, Harvard Business Review", In Harvard-Deusto Business Review, Vol.60, Pp. 4107-4114.

MOYA, S; RODRÍGUEZ, G; PRIOR, D. (2009). "Investigación en Contabilidad". Working Paper. Universidad Autónoma de Barcelona.

NELSON, R; WINTER, S. (1982). "An Evolutionary Theory of Economic Change". Cambridge, MA: Belknap Press.

NONAKA, I.; TAKEUCHI, H. (1999*). "*La organización creadora de conocimiento. Cómo las compañías japonesas crean la dinámica de la innovación". Oxford University Press.

ORTEGA, ALFONSO. (2008). "Planeación financiera estratégica". México: Mc Graw Hill. 320 p.

PENROSE, EDITH. (1959). "The theory of the growth of the firm". New York: John Wiley.

PETERAF, MARGARET. (1993)." The Cornestones of Competitive Advantage: A Resource – Base View". In Strategic Management Journal, Vol. 3, Pp. 179-191.

PLAN GENERAL DE CONTABILIDAD DE 2007, "norma de valoración número 22 sobre cambios en criterios contables, errores y estimaciones contables".PORTER, MICHAEL. (1980)." Competitive strategy". New York: Free Press, 398 p.

PORTER, MICHAEL. (1991). "Towards a Dynamic Theory of Strategy". In Strategic Management Journal, Vol. 12, Pp. 95-117.

QUINN, J. (1980). "Strategies for Change: logical Incrementalism". Homewood, IL: Irwin.

RAMÍREZ, P. D. (2002). "Contabilidad administrativa". México. McGraw Hill, 589 p.

REAL DECRETO DE ESPAÑA NO. 1514, noviembre, 16 de 2007. Nuevas Normas Contables Internacionales.

RIALP, A. (2003). "Fundamentos teóricos de la Organización de Empresas". Madrid: Pirámide, 95-143.

ROBBINS, SP. (1999). "Comportamiento Organizacional. Conceptos, Controversias, Aplicaciones". Prentice – Hall, México (8ª. Ed.)

RUMELT, RICHARD. (1991). "Toward a Strategic Theory of the Firm. Competitive Strategic" Management. Pretenci Hall, Englewood Cliffs, N.J., Pp. 556-570.

SÁEZ DE VITERI, D. (2000). "El potencial competitivo de la empresa: recursos, capacidades, rutinas y procesos de valor añadido". España. Investigaciones Europeas de Dirección y Economía de la Empresa. Vol. 6, N" 3, 2000, pp. 71-86.

SARMIENTO, S.; SÁNCHEZ, A. Y CRUZ, M. (2009). "Competitividad y desarrollo sustentable empresarial". Revista Internacional La Nueva Gestión Organizacional. México. Año 4. Número 8. Enero-Junio, 2009. pp. 112-134.

SCHMALENSEE, R. (1985). "Do markets differ much?". American Economic Review, Vol. 5.

SCHUMPETER, JOSEPH. (1934). "The Theory of Economic Development". Cambridge: HBR Press.

SHORT, J.; PAYNE, G.; KETCHEN, JR. D. (2008). Research on Organizational Configurations: Past Accomplishments and Future Challenges. In Journal of Management, Vol. 34, No. 6, Pp. 1053-1079.

SIMON, H.; MARCH, J. (1956). Organizations. Nueva York: Wiley.

SPANOS; Y; LIOUKAS S (2001). "An Examination Into the Causal Logic of Rent Generation: contrasting Porter's Competitive Strategy Framework and the resource-based view". Strategic Management Journal, Vol. 22, Pp. 907-934.

STICKEY, C., WEIL, R., (1994). Financial Accounting. Forth Worth, The Dryden Press.

TEECE, D; PISANO, G; SCHUEN, A. (1997): "Dynamic capabilities and strategic management". In Strategic Management Journal, Vol. 18 No. 7, Pp. 509-533.

TEECE, D; PISANO, G; SCHUEN, A. (1997): Dynamic capabilities and strategic management. In Strategic Management Journal, Vol. 18 No. 7, Pp. 509-533.

THOMPSON Y STRICLAND (2004): "Administración estratégica. Textos y Casos". 13va. Edición, México. Mc Graw Hill Interamericana.VÉLEZ, I. (2004). "Decisiones de inversión. Enfocado a la valoración de empresas". Bogotá, Colombia. Centro Editorial Javeriano, Pp. 232-242.

WEB EUMEDNET, Enciclopedia y biblioteca virtual de ciencias sociales, económicas y políticas:

WERNERFELT, B. (1984). “A resource-based view of the firm.” Strategic Management Journal, Vol. 5 No. 2, Pp. 171–180.

WERNERFELT, B. (1984): A resource-based view of the firm”. Strategic Management Journal, Vol. 5 No. 2, Pp. 171–180.

WESTON, F.; COPELAND, T. (1995). “Finanzas en administración”. México: Mc Graw Hill.

WESTON, J.; BRIGHAM, E. (1994). “Fundamentos de administración financiera”. México: Mc Graw Hill, 1148 p.

WING, R.L. (1988). “The Art of Strategy: A New Translation of Sun Tzu´s Classic The Art of War”.Traducción. Nueva York: Doubleday.

ZEFF, STEPHEN. (2007). “Some obstacles to global financial reporting comparability and convergence at a high level of quality”. In British Accounting Review, Vol. 39, Pp. 290-302.

# TEMA 5: LOS MODELOS DE VALORACIÓN DE EMPRESAS Y DE INTANGIBLES

## 5.1. INTRODUCCIÓN

Actualmente, los modelos de valoración de empresas son un instrumento fundamental para medir el desempeño de una compañía y para identificar los conductores de valor (value drivers) de ésta, que ayudarán en la elaboración de las estrategias de planificación, basadas en el valor de la empresa.

Los modelos de valoración de empresas, que a continuación presentaremos, son una abstracción de la realidad, expresadas en ecuaciones lógico–matemáticas (Romero, 1993), cuya solución nos ha de servir como referente del valor empresarial.

Sin embargo, no podemos olvidar que tales modelos son una representación simplificada de la realidad, que responde a unos conceptos y a una teoría, y que la realidad, como las teorías, siempre son cambiantes.

En el presente capítulo contemplaremos los diversos modelos de valoración de empresas e intangibles existentes, que es lo veremos a continuación, dando unas conclusiones finales.

## 5.2. MODELOS DE VALORACIÓN DE EMPRESAS

La valoración de una empresa es un proceso de formación de un juicio de valor sensato, basado en la experiencia y en el empleo de metodologías normalizadas (aceptadas por el mercado), que permitan la identificación de las fuentes de creación, destrucción y transmisión de valor.

En resumen, la valoración dependerá de la situación de la empresa, del momento de la transacción y del método empleado.

A continuación, nos disponemos a explicar los diversos modelos de valoración de empresas y el desarrollo de la formulación de cada uno de ellos, pero previamente dejaremos claro la importancia que tiene el empleo de una adecuada tasa de actualización en los respectivos modelos que la requieran.

Los modelos que ahora explicaremos y detallaremos son los siguientes: Modelos de valoración de intangibles, Modelos basados en la creación de valor para el accionista y las opciones reales.

Valorar una empresa es esencialmente formarse un juicio, profesional e independiente, en base a la aplicación de una serie de metodologías y a la experiencia profesional.

La valoración es un proceso básico en la identificación de las fuentes de creación, transmisión y destrucción de valor. Es indispensable su conocimiento en el mundo de las finanzas que considera las siguientes premisas (AECA, 1997):

1) El objetivo de cualquier empresa es maximizar su valor.

2) El valor de cualquier empresa viene determinado por su capacidad de generar renta.

3) Cualquier proceso de valoración debe consistir en transformar renta en valor.

Aceptar que el objetivo principal de cualquier empresa es maximizar su valor, debe entenderse bajo la actual percepción de que la generación de riqueza se entiende asociada al desarrollo y mantenimiento de ventajas competitivas de naturaleza intangible. La práctica demuestra que una empresa que no presta atención a aspectostales como a sus empleados o a sus clientes, encontrará que su valor será inferior al de otra empresa que sí losconsidera (Cornell, 1993).

En general, podemos decir que cualquier actividad que suponga un cambio en el seno de la actividad empresarial exige la realización de un proceso de valoración (García *et al*., 2005; Fernández, 2004), concretamente en ocasiones como:

La compra o venta de la empresa por razones estratégicas, de inversión, de fallecimiento del titular, etc.

Al ampliar/reducir capital, dando entrada o salida a algún socio.

En sucesiones de empresas.

Al recibir capital riesgo y a la hora de la desinversión.

Cuando se estudia el avalar a una *PYME* por parte de una Sociedad de Garantía Recíproca.

Para la utilización de otros tipos de financiación.

Cuando se quiere determinar si se ha creado valor para el accionista.

En el análisis de nuevas inversiones.

Apertura a mercados internacionales como consecuencia del proceso de globalización.Identificación de los impulsores de valor (*Value drivers* o *generadores de valor* son acciones o estrategias diseñadas por la dirección de la empresa o procedentes del entorno que afectan al valor de la empresa. Estos *generadores* o *conductores de valor* suelen influenciarse unos a otros continuamente. Ejemplos: política de precios y descuentos; nivel de calidad, grado de satisfacción del cliente, nivel de motivación de los trabajadores, calificación de la deuda, políticas adecuadas de seguridad de la información, etc.)

Otra clasificación es la que exponen Santandreu y Santandreu (1998), que consideran que los motivos pueden ser:

**De trascendencia interna.** Cuando la finalidad es informar a las personas que pertenecen a la empresa de algún proceso de valoración relativo a: conocimiento del patrimonio; ampliación de capital con medios internos; política de dividendos; motivos legales; causas de herencia; estudio de emisión de deuda; actualización contable; conocer la capacidad de endeudamiento.

**De trascendencia externa:** Cuando deba informar a terceros del valor de la empresa debido a posibles operaciones relativas a: ampliaciones de capital con medios externos; posibilidades de absorción; posibilidades de participación en otras empresas; venta; fusiones; otras.

A continuación, aclararemos algo tan fundamental como el empleo de una adecuada tasa de actualización, en los respectivos modelos de valoración que la necesiten.

## 5.2.0. La tasa de actualización en el análisis fundamental

Cuando valoramos una empresa hay dos variables fundamentales a tener en cuenta: el riesgo y el valor, las cuales evolucionan inversamente, cuando aumenta el riesgo disminuye el valor.

El riesgo se manifiesta en el coste de capital y éste en la tasa de actualización, la cual permitirá descontar los flujos futuros generados por una determinada empresa.

Para De la Torre y Jiménez (2014), la tasa de actualización debe incorporar el coste de oportunidad que sufre el inversor como consecuencia de su operación y el riesgo al que puede estar sometido la inversión.

Para estos mismos autores, la tasa de actualización, desde el punto de vista del accionista, debe asumir tanto el riesgo del mercado donde se negocian los títulos como el coste de oportunidad de la operación.

De esta manera, la metodología desarrollada por el C.A.P.M. (Capital Asset Price Model) se adecua convenientemente a las necesidades que demanda el inversor.

$Kt = Rf + (Rm - Rf) * ßt$

En donde:Kt = Rentabilidad exigida por el accionista; Rf= Rentabilidad de los activos libres de riesgo a largo plazo;Rm= Rentabilidad esperada del mercado; βt = Coeficiente de volatilidad, o coeficiente beta, del título "t".La diferencia entre Rm y Rf representa la prima por riesgo que exige el inversor del mercado.

Por otro lado, el coeficiente de volatilidad nos dice como varía la rentabilidad del título cuando varía la rentabilidad del mercado. O sea, mide el riesgo de la inversión en el mercado.

## 5.2.1 Los Modelos de Valoración de Intangibles

Los modelos de valoración de intangibles que explicaremos y desarrollaremos su formulación en detalle, son los siguientes: enfoque de coste; enfoque de mercado; enfoque ingresos/beneficios/flujos de caja

### 5.2.1.1. Valoración de Intangibles mediante enfoque de coste

Estos modelos valoran intangibles (marca, patente, etc.) atendiendo al coste de su desarrollo: adquisición, creación o mantenimiento del mismo durante cualquier etapa de desarrollo de la misma (testeo, I+D, concepto del producto, etc.)Los modelos de valoración bajo este enfoque, que vamos a estudiar son los de coste de reposición y las de coste de replicación.

#### 5.2.1.1.1. Valoración de Intangibles mediante coste de reposición

Para Smith (1997), el coste de reposición es el valor monetario de las inversiones necesarias y gastos para reemplazar y reponer los intangibles empresariales por otras con las mismas características, es decir, por otras que tenga una utilidad equivalente para el propietario.

#### 5.2.1.1.2. Valoración de Intangibles mediante coste de replicación

Según Pérez y Salinas (2008), el coste de replicación es aquel que debería de incurrirse para crear réplica del intangible empresarial en su situación actual (coste de planificación, diseño, investigación básica y aplicada, etc.). Este coste de replicación incluye los costes de desarrollo de prototipos fracasados o ineficientes, mientras que el coste de reposición no los incluiría.

## 5.2.1.2. Valoración de Intangibles mediante enfoque de mercado

El enfoque de mercado tiene en cuenta las transacciones recientes (ventas, adquisiciones, licencias, etc.) en que se han visto involucradas intangibles similares (patentes, marcas) y para las que se dispone del precio de la operación.

#### 5.2.1.2.1. Valoración de Intangibles mediante comparación de transacciones de ventas

El valor de los intangibles se calcula tomando como referencia valores de mercado abierto, donde exista evidencia de los precios a los cuales se han transferido activos intangibles (Pérez y Salinas, 2008).

## 5.2.1.3. Valoración de Intangibles mediante ingresos/beneficios/flujos de caja

El enfoque de ingresos/beneficios/flujos de caja se centra en la valoración de la capacidad de generación de beneficios o ingresos del intangible (marca, patente, etc.). Puede medirse estimando el valor presente de los beneficios o ingresos que se recibirán durante la vida del intangible.

#### 5.2.1.3.1. Relief from royalty

Este modelo supone la comparación de contratos de licencias realizados sobre activos intangibles similares (patentes, marcas, etc.) a fin de obtener un rango de referencia de tasas de royalty, las mismas se aplican luego sobre los ingresos de ventas que necesariamente deben proyectarse. El valor se establece como el valor presente de la corriente de ahorros de royalty (el dinero que la empresa ahorra por ser dueña del intangible) después de impuestos. Normalmente los ahorros se estiman como un porcentaje, que corresponde al hipotético royalty, sobre los cobros asociados específicamente con el intangible valorado (Pérez y Salinas, 2008).En definitiva, este método trata de determinar la tasa de royalty que una empresa tendría que pagar, si no fuera la propietaria del intangible y quisiera utilizarlo (Aaker, 1991).

#### 5.2.1.3.2. La Regla del 25%

Este método fue desarrollado por Robert Goldscheider (Smith y Parr, 2005; Parr, 2007; Razgaitis, 2003), el cual elaboró un estudio empírico sobre licencias comerciales a finales de los años cincuenta, en el cual detectó que los licenciatarios tendían a generar beneficios de alrededor del 20% de las ventas, sobre los cuales pagaban royalties del 5%. Así, las tasas de royalty representaban un 25% de los beneficios del licenciatario.A pesar de que Goldscheider escribió por primera vez sobre esta regla en 1971, puntualizó que había sido utilizada por expertos en valoración con anterioridad.En una valoración para licencia es habitual usar la regla del 25% del beneficio: el licenciante (propietariodel derecho) se queda con el 25% del beneficio del licenciatario (o en su defecto del 5% del volumen de ventas). Usar estos porcentajes como referencia es útil, pero no pueden ser válidos para todo tipo de activos y situaciones.

#### 5.2.1.3.3. Comparación de márgenes brutos con competidores relevantes, cuando no hay prima de precio

AUS Consultants denomina este modelo como técnica de las economías de escala, cuando una empresa posee una marca fuerte, pero no puede cobrar una prima de precio (Smith, 1997; Pérez y Salinas, 2008).Una compañía puede disfrutar de economías de escala en su producción o adquisiciones atribuibles a la marca. Para capturar el valor de estas economías de escala, se copara el margen bruto del negocio que no puede cobrar un precio primado con el margen bruto promedio de un grupo de competidores comparables. Esta diferencia se multiplica por los ingresos por ventas correspondientes a la marca.

$$GEC_m = (MB_m - MB_c)^* V_m$$

$$MB_m = \frac{MB_m}{V_m}$$

$$MB_c = \frac{\sum_{i=1}^{n} MB_i}{\sum_{i=1}^{n} V_i}$$

En donde:

GECm= ganancias por economías de escala atribuibles a la marca m; MBm= margen bruto correspondiente al negocio asociado a la marca *m*; MBc= margen bruto promedio del grupo de competidores comparables; Vm= ingresos por ventas del negocio asociado a la marca *m*; Vi= ingresos por ventas correspondientes al competidor *i* del grupo de *n* competidores comparables.

#### 5.2.1.3.4. Método de valoración de marcas de Damodaran

Damodaran (2002) propone valorar las marcas a partir de la diferencia en los ratios de capitalización sobre ventas. Las marcas fuertes permiten cargar precios superiores por los mismos productos, lo que a su vez genera márgenes de beneficio y ratios de capitalización sobre ventas superiores.

$$Valor\ de\ mercado = \left[(\frac{E}{V})_m - (\frac{E}{V})_g\right] * Ventas\ empresa\ con\ marca$$

En donde:(E/V)m = ratio de capitalización sobre ventas de la empresa con marca; (E/V)g = ratio de capitalización sobre ventas de la empresa sin marca.

#### 5.2.1.3.5. Modelo de Valoración de Interbrand

Interbrand valora una marca multiplicando el beneficio diferencial de la marca por un múltiplo. Este múltiplo, se determina cuantificando los factores que, según Interbrand, determinan la fortaleza de la marca, mediante la ponderación de siete factores: liderazgo, estabilidad, mercado, internacionalidad, trayectoria de la marca, apoyo y protección legal (Fernández, 2013).

Para el cálculo de este método se suele partir de una media ponderada del beneficio histórico antes de intereses e impuestos (EBIT) de los últimos tres años diferencial (restando el EBIT correspondiente a un producto genérico, sin marca o marca blanca) y eliminando el EBIT de las actividades que no sean resultado de la identidad de la marca.

Cuando la media ponderada de los EBIT históricos es superior a la previsión del EBIT de la marca para los años futuros se realiza una provisión para reflejar esta reducción. Para llegar al beneficio diferencial de la marca, se deduce la remuneración de los recursos y los impuestos.

#### 5.2.1.3.6. Método de valoración de propiedades intelectuales de Sam Khoury

El Doctor Sam Khoury nos muestra el empleo que se hace del método del factor tecnológico (Sullivan, 2001) para valorar las propiedades intelectuales aplicadas a los productos y procesos de la empresa Dow Chemical, dentro de los sectores de productos químicos y plásticos. En esta metodología el valor de la tecnología se basa en el flujo de caja generado por la utilidad y la ventaja competitiva que una compañía obtiene de la posesión o bien del uso de la propiedad intelectual subyacente (patentes, inventos, fórmulas, etc.).

El factor tecnológico es una expresión del incremento del flujo de caja que se espera obtener con la práctica de una tecnología específica dentro de una empresa, valorando a este factor según las dimensiones de utilidad y competitividad. Se expresa como un porcentaje del valor neto presente (VNP) del incremento esperado del conjunto de la empresa.

$$Valortecnología = VANdel\ \Delta\ flujocajaportecnología + Factortecnológico$$

La ventaja competitiva resultante se manifestará como un aumento de la cuota de mercado, como prima (incremento de precio) sobre tecnologías competitivas o como un ahorro en costes.

#### 5.2.1.3.7. Modelo de Kellog y Charnes (2000)

Los autores presentan un modelo para valorar empresas biotecnológicas. El valor tiene su origen en las ganancias que se obtendrían de sus productos y de las posibilidades de crecimiento que se pueden obtener con aquellos desarrollos que tengan en investigación.

En el proceso de análisis de biotecnología, las fases son las siguientes:

1. *Descubrimiento (discovery)*: se desarrollan y sintetizan nuevas entidades moleculares.

2. *Preclínica*: se prueban las soluciones in vitro y en animales. Si esta etapa es exitosa se debe obtener la autorización de la autoridad sanitaria para continuar con las fases siguientes.

3. *Pruebas clínicas de fase I*: prueba a un número reducido de voluntarios sanos para obtener información sobre la toxicidad del medicamento en estudio, sus dosis óptimas, sus efectos metabólicos, su distribución en el cuerpo y como el medicamento es eliminado por el organismo.

4. *Pruebas clínicas de fase II*: se empieza a evaluar la eficacia del medicamento, ya que se empieza a aplicar sobre pacientes para continuar obteniendo información sobre la seguridad del medicamento

5. *Pruebas clínicas de fase III*: trata de diseñar la forma en que se va a utilizar el fármaco tras la autorización médica. Se hacen pruebas a gran escala sobre pacientes para obtener más datos sobre la eficacia, además de las reacciones negativas que pueden surgir en los diversos pacientes.

6. *Registro en la autoridad sanitaria pertinente*: una vez conseguida la suficiente evidencia del correcto funcionamiento del medicamento, conseguida en las fases anteriores, se solicitará la autorización a la entidad que supervise a la industria farmacéutica.

7. *Posautorización*: estando ya el producto en el mercado, la compañía continúa realizando investigaciones para obtener extensiones del producto.En el modelo de árboles de decisión, el primer paso es la estimación del valor presente neto esperado del medicamento en desarrollo, sin tener en cuenta las opciones de crecimiento (Lamothe y Aragón, 2003):

$$VPEN = \sum_{i=1}^{7} \rho_i \sum_{t=1}^{T} \frac{DCF_{it}}{(1+r_d)} + \rho_7 \sum_{j=1}^{5} q_j \sum_{t=1}^{T} \frac{CCF_{jt}}{(1+r_c)^t}$$

En donde:VPEN= valor presente neto esperado; ρi= la probabilidad condicional de que la etapa *i* es la etapa final en un medicamento que alcanzó el estadio *i*-1; T= momento en que el producto deja de generar cash flows; DCFIT= cash flow de desarrollo esperado en el tiempo t, siendo i la última etapa; CCTjt= cash flow de comercialización en el tiempo t para un medicamento de calidad *j*; rd= tasa de descuento de los cashflows de desarrollo; rc= tasa de descuento de los cash flows de comercialización; *j*= índice de calidad del medicamento, donde 1 es baja calidda y 5 es sobresaliente; qj= probabilidad de que el medicamento sea de calidad j.

Inicialmente valoraremos los flujos de caja negativos que corresponden a la etapa de desarrollo del producto, ponderados por su probabilidad, para luego realizar la misma operación, ponderando el flujo de caja obtenido por la venta del medicamento por la probabilidad de que sea de una calidad determinada.

En el cálculo, se incorpora la probabilidad de abandonar el proyecto. La gran desventaja hasta aquí es que ignora las opciones de crecimiento (crear nuevos productos o innovaciones), para resolver este problema se modela otro árbol binomial para el nuevo medicamento en desarrollo, cuyo valor al momento del lanzamiento del primer medicamento se agrega a los valores de las ramas finales del primer producto.

A continuación, obtenemos el valor actual del medicamento en cuestión (A) mediante el descuento de flujos de caja de comercialización al momento inicial del lanzamiento:

$$A = \sum_{j=1}^{5} q_j \sum_{t=1}^{T} \frac{CCF_{jt}}{(1+r_c)^t}$$

Posteriormente, se construye un árbol binomial con los posibles valores de A, atendiendo a sus probabilidades de fracaso y éxito, es decir, las variaciones que se producen en el valor del activo hasta obtener valores finales.

El siguiente paso sería incluir el valor de la opción de crecimiento, ya que es asimilable comprar una opción call (derecho de compra sobre un activo) sobre el valor de un próximo medicamento.Esto implicaría construir otro árbol binomial, con los mismos supuestos que el árbol del primer activo y cuyo valor de la opción se agrega a los valores finales de este primer árbol, para ello se debe conocer las probabilidad de continuar en períodos sucesivos y los pagos que se hacen por inversión y desarrollo en el período en cuestión.

**5.2.1.3.8. Modelo de empresa de crecimiento de Scwartz y Gorostiza (2000)**

Fue desarrollado para valorar inversiones en productos y tecnologías innovadoras que irrumpen en el mercado y que no pueden ser tratados por los métodos tradicionales ya que se necesita la incorporación de la flexibilidad.En este modelo nos encontramos con dos fases (Lamothe y Aragón, 2003):

En la primera fase hay dos etapas: en la primera se desarrolla la tecnología y en la segunda se comercializa en un mercado incipiente de prueba, en donde se continuarán agregando mejoras.

En la segunda fase, la tecnología ya desarrollada se comercializa en el mercado principal Este método contempla dos series de ecuaciones estocásticas, una para costes (1) y otra para los flujos de caja (2).

(1)$dK = -Idt + (Ik)1/2\ dz$

(2)$dC = (\alpha - ŋ)\ dt + \Phi C dx$

Donde:K= costes de llevar a cabo el proyecto; I= tasa de inversión para un período infinitesimal dt; ß= desviación típica del cambio de los costes; ŋc=prima de riesgo;

Φ=volatilidad de los flujos de caja en tiempo continuo; dz,x=incremento en un proceso de Wiener (*) no correlacionado con la economía; α= tendencia de los flujos de caja.

(*) Schwartz, E.S. y Gorostiza, C.Z. (2000): Valuation of Information Technology Investments as Real Options; American Finance Association; Meeting 2001; New Orleans.

El valor del proyecto se obtiene de la siguiente fórmula:

$$V = \left(PVCash_{Incipiente} + PVCash_{Principal}\right) - \left(PVCost_{Etapa1} + PVCost_{Etapa2}\right)$$

$$PVCost_{Etapa1} = E_0\left[\int_0^{\tau_1} I_1 e^{-(r_f+\lambda_1)^t dt}\right]$$

$$PVCost_{Etapa2} = E_0\left[\left(\int_{\tau_1}^{\tau_2} I_2 * e^{-(rf+\lambda_2)(t-\tau_1)} d_t\right) * e^{-(r_f+\lambda_1)\tau_1}\right]$$

$$PVCash_{Incipiente} = E_0\left[\left(\int_{\tau_1}^{T_1} C_{1,t} * e^{-(rf+\alpha_1)(t-\tau_1)} d_t\right) * e^{-(r_f+\lambda_1)\tau}\right]$$

$$PVCash_{Principal} = E_0\left[\left(\int_{\tau_1}^{\tau_2} C_{1,t} * e^{\alpha_{1(t-\tau_1)e}{}^{-(r_f+\lambda_2)(t+\tau_1)}} d_t\right) * e^{-(r_f+\lambda_1)\tau_1} + \left(\int_{\tau_2}^{T_2} C_{2,t} * e^{\alpha_2(1-\tau_2)} e^{-r_f(t+\tau_2)} d_t\right) * e^{-(r_f+\lambda_2)(\tau_2-\tau_1)} * e^{-(r_f+\lambda_1)\tau_1}\right]$$

Donde:

PVCashIncipiente =valor presente de los flujos de caja en el mercado incipiente; PVCashPrincipal =valor presente de los flujos de caja en el mercado principal; PVCostEtapa1,

Etapa2 =valor presente de los costes de desarrollo de la tecnología en la etapa1y 2; I= tasa de inversión; rf= tasa libre de riesgo; Ƭ=variable aleatoria que determina el final de una etapa; λ1 y λ2 =tasas de fracaso para las etapas referidas; α = tasa de crecimiento ajustada por riesgo de los flujos de caja netos; ŋc=prima de riesgo.

#### 5.2.1.3.9. Modelo Schwartz y Moon

Schwartz y Moon (2000), plantean una serie de ecuaciones diferenciales y otras determinísticas para modelizar el comportamiento de una empresa de la nueva economía.Para estos autores (Lamothe y Méndez, 2013), los ingresos evolucionan según la siguiente ecuación estocástica diferencial:

$$\frac{dRt}{Rt} = \mu t dt + \sigma t dZ1$$

En donde:

R= ingresos por ventas; µt =tasa esperada de crecimiento en los ingresos que sigue un proceso de reversión a la media en el largo plazo (µ); σ = volatilidad de la tasa de crecimiento; Z1 = incorpora el componente aleatorio y es una variable estocástica que sigue una distribución normal:

$d\mu t = (\mu - \mu t)\, dt + ŋ t dZ2$

Aquí, ŋ0 es la volatilidad inicial de las tasas de crecimiento esperadas de los ingresos y K indica la velocidad a la que se espera que el crecimiento converja a su promedio en el largo plazo.

Los cash flows después de impuestos vienen dados por Yt:$Yt = (Rt - Costt) * (1 - \tau c)$

La evolución de los costes se modeliza en la siguiente ecuación:

$Costt = COGSt + Otrosgastost$

En donde:

COGS= costes de las ventas que se asumen proporcionales a los ingresos; Otros gastos= hay una parte fija y otra parte que está en función de los ingresos; Xt = cantidad de efectivo (lo emplearemos en la ecuación posterior).

Todo lo expresado aquí nos lleva a indicar que los flujos generados permanecen en la compañía, capitalizados a una tasa libre de riesgo por un período de largo plazo (T) en la que se distribuirá todo el efectivo. En donde el valor de la empresa es:

$$Valordelaempresa = Eq * (Xt * e^{-rT})$$

Hay que incluir un valor terminal (como un múltiplo sobre Ebitda, por ejemplo) al modelo anterior, ya que éste sólo asume que se extiende hasta el período T.A continuación, estudiaremos los modelos de creación de valoración.

## 5.2.2. Los Modelos de Creación de valor

Para Fernández (2000), la creación de valor es el aumento del valor para los accionistas por encima de las expectativas, lo que se refleja resto en la rentabilidad exigida por los accionistas.

Los modelos de creación de valor que explicaremos y desarrollaremos su formulación en detalle son los siguientes: Economic Value Added (EVA); Beneficio Económico; Market Value Added (MVA); Cash Value Added (CVA); Cash Flow Return on Investment (CFROI).

### 5.2.2.1. Beneficio Económico

Es el beneficio resultante de la diferencia entre los ingresos, los gastos y los intereses de capital, a una tasa vigente.$Bº\ Económicot$ = BVet − 1 ∗ (ROEt − Ket)En donde:BVet-1= valor en libros de las acciones de la empresa; ROEt= rentabilidad financiera de la compañía; Ket= tasa de rentabilidad exigida a las acciones.

### 5.2.2.2. Economic Value Added (EVA)

Este concepto tiene su origen en la consultora neoyorquina Stern Stewart & Co, en 1983, y lo podemos definir como el importe que queda una vez deducido de los ingresos la totalidad de los gastos, incluidos el coste de oportunidad de capital y los impuestos (Amat, 1999).

$EVAt = NOPATt - WACCt*ICt-$

1En donde:IC= valor contable del activo; NOPAT= resultado de las actividades ordinarias antes de intereses y después de impuestos; WACC= coste medio ponderado capital.

### 5.2.2.3. Cash Value Added (CVA)

Para Ottosson y Weissenrieder (1996), una empresa debe de tener la capacidad de identificar las oportunidades de crecimiento, que afectan positivamente a su valoración.El valor de mercado de una acción puede ser estimada por la suma del valor presente de los flujos de caja futuros, de los negocios corrientes de la empresa y el valor presente de los flujos de caja futuros derivados de las oportunidades de crecimiento y las futuras inversiones (Milla, 2010).

$CVAt = OCFt - OCFDt$

En donde:

OCF= suma del Ebitda, las inversiones incrementales en necesidades operativas de fondos (NOF) y las inversiones incrementales en activos fijos no estratégicos; OCFD= flujos de caja necesarios para cubrir las expectativas de los inversores en relación con las inversiones estratégicas en activos fijos.

### 5.2.2.4. Cash Flow Return on Investment (CFROI)

Para Madden (2003), el CFROI es la tasa interna de retorno de los flujos brutos de caja, ajustados por inflación, de la totalidad de los proyectos e inversión existentes en una empresa.

$$CFROI\ t = TIR \sum_{t=0}^{n} \frac{FBCt}{(1 + WACCsi)^{t}} = 0$$

En donde:

FBC= flujos brutos de caja, ajustados por inflación, de todos los proyectos de inversión existentes en una empresa en un momento dado; WACC= coste medio ponderado del capital también ajustado por inflación.

#### 5.2.2.5. Market Value Added (MVA)

El valor del mercado añadido (MVA) equivale al valor actual de los EVA futuros descontados al WACC.

$$MVA\ t = \sum_{t=0}^{n} \frac{EVAt}{(1 + WACC)^{t}} = 0$$

En donde:EVA= valor económico añadido; WACC= el coste medio ponderado del capital.

A continuación, estudiaremos los modelos de opciones reales.

### 5.2.3. Los Modelos de Opciones reales

Las opciones reales son modelos de decisión basados en la incertidumbre relacionada con las inversiones, en donde el valor de la empresa se obtiene empleando la teoría de las opciones financieras y sus diversas formulaciones, como el caso del los métodos de simulación numérica de arboles binomiales, desarrollado por Cox et al. (1979); el Método de Montecarlo de Boyle (1977), y el de árboles trinomiales también de Boyle (1986) y el modelo de opciones de Black et al. (1973), conocido comúnmente como método de valoración en tiempo continuo de Black & Scholes.

Inicialmente, hay que aclarar la definición de opción, la cual supone el derecho, pero no la obligación, de desarrollar una actividad en el futuro. Existen dos clases de opciones, la del derecho a comprar llamada comúnmente call y la del derecho a vender llamada put.Desde un punto de vista financiero, la opción es un contrato que proporciona a su propietario el derecho, no la obligación, a comprar o vender una cantidad de activos, a un precio establecido, en una fecha determinada o en cualquier momento anterior a dicha fecha que se haya establecido.

El poseedor ejercerá dicha opción cuando le convenga, para ello deberá pagar la respectiva prima por tal opción. Cuando ésta se pueda ejercer en cualquier momento del plazo del contrato, se la denominará que es de estilo americano y cuando sólo puede ser ejercerse en una fecha determinada de vencimiento se denomina como estilo europeo.

El argumento que avala el empleo de los modelos de opciones reales, en la valoración de empresas, es evitar la rigidez que presenta el modelo VAN en el cálculo de los flujos de caja

futuros descontados, ya que éstos son derechos que poseen las empresas sobre determinados activos y que les ofrecen diferentes caminos o alternativas a seguir, proporcionándoles la ventaja de poder adaptarse al entorno con mayor flexibilidad y soportando menores riesgos (Mascareñas et al., 2004).

Según Myers (1984), bajo el enfoque de las opciones reales, el activo total de la empresa se compone de dos elementos básicos: el de las inversiones ejecutadas y en funcionamiento (que recogen el valor de los activos tangibles e intangibles que actualmente posee y utiliza la empresa) y el de sus oportunidades futuras de inversión (opciones reales).Para Lamothe et al., (2003), incorporando la flexibilidad que le aporta la Teoría de Opciones, el nuevo concepto del VAN sería:

$$VAN(ampliado) = VAN(tradicional) + \underbrace{OR_1 + OR_2 + \ldots + ORn}_{Flexibilidad}$$

En donde:

*OR1+…+ ORn* = primas de cada una de las opciones reales presentes en el proyecto de inversión.*VAN* tradicional = El activo subyacente

Por tanto, la Teoría de Opciones permite valorar la flexibilidad en la gestión de las empresas, es decir, en su toma de decisiones (la opción de abandonar, diferir, expandir, reducir, etc.).

Los elementos que determinan el valor de una opción financiera son distintos de los que influyen en una opción real, por lo que las claves en el cálculo de las opciones financieras son el precio de la acción, los dividendos, la tasa libre de riesgo, la volatilidad que incorporan los niveles de incertidumbre y la fecha de vencimiento; mientras que en las opciones reales son (Copeland et al., 2000): la fecha de vencimiento del contrato, la incertidumbre de los flujos de caja, el valor presente de los flujos de caja, el valor perdido a lo largo de la duración de la opción, la tasa libre de riesgo y el coste de la inversión.

La mayoría de los proyectos de inversión implican la realización de un desembolso para comprar un activo, lo que es análogo al ejercicio de una opción. Así, la cantidad invertida es el precio de ejercicio (E), el valor actual de los flujos de caja esperados se corresponde con el precio del activo subyacente (S) y el periodo de tiempo durante el cual existe la oportunidad de inversión (tiempo que la empresa puede esperar sin perder la oportunidad de invertir) es el tiempo hasta el vencimiento (t). El valor temporal del dinero viene dado por la tasa de interés sin riesgo (Rf) y el valor del riesgo del proyecto viene reflejado por la volatilidad de los flujos de caja futuros (σ). El valor que se va perdiendo durante la vida de la opción (o los flujos de caja a los que se renuncia mientras no se ejerza la opción) se corresponde a la variable dividendos de las opciones financieras (d) (Damodaran, 2006; Fernández, 2004; Mascareñas et al. 2004,Leslie y Michaels, 1997; Adam y Goyal, 2002; Al-Horani et al., 2003; Ruíz y Gil, 2004).

En la toma de decisiones empresariales la incertidumbre es una constante y la herramienta para resolverla son las opciones. Existen diversos tipos de opciones reales (Amram y Kulatilaka, 2000, Copeland et al. 2000, Lamothe y Méndez, 2013): diferir o posponer la inversión; abandonar; crecimiento; reducir; flexibilidad; aprendizaje; múltiples fuentes compuestas o rainbow.

Según el grado de exclusividad, dentro de las opciones de crecimiento, podemos encontrar dos tipos de opciones:

Opciones exclusivas: ofrecen el derecho exclusivo a ejercitarlas. Estas resultan de patentes, del conocimiento exclusivo por parte de la empresa o de una tecnología que la competencia no puede imitar. Son las opciones más valiosas.

Opciones compartidas: representan oportunidades "colectivas" del sector, como la posibilidad de introducirse en un mercado no protegido por grandes barreras, o de construir una nueva fábrica para abastecerse un particular segmento del mercado. Estas opciones son menos valiosas que las anteriores.

Encontramos dos tipos de grupos para valorar las opciones reales:

El método de Black-Scholes, consistente en un modelo analítico de tiempo continúo.Los métodos numéricos de valoración, que a su vez, se dividen en: Modelos en tiempo discreto mediante simulación organizada binomial; Modelos en tiempo discreto mediante simulación organizada trinomial; Modelo en tiempo discreto mediante simulación aleatoria del subyacente, conocido como de Montecarlo.

Los modelos de opciones reales que explicaremos y desarrollaremos su formulación en detalle son los siguientes: método de Black-Scholes; modelos de árboles binomiales; modelos de árboles trinomiales; modelo de simulación de Montecarlo.

### 5.2.3.1. El método de Black-Scholes

Este método de valoración de opciones calcula el valor de la opción a partir de una cartera de títulos negociables en el mercado que tienen el mismo retorno que la opción y que imitan sus fluctuaciones de valor a lo largo del tiempo (Amram y Kulatilaka, 2000).En esta valoración, las fórmulas utilizadas son (Lamothe et al., 2003):

$$C = S * e^{-qt} * N(d_1) - E * e^{-rt} * N(d_2)$$

$$P = E * e^{-rt} N(-d_2) - S * e^{-qt} * N(-d_1)$$

$$d_1 = \frac{In\left(\frac{S}{E}\right) + \left(r - q + \frac{\sigma^2}{2}\right)t}{\sigma\sqrt{t}}$$

$$d_2 = d_1 - \sigma\sqrt{t}$$

En donde:

*C* = Precio *call* europea; *P* = Precio *put* europea; *Q* = Tasa de dividendos; *R* = Tipo de interés libre de riesgo; *t* = Tiempo a vencimiento; *S* = Precio del activo subyacente; *σ* = Volatilidad del activo subyacente; *E* = Precio del ejercicio o strike; *N(d)* = Valor de la distribución normal estándar.

Conseguir replicar las condiciones que interactúan en las opciones financieras a las opciones reales, presenta unas dificultades que hace inicialmente poco práctica la utilización de este método.

### 5.2.3.2. Modelos de Árboles Binomiales

El modelo se apoya en la hipótesis de que el precio del activo subyacente evoluciona a lo largo del tiempo siguiendo un proceso binomial que describe dos posibles movimientos, uno superior (up) y otro inferior (down) al precio del ejercicio. En el árbol binomial, en cada período, el activo subyacente sólo puede asumir uno de dos valores posibles: up es el salto alcista y down el salto bajista del activo subyacente, éstos se calculan a través de la siguiente formulación:

$$up = e^{\sigma\sqrt{t/n}} \qquad down = e^{-\sigma\sqrt{t/n}}$$

En cada periodo del árbol binomial se supone que el precio de la acción hoy, sólo puede asumir una de dos posibilidades: (uS) en el caso favorable y (dS) en el caso desfavorable, con unas probabilidades asociadas (p) y (1-p) respectivamenteEl cálculo de las probabilidades up y down son los siguientes:

$$p_u = \frac{e^{(r-q)\Delta_t} - d}{u - d} \qquad p_d = 1 - p_u \;\; ; \qquad \Delta_t = \frac{t}{n}$$

En cada nodo del árbol binomial se calcula la prima de la opción, donde se multiplica el precio del activo subyacente por la probabilidad de que suba o baje, para luego éstos descontarse a la tasa libre de riesgo mediante las siguientes fórmulas (Lamothe et al., 2003):

$$C = r^{r-n}\left[\sum_{j-0}^{n}\left(\frac{n!}{j!(n-j)!}\right)p^{j}(1-p)^{n-j}MAX\left[0;u^{j} * d^{n-j} * S - E\right]\right]$$

$$P = r^{r-n}\left[\sum_{j=0}^{n}\left(\frac{n!}{j!(n-j)!}\right)p^{j}(1-p)^{n-j}MAX\left[0;E - u^{j} * d^{n-j} * S\right]\right]$$

El principal problema que encontramos al aplicar el modelo binomial es la estimación de las probabilidades asociadas de ocurrencia de las variables y la dificultad que supone encontrar un valor en el mercado que replique exactamente la evolución de la empresa a valorar.

### 5.2.3.3. Modelos de Árboles Trinomiales

La formulación de este modelo fue realizada por Boyle (1986). Este método entiende que el subyacente se mueve en tres posiciones: favorable (up), desfavorables (down) e intermedia (medium), por lo que a partir de cada nodo siempre habrá tres posibles opciones. En este método la incertidumbre se medirá como la desviación de la tendencia esperada. Boyle (1986) propone la siguiente formulación:

$$u = e^{\sigma\sqrt{2t/n}} \qquad d = e^{-\sigma\sqrt{2t/n}}$$

$$p_u = \left( \frac{e^{[(r-q)\Delta_t/2]} - e^{\left[-\sigma\sqrt{\Delta_t/2}\right]}}{e^{\left[\sigma\sqrt{\Delta_t/2}\right]} - e^{\left[-\sigma\sqrt{\Delta_t/2}\right]}} \right)^2 \qquad p_d = \left( \frac{e^{\left[\sigma\sqrt{\Delta_t/2}\right]} - e^{[(r-q)\Delta_t/2]}}{e^{\left[\sigma\sqrt{\Delta_t/2}\right]} - e^{\left[-\sigma\sqrt{\Delta_t/2}\right]}} \right)^2$$

$$p_m = 1 - p_u - p_d$$

Se debe calcular la prima de las opciones en cada nodo del árbol, multiplicando el valor del activo subyacente (up, medium y down) por la probabilidad de ocurrencia, para luego descontar a la tasa libre de riesgo (Lamothe y Aragón, 2003). El árbol decisional mejora con la consideración de la opción intermedia.

### 5.2.3.4. Modelo de simulación de Montecarlo

El método fue creado por Boyle (1977) y está considerado como un sistema de simulación numérica, que puede ser utilizado en la valoración de las opciones financieras.

Este modelo nos permite analizar miles de posibles alternativas en la evolución del activo subyacente, a lo largo de un período establecido, lo que permitirá determinar la estrategia óptima y calcular su retorno (Amram y Kulatilaka, 2000). Su utilización nos lleva a tener que estimar el valor de la empresa, para cada extremo del intervalo establecido en la variable considerada representativa de los resultados futuros, teniendo un valor de la empresa para el escenario optimista y otro para el escenario pesimista.

En el desarrollo de éste se supone que el activo subyacente se distribuye de forma lognormal, procedente de un proceso browniano analíticamente. Para valorar la opción, se determina su valor intrínseco al vencimiento en cada serie generada y se actualiza ese valor. Se tendrán tantas primas como posibilidades generadas y se actualiza ese valor. El valor de la opción se calcula como una medida aritmética de la prima descontada.

Este modelo es adecuado para valorar las opciones, tipo europeas (Lamothe et al., 2003), es decir, con fecha de vencimiento única y su formulación es:

$$S + dS = S\exp\left[\left(\mu - \frac{1\sigma^2}{2}\right)dt + \sigma\right]$$

$$S + \Delta S = S\exp\left[\left(\mu - \frac{1\sigma^2}{2}\right)\Delta t + \sigma\varepsilon_t\sqrt{\Delta_t}\right]$$

En donde:*dt* = Proceso de desviación estándar uno y media cero expresado en tiempo discreto; Δ*S* = La tasa de variación en tiempo discreto de *S* para un intervalo de tiempo llamado salto temporal ***Δt; Δt*** es una variable aleatoria que se distribuye *N* (0,1).

Los principales inconvenientes que encontramos en este modelo son la dificultad para definir los parámetros necesarios para valorar adecuadamente las opciones reales y para cuantificar la volatilidad de las fuentes de incertidumbre, además de una mayor complejidad de cálculo si lo comparamos con el valor actual.

Una vez llegados a este punto es fundamental expresar nuestras consideraciones finales sobre el tema estudiado en el presente capítulo.

## 5.3. CONSIDERACIONES FINALES

Toda valoración de empresas responde a la necesidad específica de quien la solicita y de quien la lleva a cabo, esto nos permite afirmar la no existencia de unanimidad en la utilización de los distintos modelos y que en el empleo de éstas se está sujeto a juicios de carácter subjetivo, como las predicciones sobre el comportamiento futuro de diversos aspectos del desarrollo del negocio y de su entorno económico.

Una correcta valoración de empresas requiere conocer la actividad a la que se dedica la compañía objeto de la valoración; el entorno económico en el que se actúa; la futura evolución de la economía; la estructura, capacidades y recursos disponibles en la organización y considerar el modelo más adecuado en cada valoración. Consideramos que la actividad de valorar empresas debe ser el resultado de un proceso bien estructurado y de la aplicación de unas fórmulas probadas, que permitan llegar a un intervalo de valor posible.

Con referencia a la valoración de empresas cuyo negocio se centra internet, es un proceso que se compone de una serie de pasos a los que ya hemos hecho alusión anteriormente, Juan Mascareña (2001): conocer la empresa y su cultura organizativa, lo que implica conocer a su personal, su forma de actuar y de resolver los problemas; conocer al equipo directivo; conocer el negocio y su entorno, quiénes son sus proveedores, clientes y competidores, cuál es su salud financiera y cuál ha sido su evolución histórica, analizar el sector en el que centra sus actividades y, por extensión, la situación general, estudiar su plan de negocio con objeto de estimar su viabilidad futura; prever el futuro, consiste e calcular el valor de la empresa en relación a los flujos de caja que se estima genere en el futuro, para ello habrá que crear una serie de escenarios futuros y aplicar una serie de métodos de valoración; matizar los resultaos obtenidos para adecuarlos al objetivo de la valoración. Entre los métodos a aplicar a estas empresas cuyo negocio se centra en internet tenemos: la valoración de los flujos de caja estimados; la valoraión a través de las opciones reales. No obstante, siguiendo al Reputation Institute hoy es importante también valorar la información relativa a la ética de la empresa Respeto a los datos y a la economía de datos, transparencia, marca y calidad.

En el ámbito académico hay una especial predilección por los modelos basados en el descuento de flujos de caja, ya que son consideradas como las técnicas más completas y las más utilizadas en los procesos de valoración empresariales. Sin embargo, afirmamos que los recursos intangibles, como elementos generadores de resultados económicos empresariales son ignorados en la elaboración de los cash flows.

Además, este modelo tampoco tiene en cuenta las posibles opciones de que el plan no se cumpla, tanto por las desviaciones positivas como negativas. Estas dos limitaciones hacen que el modelo de flujos descontados “penalice” el valor de la empresa.

Los modelos de las opciones reales surgen como complemento del modelo de flujos descontados, para resolver el problema de la rigidez del plan financiero, ya que incorporan

flexibilidad al plan financiero, valorando la opción de poder tomar un nuevo camino al no cumplirse los objetivos establecidos en dicho

Las opciones reales no sólo reconocen el valor de la propiedad sobre la corriente de renta de las inversiones, sino también el valor los derechos de decisión sobre la explotación de oportunidades futuras.

## 5.4. BIBLIOGRAFÍA

AAKER, D. (1991): Managing Brand Equity: Capitalizing on the value of a brand name, Ed. The Free Press. New York. Estados Unidos

ADAM, T. AND V.K. GOYAL (2002), 'The Investment Opportunity Set and its Proxy Variables: Theory and Evidence'; SSRN Electronic Paper Collection (January).

ADSERÀ, X.; VIÑOLAS, P. (2003): Principios de Valoración de Empresas. Ed. Deusto. Bilbao.

(AECA) ASOCIACIÓN ESPAÑOLA DE CONTABILIDAD Y ADMINISTRACIÓN DE EMPRESAS (1997): Principios de Valoración de Empresas, Estudio de Aplicabilidad de los Diferentes Métodos de Valoración. Documento 5. Ed. Gráficas Ortega. Madrid.

AMAT, O. (1999): EVA. Un nuevo enfoque para optimizar la gestión, motivar y crear valor. Gestión 2000.Barcelona.

AMRAM, M. Y KULATILAKA, N.: (2000). Opciones Reales. Harvard Business School Press. Gestión 2000.Barcelona

AL-HORANI, A., P.F. POPE AND A.W. STARK (2003), 'Research and Development Activity and Expected Returnsin the United Kingdom', European Finance Review, Vol. 7, No. 1, pp. 27–46

BLACK, F.; SCHOLES, M. (1973): The pricing of options and corporate liabilities; journal of political economy, 81;mayo-junio.

BOYLE, P. (1977): Options: a Monte Carlo approach"; journal of financial economics 4; chapter 1.

BOYLE, P. (1986). Option valuation using a three-jump process. International Options Journal, Vol. 3, 7-12.

BREALEY, R.A.; MYERS, S.C. (1999): Fundamentos de financiación empresarial. Ed. Mc Graw-Hill.

BRILMAN, J.; CAUDE M. (1990): Manual de Valoración de Empresas; Ediciones Díaz de Santos S. A. Madrid.España.

COPELAND, T.; KOLLER, T.; MURRIN, J. (2000): Valuation Measuring and Managing the Value of Companies. Ed. John Wiley & Sons, Inc. New York.

CORNELL, B. (1993): Corporate Valuation, Business One Irwin.

COX, J.C.; ROSS, S.A.; RUBENSTEIN, M. (1979): Option pricing: a simplified approach; journal of financial economics; nº7.

DAMODARAN, A. (2002): Investment Valuation. Ed. Wiley Finance. Second. Edition New York.

DAMODARAN, A. (2006): Damodaran on Valuation: Security Analysis for Investment and Corporate Finance. JohnWiley & Sons, Inc. New Jersey.

DE LA TORRE GALLEGOS, A.; JIMÉNEZ NAHARRO, F. (2014): Valoración de empresas y análisis bursátil. Pirámide. Madrid.

FERNÁNDEZ, P. (2000): Creación de valor para los accionistas. Ed. Gestión 2000. Barcelona.

FERNÁNDEZ, P. (2004): Valoración de Empresas. Ed. Gestión 2000. Segunda Edición Madrid.

IESE, Barcelona.FERNÁNDEZ, P. (2013): Valoración de empresas y sentido común; cuarta edición; University of Navarra - IESEBusiness School; 29 de abril; http://ssrn.com/abstract=2202141

GARCÍA, R.; JIMÉNEZ, F.; PÉREZ, C. (2005): La valoración de pequeñas y medianas empresas. XV JornadasHispano-Lusas de Gestión Científica, Sevilla.

JIMÉNEZ NAHARRO, F.; SANTIAGO MORENO, I.; DE LA TORRE GALLEGOS, A. (2013): M2M Marketplace: el valor de lo intangible. Digital@tres. Sevilla.

KELLOGG, D.; CHARNES, J. M. (2000): Real-options valuation for a biotechnology company. Financial Analysts Journal. 56.3.May/Jun.

LAMOTHE, P.; ARAGÓN, R. (2003): Valoración de Empresas Asociadas a la Nueva Economía. Ed.Pirámide.Madrid.

LAMOTHE, P.; MÉNDEZ, M. (2013): Opciones reales. Métodos de simulación y valoración; Ed. Ecobook; Ecobook Editorial del Economista; Madrid.

LESLIE, K.J.; M.P. MICHAELS (1997), “The Real Power of Real Options”, The McKinsey Quarterly, Number 3, pp.5-22.

LEV B. (2013): Ganar la confianza de los accionistas. Guia para fortalecer el valor de la empresa a traves de integrida; Ed. Profit. Barcelona.

MADDEN, B.J. (2003): Cash Flow Return on Investment. CFROI Valuation. A total system approach to valuing the firm; Butterworth-Heinemann Finance; Oxford.

MARTÍN, J.L.; TRUJILLO, A. (2000): Manual de valoración de empresas; Ed. Ariel; primera edición; Barcelona.

MASCAREÑAS, J.; LAMOTHE, P.; LÓPEZ LUBIÁN, F.J. Y DE LUNA, W. (2004): Opciones Reales y Valoración de Activos. Prentice Hall, Madrid.

MILLA GUTIÉRREZ, A. (2010): Creación de valor para el accionista. Díaz de Satos. Madrid.

MYERS, S.C. (1984): Finance theory and financial strategy; Interfaces 14; Enero-Febrero.

OHLSON, J.A. (1989): Accounting earnings, book value, and dividends: The theory of clean surplus equation.Working Paper. Lancaster University. September.

OHLSON, J.A. (1995): Earnings, book values, and dividends in equity valuation. Contemporary Accounting Research; Spring, pp. 661-687.

OTTOSON E.; WEISSENRIEDER, F. (1996): Cash Value added-A new method for measuring financial performance; Gothenburg University; working paper 1996:1.

PARR, R.L. (2007): Royalty rates for licensing intellectual property. Ed. John Wiley & Sons. Estados Unidos.

PÉREZ CASTRO, C. Y SALINAS, G. (2008): Valoración y evaluación de marcas. Ed. Deusto. Barcelona.

PETERS, T.J.; WATERMAN, R.H.JR. (1994): En busca de la excelencia: lecciones de las empresas mejor gestionadas de Estados Unidos; Ed. Folio; Barcelona.

RAZGAITIS, R. (2003): Valuation and pricing of technology-based intellectual property. Ed. Jon Wiley & Sons. Estados Unidos.

ROJO, A. (1996): Valoración de Empresas y Partes de Empresas. Ed Instituto de Auditores Censores Jurados de Cuentas de España. Escuela de Auditoría. Madrid.

ROMERO, C. (1993): Técnicas de Gestión de empresas. Ed Mundiprensa; Madrid.

RUIZ MARTÍNEZ, R.J. Y GIL CORRAL, A.M. (2004): El valor de la empresa. Ed. Instituto Superior de Técnicas y Prácticas Bancarias. Madrid.

RUIZ, R.; JIMÉNEZ, F. (2000): Opciones Reales sin Soluciones Ficticias. Revista Profesional de GestiónFinanciera Banca & Finanzas, Nº 60. Madrid.

SANTANDREU, E.; SANTANDREU P. (1998): Valoración, Venta y Adquisición de Empresas. Ed. Gestión 2000. Barcelona.

SCHWARTZ, E.S. Y GOROSTIZA, C.Z. (2000): Valuation of Information Technology Investments as Real Options; American Finance Association; Meeting 2001; New Orleans.

SCHWARTZ, E.S. Y MOON, M. (2000): Rational Pricing of Internet Companies, Financial Analysts Journal, mayo junio.

SMITH, G.V. (1997): Trademark Valuation. Ed. John Wiley & Sons. Estados Unidos.

SMITH, G.V. ; PARR, R.L. (2005): Intellectual Property. Ed. John Wiley & Sons. Estados Unidos.

SULLIVAN P.H. (2001): Rentabilizar el capital intelectual. Paidós, Barcelona.

TERMES, R. (1998): Inversión y Coste de Capital. Ed. Mc Graw Hill. Madrid.

TOBIN, J. (1969): A general equilibrium approach to monetary theory; Journal of money, credit and banking; 1.

UNIÓN EUROPEA DE EXPERTOS CONTABLES (UEC); (1962): Evaluación de Empresas y Partes deEmpresas Reglas formuladas por la Comisión Especial UEC. Ed. Deusto. Bilbao.

WESTON, J.F.; COPELAND T. (1995): Finanzas en Administración. Ed. McGraw-Hill, México.__

# CAPÍTULO 6: ENCUESTA SOBRE VALORACIÓN DE EMPRESAS Y CIBERSEGURIDAD

Para ampliar el estudio se decidió pasar un cuestionario a directivos de empresas, profesores universitarios, auditores de cuentas, para observar el grado de implicación de las empresas en materia de ciberseguridad.

Elaboramos una encuesta en base al desarrollo de la tesis. La encuesta tiene varios bloques:

1.- Identificación de la empresa, con Código CNAE

2.- Bloque relacionado con los intangibles

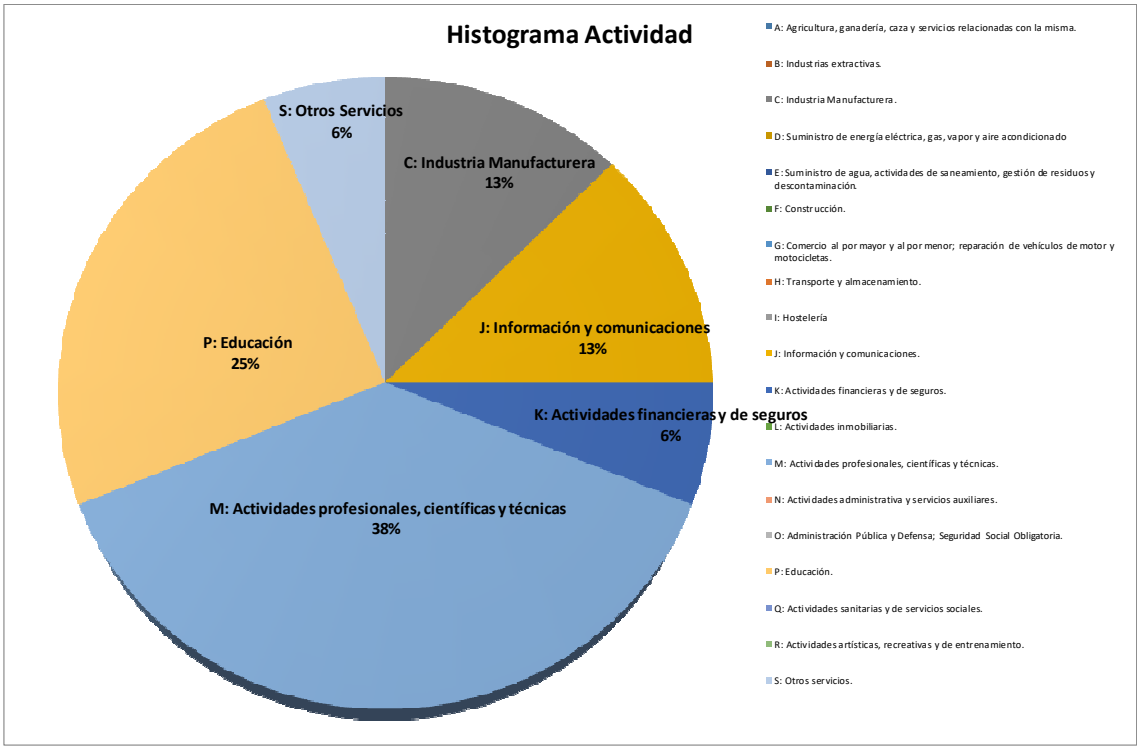
3.- Bloque de Valoración de empresas y auditoría

4.- Bloque de seguridad de la información y sectores donde sería más necesario la aplicación de unos mínimos deseables por encima de los mínimos normativos.

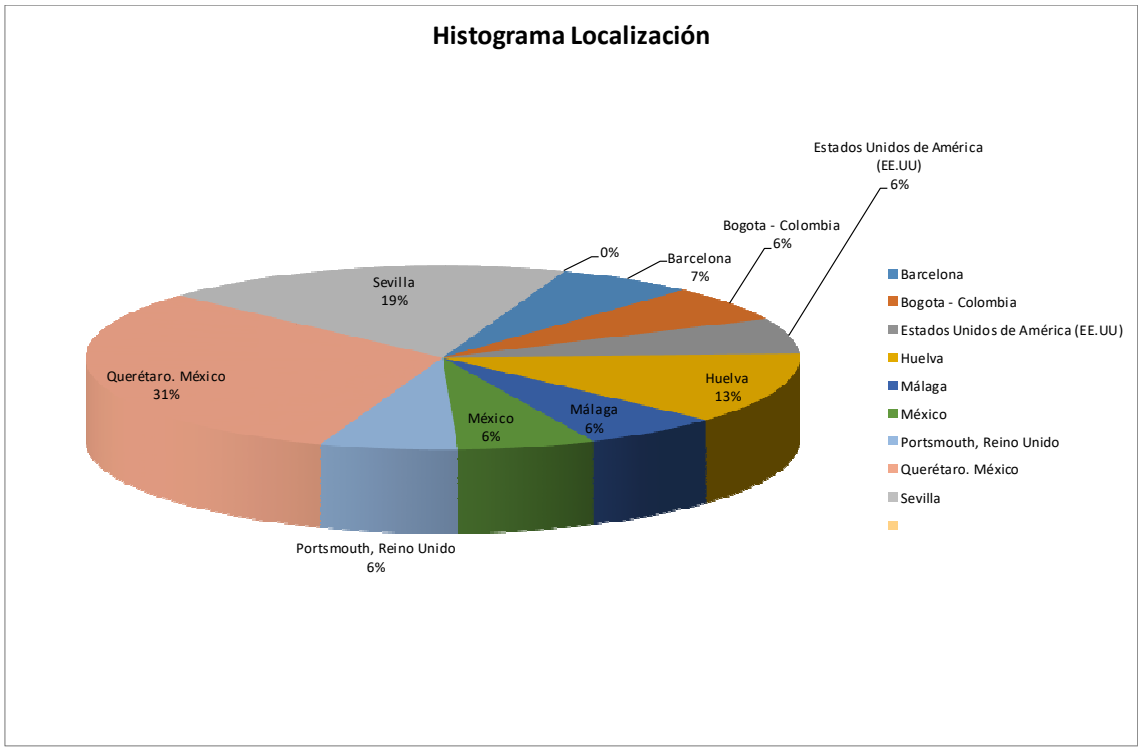
Esta encuesta se envió a través de Google.

**Resultados de la Encuesta**

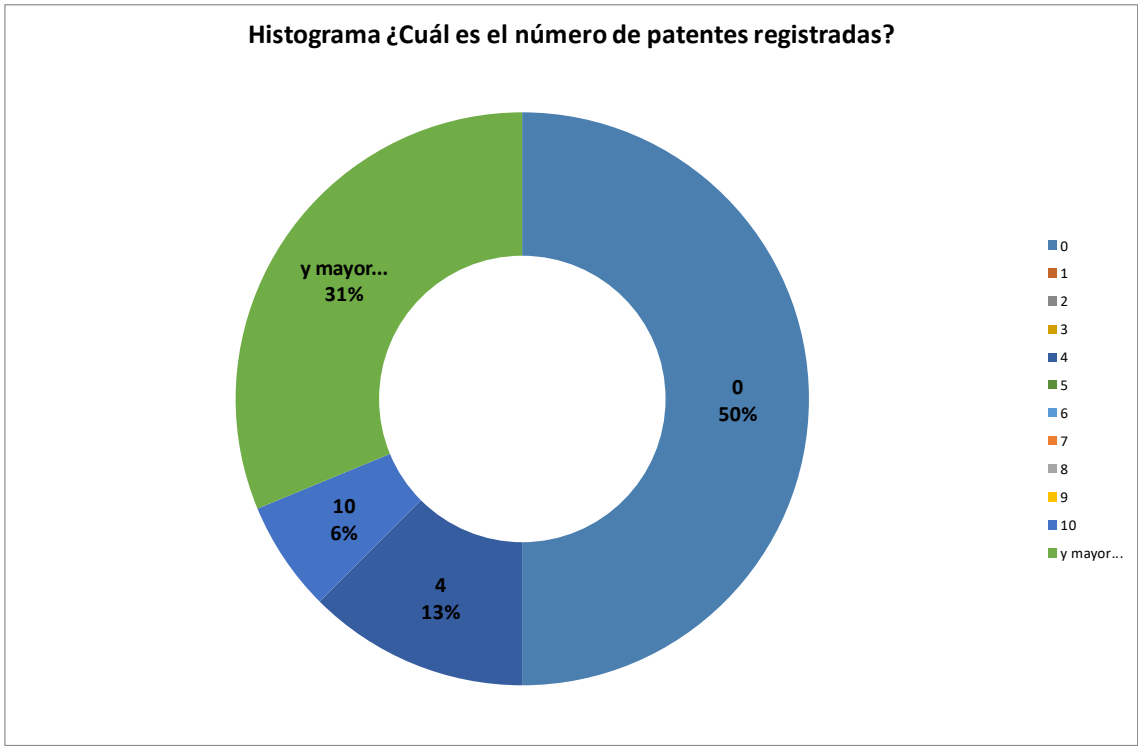
**Indique el sector al que pertenece según código CNAE (Código Nacional de Actividades Económicas):**



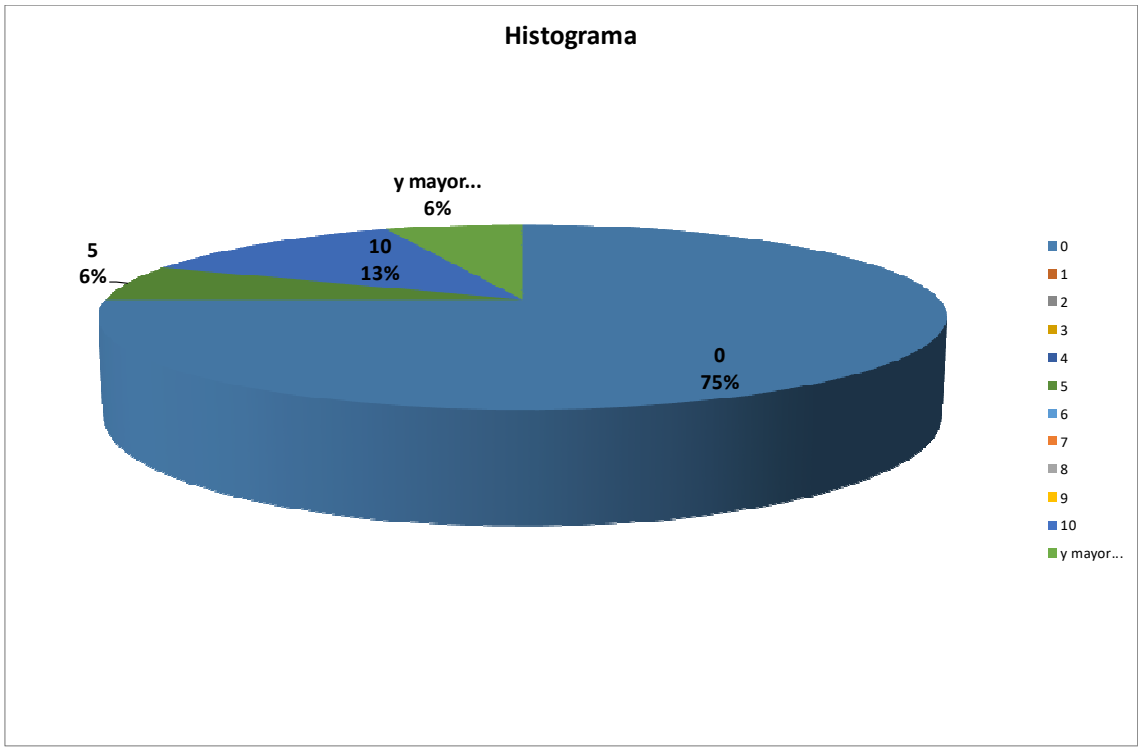

**Indique la provincia sede principal de la empresa:**



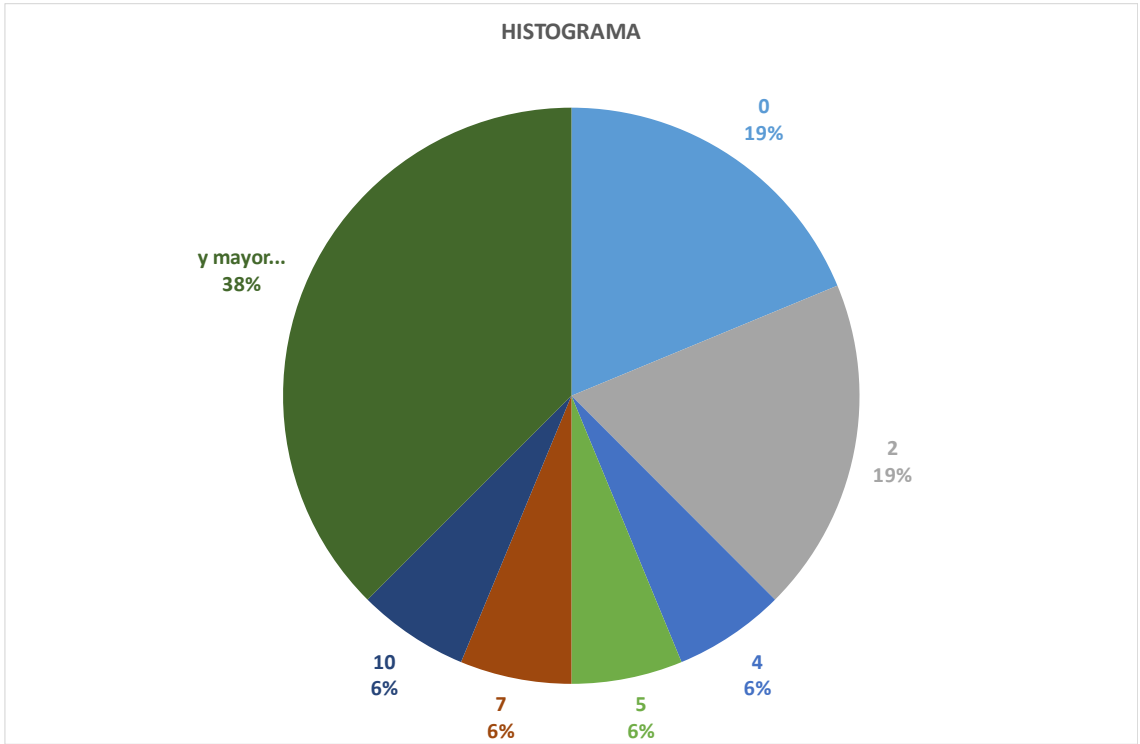

**En su empresa, ¿Cuál es el número de patentes registradas?**



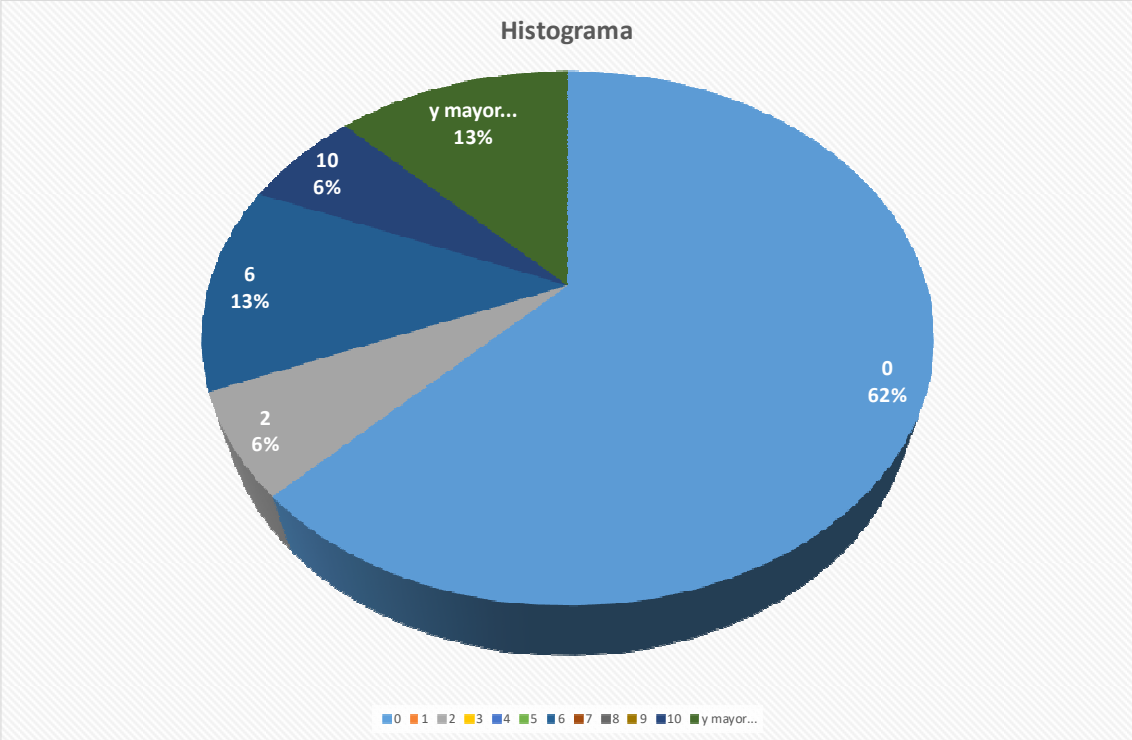

**¿Cuál es el número de patentes registradas específicas en seguridad de la información?:**



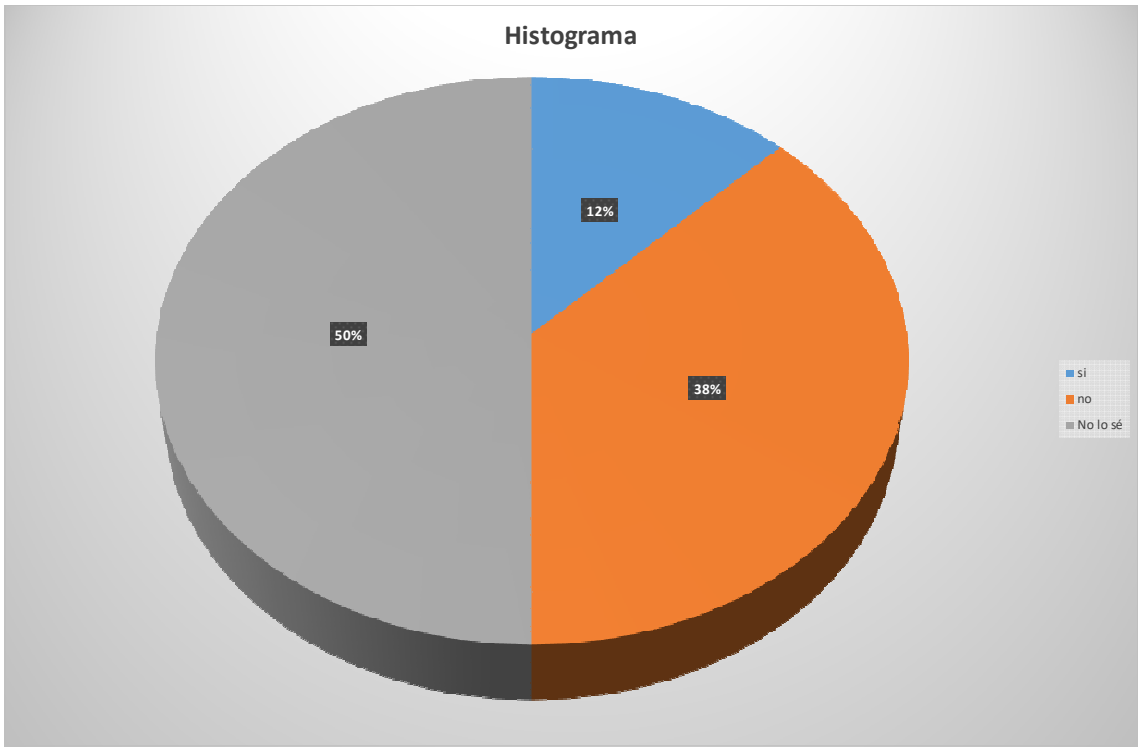

**¿Cuál es el número de proyectos de I+D+i en los últimos dos años?:**



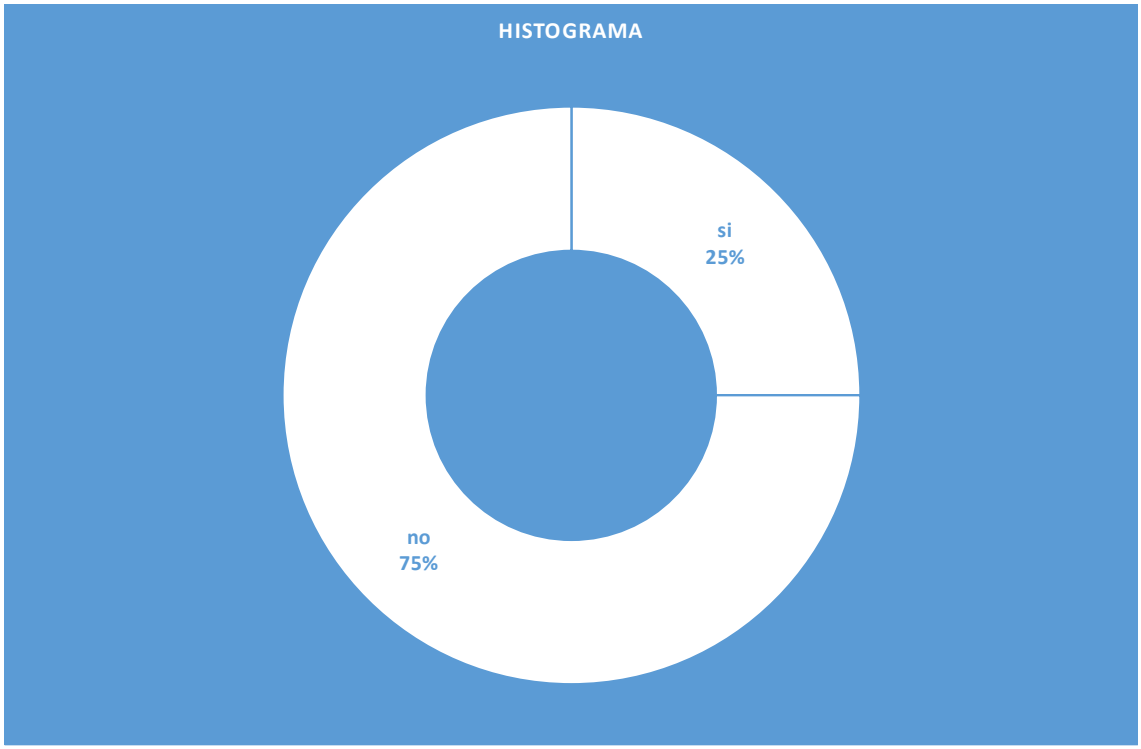
**¿Cuál es el número de proyectos de I+D+i en los últimos dos años específicos en seguridad de la información?**




**¿Su empresa encarga informes motivados con el objeto de acogerse a las deducciones fiscales en inversiones específicas en seguridad de la información u otra?**



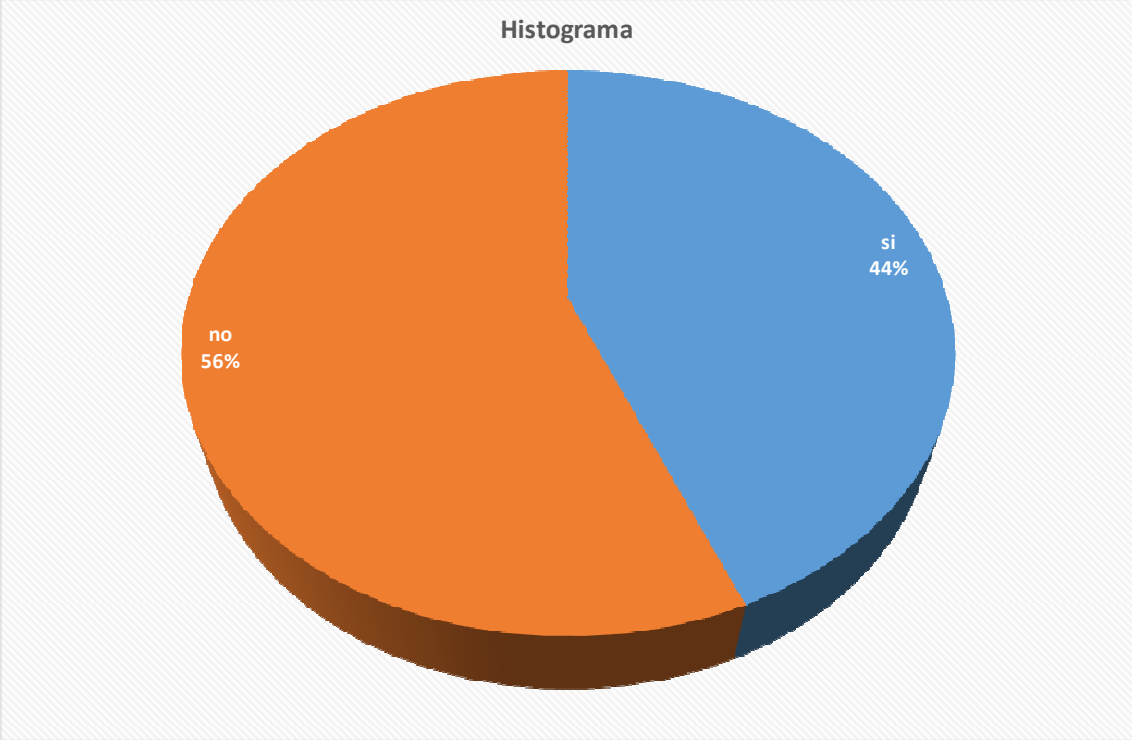

**¿Conoce alguna metodología de valoración de intangibles?**




**Algunos de los métodos conocidos: Coste o mercado, Capitalización de beneficios esperados, opciones reales y múltiplos comparativos, la capitalización de ganancias, diferenciales de beneficios brutos**

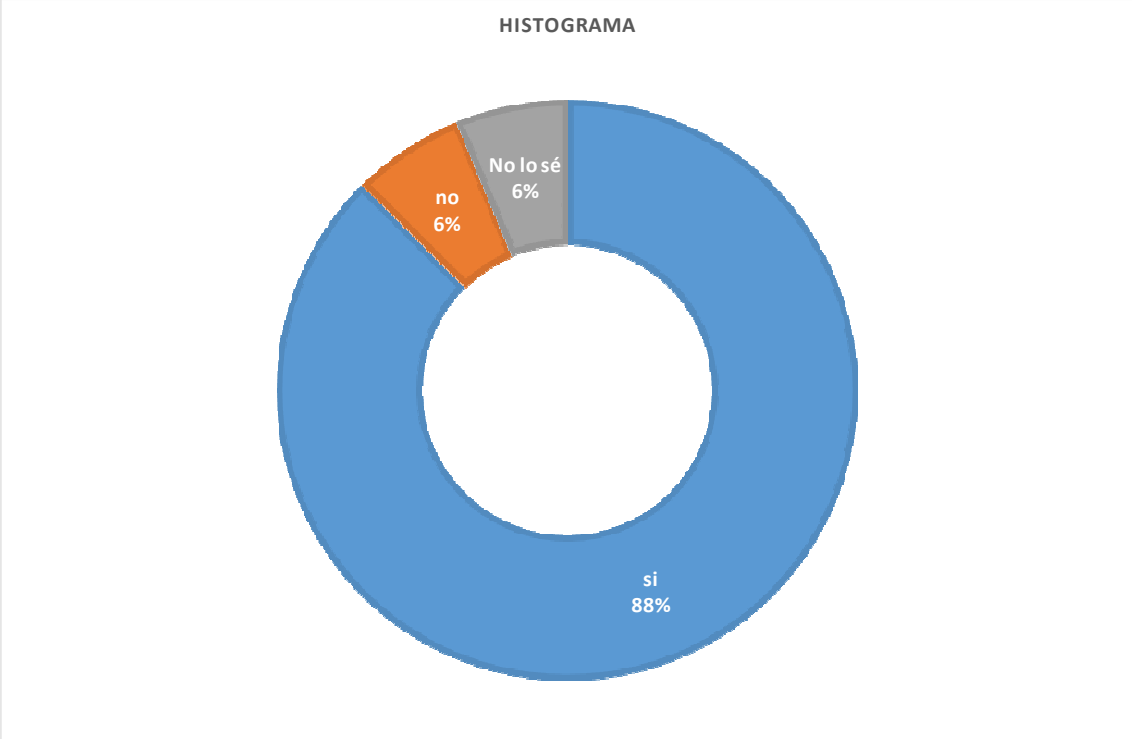
**Bloque A: Intangibles**

**¿Existe un sistema de gestión de seguridad de la información específico, confeccionado por la entidad, para la organización, basado en la mejora continua y en los mínimos establecidos en las normas ISO (International Organization for Standardization) 27001? Comente lo más relevante.**



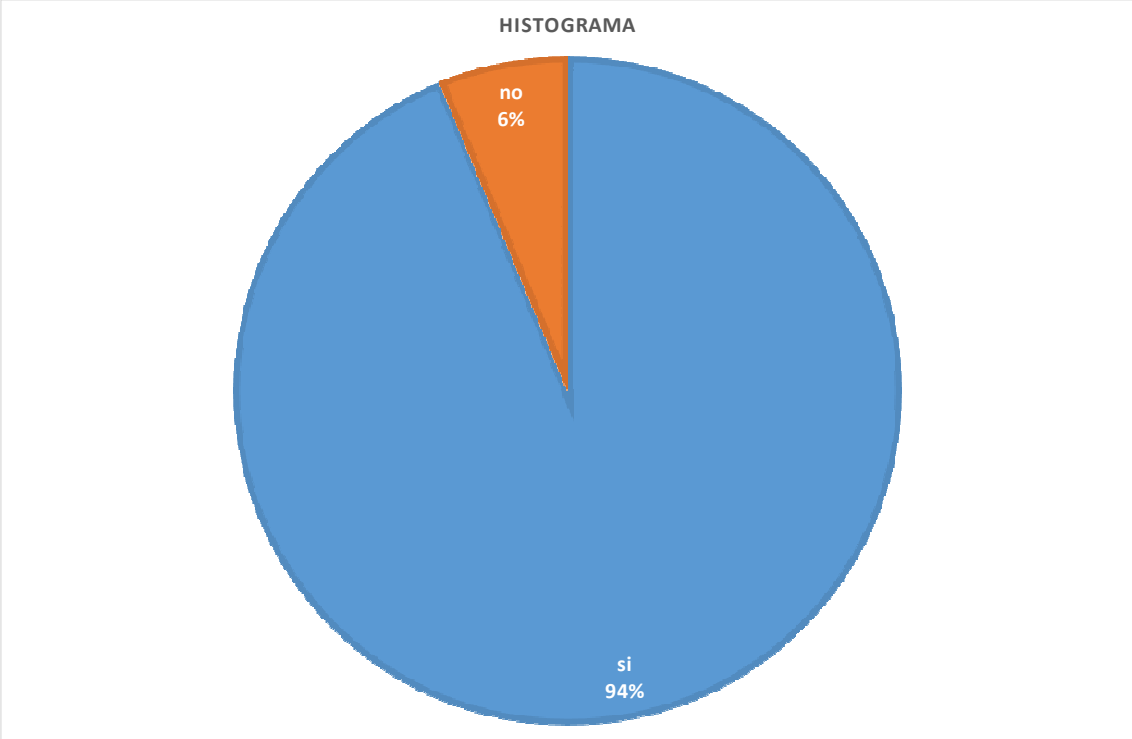

Algunos comentarios de los que han contestado si: La entidad está certificada en ISO, sin acceso a esa información, se encarga de ello el Centro de Cálculo de la Escuela Superior de Ingeniería, hay repositorio de Empresas Privadas. Hay un sistema de manejo de credenciales y licencias, la empresa cuenta con un sistema gestionado por el departamento de TI, existe un departamento de "Compliance", pero no se sigue según ISO 27001, etc

**¿Cree que el valor de la empresa aumentaría, si se implementasen unos sistemas de gestión integrados específico elaborado por la propia organización: ¿seguridad de la información (ISO 27001), calidad (ISO 9001), medioambiental (ISO 14001), seguridad laboral (OHSAS 18001), etcétera? Comente lo más relevante.**



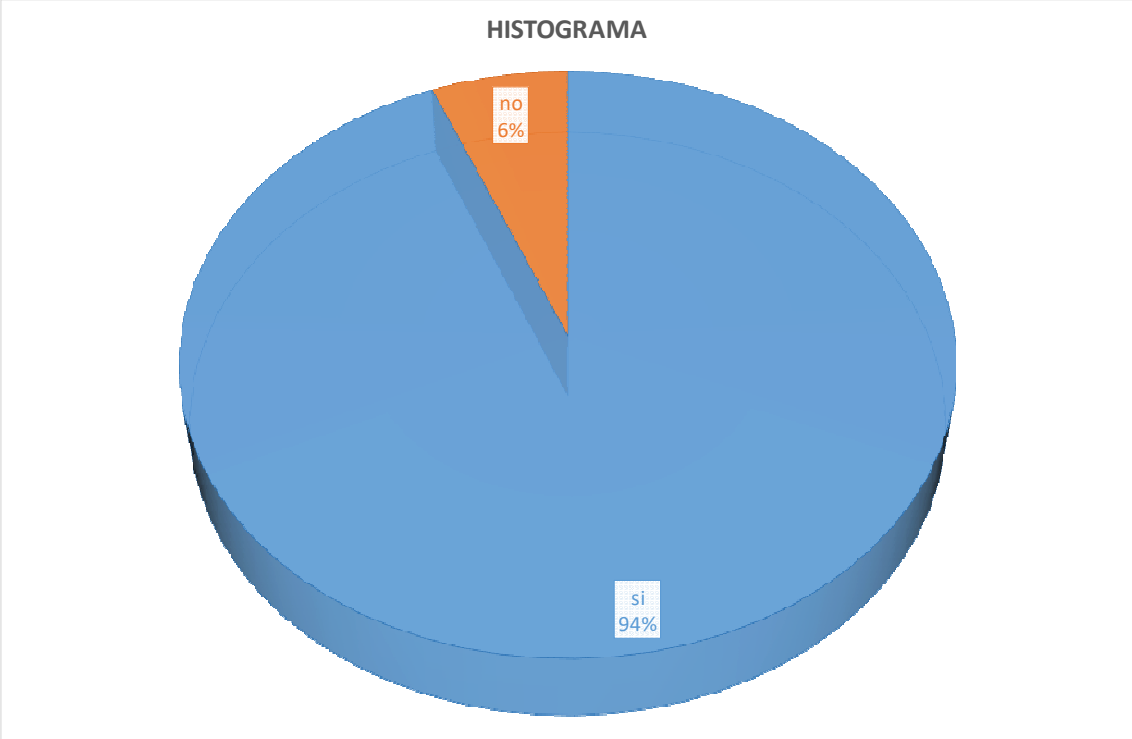

Algunos comentarios: pienso que al menos haría reflexionar a la empresa sobre su gestión, aparte de aumentar la seguridad de la empresa, mejoraría la imagen de esta de cara al exterior, en la medida en la que estos estándares permitan obtener certificados de calidad, entiendo que el valor sí aumentaría, ya existen ya que la empresa cotiza en bolsa, por supuesto, esto hablaría de una empresa estándares globales de calidad, los sistemas de calidad ayudan mucho al valor de las empresas, ya que son elementos solicitados por los clientes, claro que garantiza que se cumplan criterios específicos a los problemas actuales de la empresa, ya que lo consolida como empresa comprometida con la seguridad

**¿Cree que un programa de auditoría continua de elaboración propia de los sistemas de gestión de seguridad de la información añadiría valor a la empresa? Comente lo más relevante.**



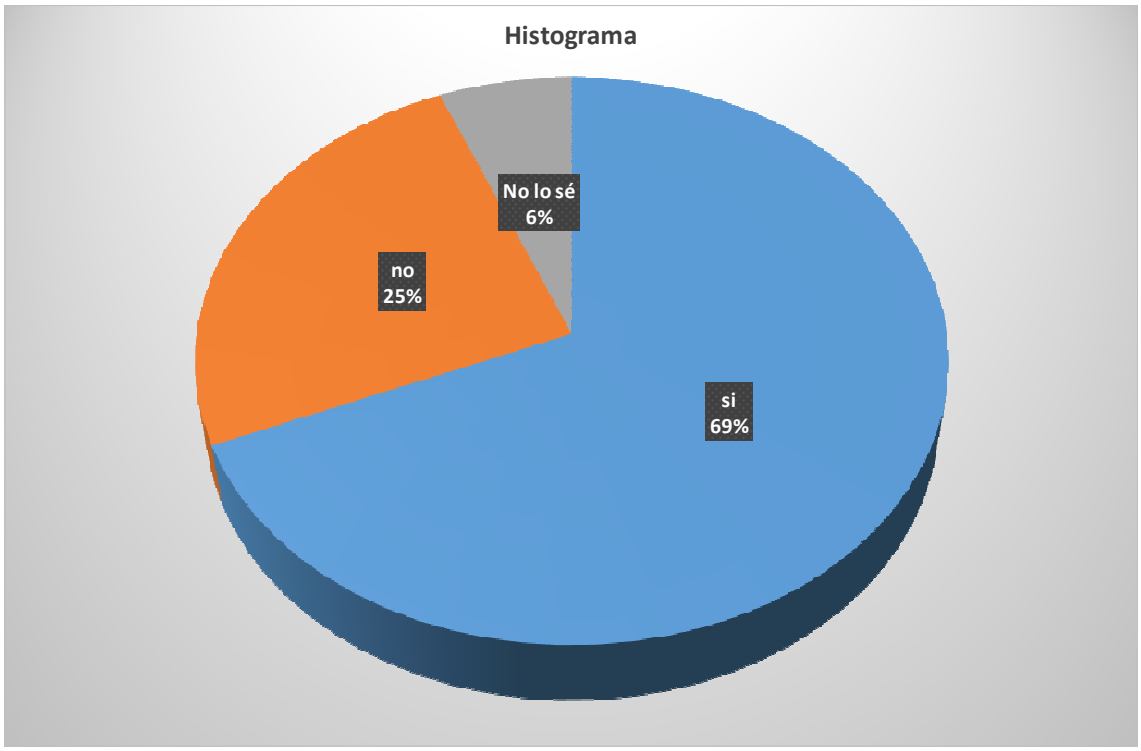

Algunos comentarios: permitía realizar controles internos en tiempo real, una auditoría siempre aporta valor. En este caso en concreto, podría ayudar a detectar fugas de seguridad. Aun así, es preferible una auditoría externa, considero que ya no lo están haciendo desde el Vicerrectorado de Investigación, considero que más que una auditoría continua, sería necesario establecer períodos anuales de revisión, sólo hay que ser muy cuidadosos de no interferir con la operación porque puede incrementar los tiempos de desarrollo, pudiera aumentar la seguridad en la información sensible, haciendo la información más cara, ya que garantizaría que el sistema de gestión de seguridad esté al día, pues aporta valor a los procesos de gestión.

**¿Cree que debe existir en la organización una comisión de auditoría interna y una comisión específica de seguridad de la información dependiente directamente de la alta dirección, siempre implicada en la mejora continua, basada en la relación con los profesionales nacionales e internacionales más cualificados en esta materia? Comente lo más relevante**



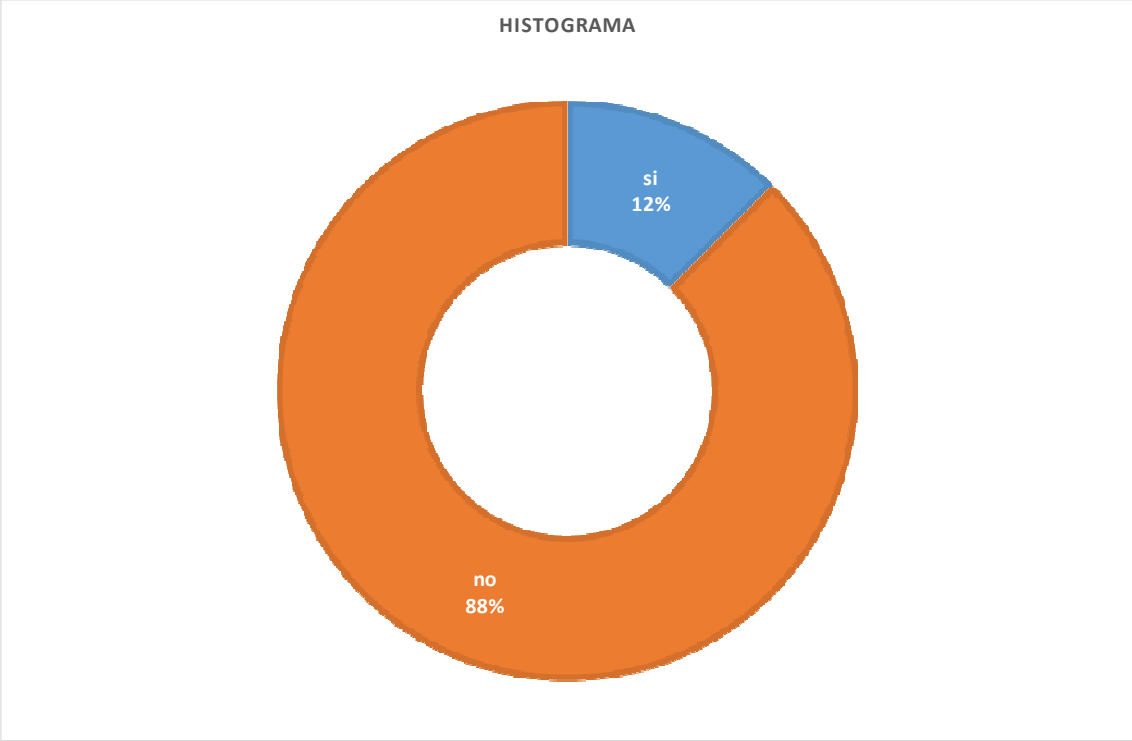

Algunos comentarios: es necesario una comisión de auditoría interna y externa que funcionen al unísono, En nuestro caso debería ser a nivel de la Universidad o de la Junta de Andalucía, esta pregunta propone un caso muy extremo que sería viable para empresas de base tecnológica, pero no para las pymes. Tampoco creo que sea conveniente que dependa directamente de la alta dirección, Idealmente sí. Pero en la práctica son pocas las empresas que dan un tratamiento especial a su seguridad de la información. Principalmente por desconocimiento o por ahorrar costos, también un comité de certificación externo que avale que no se está viciando el sistema, existe en EATON, ya que este bueno para la compañía y una mejor gestión, considero que por tratarse de activos distintos deben ser diferentes las entidades que los regulan

**¿Cree que los mínimos establecidos en la ISO 27001 deben contemplar la información expuesta e interconectada sobre las operaciones online en las cuentas anuales de la organización, así como los instrumentos utilizados y las cuentas asociadas a dichos instrumentos? Comente lo más relevante.**




Algunos comentarios: eso nos haría evaluar mejor el riesgo cibernético, la información referente a las cuentas de una empresa no debería estar expuesta, sería un fallo de seguridad, la norma ISO 27001 describe cómo gestionar la seguridad de la información de la empresa. Esto incluye cualquier tipo de flujos de información digital, impresa e incluso oral, no conozco la ISO 27001, es información que de ser filtrada podría afectar de forma negativa a la organización No conozco la norma

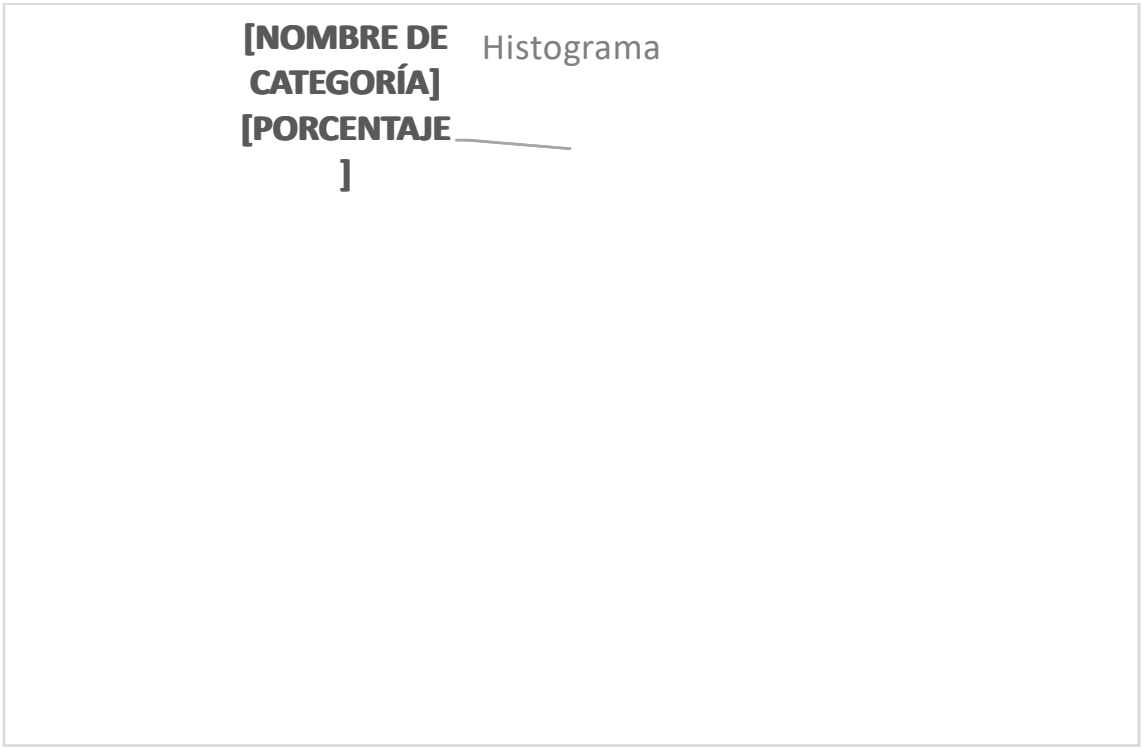
**¿Cree que existe la seguridad de la información en una organización al 100%? Comente lo más relevante**




Algunos comentarios: No, siempre puede haber ciberamenazas y vulnerabilidades, No. En prensa estamos viendo como incluso los gobiernos más poderosos tienen este tipo de problemas No. Siempre hay una información que se puede "escapar" ante cualquier sistema de control, aquí tenemos que distinguir entre seguridad y vulnerabilidad. Una empresa puede tomarse muy en serio la seguridad de la información, dedicando recursos para ello, pero a día de hoy no existe una invulnerabilidad del 100%, siempre hay un riesgo, No creo que exista un sistema de información cien por cien seguro. No. Es prácticamente imposible, No. Todos los

sistemas humanos son propensos a fallar. Sin embargo, la probabilidad de que esto suceda depende de la robustez de las normas y sistemas de protección, No. Ningún sistema es infalible, No ya que pudiera depender siempre de las personas y pudiera existir la manera de filtración de información No, sin embargo, creo que un buen sistema de seguridad se puede acercar, No, ya que siempre se está desarrollando tecnologías nuevas, que por su propio carácter de novedosas pueden tener fallos

**Un sistema de gestión de la seguridad de la información conlleva que una organización gestione y garantice que los riesgos de la seguridad de la información sean conocidos, gestionados y tratados en base a los criterios definidos por la propia organización de acuerdo con la estrategia de seguridad. Comente lo más relevante**




Algunos comentarios: La empresa puede hacer un estudio para conocer los riesgos a los que se expone, pero esto no quiere decir que conozca todos los riesgos Estoy de acuerdo. De hecho,

supongo que el Servicio de Informática y Comunicaciones se encarga de ello, La fórmula es evitar el riesgo, el coste sea mayor que el riesgo, Antes de llevar a cabo un plan de implementación de un sistema para la gestión de la información. Debe llevarse a cabo un análisis de riesgos y vulnerabilidades de la empresa, Las personas deben estar convencidas de que la seguridad proviene principalmente de ellos, Es de suma importancia que se conozcan los riesgos de seguridad ya que eso permitirá, solución y gestionar posibles brechas de seguridad, siempre debe haber una comunicación al interior de la empresa para sintonizar a los empleados con los objetivos del negocio

**¿En qué sectores económicos o sociales cree que se puede actuar preferentemente en materia de seguridad? Comente lo más relevante.**

Banca, tecnológicas, Sanidad..., Sistema Financiero, sobre todo empezar por los sectores estratégicos, en todos, En el sector económico cobran particular importancia las entidades bancarias y las transferencias y compras por internet. En lo social las redes sociales, por la gran cantidad de información personal que tienen, Entiendo que de manera directa, la materia de seguridad es especialmente sensible en operaciones que impliquen transacciones económicas. En estos casos es especialmente recomendable unos sistemas de encriptación efectivos. En cualquier caso, desde el punto de vista social, cada vez son más frecuentes los sistemas de encriptación en mensajes punto a punto, En todas las empresas que tengan propiedad intelectual, salud, finanzas, energía y comunicación, Empresas de telecomunicaciones y bancos, Desarrollo de tecnología. En esta industria se concentra secretos de negocios y es donde una brecha de seguridad puede ocurrir de forma no deseada, Ventas por internet, cuentas bancarias, administración de innovación de empresas, seguridad de patentes, den los sectores que tenga un mayor conocimiento de los peligros en la seguridad informática, Seguridad financiera, seguridad industrial (patentes, fórmulas de productos, procesos, etc.), Telecomunicaciones, sector financiero y sector industrial, contabilidad

**¿Qué asuntos se deben abordar ante una problemática de seguridad de la información? Comente lo más relevante.**

La valoración del riesgo, asegurar la empresa ante riesgos cibernéticos Buscar soluciones técnicas y organizativas para evitar que vuelva a repetirse Lo relacionado con las personas, En

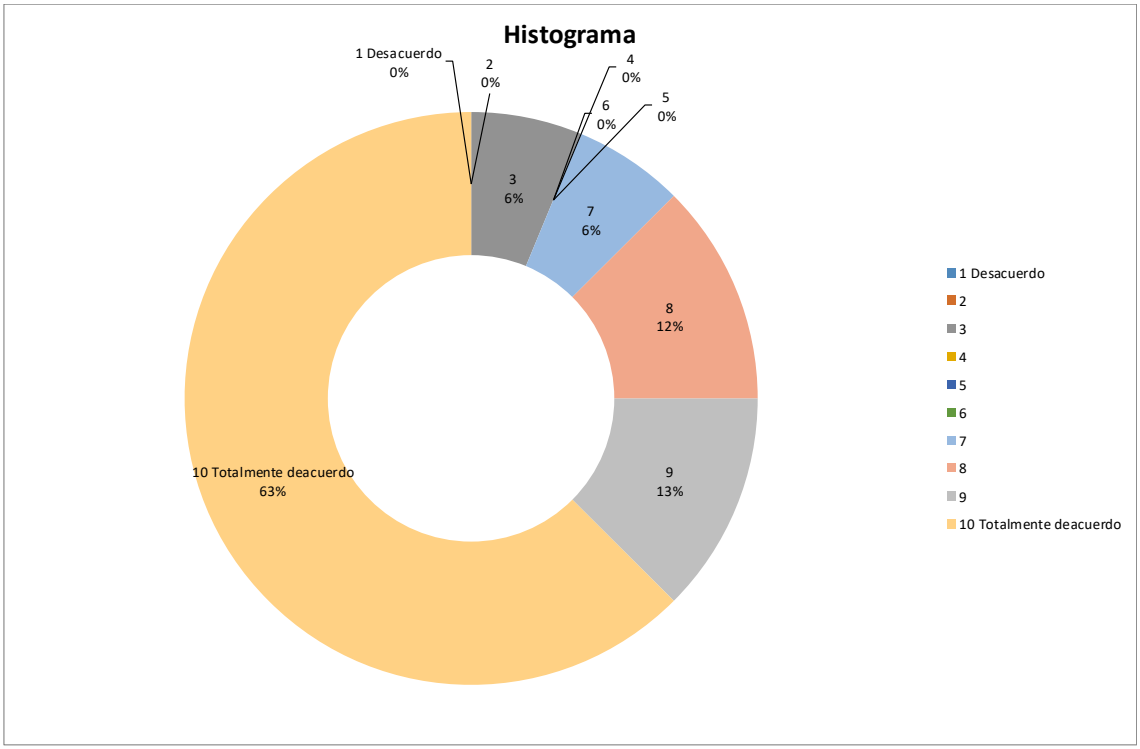
la información financiera y contable, y en las patentes, Prácticamente aborda la seguridad de la información en su totalidad. Las jornadas de ciberseguridad promovidas por Cartuja son una buena respuesta, Una vez dada una situación o una filtración de información, el primer paso debe ser garantizar qué el error no se propague en el sistema y robustecer las porciones de información que no han sido violadas. Habiendo asegurado el perímetro, habría que seguir con una valoración de los daños y consecuencias, Evaluar los daños, tomar medidas correctivas, tomar medidas preventivas Información robada, copiada, mejoras para evitar recurrencias, Es importante decir cual la razón de la brecha de seguridad, así como la configuración de estrategias que permiten prevenir dichos problemas Se deben investigar las causas de los incidentes informáticos y posteriormente trabajar en planes de prevención y mitigación, Detectar los fallos del sistema, planificar lo problemas, control posterior

**¿Qué sector/es económico o social cree que es el que más atención necesita en la seguridad de la información: Petróleo y Energía; Materiales Básicos, Industria y Construcción; Bienes de Consumo; Servicios Financieros e Inmobiliarios; Servicios de Consumo; Tecnología y Telecomunicaciones; Pequeña y Mediana Empresa; ONGD? Comente lo más relevante.**

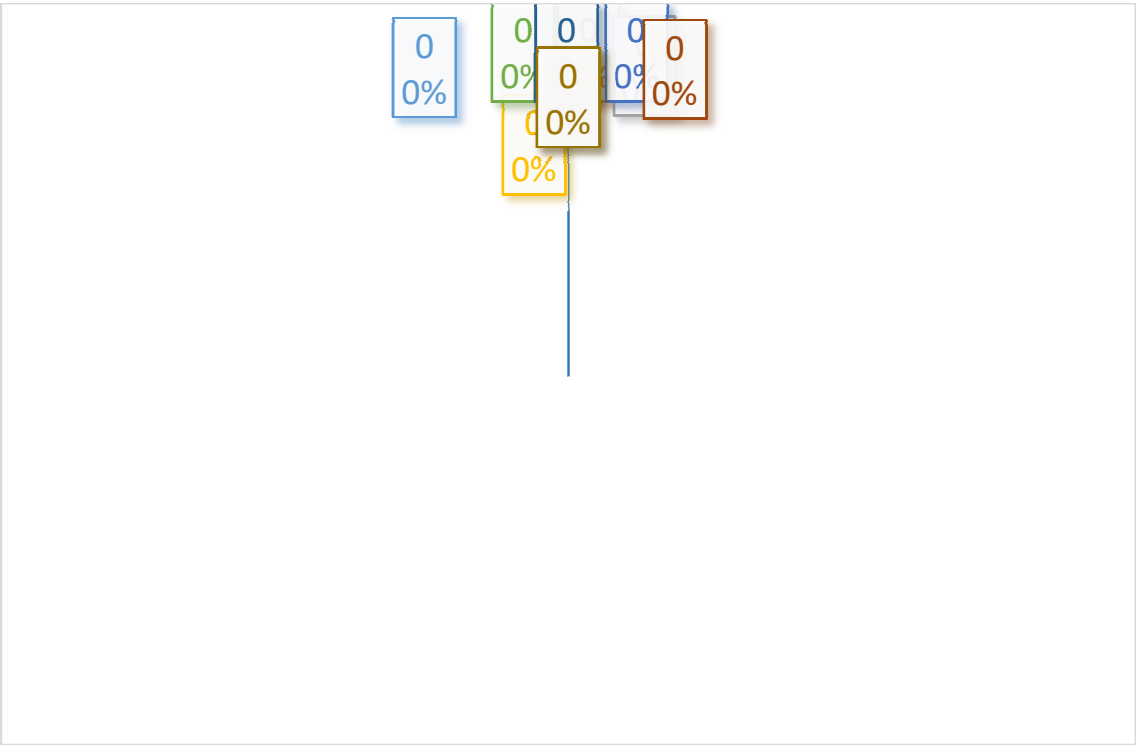
Especialmente telecomunicaciones Banca, tecnología, sanidad, Servicios Financieros e Inmobiliarios, Los estratégicos. Defensa, comunicaciones, transporte, energía. En todos, Industria, comercio y servicios, Esto es muy relativo a cada entidad particular. Sin embargo, debido a su naturaleza, yo diría que el sector de la "tecnología y telecomunicaciones". Además, atendiendo a lo crítico del valor monetario, también son esencialmente sensible los "servicios financieros e inmobiliarios", Cualquiera de ellos es suficientemente importante como para no ser descartado, En todos los sectores en los que Exista riesgo económico asociado a una filtración de información ENERGÍA, Servicios financieros, datos civiles, tecnología y telecomunicaciones, petróleo y energía, defensa Sector tecnológico, telecomunicaciones, banca, Servicios financieros e inmobiliarios, bienes de consumo, pagos a través de la red, debido al posible robo de información e identidades Tecnología y telecomunicaciones ya que cuenta con intuición suya como de otras empresas, lo que incrementa el efecto negativo que tendría un problema de seguridad, Tecnología y Telecomunicaciónes, Petróleo y Energía, Industria y Construcción

## BLOQUE B: VALORACIÓN DE EMPRESAS Y AUDITORÍA

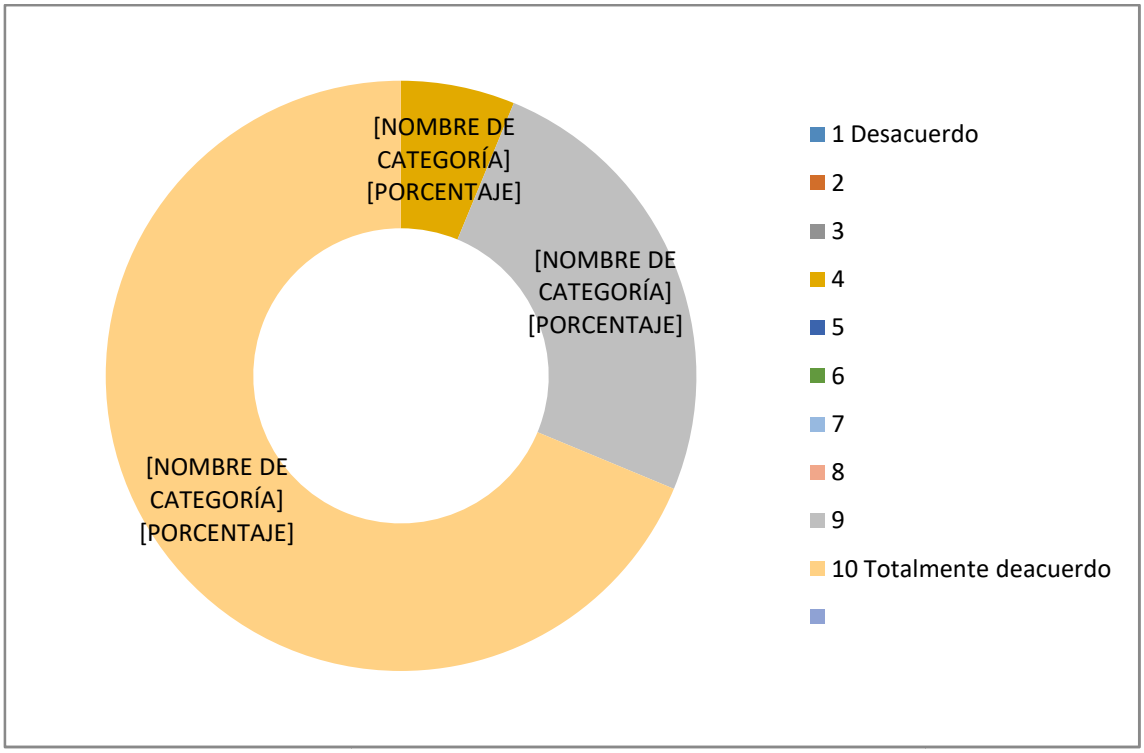
**El valor de la empresa se incrementa cuando se implementa un sistema de gestión de seguridad de la información con mínimos deseables por encima de los mínimos normativos ISO 27001**



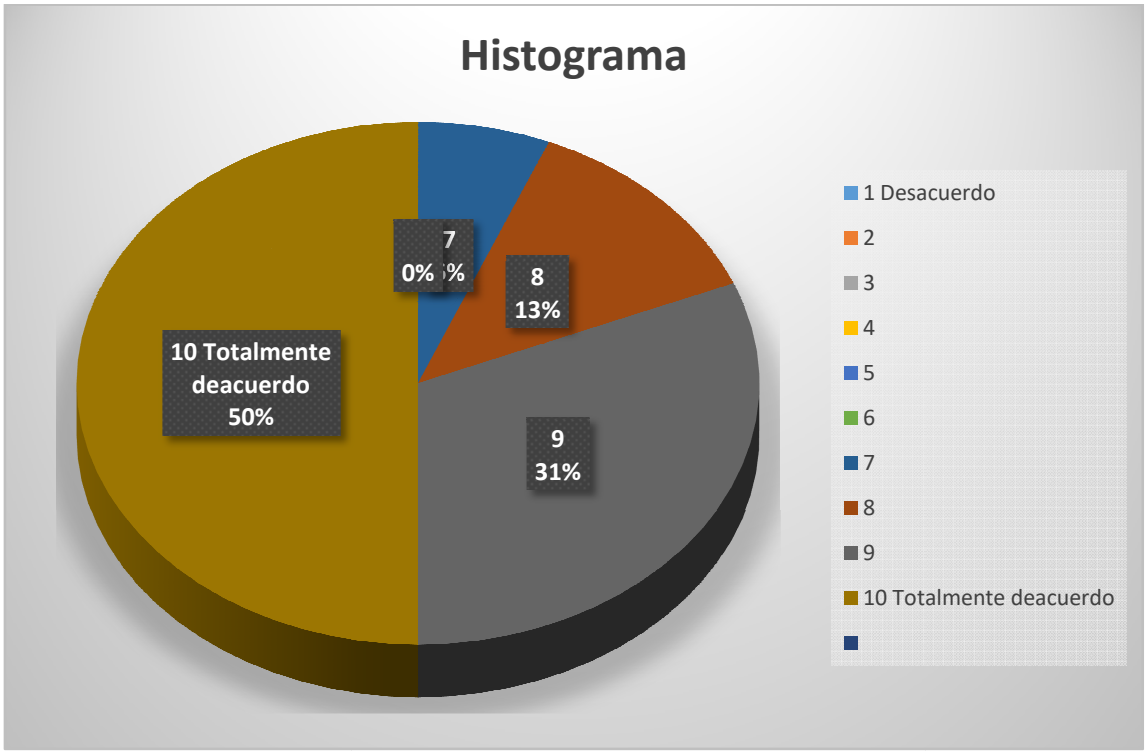
**Genera confianza y por tanto valor para la organización la implementación de un modelo de gestión adecuado, donde la alta dirección y todo el personal se encuentre vinculado y que el sistema de gestión suponga una mejora continua**



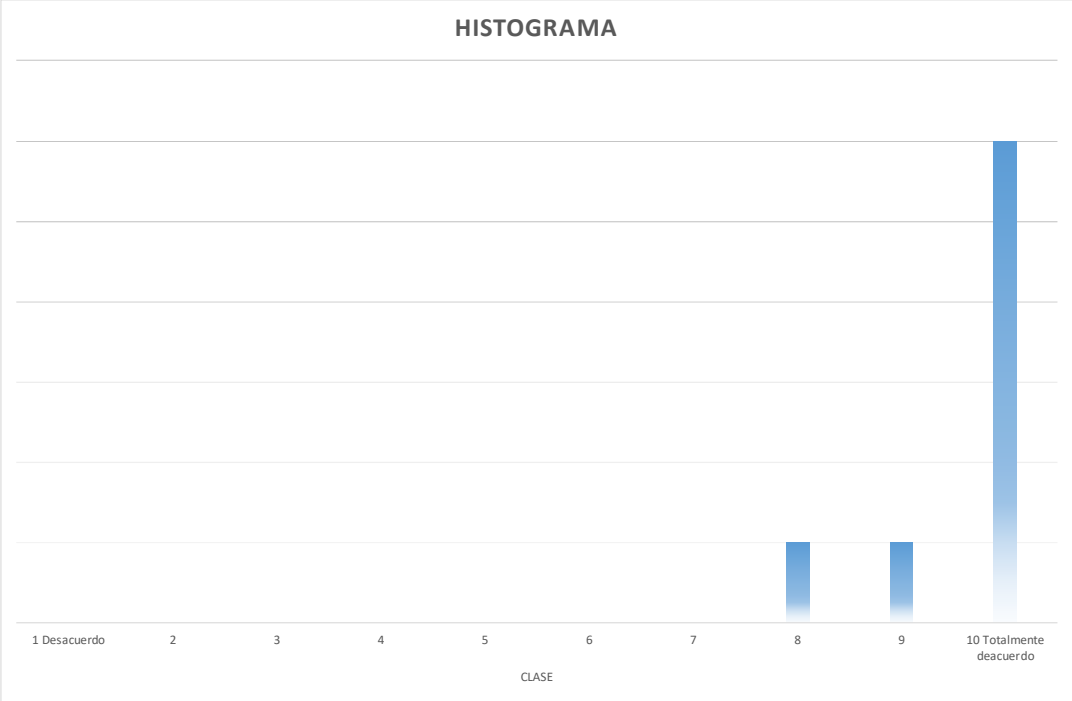

**El objetivo de la mejora continua del sistema de gestión es aumentar la eficacia y la eficiencia de los procesos para la consecución de los objetivos de negocio.**



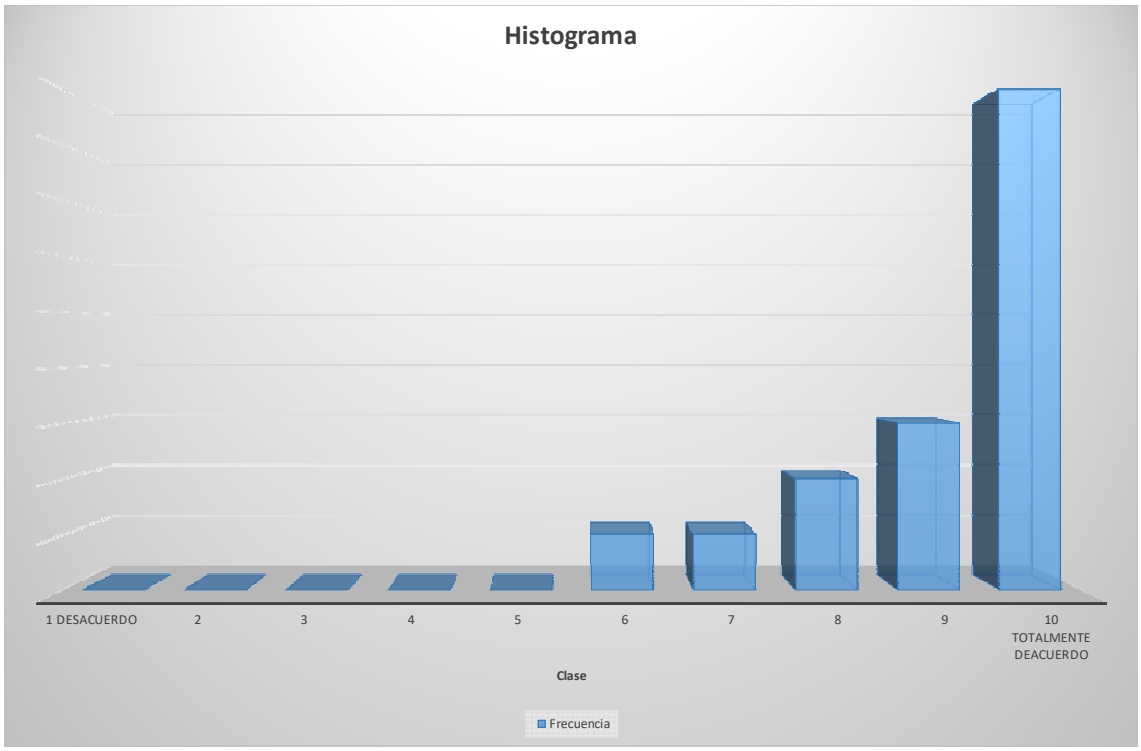

**El proceso de implementación de un sistema de gestión de la información añadiría valor y debería hacerse de forma documentada, sistemática, estructurada, repetible, eficiente y adaptado a los cambios que se produzcan en los riesgos, el entorno y las tecnologías con evidencias claras de su trazabilidad**



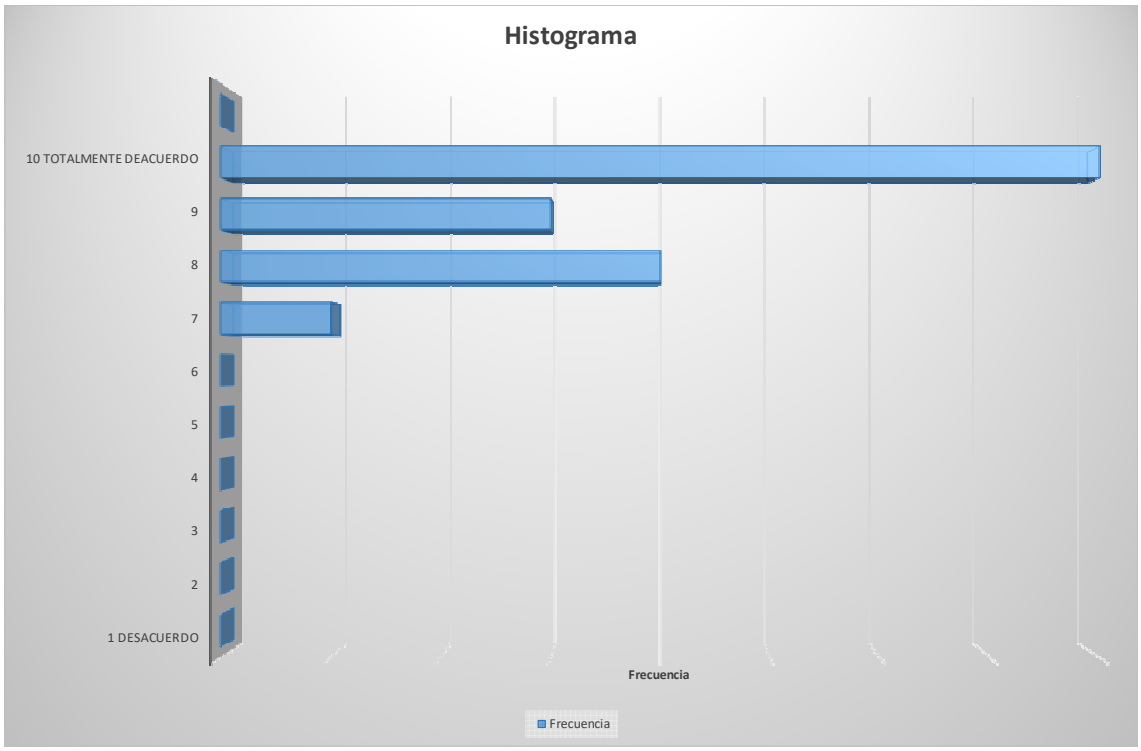
**Las causas de la mala gestión de la seguridad de la información pueden desembocar en una serie de grandes consecuencias: pérdida documental, pérdida de la confidencialidad, indisponibilidad de la información, alto tiempo de recuperación, baja productividad, aumento de los costes, disminución del nivel de servicios, pérdida de reputación, pérdida de oportunidad de negocio**



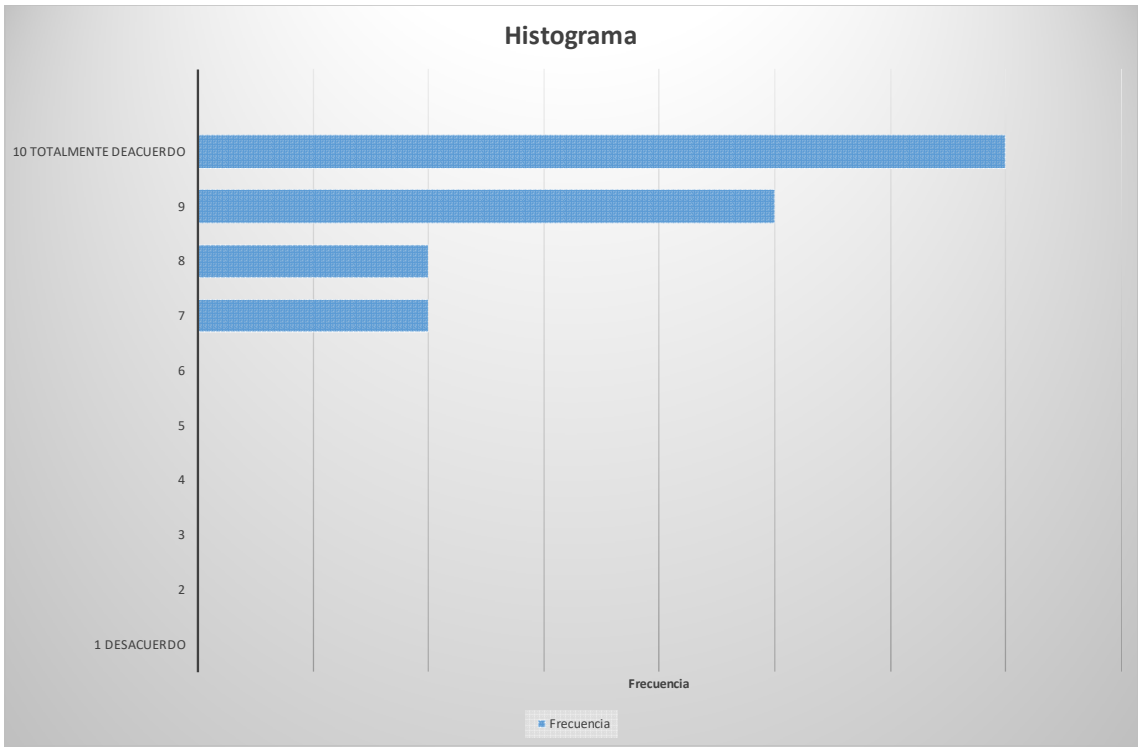

**Las ventajas de la implantación de un sistema de gestión de la seguridad de la información vienen dadas por: reducción del riesgo, aumento del retorno sobre la inversión en seguridad; aumento de madurez en el sistema de seguridad; cumplimiento legal; generación de valor y factor diferenciado**



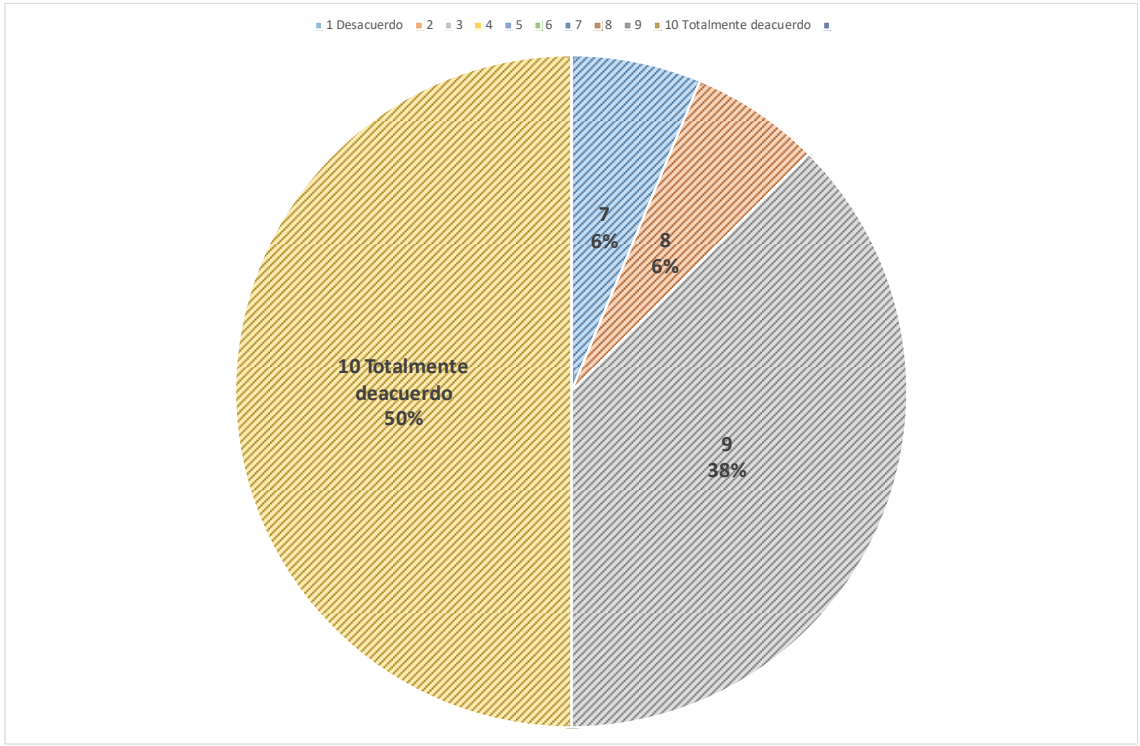

**Una auditoría de sistemas de gestión de seguridad tiene entre sus objetivos la protección de la información en sus tres aspectos: confidencialidad, integridad, y disponibilidad**




**El objetivo de la auditoría de los sistemas de gestión de la seguridad de la información es determinar el nivel de eficiencia y eficacia de los procesos de la tecnología de la información, decimos que la auditoría tiene un objetivo de gestión**

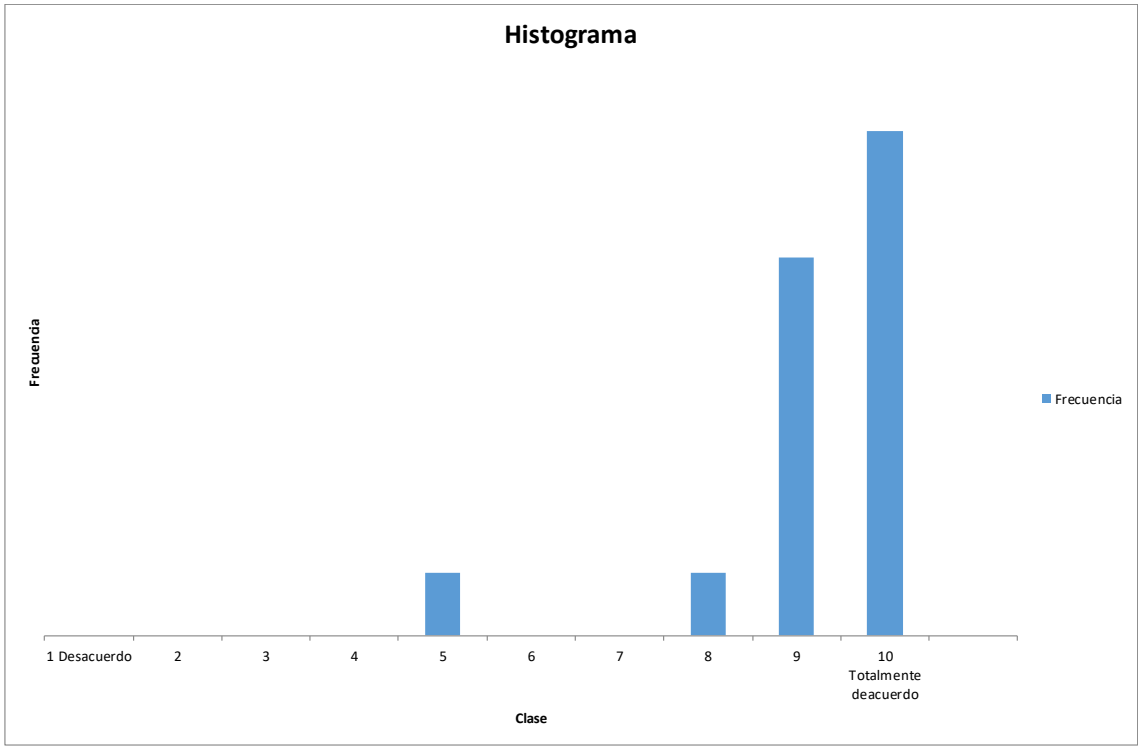



**Cuando hablamos de una auditoría de cumplimiento nos referimos a que su objetivo es verificar el cumplimiento por parte de la organización de lo dispuesto en la legislación vigente, en normas y estándares o acuerdos contractuales**

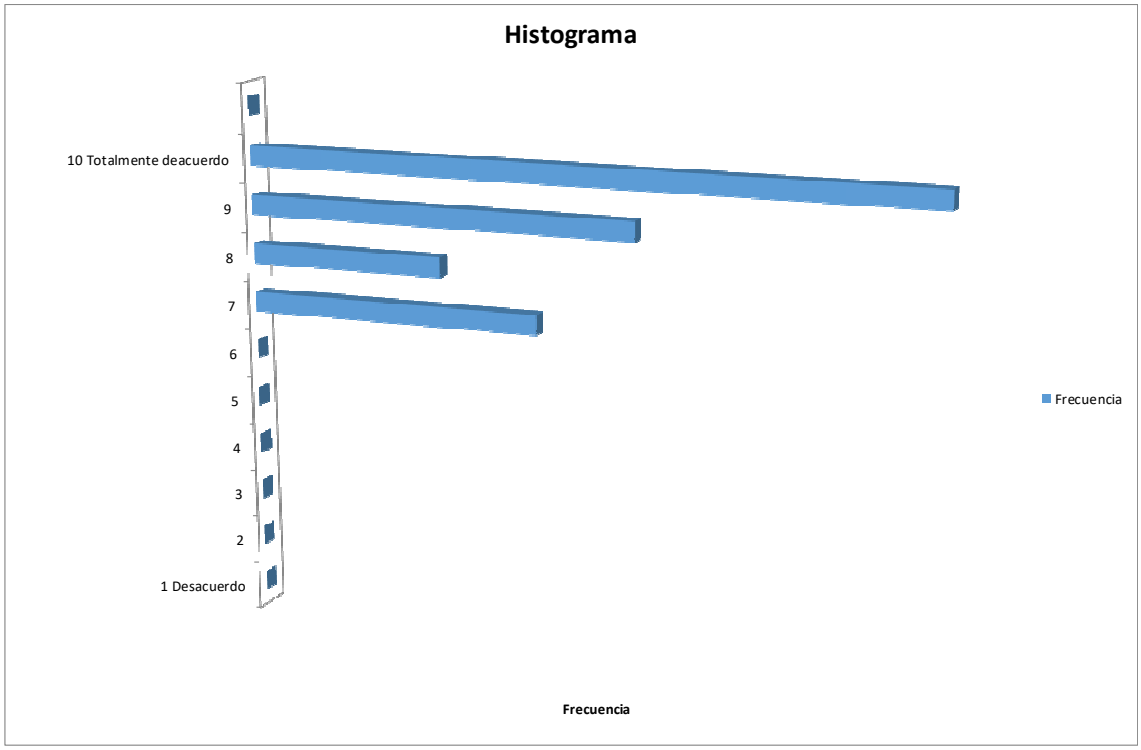



**El auditor debe contemplar la revisión de los aspectos organizativos internos, así como la obtención de evidencias, observando las actas de asignación de responsabilidades,**

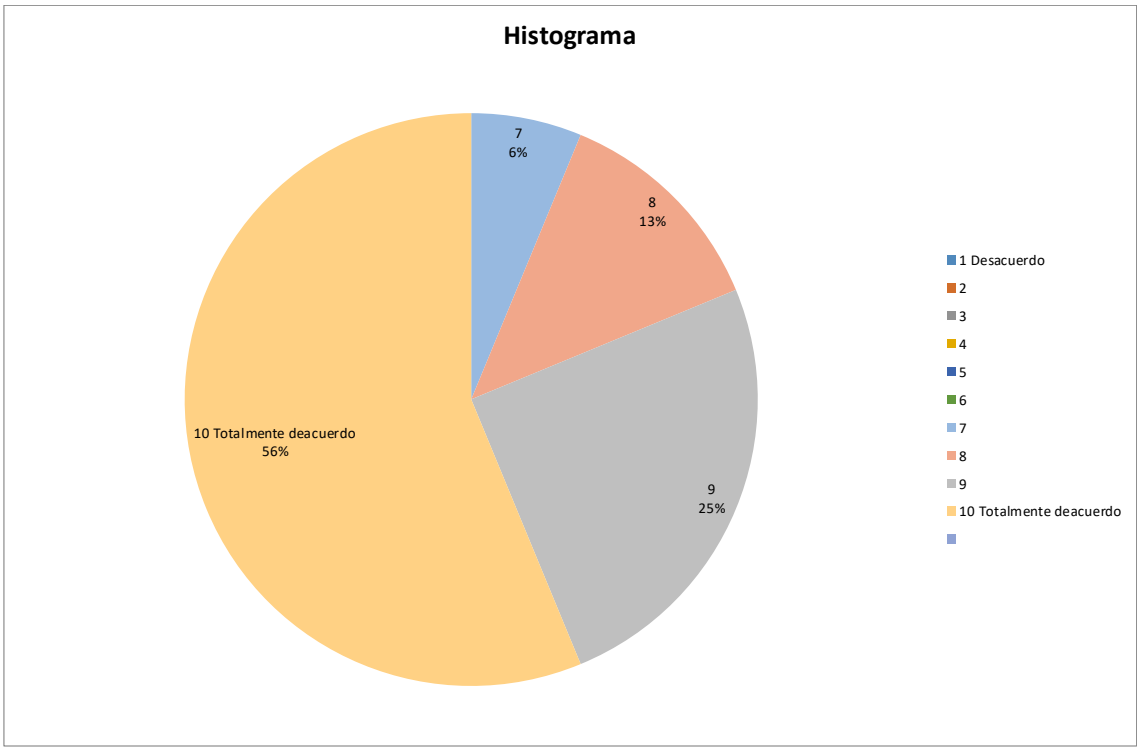
**entrevistas, comprobación de los controles de los dispositivos móviles y teletrabajo, en caso de que existan**



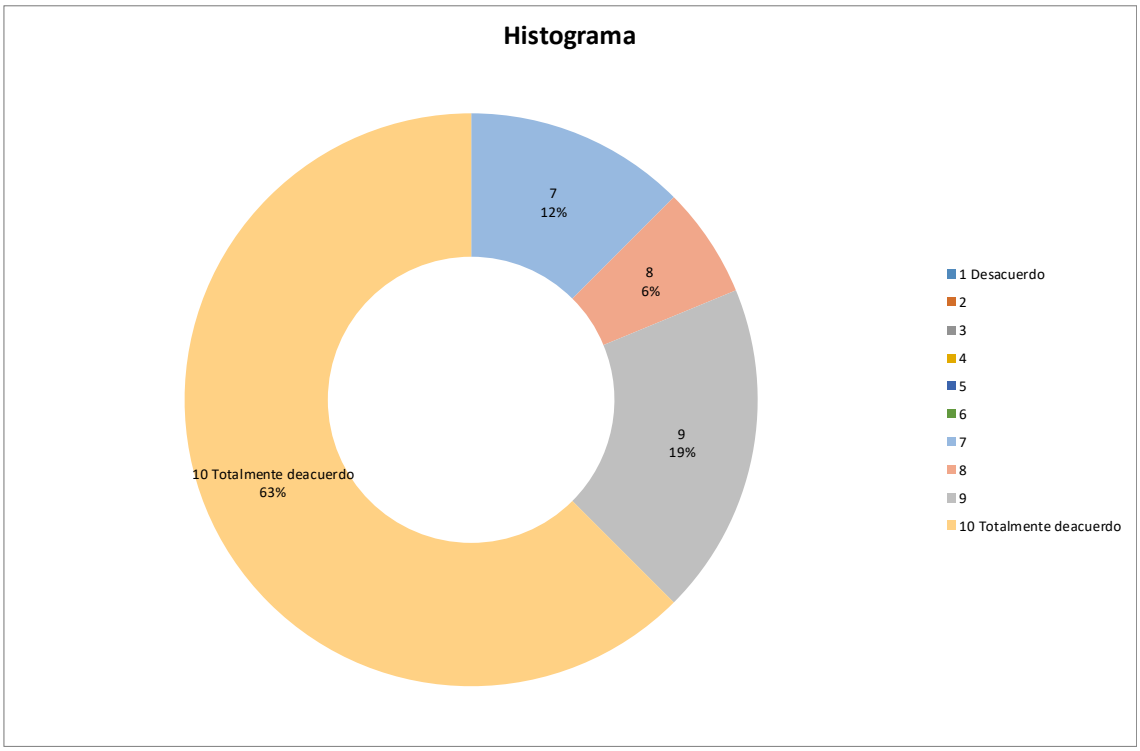

**El auditor debe revisar la gestión de los activos de información y los responsables de los mismos, comprobación de la clasificación de la información, comprobación de la gestión en la manipulación de los soportes**



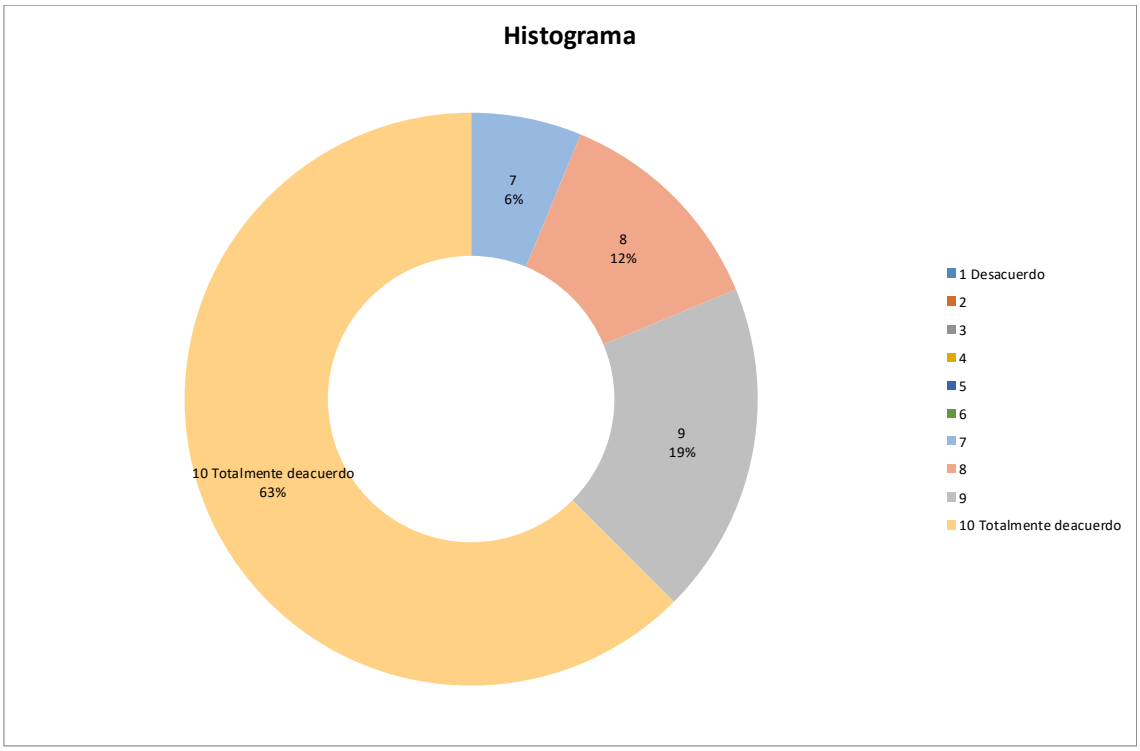
**Es importante por parte del auditor la comprobación de los controles de acceso, comprobación de la gestión de acceso de usuario, comprobación de las responsabilidades de usuario, comprobación de los controles de acceso a los sistemas y aplicaciones.**



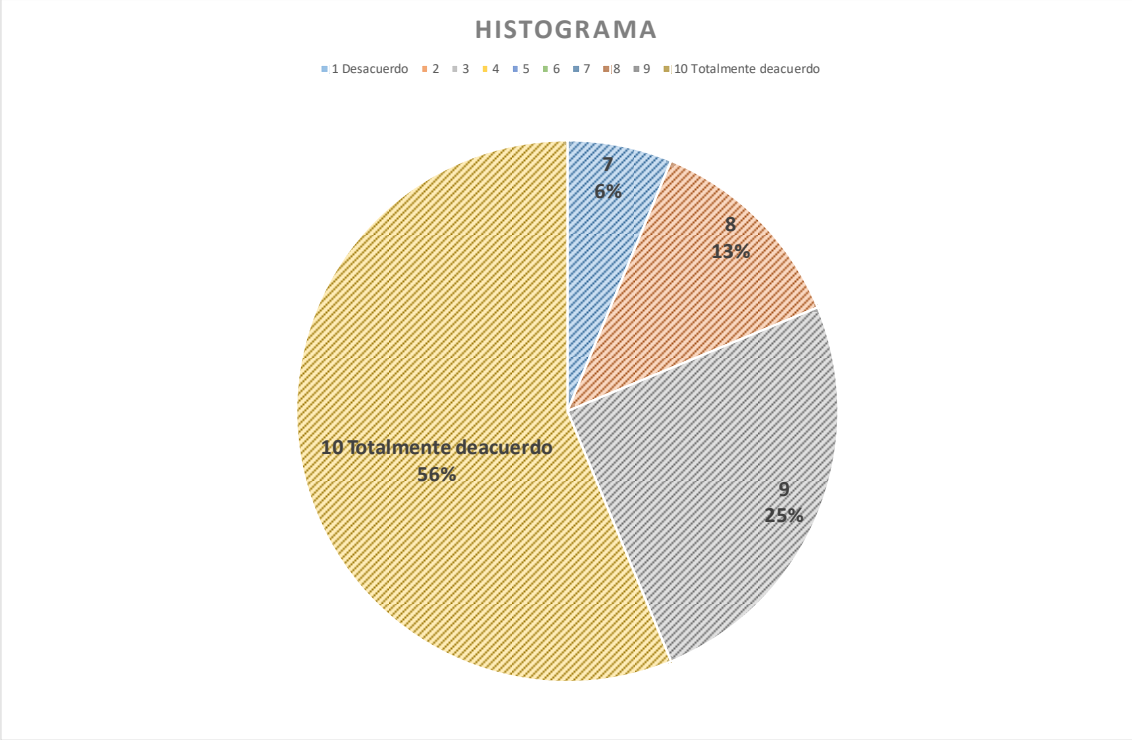

**El auditor debe revisar la criptografía para proteger la confidencialidad, autenticidad e integridad de la información, comprobación de los controles criptográficos con un sistema de claves que de soporte al uso de las técnicas criptográficas que se hayan implantado**



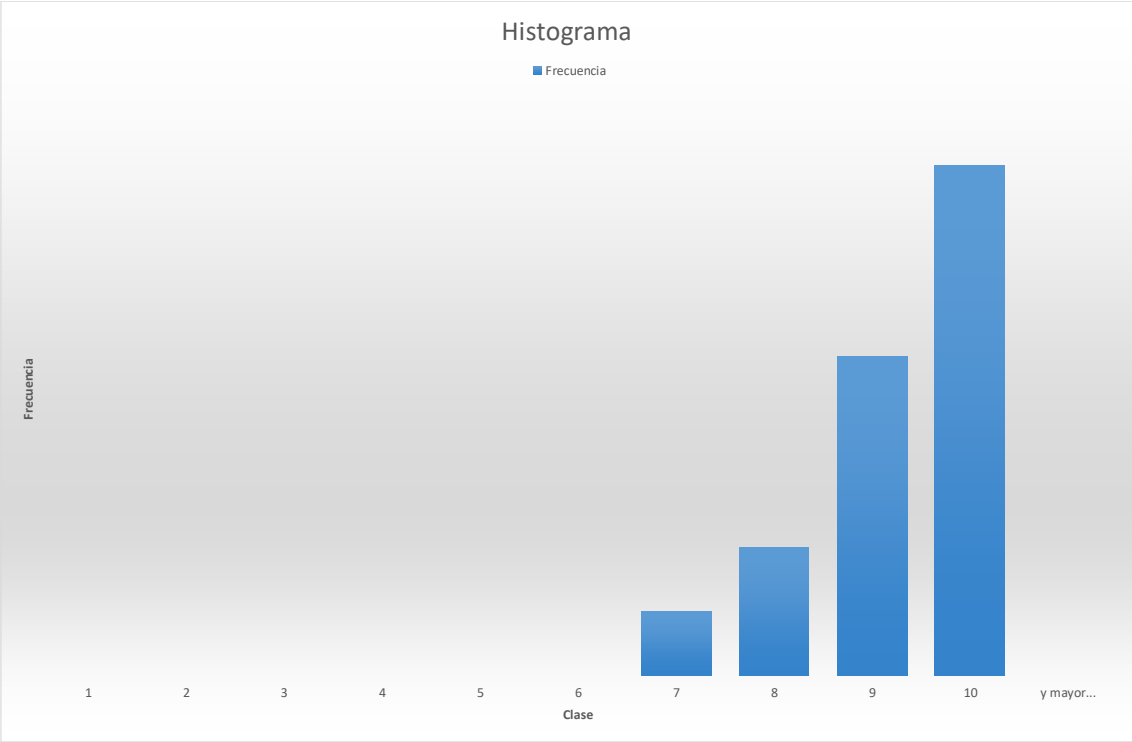
**El auditor debe revisar la seguridad física en áreas seguras y del entorno, la seguridad del equipamiento**



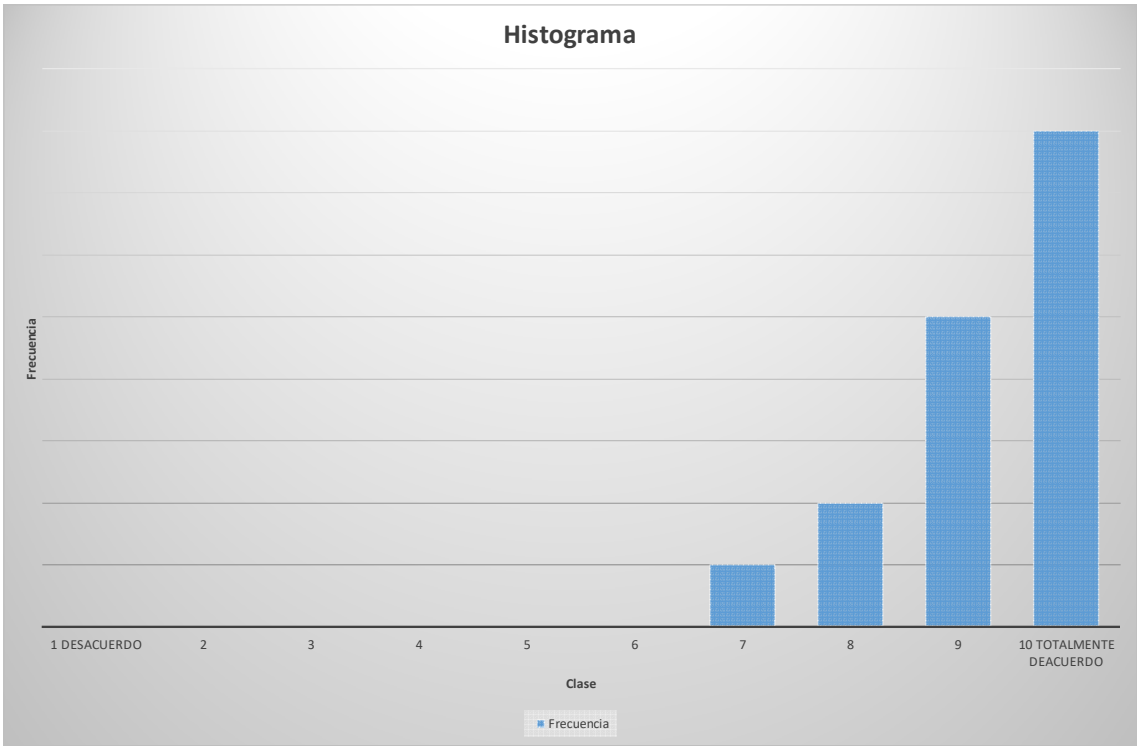
**El auditor debe comprobar las responsabilidades y procedimientos de operación, comprobación de la protección contra código malicioso, comprobación de la gestión y copias de seguridad, comprobación del registro y la supervisión, control de software operativo, revisión de la gestión de vulnerabilidades técnicas, comprobación de las consideraciones sobre la auditoría de los sistemas de información**



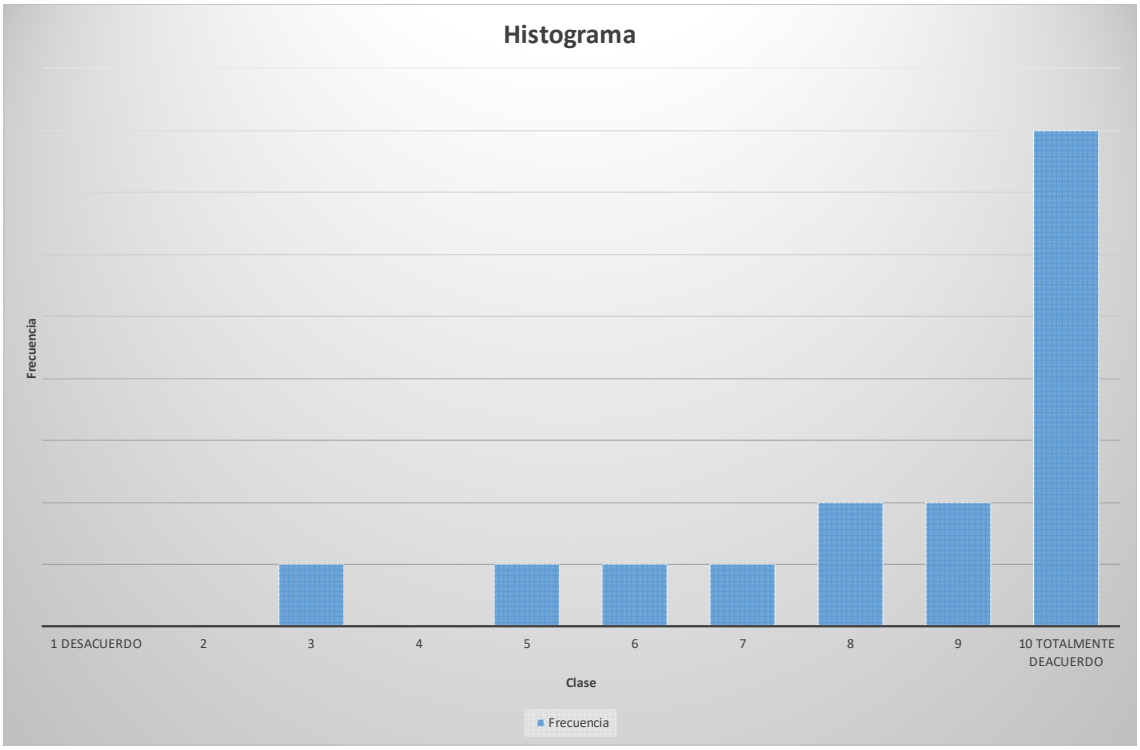

**El auditor debe revisar la seguridad en las comunicaciones, seguridad en las redes e intercambio de información**




**El auditor debe contemplar el grado de satisfacción con la calidad de la información que recibe de los distintos riesgos de la empresa: cumplimiento legal, regulación del gobierno y su impacto, riesgo operacional, incertidumbre, posible interrupción al modelo de negocio, riesgo de la cadena de suministro, falta de innovación, ritmo de cambio tecnológico, riesgo de sistémico global, seguridad cibernética.**

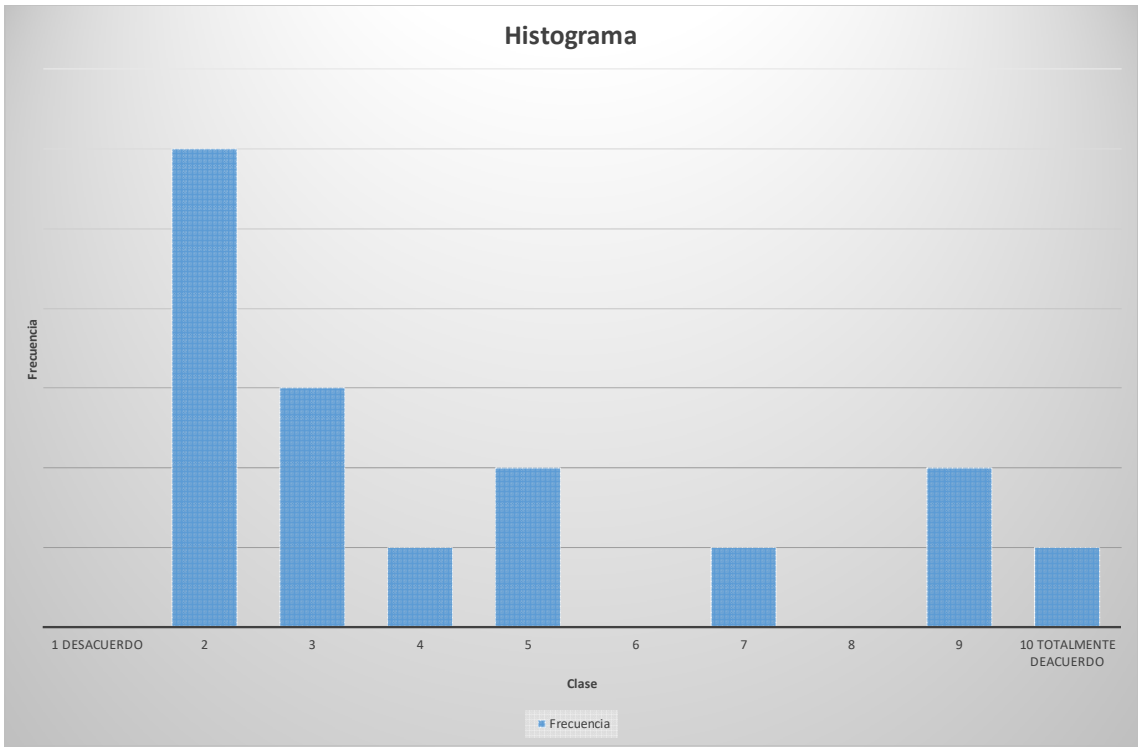


**Debería ser obligatorio que las organizaciones publicaran su mapa de riesgo detalladamente para un mayor grado de transparencia y un informe de auditoría interno y externo donde se ponga de manifiesto los riesgos cibernéticos y sus consecuencias**

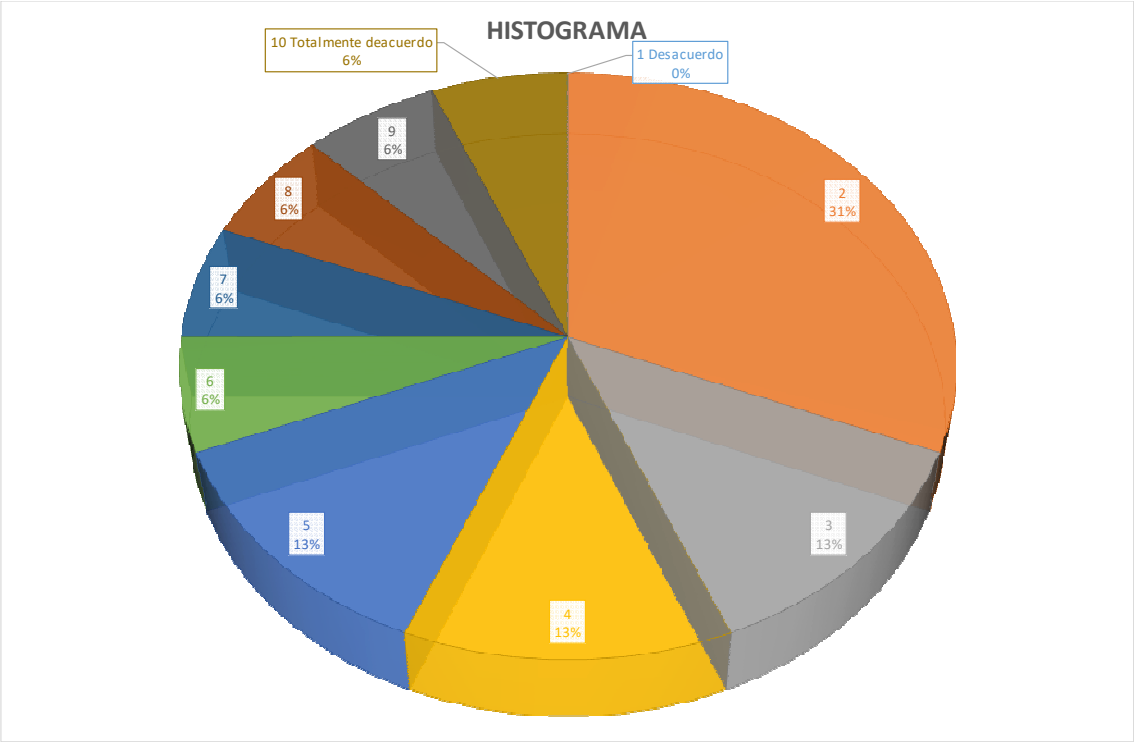



**BLOQUE C: SEGURIDAD DE LA INFORMACIÓN Y SECTORES DONDE SERÍA MÁS NECESARIO LA APLICACIÓN DE UNOS MÍNIMOS DESEABLES POR ENCIMA DE LOS MÍNIMOS NORMATIVOS**

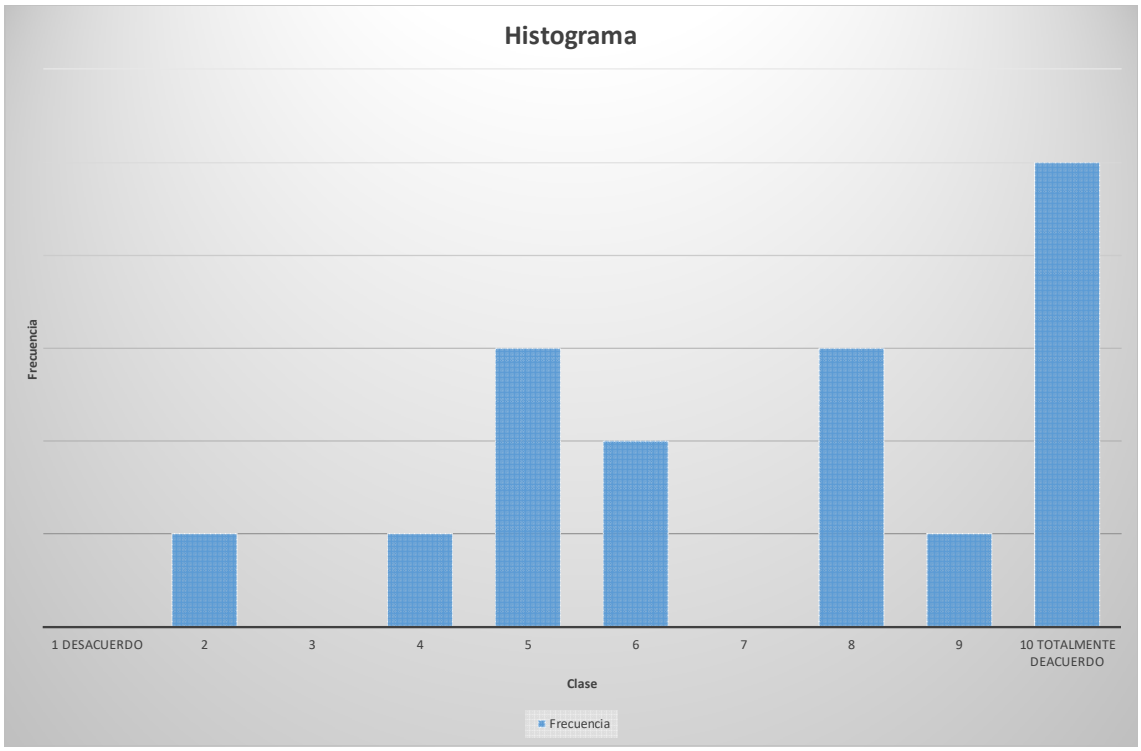
**En el balance de situación de su empresa, la masa patrimonial de Inmovilizado Intangible es realmente representativa de la actividad en intangibles.**


Histograma
Frecuencia
1 DESACUERDO
2
3
4
5
6
7
8
9
10 TOTALMENTE DEACUERDO
Clase
Frecuencia

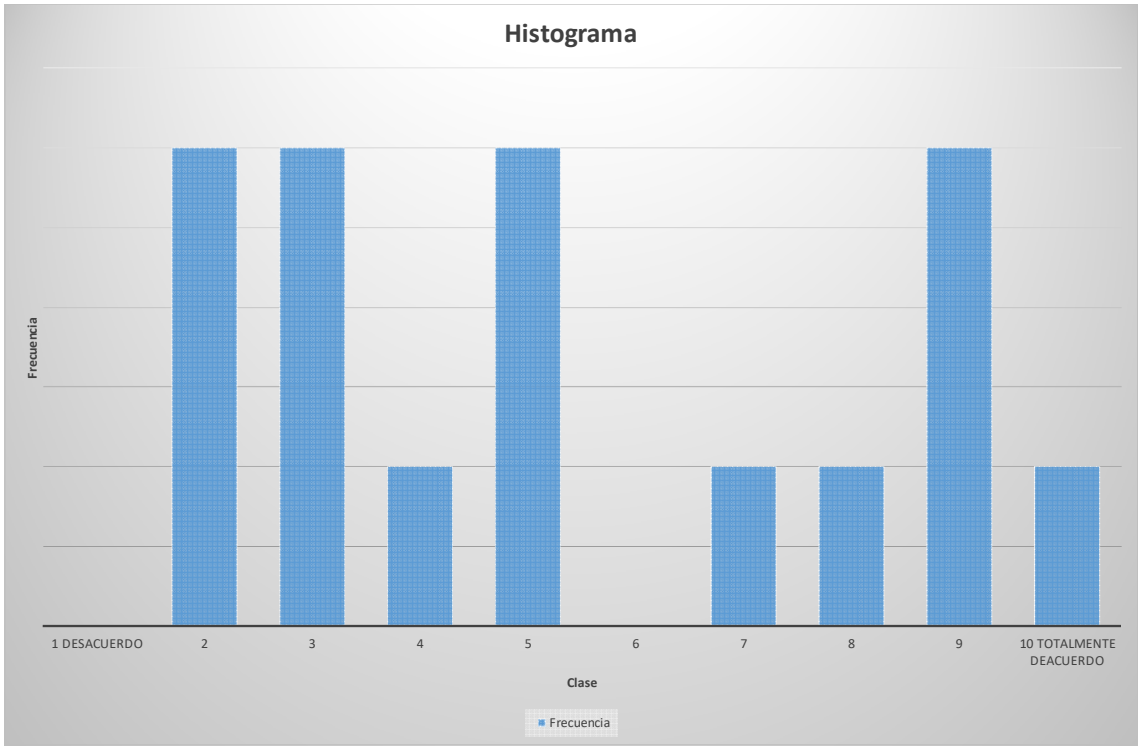
**Se refleja con detalle el valor de sus intangibles como: patentes, marcas, diseños y modelos de utilidad entre otros.**



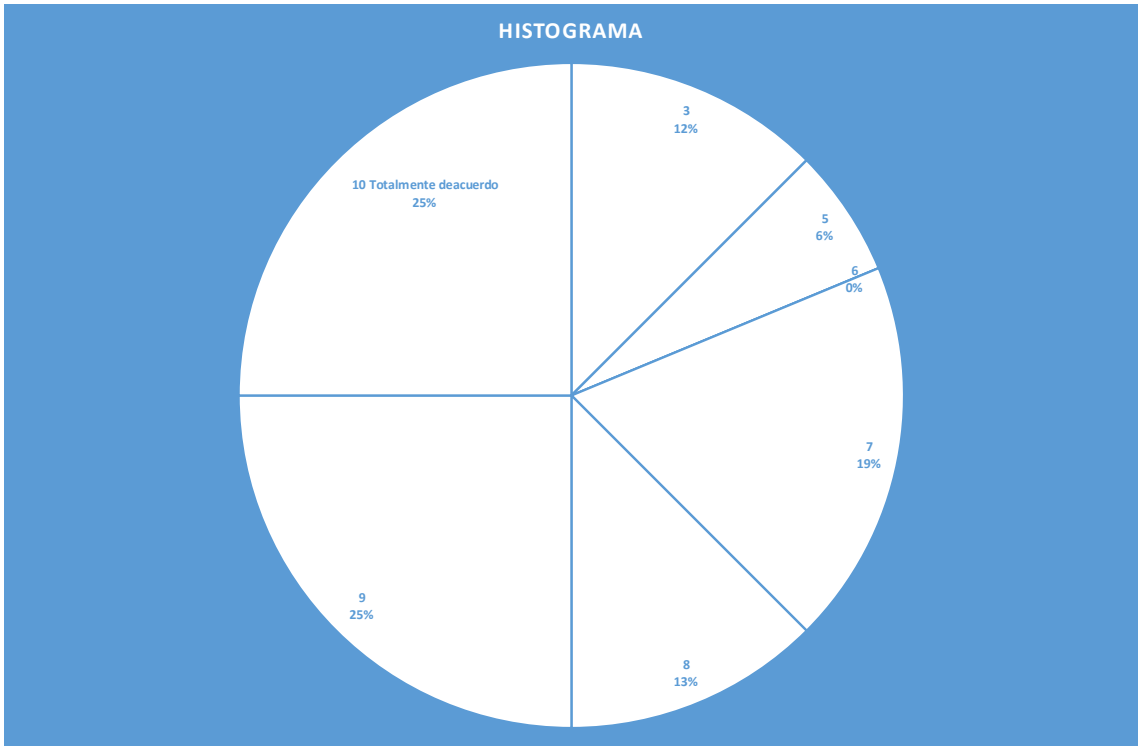

**Sería conveniente, a raíz de los graves problemas creados por la seguridad de la información, deslindar la masa patrimonial del inmovilizado intangible general de las inmovilizaciones por seguridad de la información.**



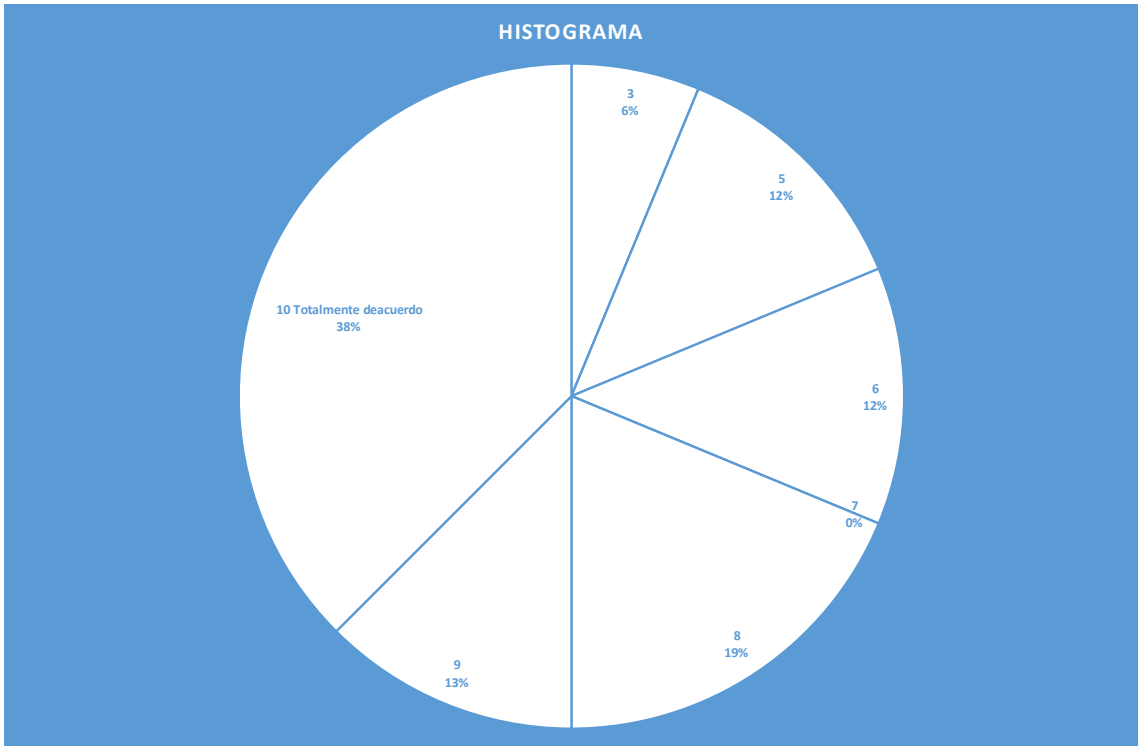

**La contabilidad contempla la importancia de este inmovilizado, en aras a una mejor valoración del mismo y de la empresa en su conjunto.**



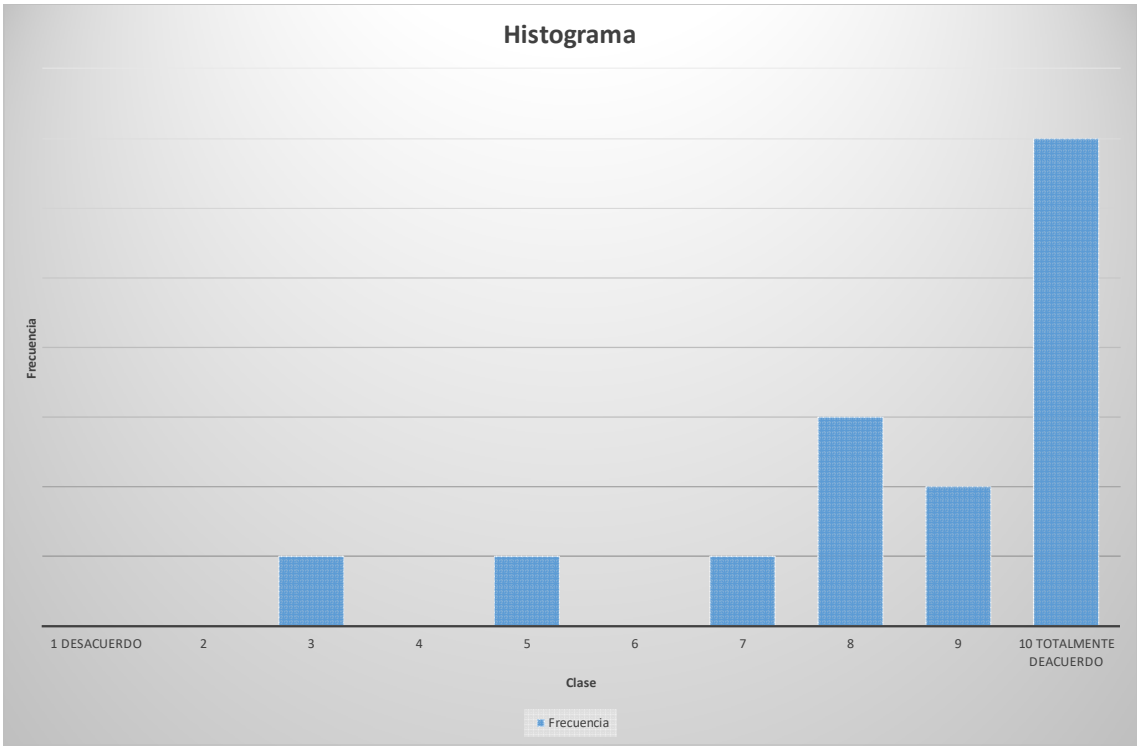
**Sería oportuno deslindar en la contabilidad actual, para una mayor información, las operaciones por acreedores y deudores de tráfico mercantil online de las y tradicionales**



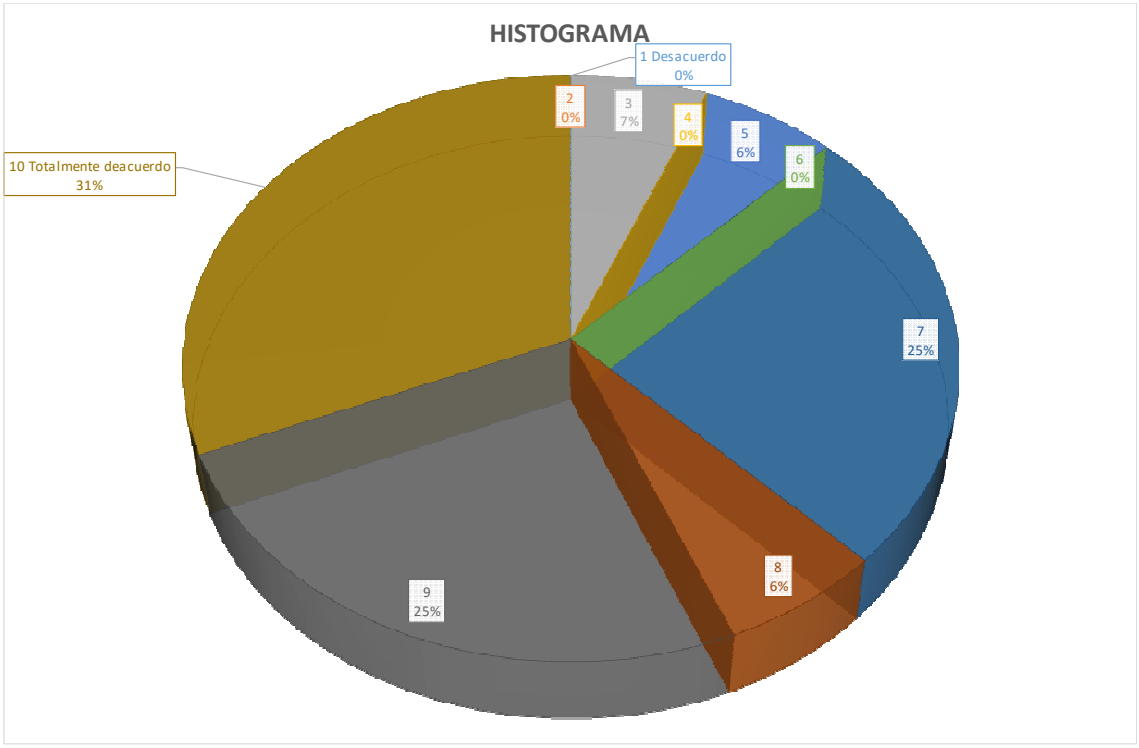

**Sería conveniente en la contabilidad deslindar las ventas tradicionales y las ventas online**



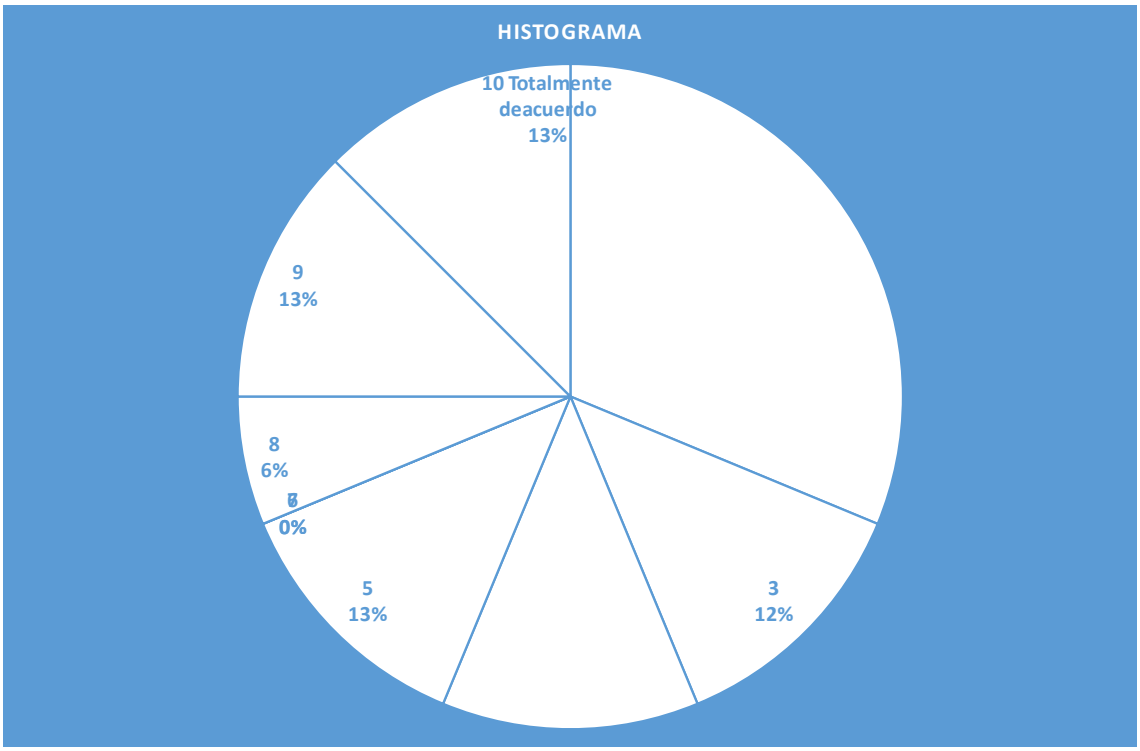
**Sería conveniente que el informe de auditoría contemplara en un párrafo aparte e independiente la información cualitativa y cuantitativa por los incidentes por seguridad de la información contrastando este informe con el de auditoría interna**



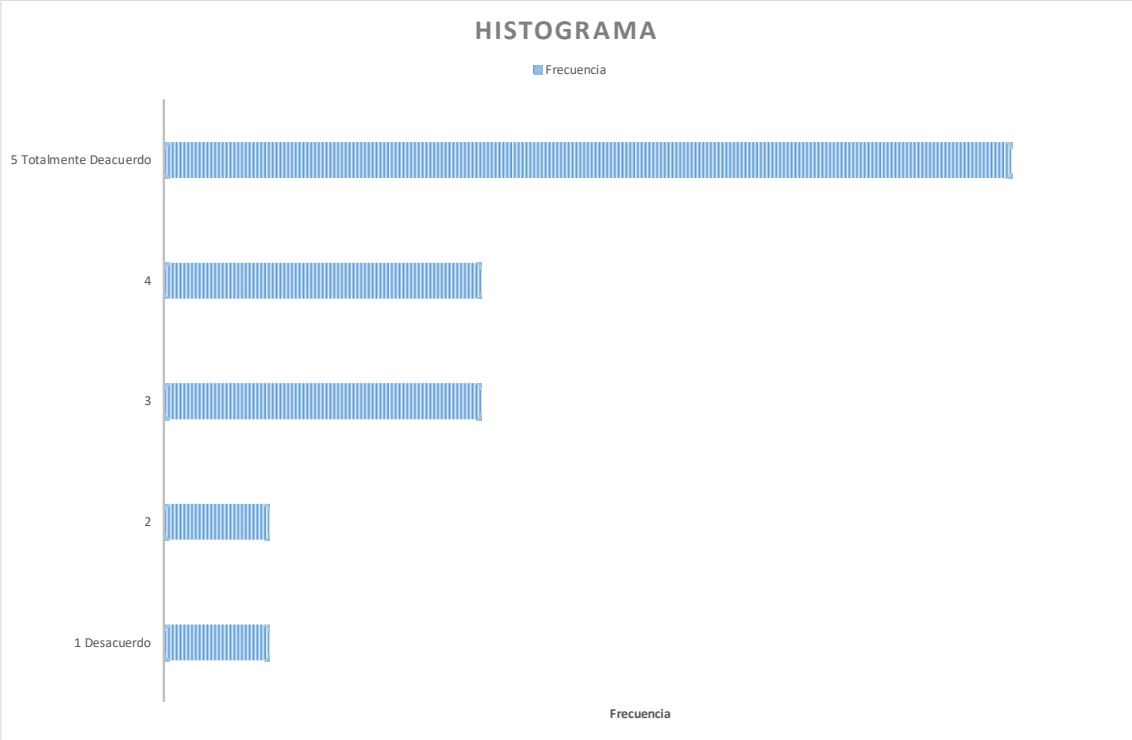

**Los estados contables actuales deberían contemplar, al menos con información textual o narrativa, la importancia del talento y sus indicadores ante la problemática de ciberamenazas**



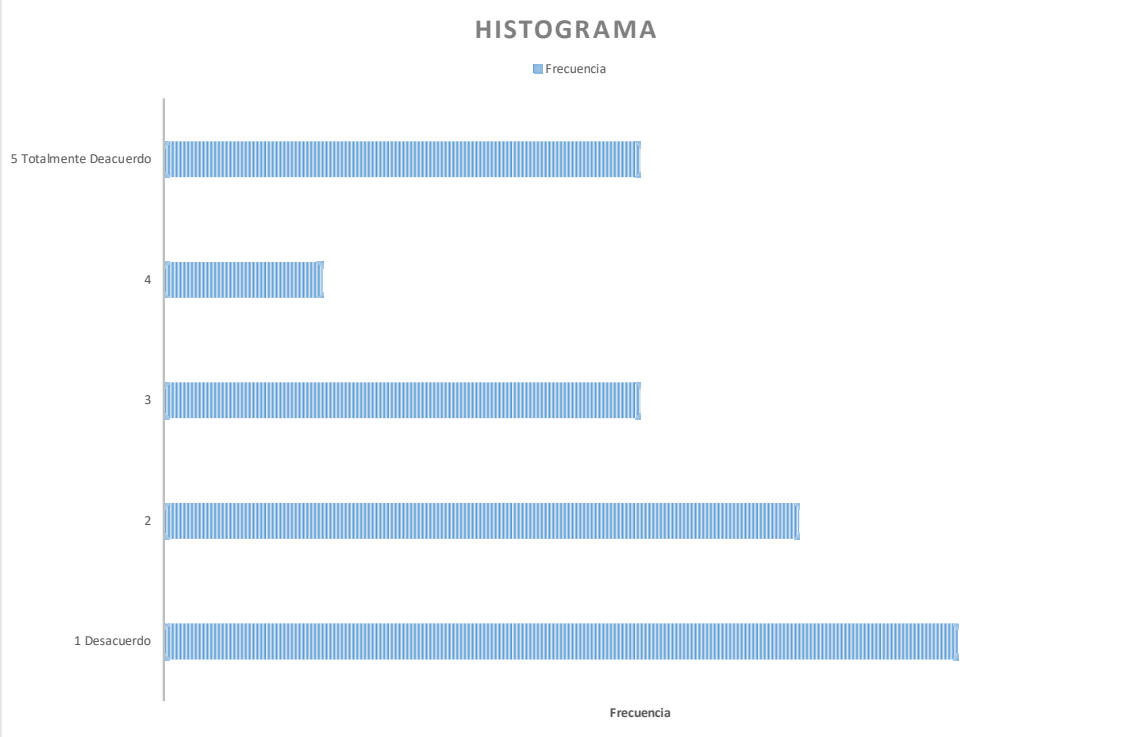

**La carta del presidente en el informe anual contempla la importancia de los problemas de ciberseguridad, y se detalla la información a este respecto**



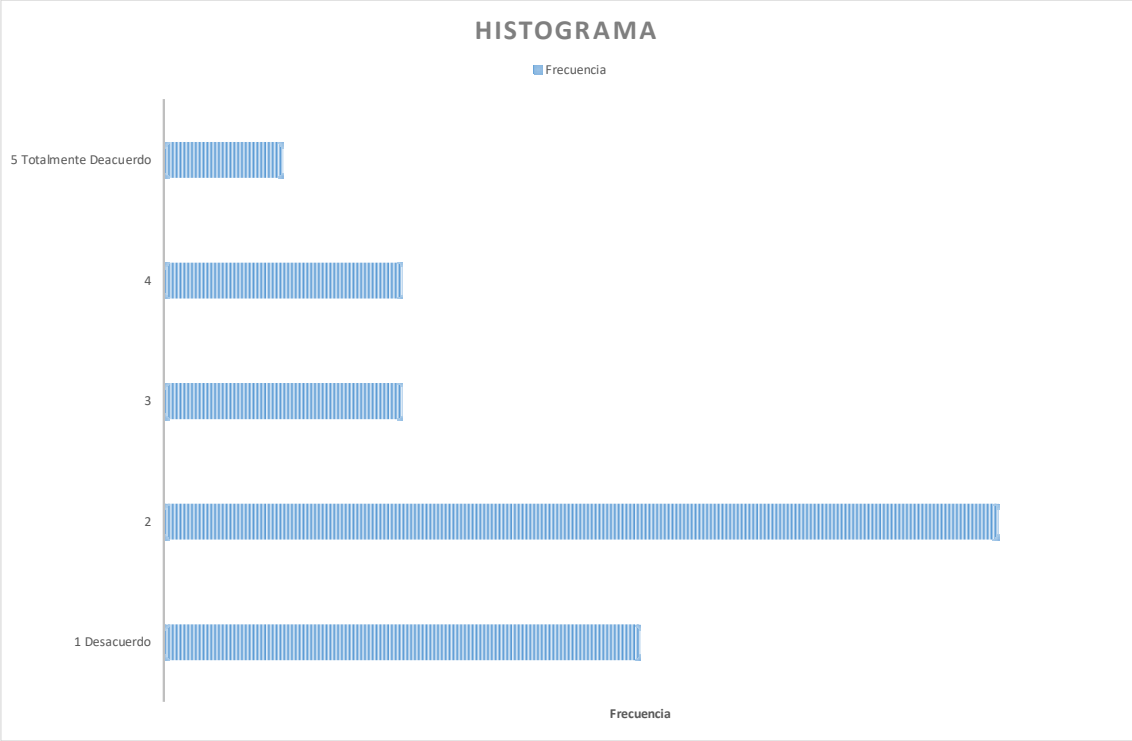
**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Los mismos empleados de la compañía]**



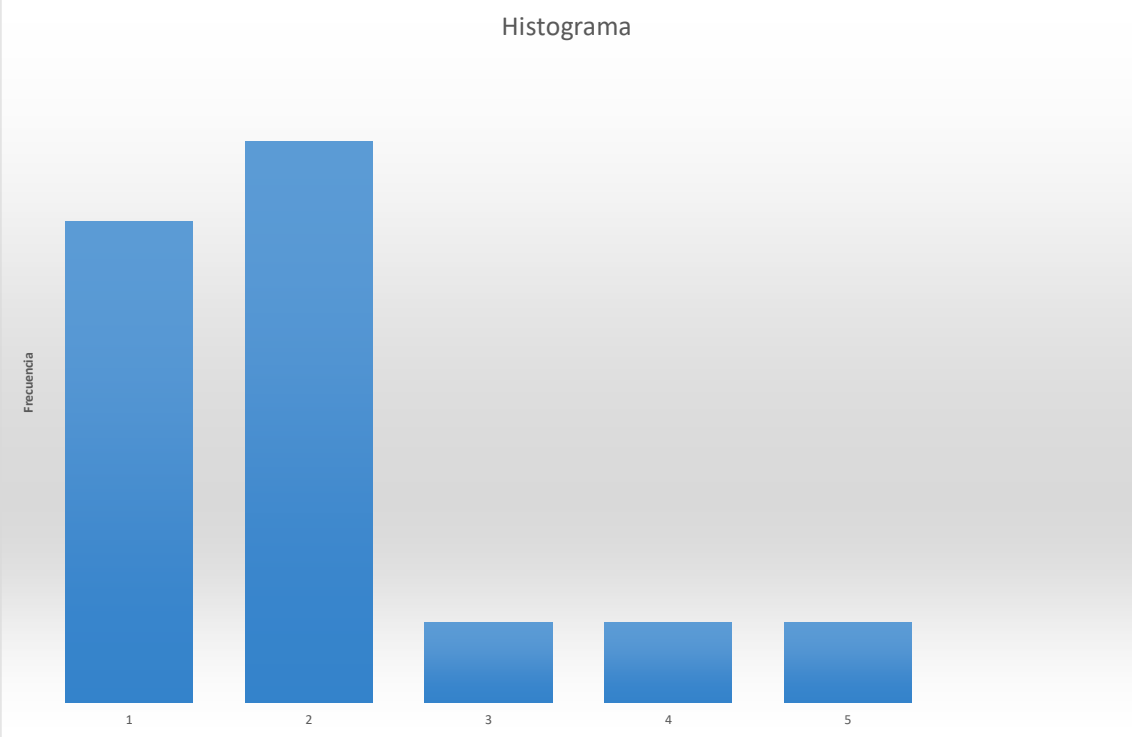

**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Los proveedores]**



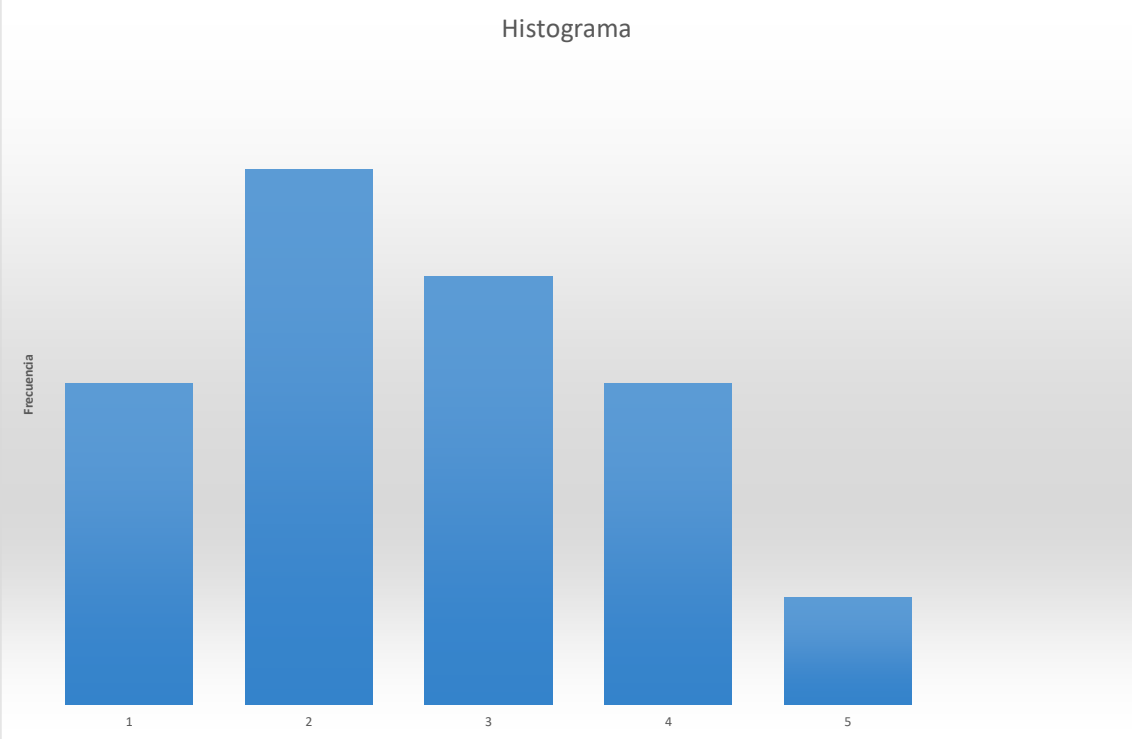
**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Los clientes]**



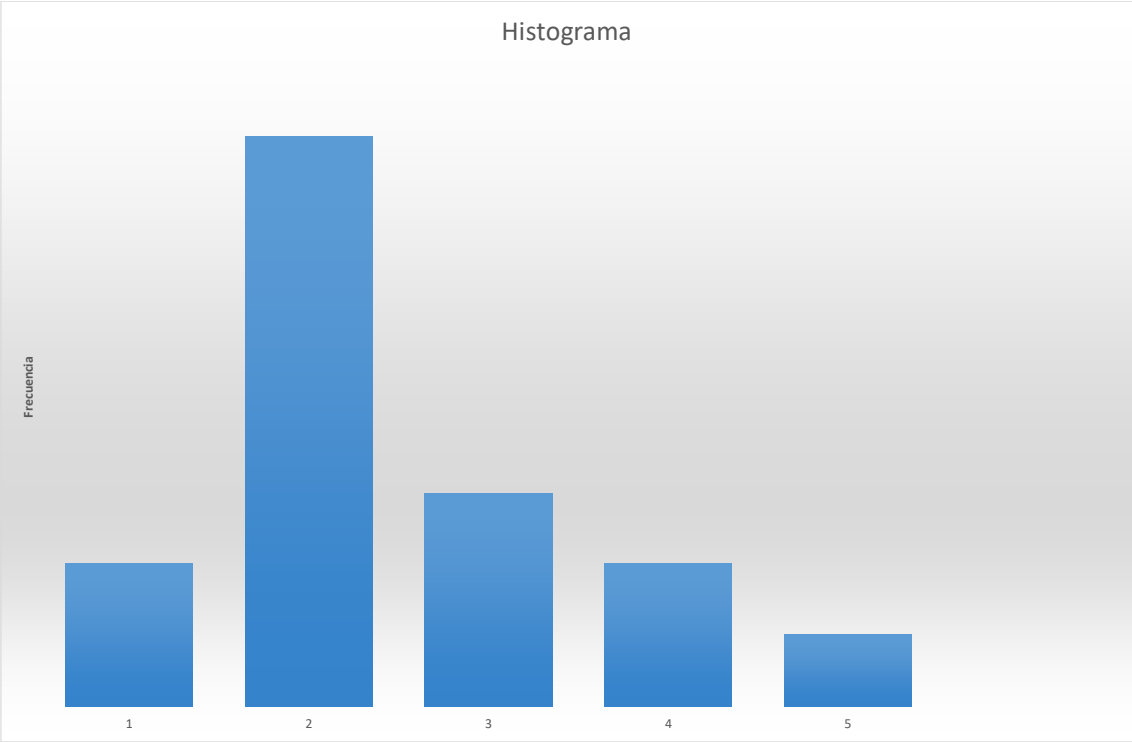

**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Los asesores, consultores]**



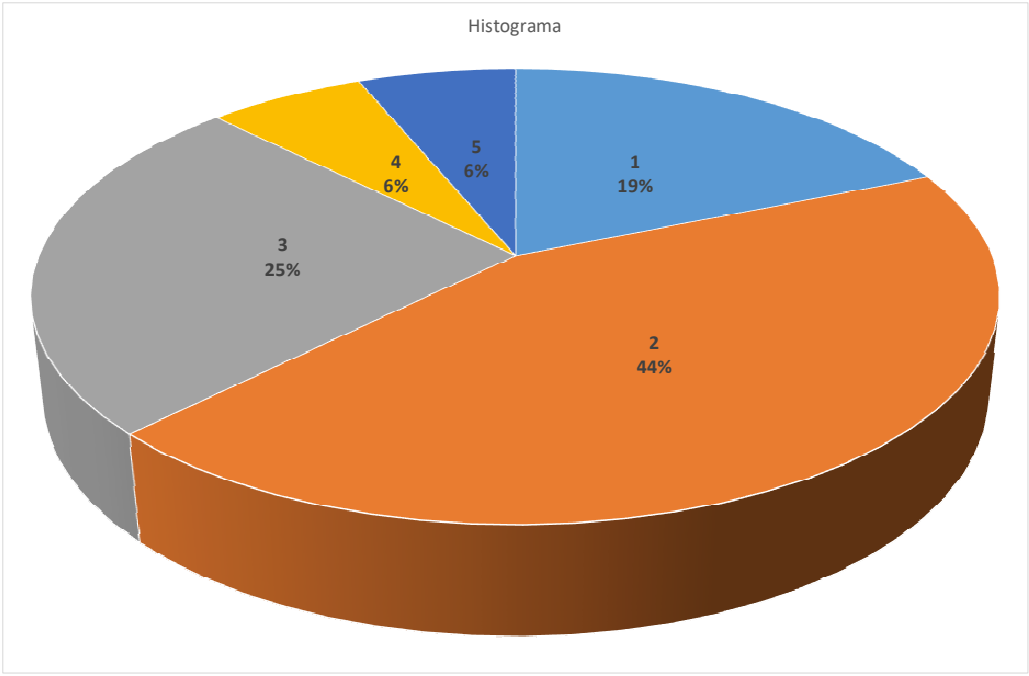
**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Representantes de los trabajadores por reivindicaciones]**



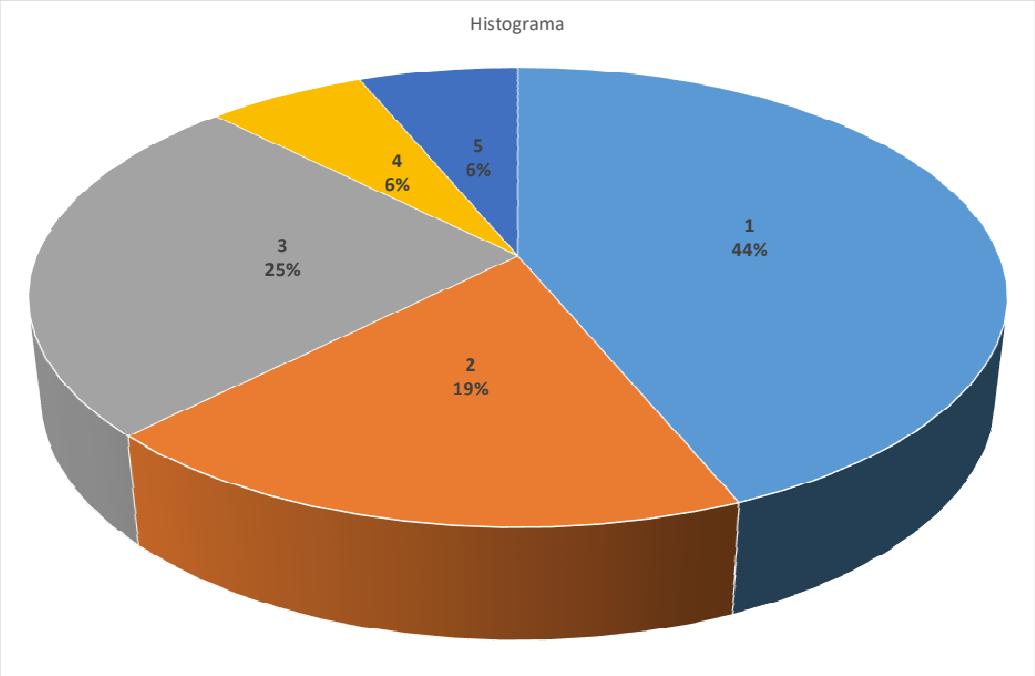

**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Hackers, apasionados por la investigación sin hacer daño]**



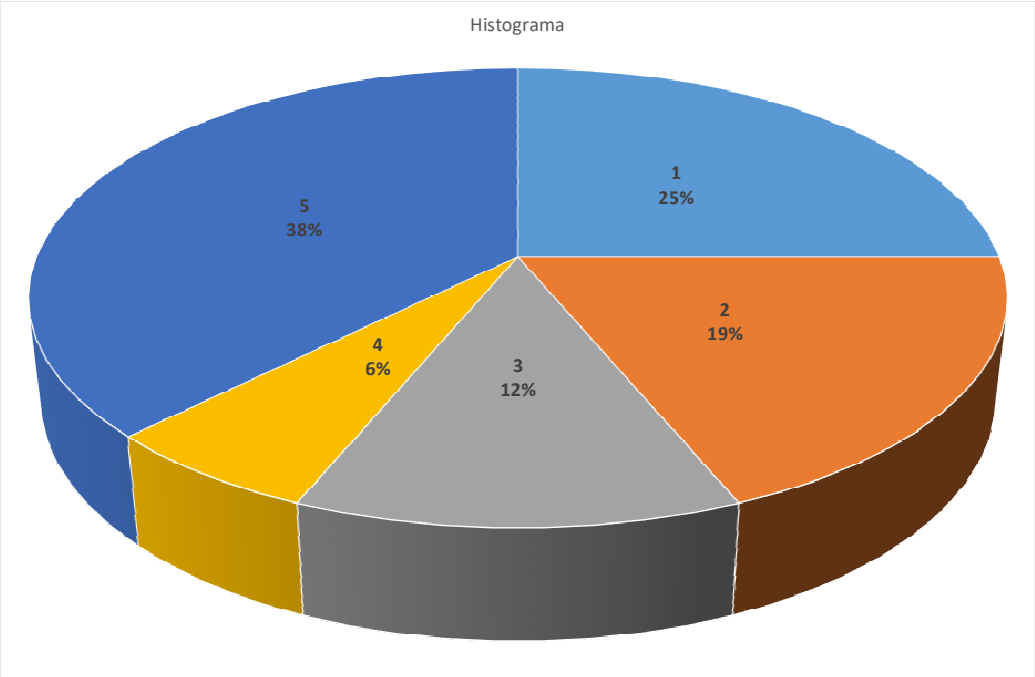

**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Crackers, conocimientos sobre computación, empieza a investigar la forma de bloquear protecciones o claves de acceso con programas propios o conseguidos en páginas webs (dañar información, robar datos, copiar programas, hacer mail bombing llenando el correo hasta dejarlo inutilizado]**



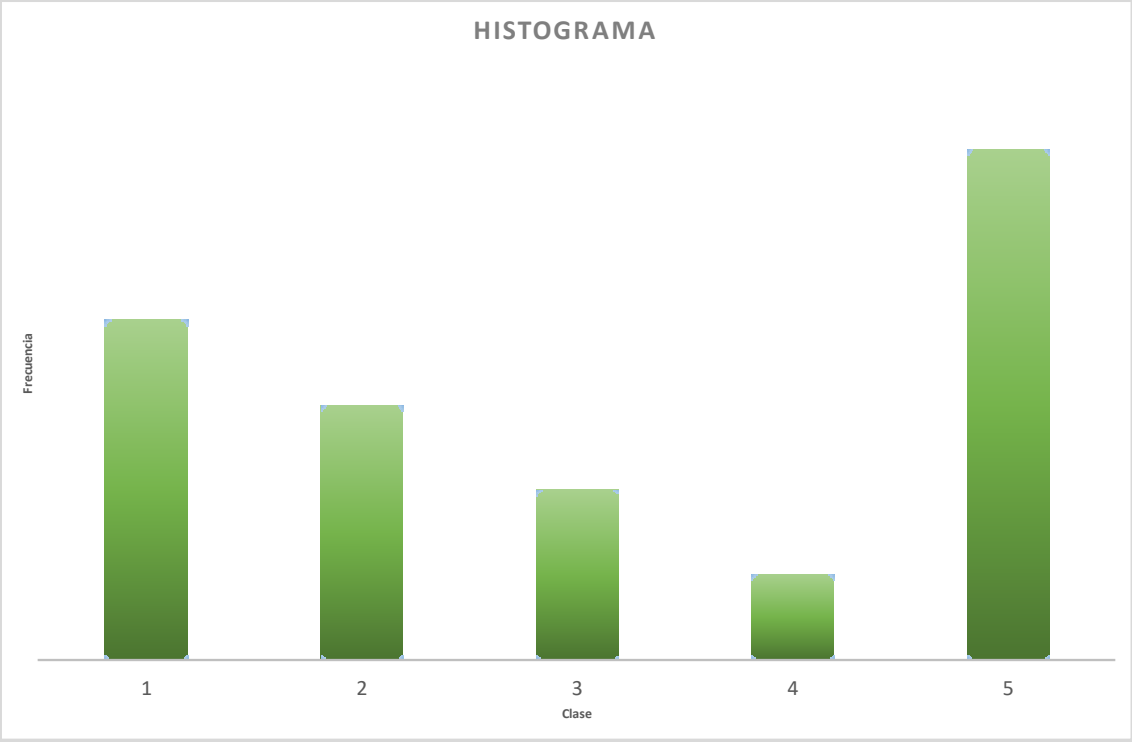
**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Phreakers, ejecuta programas de telefonía para interceptar llamadas.]**



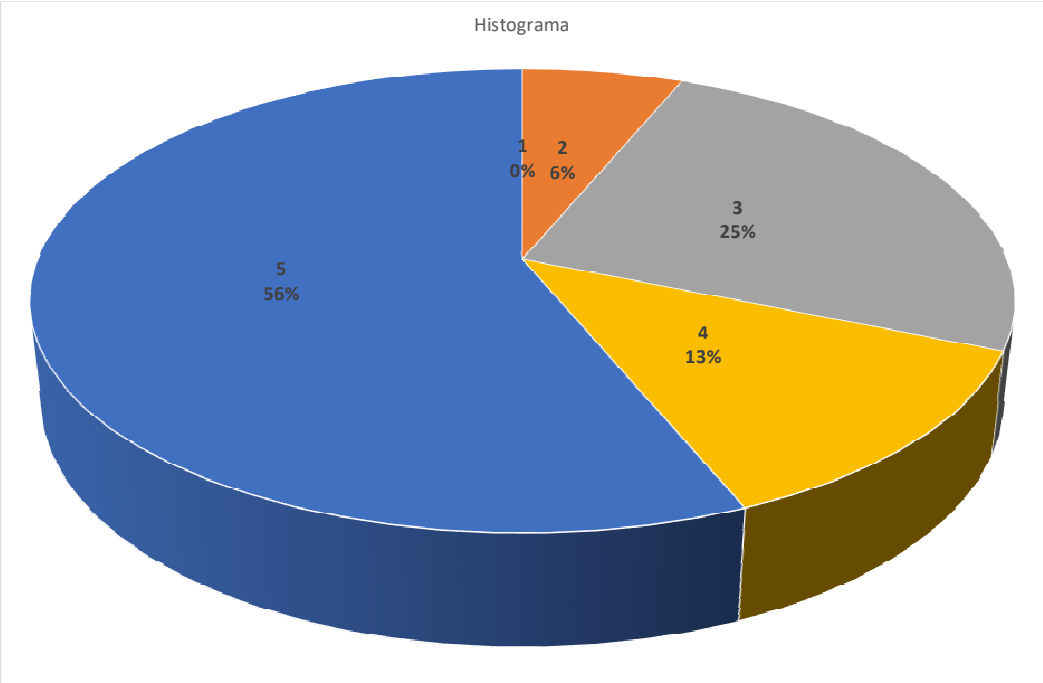

**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Delincuentes informáticos (interceptar compras en red, para que haciendo uso del nombre, número de tarjeta de crédito y fecha de expiración, realizar compras para proporcionar una dirección de envío), pedir dinero por encriptar los archivos relacionados con el objeto social de la empresa.]**



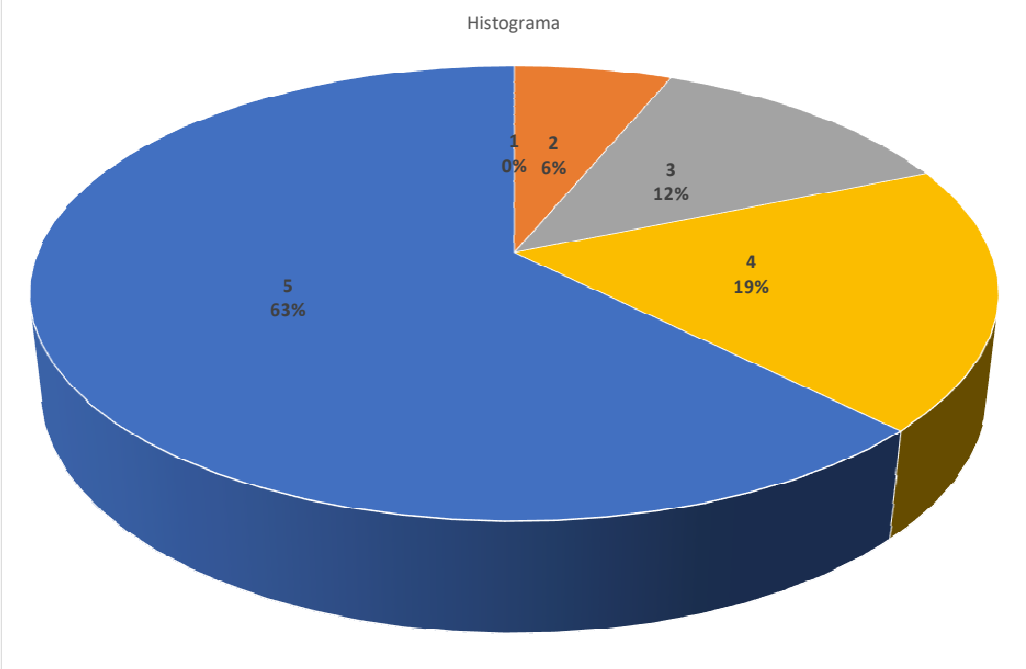

**En la situación actual de su empresa, al día de hoy, ¿quién o quiénes creen que fomentan o son los responsables de las ciberamenazas?: [Crackers relacionados con los competidores]**



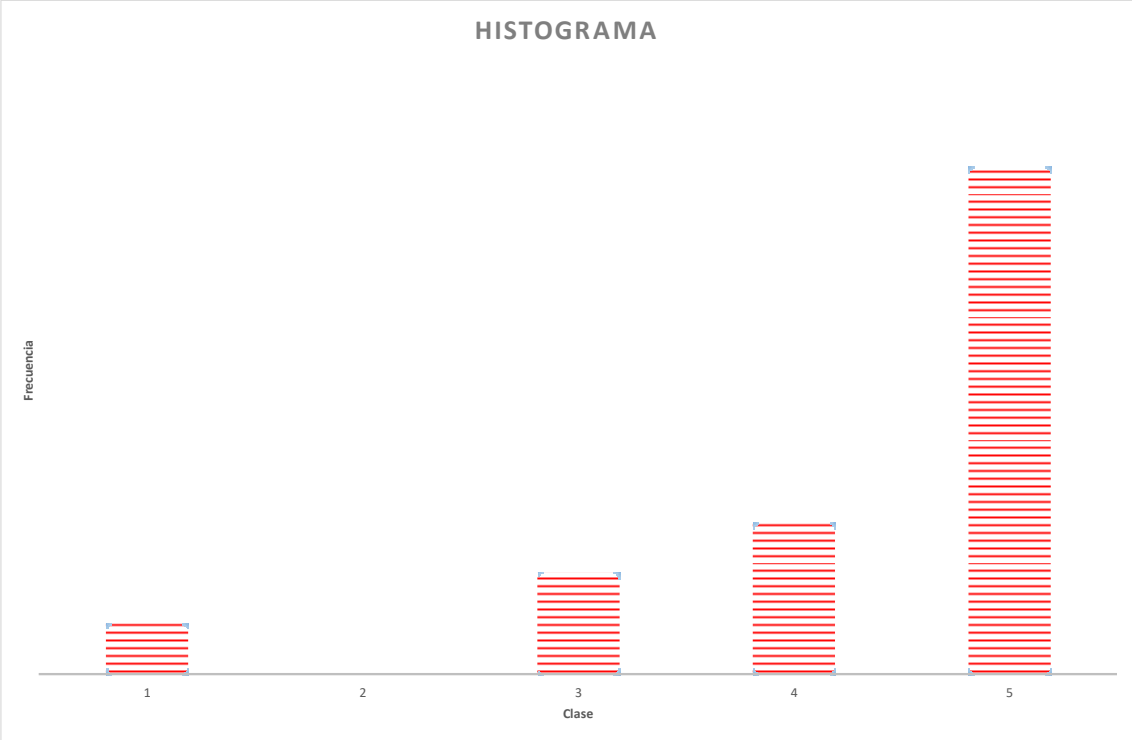

**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [observar la evolución histórica de los intangibles específicos en seguridad de la información y su composición]**



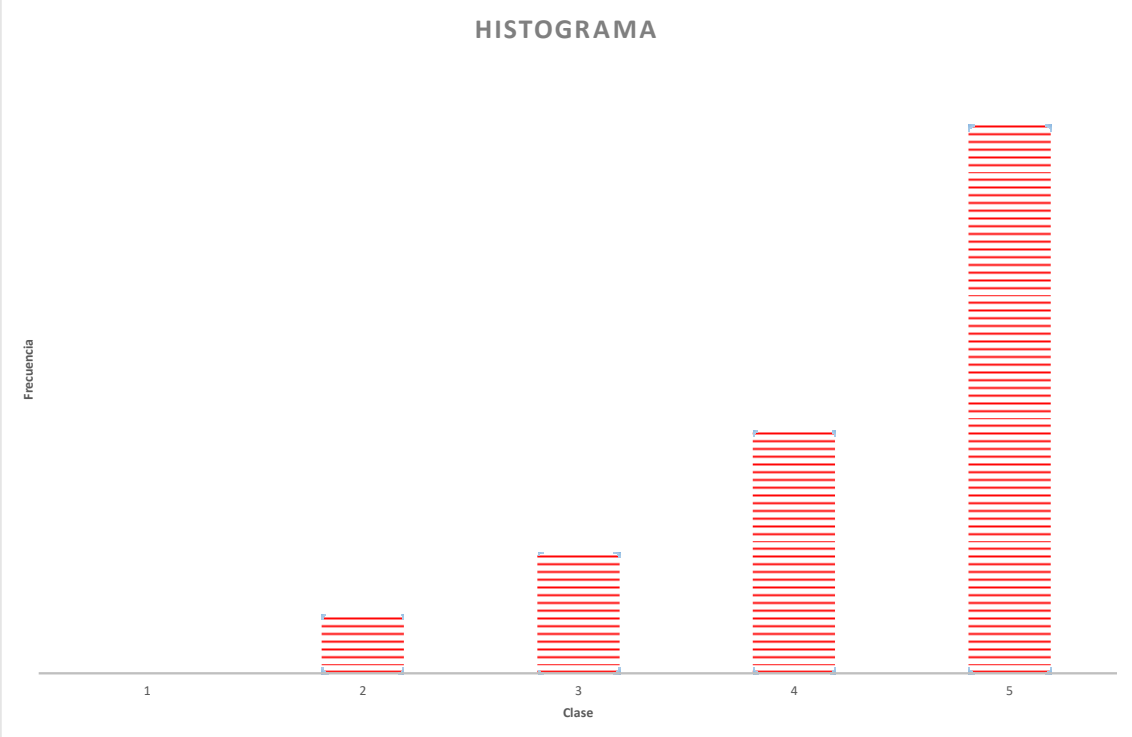

**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [sistema de gestión de la seguridad de la información]**



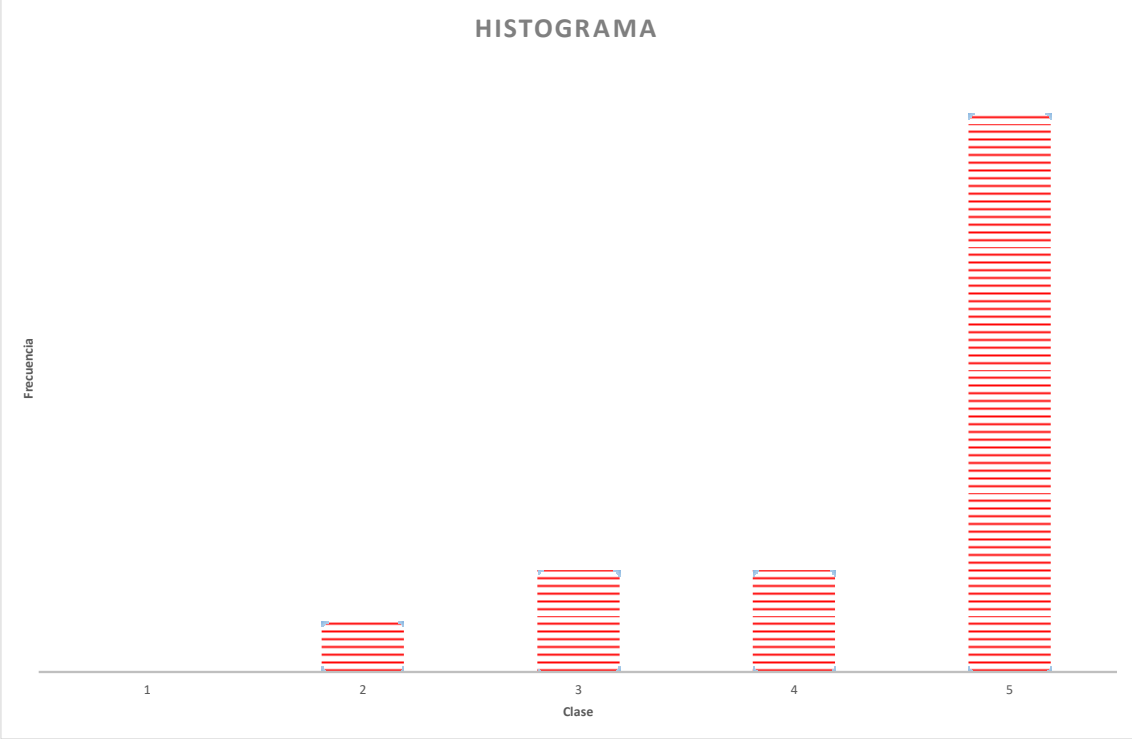
**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [la importancia del sistema de gestión de la seguridad de la información en las cuentas anuales]**



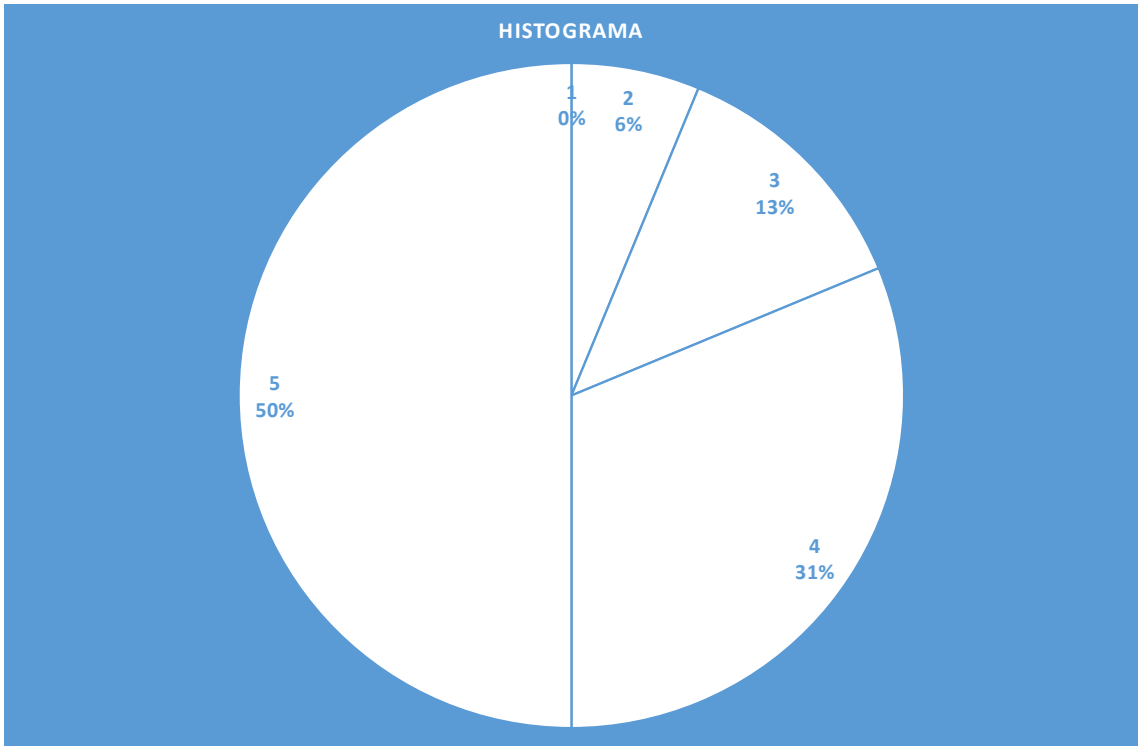

**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [en el informe de gestión]**



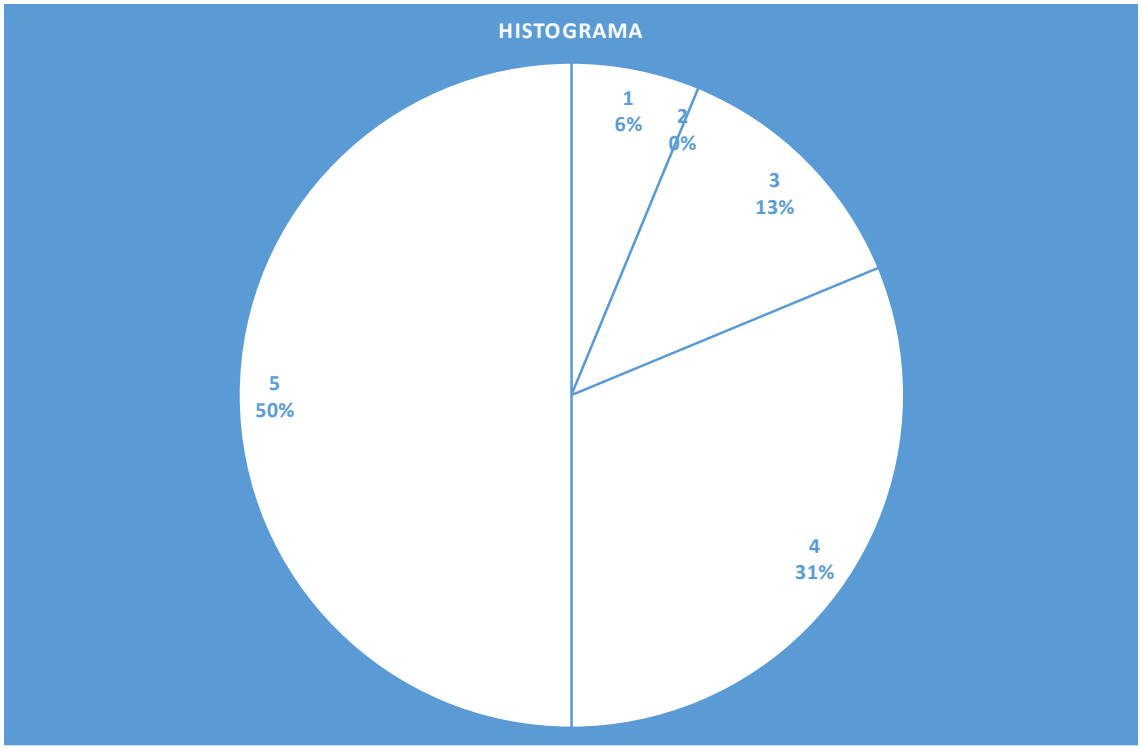
**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [en el informe de auditoría interna y externa (salvedades por ciberseguridad),]**



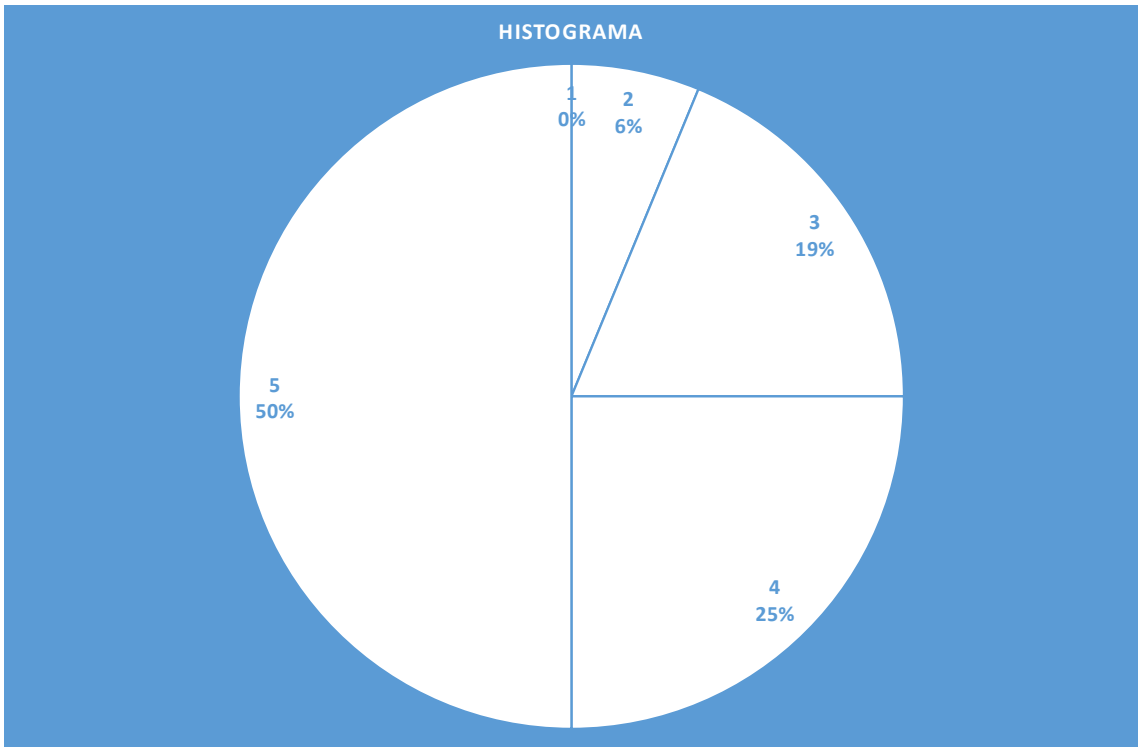

**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [informe de buen gobierno,]**



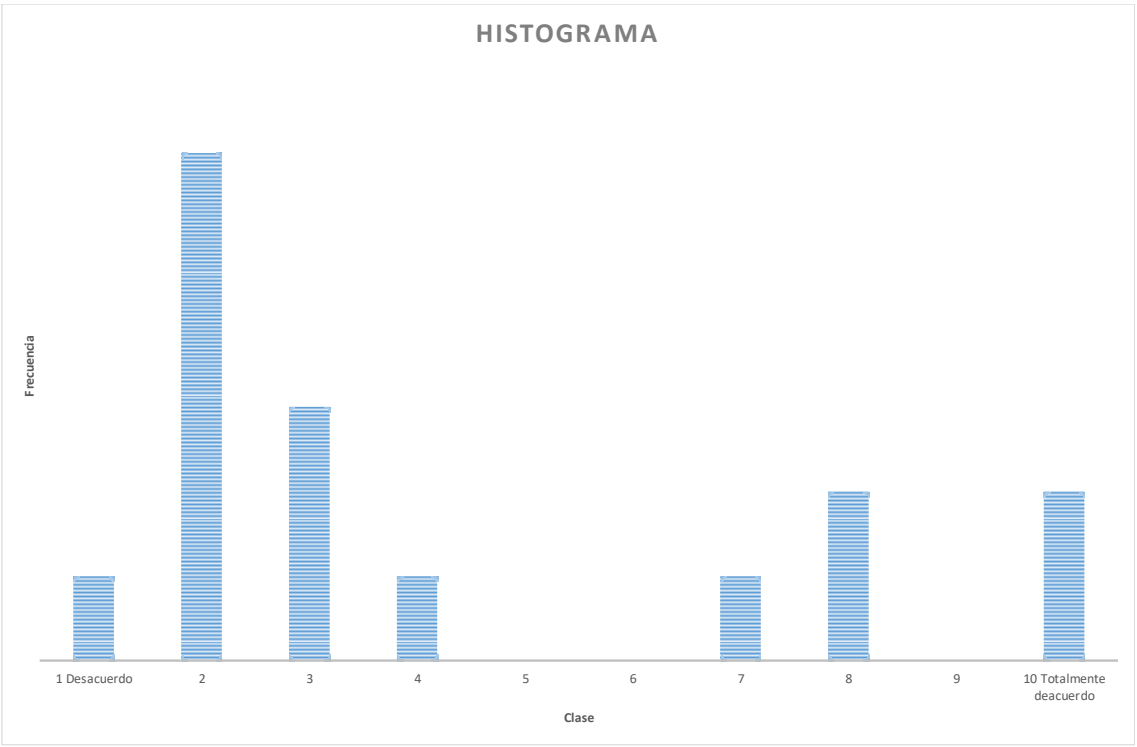
**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [informe de responsabilidad social corporativa,]**



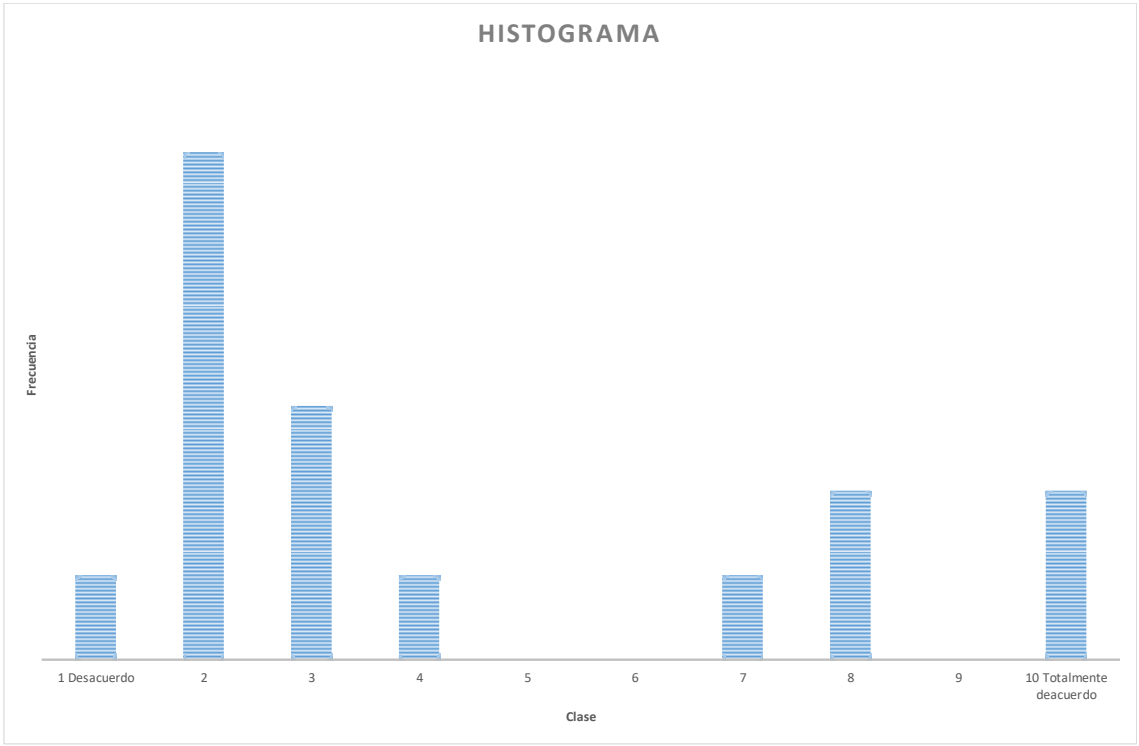

**Sería interesante en las empresas expuestas a las ciberamenazas y vulnerabilidades: [informe de reputación.]**



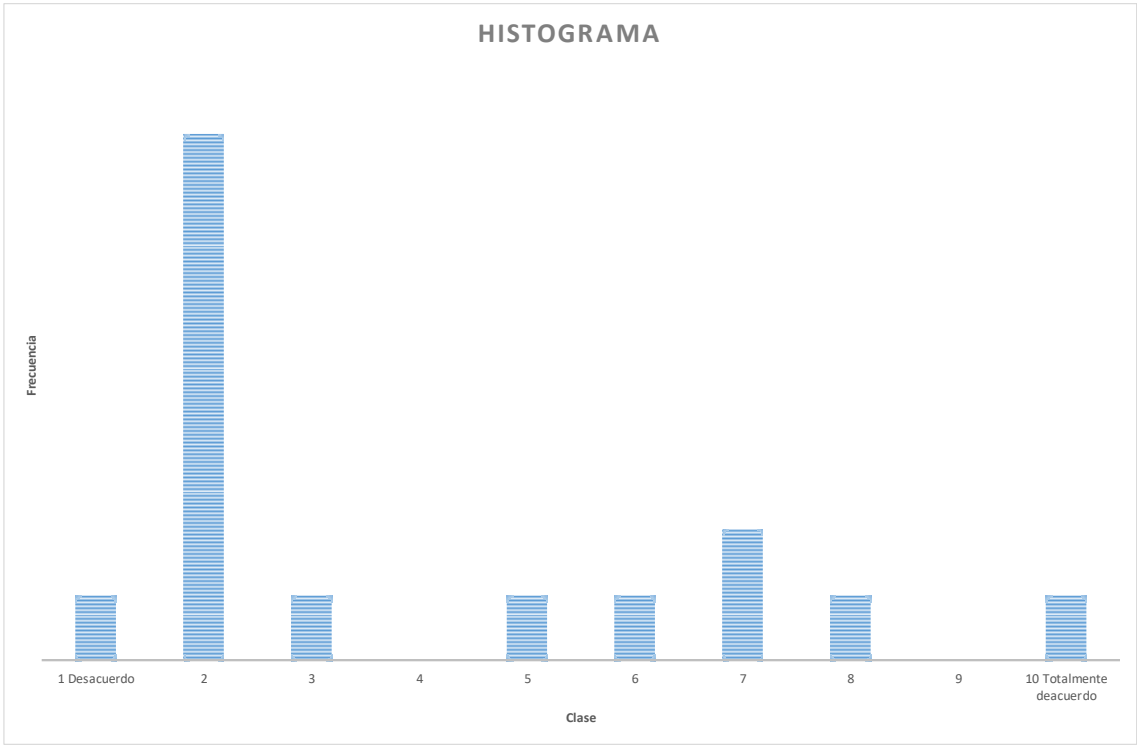

**Existe un protocolo escrito y aprobado por la alta dirección sobre las actuaciones de la organización ante problemas de seguridad de la información.**



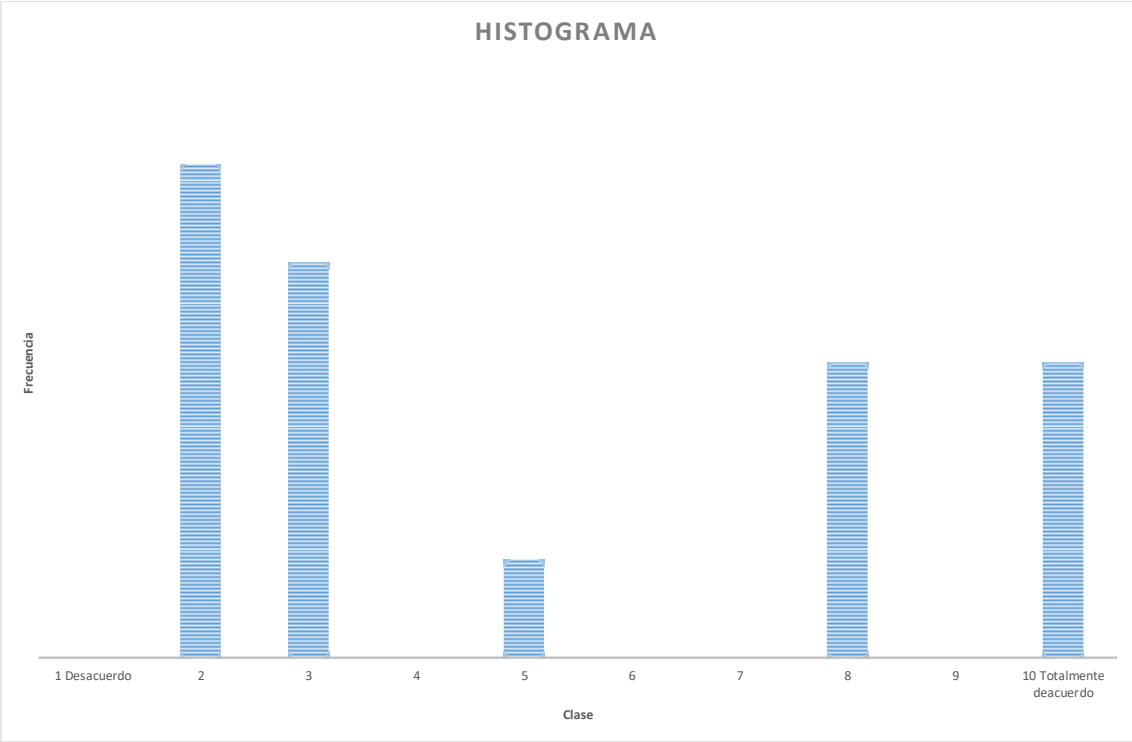

**Existe una relación detallada de los activos de información y sus propietarios.**



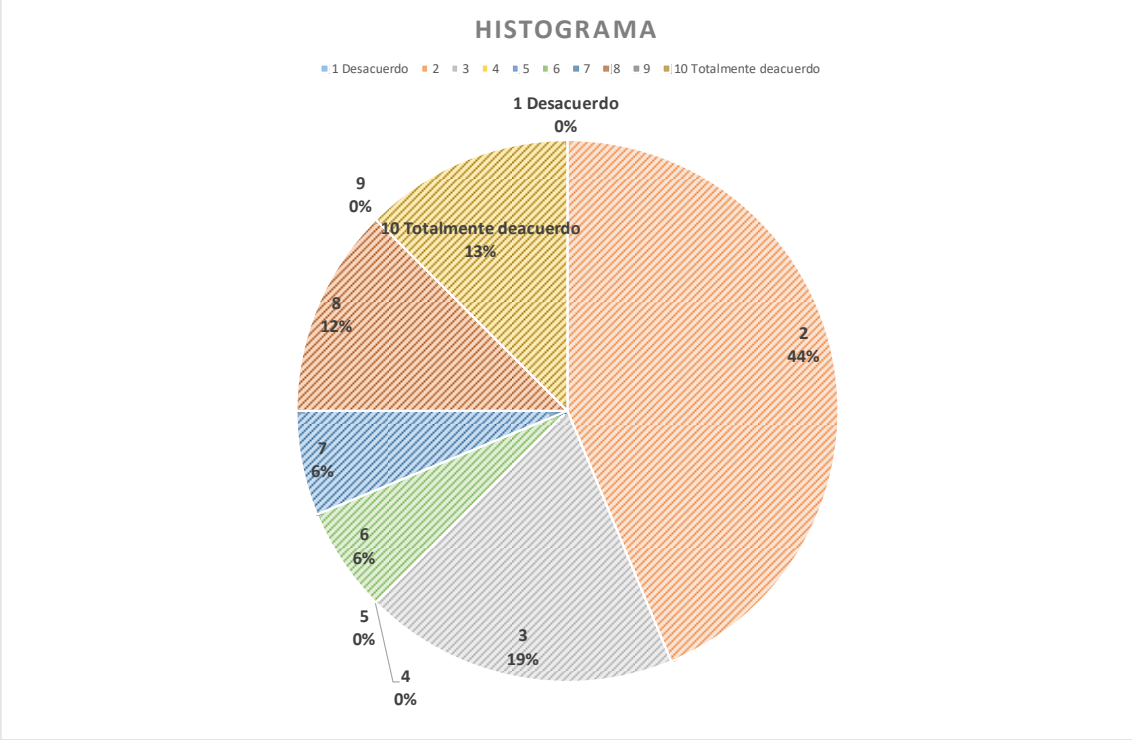

**Existe información histórica sobre el número de ataques y sus consecuencias.**



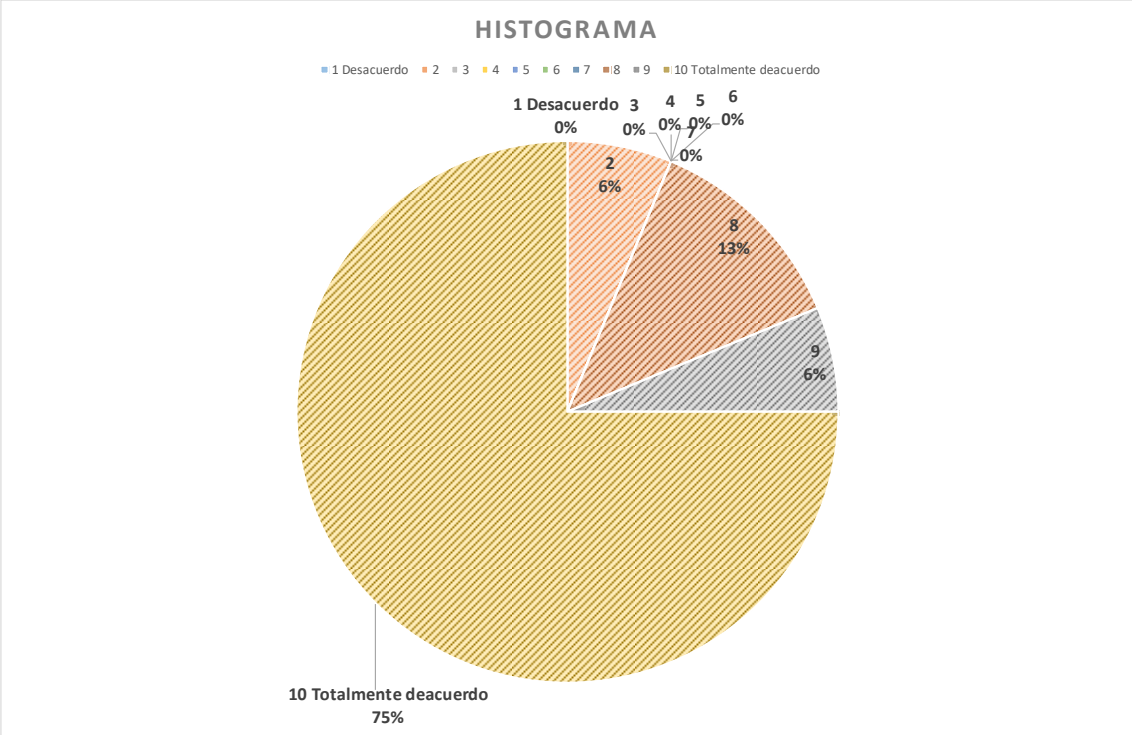

**Tiene la compañía una actitud proactiva ante los problemas de seguridad de la información.**



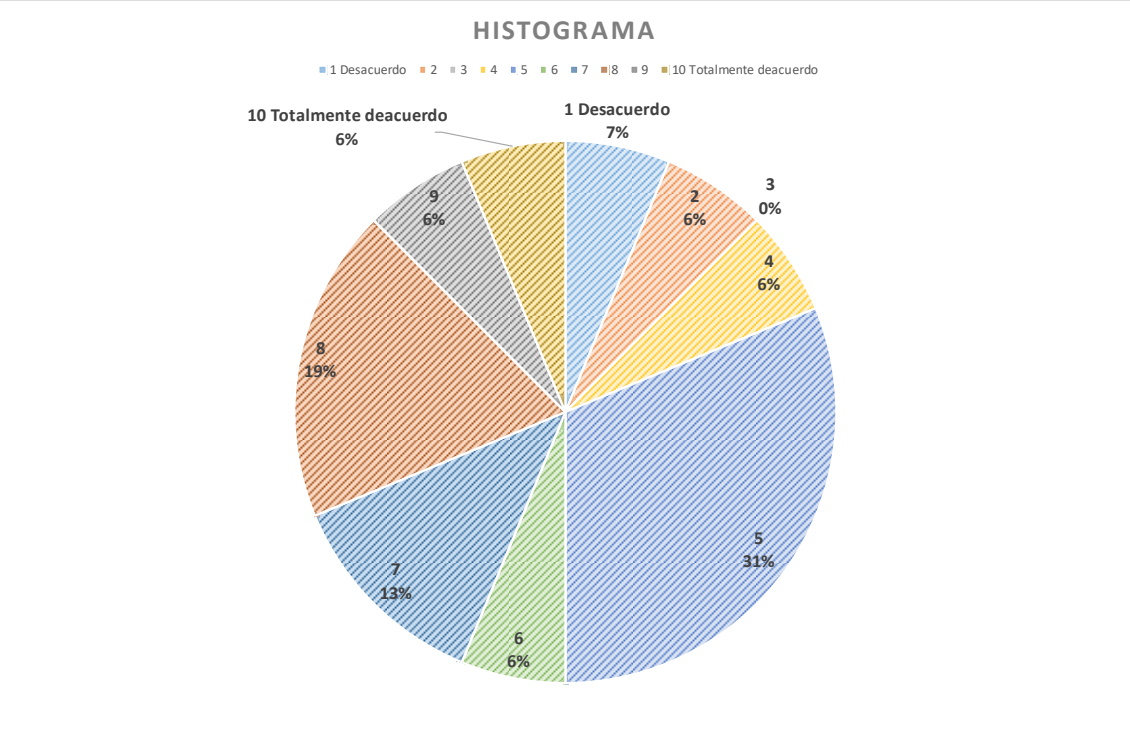

**Se audita inmediatamente ante un incidente el grado de cumplimiento de los protocolos aprobados por la alta dirección.**



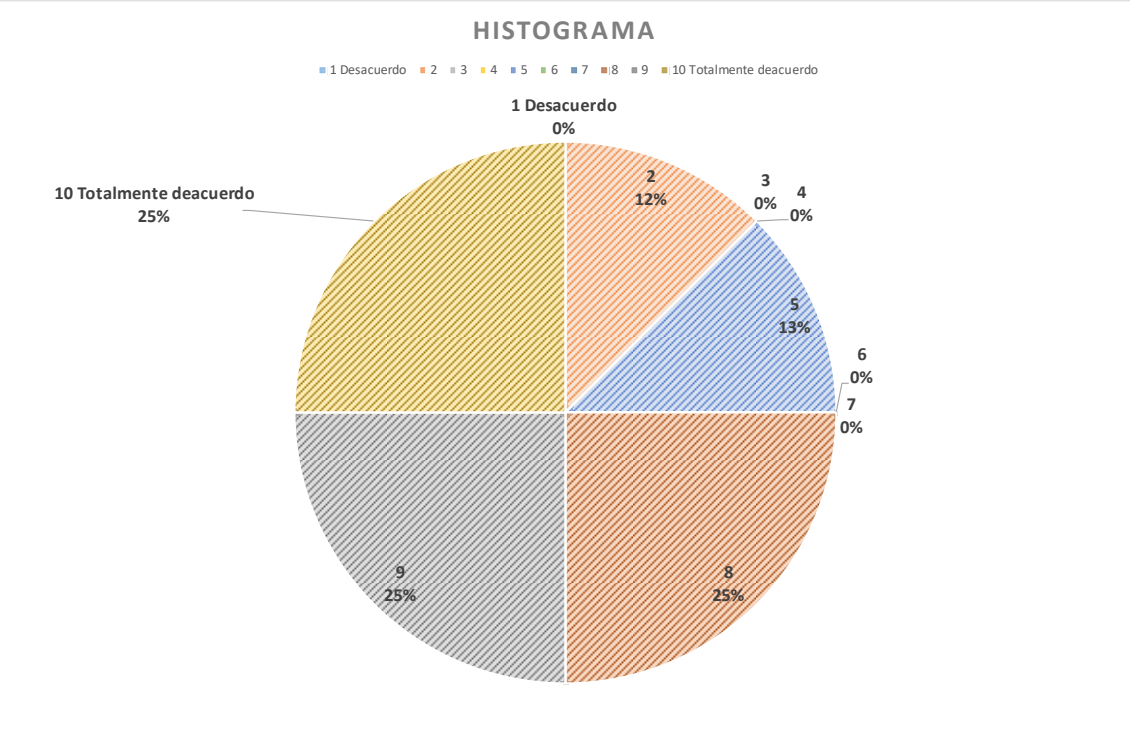

**La contabilidad debe adaptarse al nuevo paradigma digital.**



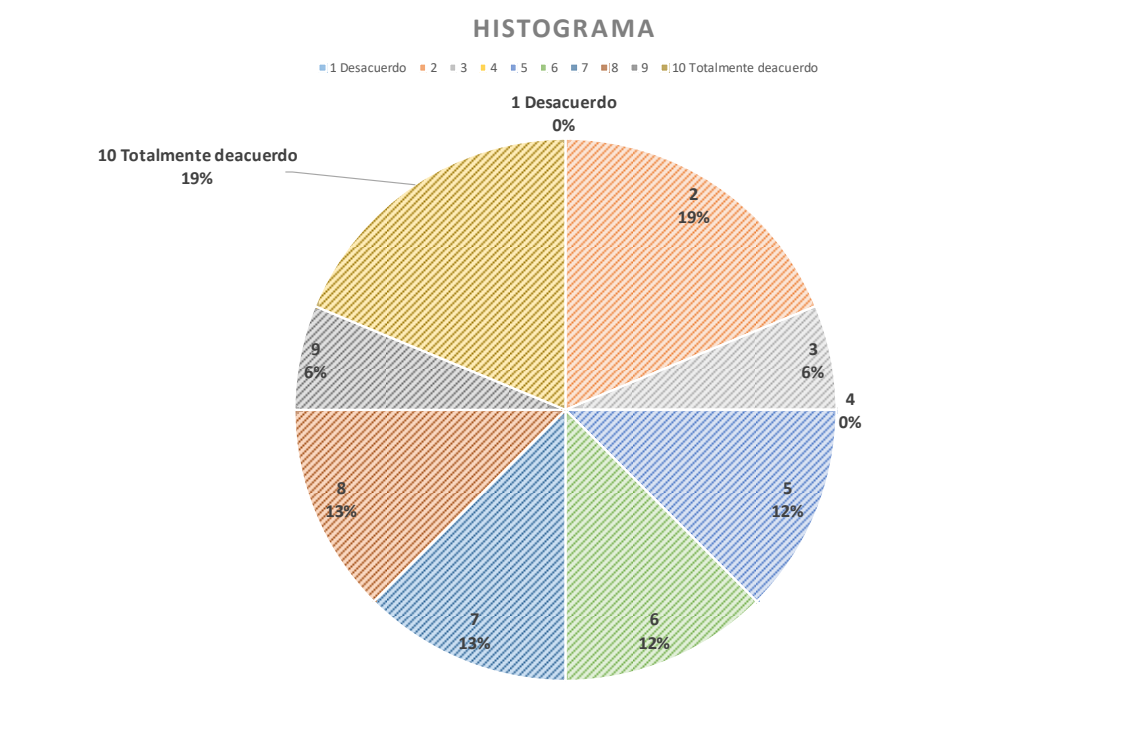
**Se puede confundir la ciberseguridad, desde el punto de vista empresarial, con la ciberseguridad nacional para defender y proteger las infraestructuras críticas.**



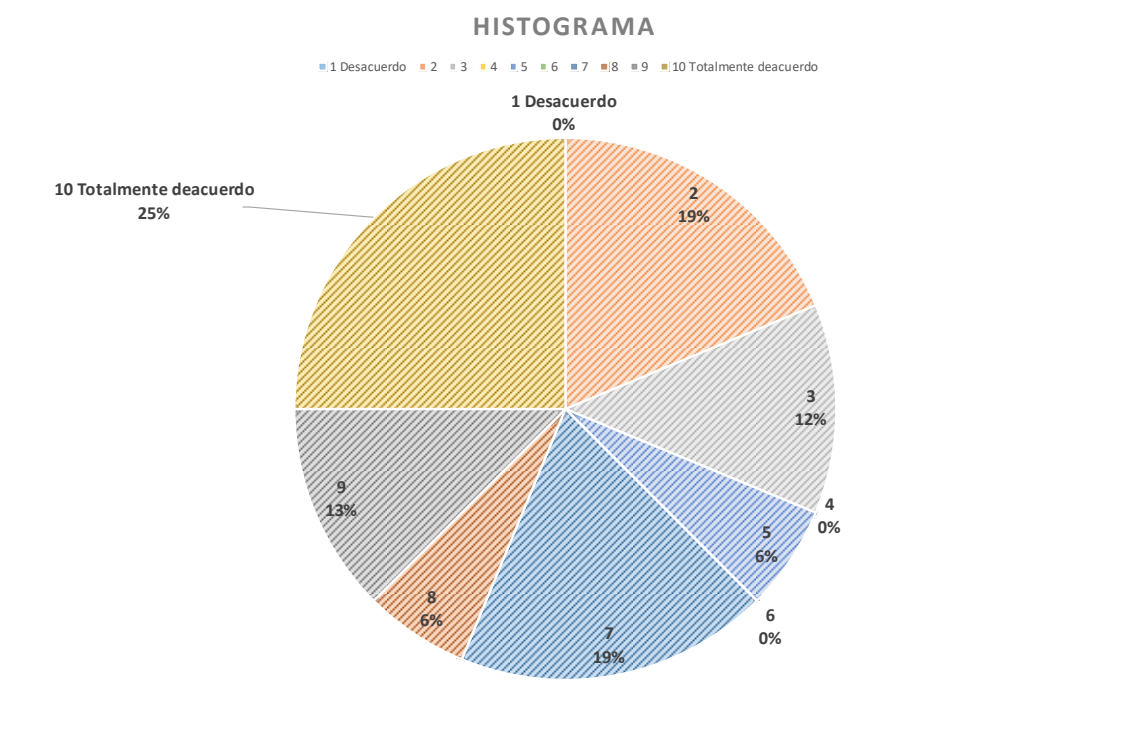

**La ciberseguridad se enmarca en el contexto de lo empresarial, más allá de una exigencia de cumplimiento, como una responsabilidad que implica a los miembros del Consejo de Administración para entender y construir una estrategia corporativa que permita proteger y asegurar la resiliencia de las operaciones y la reputación de la empresa.**



**El negocio está informado sobre el incremento del nivel de exposición de la información de la empresa y sus consecuencias.**




**Tiene obligación la organización de dar información en sus informes anuales de los riesgos y especialmente de los riesgos cibernéticos en aras a mayor nivel de transparencia.**



# CAPÍTULO 7: LA METRICA DE LOS INTANGIBLES. LA INFORMACIÓN CUALITATIVA EN LA VALORACIÓN DE INTANGIBLES. HOJAS DE TRABAJO DE LAS EMPRESAS MÁS INTERNACIONALES DE ESPAÑA, SEGÚN LA BOLSA DE VALORES.

TRABAJO EMPÍRICO.

El trabajo empírico que se realiza está basado en la importancia de los riesgos de seguridad de la información para las empresas y en la importancia de los intangibles desde el punto de vista estratégico (ventajas competitivas-liderazgos-planes estratégicos). Hemos tomado una hoja de trabajo donde se señalan distintos ítems en base al desarrollo de la tesis y relacionados con la encuesta realizada a directivos de empresas, consultores en ciberseguridad y seguridad de la información, asesores, profesores universitarios, auditores de cuenta a nivel nacional e internacional.

Hemos tomado como referencia de nuestro estudio empírico el informe de 2015 "Posición internacional de la empresa cotizada española"[78], donde se pone de relieve la importancia e influencia que tienen las empresas cotizadas en Bolsa sobre el gran impulso económico exterior de la economía española. Este peso se da tanto en términos absolutos como relativos. Un protagonismo que viene de lejos y es creciente, especialmente en los últimos veinticinco años. En base a lo anterior hemos elegido las siguientes empresas para aplicarles los ítems de nuestra hoja de trabajo y así medir mejor la información cualitativa de los activos intangibles: Inditex, AENA, Abertis, Ferrovial, Gas Natural, Telefónica.

La interpretación de los datos y cifras que se recogen en el informe deja pocas dudas de la potencia expansiva que sobre los negocios y el capital tiene la conjunción de un mercado de valores moderno, eficiente y seguro con empresas bien dirigidas y capaces de convertir su cotización en Bolsa en un aliado de sus proyectos de crecimiento. La mejor validación de este hecho es la elevada presencia y liderazgo internacional que un buen número de empresas españolas cotizadas tienen en el escenario económico y social internacional.

La experiencia del grupo Telefónica y BME (Bolsas y Mercados Españoles) pueden servir de paradigma y aval de la importante relación entre empresa y mercado de valores. Telefónica cotiza en Bolsa española desde hace casi noventa años y en la Bolsa de New York un poco más tarde. Desde hace ya tiempo, esta compañía ocupa posiciones de liderazgo internacional en sus respectivos sectores de actividad.

Se puede resaltar de este informe que la internacionalización y tamaño de la empresa son variables que se realimentan y, en este proceso, la cotización de los negocios en los mercados de valores aporta aspectos positivos en casi todos los órdenes de la vida de las empresas sin casi necesidad de incentivos adicionales. No hablamos solo de financiación, donde los datos son casi irrefutables, sino de un orden de funcionamiento mucho más amplio y natural. La

[78] http:bolsasymercados.es

apertura al exterior es, tal vez, una de las variables más significativas y cuantificables del proceso.

Paralelamente, la salida a Bolsa promueve un efecto transformador radical sobre el funcionamiento de las empresas y su ecosistema relacional que, como algunas evidencias empíricas señalan, conducen a un aumento del tamaño, de actividad y empleo que lleva aparejado una mayor proyección internacional. Este recorrido se hace mucho más complejo estando fuera de los mercados.

Es importante subrayar para conectar con lo fundamental de la tesis que cualquier fórmula que abra el espectro de relaciones de la empresa a más potenciales clientes e inversores es positiva para orientar su crecimiento de forma global. El grupo Telefónica a través de su proyecto Open Future, el ecosistema de innovación abierta de Telefónica, dentro del cual se enmarca, entre otras iniciativas, WAYRA[79], la incubadora de Startups de Telefónica, y mercados como el MAB (mercado alternativo bursátil[80]) o MARF (mercado alternativo de renta fija)[81] impulsados y gestionados por BME (Bolsas y Mercados Españoles) para empresas de tamaño pequeño y medio, tienen ya una trayectoria de varios años. Comparten de base el objetivo de acercar el objetivo a las empresas a fondos inversores interesados en participar en negocios en perspectivas interesantes de crecimiento y expansión.

A partir de ahí, el proceso conlleva casi de forma implícita, el aprendizaje y desarrollo de una gestión multifocal con peso relevante de la innovación (seguridad de la información) y el conocimiento, requisitos hoy indispensables para enfrentarse y ganar en un mercado global. En este punto ser o no ser internacional deja de ser una elección porque automáticamente va incorporado al ADN de las empresas comprometidas.

La internacionalización de la economía es un objetivo estratégico. La favorable evolución del sector exterior de la economía española en los últimos años, singularmente de las exportaciones de bienes y servicios, así como de la inversión española en el exterior y de la extranjera en España se ha convertido en una realidad sobre la que asentar las bases de un crecimiento sólido y duradero. Las cifras han sido tan positivas que han situado a nuestra economía en posiciones punteras en cuanto a volúmenes de exportación, inversión extranjera directa recibida y también española emitida al exterior, principalmente en las relaciones con Europa y Latinoamérica. Todo ello queda bien recogido a través de los diferentes contenidos del informe de 2015, impulsado por Telefónica y BME (Bolsas y Mercados Españoles).

En 2014, el 64,07% de la cifra de negocio total de empresas del Ibex 35 tuvo su origen fuera de España. Morgan Stanley Capital International[82] (MSCI) es un proveedor de índices sobre acciones, bonos y hedge Funds. Los índices de MSCI son utilizados como índices de referencia.

A modo de resumen sólo comentamos que las 25 empresas cotizadas españolas que MSCI seleccionó a 31 de marzo de 2015 para sus índices de Bolsas desarrolladas, casi la mitad 12,

[79] Wayra.co>about (somos la aceleredara de startups digitales de Telefónica y ayudamos a los mejores emprendedores a crecer y forma empresas de éxito).
[80] http://www.bolsasymercados.es>mab
[81] www.bmerf.es>Portadas>HomeMARF
[82] https://www.msci.com

ocupan un puesto en el Top 10 de tamaño por capitalización de su sector en el mundo. Dos de ellas eran las primeras (Inditex y AENA), 3 eran segundas (Abertis, Ferrovial y Gas Natural) y otras 2 eran cuartas (ACS y Telefónica). El resto también se posiciona de manera destacada teniendo en cuenta que se trata de una comparativa internacional.

El trabajo empírico lo vamos a desarrollar en base a las anteriores empresas citadas por su internacionalización y por formar parte de un índice de referencia importante como lo es MSCI: Inditex, AENA, Abertis, Ferrovial, Gas Natural, Telefónica.

Comenzaremos estudiando los distintos apartados que se señalan en la hoja de trabajo.

**INFORMACIÓN, TECNOLOGÍA Y CAMBIO ORGANIZACIONAL EN**

**EL NUEVO PARADIGMA DIGITAL.**

**HOJA DE TRABAJO SOBRE MÉTRICA DE LOS INTANGIBLES:**

**LA SEGURIDAD DE LA INFORMACIÓN.**

**INDITEX**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente. Alusión a las ciberamenazas y vulnerabilidades.<br><br>No se alude ni implícita ni explícitamente a este asunto. | En 2015 se presenta un informe integrado (International Integrated Reporting Council IIRC[83]), este informe está basado en los principios del Pacto Mundial de la ONU, los principio e indicaciones del G4 (opción exhaustiva) de Global Reporting Initiative y el Marco Internacional IR y los recogidos en la norma AA1000APS (2008) de Accountability[84].<br><br>El informe anterior está verificado porSGSICS[85]Ibérica, | En 1963[87], D. Amancio Ortega Gaona funda una empresa dedicada a la fabricación de prendas de vestir que crece progresivamente hasta contar con varios centros de fabricación, que distribuyen su producto a distintos países.<br><br>La primera tienda Zara abrió en 1975 en La Coruña, lugar en el que inició su actividad el Grupo y en el que se ubican los servicios centrales de la compañía a día de hoy. Durante los diez años siguientes, la cadena se extiende rápidamente por toda España y en 1985 se crea INDITEX como cabecera del grupo de empresas.<br><br>Tras la expansión por España es cuando las fábricas de la organización dirigen toda su producción hacia la cadena Zara. En los años siguientes se produce |

[83] Integratedreporting.org

[84] http://www.iasplus.com>sustainability, La NormaAA1000APS (2008) fue desarrolladautilizando un enfoque amplio en el que participaron múltiples grupos de interés. Aparecieron por primera vez en la Norma Marco Accountability publicada en 1999. Los principios de AccountAbility para el desarrollo sostenible. www.accountability.org

[85] https://www.iso.org>organization

| | | |
|---|---|---|
| | S.A. y por KPMG asesores[86]. | la salida fuera de las fronteras españolas abriendo tiendas en Oporto (1988), Nueva York (1989) y París (1990). Sus tiendas, ubicadas siempre en emplazamientos privilegiados, están ya presentes en más de 400 ciudades en Europa, América, Asia y África. |
| 2.- % del inmovilizado intangible respecto al total activo (balance consolidado). | 2,282% | |
| 3.- % del importe dedicado a sistema de seguridad de la información respecto al total activo. | 0%, en el ejercicio 2015. | |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad | No se informa. | |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al Sistema de Seguridad de la Información. | No se especifica. | |
| 6.- Visión holística sobre los distintos sistemas de gestión integrados, siendo uno de ellos la contabilidad como sistema de información integrada. | No existe información integrada de los distintos sistemas de gestión integrados, ni siquiera se informa deun sistema de gestión de la seguridad de la información. Sistemas de gestión integrados ISO 9001[88], ISO 14.001[89], ISO 27.001, OHSAS 18.001.[90] | Por tanto, existe una ausencia de visión global de la dirección. |
| 7.- Objetivos de la Comisión de Auditoría Interna en su reglamento, respecto al sistema de gestión de la | No existen estas comisiones en el informe de buen gobierno de la | |

[87] Historia de Inditex: www.inditex>our_history

[86] Home.kpmg.com

[88] La ISO 90001: 2008 es la base del sistema de gestión de la calidad ya que es una norma internacional y se centra en todos los elementos de administración de calidad, para administrar y mejorar la calidad de sus productos y servicios.

[89] La ISO 14001 es la norma internacional de sistemas de gestión medioambiental (SGA), priorizar y gestionarlos riesgos ambientales, como partede sus pr´cticas de negocios habituales.

[90] Establece los requisitos mínimos de las mejores prácticas en gestión de la Seguridad y Salud en el trabajo.

| | | |
|---|---|---|
| seguridad de la información | empresa, por tanto no existe reglamento, ni actas. | |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información. | No existe una comisión de comunicación externa ni interna, tampoco reglamento ni actas a este respecto. | |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento. | No existe esta comisión tampoco una similar con funciones en riesgos de ciberseguridad. | |
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información. | No existen las comisiones y por tanto no existe relación entre ellas. | |
| 11.- Informe de Auditoría externa: observación de salvedades e información de riesgos por seguridad de la información. | No existen salvedades por riesgos de ciberseguridad. | |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información. | No se especifica nada respecto a los estados contables, ni en el resto de los informes a los que se hace alusión. Tampoco se dice nada en el informe de gestión como prolongación de las cuentas anuales. | |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información. | No aparece información en el informe anual sobre presupuestos en materia de ciberseguridad. | |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e | No aparece alusión a la relación con consultores externos ni relaciones institucionales en esta materia. | |

| | | |
|---|---|---|
| internacionales. | | |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información. | No aparece información sobre primas de ciberseguros. | |
| 16.- Mínimos deseables por encima de la ISO 27001. | Tampoco se tiene información voluntaria con referencia a los mínimos deseables por encima de la ISO 27001. | |
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe información a este respecto. | |
| 18.- Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados | No existe información a este respecto. | |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva. | No existe información a este respecto. | |
| 20.- Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional). | No existe información a este respecto. | |

**AENA**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente.<br>Alusión a las ciberamenazas y vulnerabilidades.<br><br>En la carta del presidente no se hace alusión explícita a la seguridad de la información. | Ejercicio2015<br>No presenta informe integrado. | Sobre la historia de Aena[91], primer operador aeroportuario del mundo por número de pasajeros es reconocida como una empresa excelente. |
| 2.- % del inmovilizado intangible respecto al total activo | 0,59% | |

[91] www.aena.es>corporativa>historia_aena

| | | |
|---|---|---|
| El porcentaje es de 0,59%. | | |
| 3.- % del importe dedicado a sistema de seguridad de la información respecto al total activo. | 0% | |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad. | No existe información a este respecto. | No existe información. |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al Sistema de Seguridad de la Información. | No existe información a este respecto. | En el informe de Buen Gobierno, no existen comisiones espécificas de seguridad de la información, tampoco comisión de riesgos donde se ponga de relieve los riesgos por ciberseguridad y riesgos de seguridad de la información. |
| 6.- Visión holística sobre los distintos sistemas de gestión integrados, siendo uno de ellos la contabilidad como sistema de información integrada. | No existe información a este respecto. | |
| 7.- Objetivos de la Comisión de Auditoría Interna en su reglamento, respecto al sistema de gestión de la seguridad de la información. | No existe información a este respecto. | Aparece una comisión de auditoría, pero no de auditoría interna, no se da información sobre el reglamento de auditoría, no parece en el informe de buen gobierno una comisión de seguridad de la información ni de la relación de ésta con una comisión de riesgos |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información. | No existe. | No existe una comisión de comunicación ni reglamento de funcionamiento. |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento | No existe. | No existe Comisión de la seguridad de la información y, por tanto, no existe reglamento de funcionamiento. |
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información | No existe. | No existe información a este respecto. |
| 11.- Informe de Auditorías externa: observación de salvedades e información de | No existe. | En el informe de auditoría no se hace alusión a salvedades relacionadas con ciberamenazas ni vulnerabilidades. |

| | | |
|---|---|---|
| riesgos por seguridad de la información. | | |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información. | No existe. | No se da información ni en la memoria ni en los estados contables formalizados ni en el informe de buen gobierno ni en el informe de responsabilidad social corporativa ni en el informe de reputación sobre las ciberamenazas sufridas, inversiones a este respecto, consecuencias, etc. |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información | No existe. | No se tiene información al respecto. |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e internacionales. | No existe. | No existe información a este respecto, no se detalla consultores en materias de seguridad de la información. |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información. | No existe. | En la cuenta de resultados no aparece movimiento alguno relacionado con las primas de seguros por ciberseguridad ni información de las compañías con las que se contratan |
| 16.- Mínimos deseables por encima de la ISO 27001. | No existe información. | No se tiene informacion a este respecto. |
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe | No existe información relativo a este apartado. |
| 18.- Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados. | No existe. | No existe información relativo a este apartado. |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva. | No existe. | No aparece información sobre cursos de formación, investigación, desarrollo e innovación en materia de seguridad de la información. |
| 20.- Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional). | No existe. | No existe esta información en el informe anual ni de buen gobierno ni de responsabilidad social corporativa ni reputacional. |

**ABERTIS**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente. Alusión a las ciberamenazas y vulnerabilidades.<br><br>En la carta del presidente no se hace alusión específica a seguridad de la información. | Ejercicio 2015 Presenta informe anual integrado. | Historia de Abertis.[92] |
| 2.- % del inmovilizado intangible respecto al total activo. | 62,97%<br>En 2016 el porcentaje es de un 67,028% | Gestión de infraestructuras de telecomunicaciones satélites que surgieron como consecuencia de la toma de control de Hispasat. |
| 3.- % del importe dedicado a sistema de seguridad de la información respecto al total activo. | No existe información específica. | No se detalla. |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad. | No existe. | No existe información a este respecto. |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al Sistema de Seguridad de la Información | No existe. | |
| 6.- Visión holística sobre los distintos sistemas de información integrados, siendo uno de ellos la contabilidad como sistema de información integrada | No existe. | No aparece información. |
| 7.- Objetivos de la Comisión de Auditoría Interna en su reglamento, respecto al sistema de gestión de la seguridad de la información | No existe. | |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información | No existe. | No existe comisión de comunicación. |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento | No existe. | No se tiene información a este respecto. |

[92] Historia de Abertis. http://www.abertis.com>sobre-abertis

| | | |
|---|---|---|
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información | No existe. | No existe información a este respecto. |
| 11.- Informe de Auditorías externa: observación de salvedades e información de riesgos por seguridad de la información | No existe. | No aparece información a este respecto. |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información | No existe. | No aparece, información ni genérica ni detallada en los estados contables formales ni en la memoria. |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información | No existe. | No se hace alusión a este respecto. |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e internacionales | No existe. | No se tiene información de la entidad con consultores externos, nacionales o internacionales, ni con instituciones. |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información | No existe. | |
| 16.- Mínimos deseables por encima de la ISO 27001 | No existe. | No se hace alusión a la ISO 27001 en ningún sitio del informe. |
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe. | No existe relación detallada en las cuentas anuales de los activos de información ni de sus propietarios. |
| 18.- Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados. | No existe. | No aparecen en los estados contables formales ni en la memoria. |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva. | No existe. | No se tiene información a este respecto. |
| 20.- Cambio organizacional ante el nuevo paradigma digital | No existe. | No existe información a este respecto. |

| | | |
|---|---|---|
| (cambio tecnológico, información y cambio organizacional). | | |

**FERROVIAL**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente. Alusión a las ciberamenazas y vulnerabilidades | 2015<br><br>No existe información explícita a este respecto.<br><br>Presenta un informe anual consolidado integrado. | Historia de Ferrovial.[93] |
| 2.- % del inmovilizado intangible respecto al total activo. | 8,34% | |
| 3.- % del importe dedicado a sistema de seguridad de la información respecto al total activo. | 0% | No existe información al respecto ni en la memoria ni en los estados contables formalizados. |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad. | No existe. | No se da información a este respecto. |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al Sistema de Seguridad de la Información | No existe. | No aparece una comisión específica de seguridad de la información. Tampoco se hace alusión a la existencia de un sistema de gestión de la seguridad de la información. |
| 6.- Visión holística sobre los distintos sistemas de gestión integrados, siendo uno de ellos la contabilidad como sistema de información integrada | No existe. | No existe información a este respecto. |
| 7.- Objetivos de la Comisión de Auditoría Interna en su | No existe. | No existe información a este respecto. Existe una comisión de auditoría y control que trata |

[93] Historia de Ferrovial,www.ferrovial.com>compañía>historia

| | | |
|---|---|---|
| reglamento, respecto al sistema de gestión de la seguridad de la información. | | temas genéricos de auditoría, pero no tiene encuenta aspectos del control interno y seguridad de la información. |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información | No existe. | No existe esta comisión en el informe de buen gobierno de la empresa. |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento | No existe. | No existe como tal esta comisión. |
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información | No existe. | No existe esta información en el informe anual integrado de la compañía. |
| 11.- Informe de Auditorías externa: observación de salvedades e información de riesgos por seguridad de la información | No existe. | No aparece información en el informe de auditoría de la compañía de riesgos por ciberamenazas, vulnerabilidades u otras causas. |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información | No existe. | No existe información al respecto. |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información | No existe. | No existe información a este respecto en el informe económico integrado. |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e internacionales | No existe. | No se percibe esta actitud proactiva en el informe anual. |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información | No existe. | No existe información sobre primas y ciberseguros. |
| 16.- Mínimos deseables por encima de la ISO 27001 | No existe. | No existe información a este respecto en la información anual integrada. |

| | | |
|---|---|---|
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe. | No existe información detallada dentro de inmovillizado de la compañía. |
| 18.- Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados. | No existe. | No existe esta información en las información integrada de la compañía. |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva. | No existe. | Existe información sobre el talento y sobre el capital intelectual, pero no referido a la seguridad de la información. |
| 20.- Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional). | No existe. | No se precibe una transformación digital. |

**GAS NATURAL FENOSA**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente.<br>Alusión a las ciberamenazas y vulnerabilidades.<br><br>No se alude explíctamente a este asunto. | 2015<br>No presenta Informe integrado. | Historia de Gas Natural Fenosa.[94] |
| 2.- % del inmovilizado intangible respecto al total activo | 0,83% | No aparece información sobre las inversiones en sistemas de gestión de la ciberseguridad. |
| 3.- % del importe dedicado a sistema de seguridad de la | No existe | No existe información a este respecto |

[94] Historia de la Compañía, www.gasnaturalfenosa.com>la+compania

| | | |
|---|---|---|
| información respecto al total activo. | | |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad. | No existe. | No se tiene información a este respecto. |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al sistema de seguridad de la Información. | No existe. | No existe información sobre los sistemas de gestión de la seguridad de la información. No existe comisión para seguridad de la información ni su relación con la auditoría interna y por tanto su vinculación con el control interno. |
| 6.- Visión holística sobre los distintos sistemas de información integrados, siendo uno de ellos la contabilidad como sistema de información integrada. | No existe. | No existe información sobre los sistemas de gestión integrados y en concreto no se tinene información sobre un sistema de gestión de la información. |
| 7.- Objetivos de la Comisión de Auditoría Interna en su reglamento, respecto al sistema de gestión de la seguridad de la información. | No existe. | Existe una comisión de auditoría interna, Compliance y Control interno. Existe un área de estrategia y desarrollo, pero no existe información sobre seguridad de la información. |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información. | No existe. | No existe en el informe de buen gobierno una comisión de comunicación interna y externa relacionada con todos los stakeholders dela compañía. |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento. | No existe. | No existe esta comisión como tal, tampoco existe una comisión que trata de la seguridad de la información. |
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información. | No existe | No existe información a este respecto en el informe anual. |
| 11.- Informe de Auditorías externa: observación de salvedades e información de riesgos por seguridad de la información | No existe. | No existe información a este respecto en el informe anual. |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad | No existe. | No existe información a este respecto. |

| | | |
|---|---|---|
| social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información. | | |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información. | No existe. | No existe información a este respecto en el informe anual. |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e internacionales | No existe. | No existe información a este respecto en el informe anual a este respecto. |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información. | No existe. | No existe información a este respecto en el informe anual. |
| 16.- Mínimos deseables por encima de la ISO 27001. | No existe. | No existe información a este respecto. |
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe. | No existe información a este respecto en el informe anual. |
| 18.- Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados. | No existe. | No existe información a este respecto en el informe anual. |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva. | No existe. | No existe información a este respecto en el informe anual |
| 20.- Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional). | No existe. | No existe información a este respecto en el informe anual. |

**BANCO DE SANTANDER**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente. Alusión a las ciberamenazas y vulnerabilidades. | 2015 Informe integrado. | En la intervención de la presidenta Ana Botín, se hace referencia, y ya lo hizo en el informe anual de 2014 a la transformación |

| | | |
|---|---|---|
| | | digital. Aunque no se refiere explícitamente a la seguridad de la información. Historia del Banco.[95] |
| 2.- % del inmovilizado intangible respecto al total activo. | 0,17% | |
| 3.- % del importe dedicado a sistema de seguridad de la información respecto al total activo. | No existe. | No aparece información a este respecto. |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad. | No existe. | No existe información a este respecto. |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al Sistema de Seguridad de la Información. | No existe información específica. | |
| 6.- Visión holística sobre los distintos sistemas de Gestión de información integrados, siendo uno de ellos la contabilidad como sistema de información integrada. | No existe. | No existe información a este respecto. |
| 7.- Objetivos de la Comisión de Auditoría Interna en su reglamento, respecto al sistema de gestión de la seguridad de la información | No existe. | No existe información en este sentido. |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información | No existe. | No existe información. |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento | No existe. | No existe esta comisión como tal. |
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de | No existe. | No existe información a este respecto. |

[95] www.santander.com

| | | |
|---|---|---|
| sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información. | | |
| 11.- Informe de Auditorías externa: observación de salvedades e información de riesgos por seguridad de la información. | No existe. | No aparece información a este respecto. |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información. | No existe. | Sólo aparece información en el informe de buen gobierno en la Comisión de Riesgos. |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información. | No existe. | No se tiene información a este respecto. |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e internacionales. | Existe poca información al respecto. | Santander Cyber-Security Program para implementarlo en todos los bancos con fin de establecer tres líneas de defensas, un eje de actuación de ciberresiliencia y un control de accesos y segregación de funciones. El grupo ha evolucionado su modelo interno de referencia de ciberseguridad, inspirado en los estándares internacionales (el framework del NIST National Institute of Standard and Technology. |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información. | No existe información en las cuentas anuales, concretamente en la cuenta de resultados. | Ha contratado un seguro con cobertura global para cubrirse de riesgos de ciberseguridad. En el ejercicio anterior se firmo una póliza con alcance mundial por el aumento de los incidentes relacionados con los ataques informáticos (Zurich Insurance, con dos tipos de cobertura. Unoa nivel local yotro a nivel global). No se tiene información de la prima. El Banco no da información de la cantidad que destina a esta amenaza, pero sí reconoce que tiene una total atención ante los riesgos relacionados con la ciberseguridad. |
| 16.- Mínimos deseables por encima de la ISO 27001. | No existe. | No existe información a este respecto. |
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe. | No aparece información a este respecto. |
| 18.- Aparecen detallados los | No existe. | No aparece información relacionada con los |

| | | |
|---|---|---|
| activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados. | | activos de información ni en el balance de situación ni en la memoria. |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva. | No existe. | No aparece información espeífica sobre aspectos estratégicos relacionasos con el capital humano. |
| 20.- Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional). | No existe. | Aparece información sobre la comisión de riesgos y de auditoria (auditoría interna-control interno) relacionada con la ciberseguridad. |

**TELEFÓNICA**

| CONCEPTOS RELACIONADOS | EJERCICIO ECONÓMICO | NOTAS SOBRE LA COMPOSICIÓN |
|---|---|---|
| 1.- Carta del Presidente. Alusión a las ciberamenazas y vulnerabilidades.<br><br>Informe integrado de 2015.<br><br>En **el informe integrado 2015** Telefónica tiene como objetivo liderar el cambio digital contando con tres olas: la conectividad; la ola de los servicios digitales o conectividad y la ola del Big Data sobre el que están empezando a trabajar. | 2015 Informe integrado | Historia de Telefónica.[96] |
| 2.- % del inmovilizado intangible respecto al total activo. | 33% | 33% en el ejercicio 2015. En el ejercicio 2014 el 39% |
| 3.- % del importe dedicado a sistema de seguridad de la información respecto al total activo. | No existe. | No se especifica. |
| 4.- Percepción sobre la cotización de las acciones en la Bolsa de Valores de las políticas de ciberseguridad. | No existe. | No se especifica. |
| 5.- Información en el Informe de Buen Gobierno de las empresas respecto al Sistema | No existe. | |

[96] https://telefonica.com>about_telefonica

| | | |
|---|---|---|
| de Seguridad de la Información. | | |
| 6.- Visión holística sobre los distintos sistemas de información integrados, siendo uno de ellos la contabilidad como sistema de información integrada. | No existe. | No se tiene información a este respecto. |
| 7.- Objetivos de la Comisión de Auditoría Interna en su reglamento, respecto al sistema de gestión de la seguridad de la información. | No existe. | Información sobre las distintas comisiones, existe una comisión de auditoría y control, otra de innovación y otra de estrategia. Se relacionan con la transformación digital y la seguridad y privacidad. |
| 8.- Objetivos de la Comisión de comunicación en su reglamento. Comunicación interna y externa con adecuación a todos los stakeholders, respecto al sistema de seguridad de la información. | No existe. | No existe como tal. |
| 9.- Objetivos de la Comisión de la Seguridad de la Información en su reglamento. | No existe. | No existe como tal, aunque sí se dedica mucha información a la transformación digital. |
| 10.- Relación documentada entre la Comisión de Auditoría (interna, externa y de sistemas), la Comisión de Comunicación (interna y externa), la Comisión de Seguridad de la Información. | No existe. | No existe información a este respecto. |
| 11.- Informe de Auditoría externa: observación de salvedades e información de riesgos por seguridad de la información. | No existe. | No existe información a este respecto. |
| 12.- La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información. | No existe. | No existe información a este respecto. |
| 13.- Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información. | No existe. | No existe información a este respecto. |
| 14.- Actitud proactiva en relación con la ciberseguridad y seguridad de la información. | Clara actitud proactiva, relaciones | Existe una actitud proactiva. |

| | | |
|---|---|---|
| Relación con consultores externos e instituciones nacionales e internacionales. | institucionales y privadas. | |
| 15.- Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información. | No existe. | No existe información a este respecto. |
| 16.- Mínimos deseables por encima de la ISO 27001. | No existe. | No existe información a este respecto. |
| 17.- Relación detallada de todos los activos de información y sus propietarios. | No existe detallado en sus cuentas anuales. | Sí se da información de los activos más importantes en materia de transformación digital. |
| 18.- Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados. | No existe. | |
| 19.- Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva | Existe información sobre cursos de formación, se informa en las conclusiones y en las notas a pié de página, también en el capítulo 3. | Existe información sobre el capital humano. Se informa en el capitulo 3 y en las conclusiones. |
| 20.- Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional) | Existe información a este respecto, se desarrolla en el apartado de conclusiones y capítulo 3. | Existe información sobre el cambio organizacional, se informa en el capítulo 3 y las conclusiones. |

**BIBLIOGRAFÍA/INFOGRAFÍA:**

http://www.telefonica.es
https://www.bancosantander.es
https://www.inditex.com
www.ferrovial.com
https://www.unionfenosadistribucion.com
https://www.abertis.com
www.aena.es

# CAPÍTULO 8: VALORACIÓN DE TELEFÓNICA CONSIDERANDO LA SEGURIDAD DE LA INFORMACIÓN.

## 8.1.- INTRODUCCIÓN

Desde finales del siglo XX y, sobre todo, a partir del 2000 la estructura de la actividad empresarial y el modelo de negocio han cambiado sustancialmente con respecto a la empresa tradicional. Uno de los cambios más importantes está en que cada vez más en los nuevos sectores de la economía los modelos de negocios se sustentan cada vez más en aspectos innovadores y, por tanto, intangibles. Los activos intangibles se hacen cada vez más importantes y dan a la empresa un mayor potencial de crecimiento y competitividad, de la misma forma también incorporan un mayor nivel de riesgo. El analista debe ver estos riesgos como una fuente de oportunidades y no como algo negativo, por lo que una de las labores fundamentales que debe ejercer el analista y gerente de la empresa es saber identificar y valorar el efecto de estos intangibles, así como gestionar el riesgo que se produce por la mayor participación de estos activos en la actividad de la empresa.

Por otro lado, la evolución y revolución tecnológica de los últimos años ha abierto en los mercados nuevas oportunidades y nuevos riesgos, esta situación se magnifica cuando se produce un desfase bastante importante entre el desarrollo de la tecnología y el conocimiento de la misma. Por tanto, aquellas empresas que consigan que sus responsables sean conocedores de estos avances y estén al día de los últimos acontecimientos, productos y/o servicios relacionados con las nuevas tecnologías conseguirán una mayor ventaja competitiva, tendrán la capacidad de ser las primeras empresas en posicionarse en los nuevos mercados y estarán expuestas a un menor nivel de riesgo en el campo de la seguridad de la información en la red.

En este contexto tecnológico, todos los activos relacionados con la información, almacenamiento de la misma y con los aspectos intangibles de la empresa y mercados tienen cada vez mayor valor, además, debido a la facilidad de movimiento, estos activos pueden dar la vuelta al mundo en un segundo a través de la red y ser almacenados en cualquier punto de la red. Esta facilidad de intercambio, almacenamiento y también de ocultación de los mismos (en una gran parte de las ocasiones son activos estratégicos para la empresa y debido a su alto nivel de confidencialidad son conocidos por pocos responsables de la empresa) hace que su atractivo para ser atacados, robados, etc. sea cada vez mucho mayor y la recompensa que se pueda obtener por conseguirlo sea muy suculenta. Es por este y otros motivos por el que en el 2016 las profesiones relacionadas con la ciberseguridad en la empresa se han convertido en una de las más demandadas y con mayor nivel de crecimiento (Acquisdata. Industry Snapshoot (2017): United States Software and Information Technology. Australia).

De esta manera, en este capítulo vamos a valorar el intangible de una de las empresas que en el mercado español más trabaja en el campo de la ciberseguridad, Telefónica. Así, los activos intangibles de telefónica (bases de datos, patentes, propiedad industrial e intelectual, etc.) son los que tienen más probabilidad de ser atacados en la red. Vamos a valorar estos activos, vamos a ver a qué riesgo se descuentan en Bolsa, cómo gestionar para conseguir el máximo valor y ver los euros que telefónica podría perder si estos activos son atacados.
El valor de los activos intangibles depende del valor del negocio donde dichos activos se gestionan y rentabilizan, el valor de éstos representará una parte del valor de la empresa.

Para valorar telefónica utilizaremos el modelo de flujos descontados y las opciones reales, encuadrados dentro del análisis fundamental, y para valorar los intangibles utilizaremos los múltiplos comparativos.

## 8.2. TELEFÓNICA EN LA BOLSA DE MADRID.

Telefónica cotiza en el mercado español y en mercados internacionales, en este epígrafe analizaremos la cotización de Telefónica en los últimos años en la Bolsa de Madrid y aplicaremos el modelo de mercado para calcular la tasa de rentabilidad que se le puede exigir a Telefónica en función de su situación en el mercado y, concretamente, en el IBEX. Así, esta tasa de rentabilidad servirá como tasa de actualización con la que descontar el riesgo de la renta que generará telefónica en los próximos años.
En primer lugar, analizaremos la evolución de la cotización de telefónica desde 2008 hasta la actualidad.

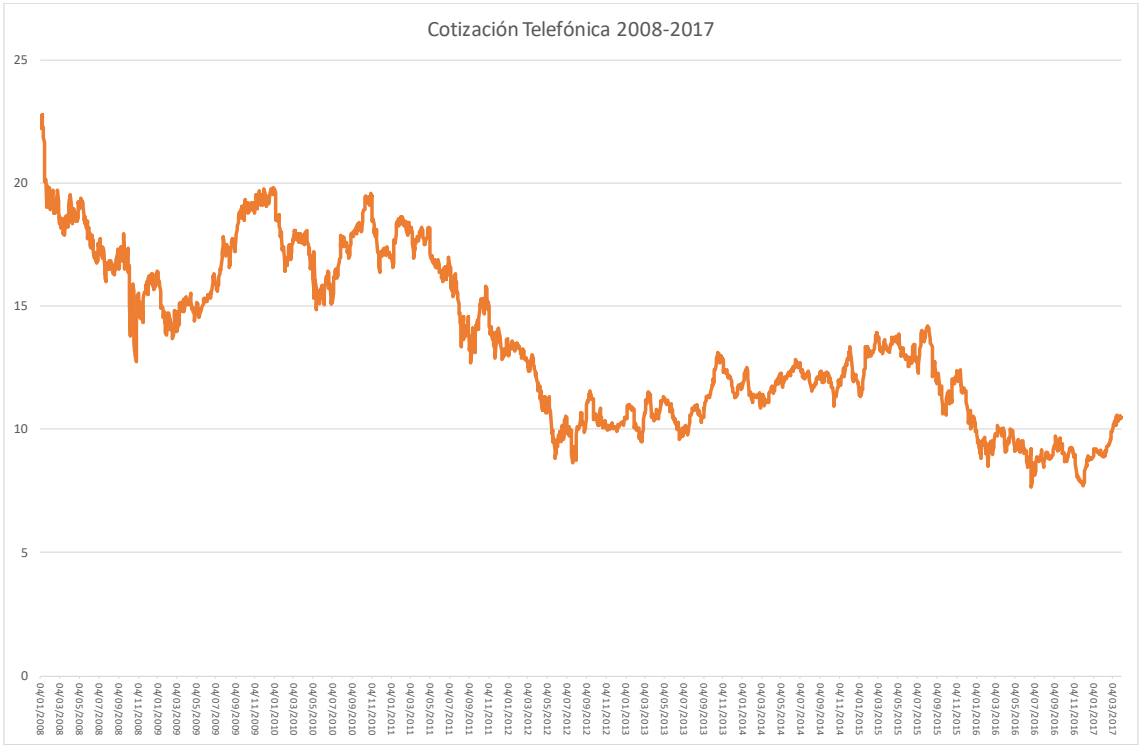



Fig. 1 Cotización Telefónica. Fuente: Jiménez Naharro, F. Sánchez Montañés, C. (2017)

Comprobamos cómo en estos últimos meses telefónica está alcanzando sus valores mínimos (diciembre 2016) de los últimos años.

Si ajustamos estas cotizaciones a una distribución estadística quedaría una figura como la que representamos a continuación.

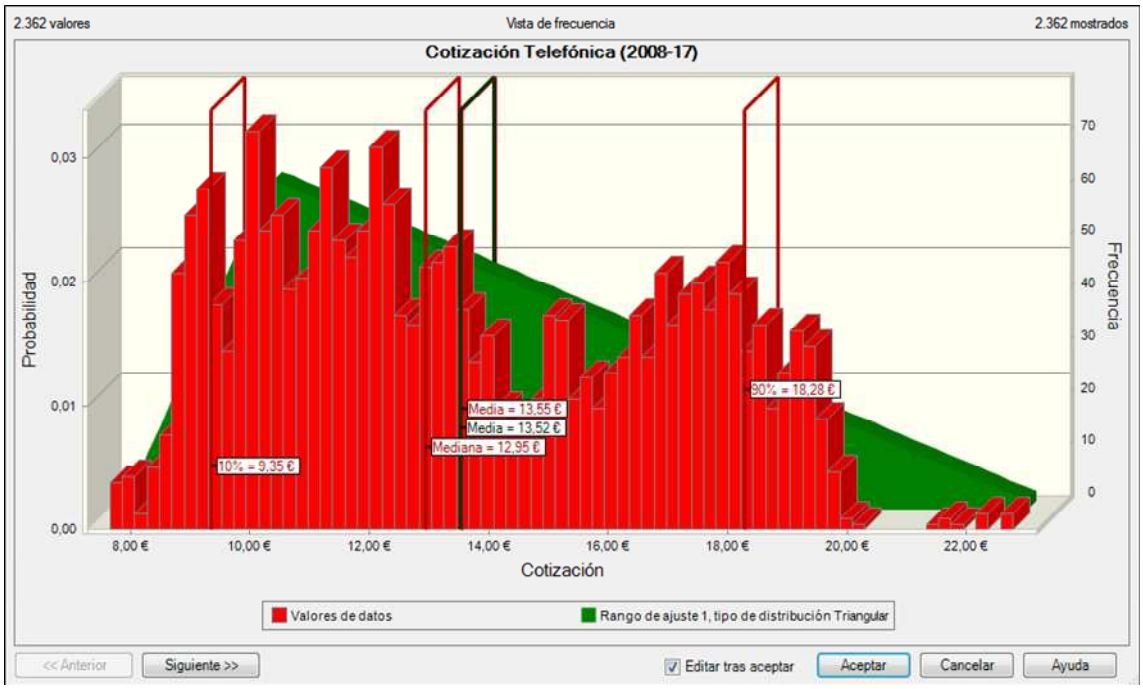



Fig. 2, Cotización Telefónica. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

La distribución estadística es una distribución triangular con un valor medio de 13,55 €/acción y una mediana de 12,95 €/acción, al estar ambos valores muy próximos comprobamos que no hay una dispersión excesiva.

Seguidamente, debemos comprobar la relación entre la rentabilidad anual por sesión de telefónica con respecto a la rentabilidad anual por sesión del Ibex35, esta relación se representa a través del Modelo de Sharpe.

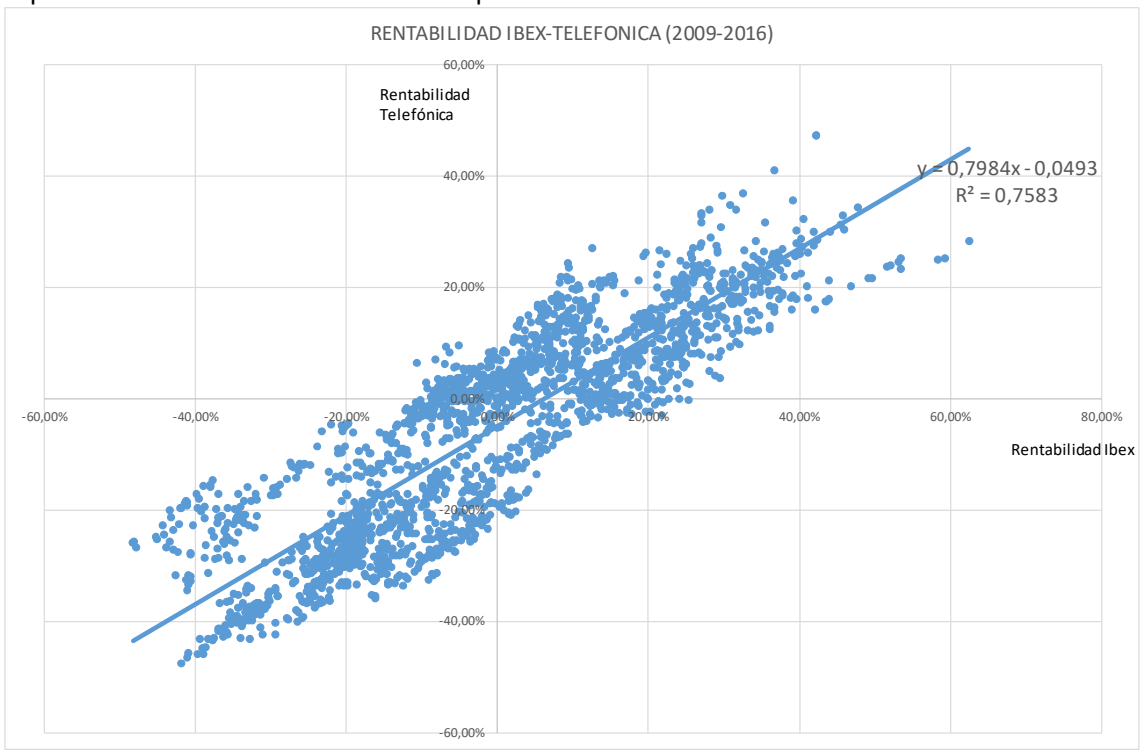



Fig. 3, Rentabilidad IBEX-35.Fuente: Jiménez Naharro, F., Sánchez Montañés,C. (2017)

En este gráfico comprobamos que la relación lineal entre el Ibex 35 y Telefónica se representa por la pendiente de la función que es el coeficiente beta y que alcanza un valor de 0,7984, coeficiente que vamos a aproximar a 0,8.

Por otro lado, comprobamos como la relación entre las variaciones de la rentabilidad del Ibex y Telefónica es de un 75,83%, que vamos a aproximar a un 76% (riesgo sistemático). Esto quiere decir que el 76% de las variaciones de la rentabilidad del Ibex y el 24% restante depende de la propia Telefónica, esto nos servirá más adelante para hacer algunas consideraciones acerca del valor, prima de riesgo y riesgo de telefónica.

Seguidamente, si consideramos que la prima de riesgo del mercado español está en el 5% (Fernández, 2017), la tasa de los bonos del tesoro se sitúa en el 2% y la beta de telefónica es de 0,8, la línea de mercado sitúa a telefónica con una rentabilidad exigida del 6%, rentabilidad que vamos a comenzar a utilizar como tasa de descuento.

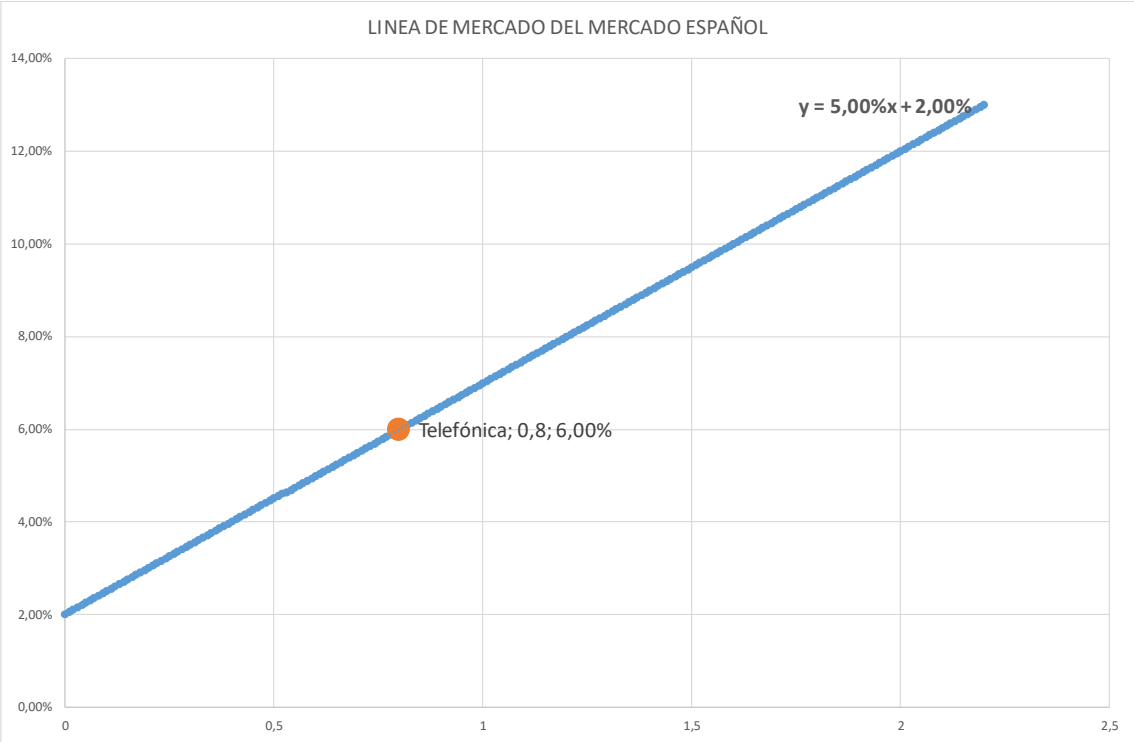



Fig. 4, Línea de mercado. Fuente: Jiménez Naharro, F. Sánchez Montañés, C. (2017)
$K=0.02+0.05*\beta_t$, $K=0.02+0.05*0.8$, $K=6\%$

## 8.3. VALORACIÓN ESTÁTICA DE TELEFÓNICA

Tradicionalmente se ha asociado la idea de valor en la empresa al patrimonio de la misma, valorado mediante los activos y pasivos en balance. De esta forma, se define el **valor estático o análisis estático** como cualquier tipo de modelo que utilice exclusivamente la información derivada de la composición de los activos y pasivos de una empresa.

El principal inconveniente que presenta el enfoque estático, también llamado analítico, es que no tiene en cuenta la posible situación futura de la empresa. Esto supone obviar el principio de la gestión continuada; hecho que no se corresponde con la línea que seguimos, ya que a lo largo de nuestro estudio vamos a considerar que la empresa va a continuar con su actividad. Como consecuencia de lo anterior, comprobamos cómo estas aproximaciones sólo suelen ser

válidas para empresas que pretenden acometer un proceso de liquidación, aunque debido a su facilidad de cálculo se utiliza en muchos informes, sobre todo para delimitar valores mínimos.

Entre los modelos de valor estático los más utilizados son Activo Neto Contable o Patrimonio Neto (valores globales) y valor teórico (valor por acción), que sería el patrimonio neto entre el número de acciones. A continuación, comprobamos la relación existente entre valor teórico y estático.

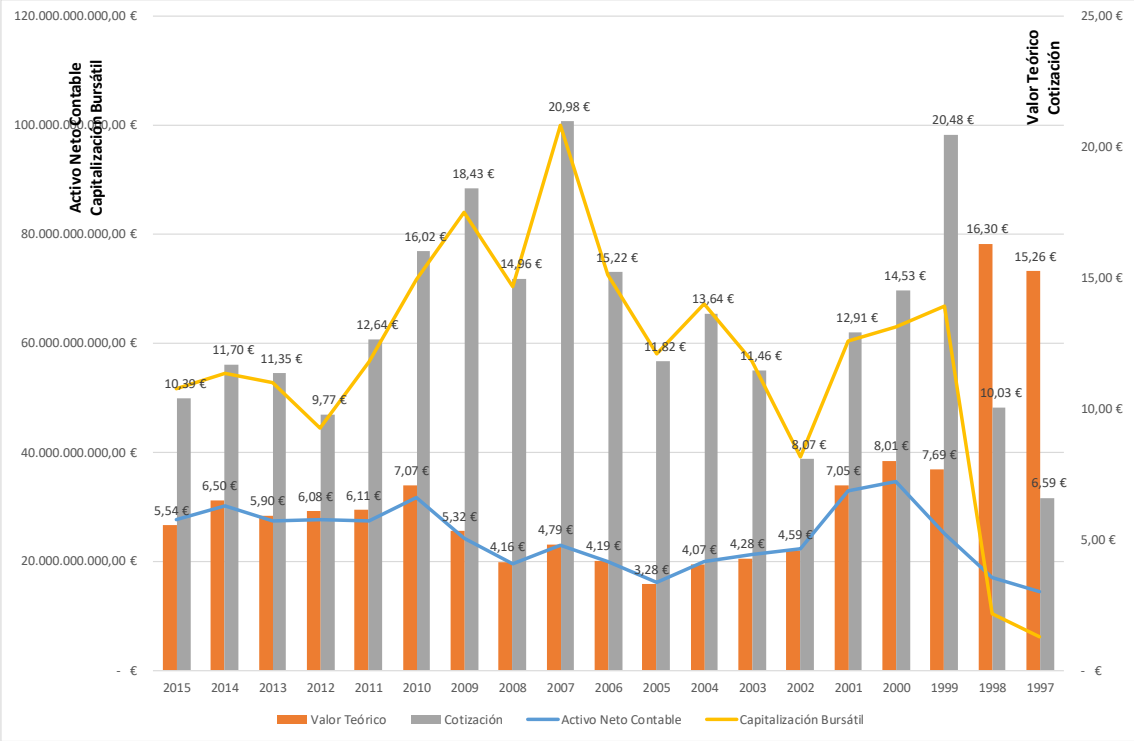


Fig. 5. Valor Teórico. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

Seguidamente, comprobamos como desde 1999 la cotización siempre está muy por encima del valor en libros o valor teórico. Por término medio, la cotización está por encima del valor teórico en un 138,74%.

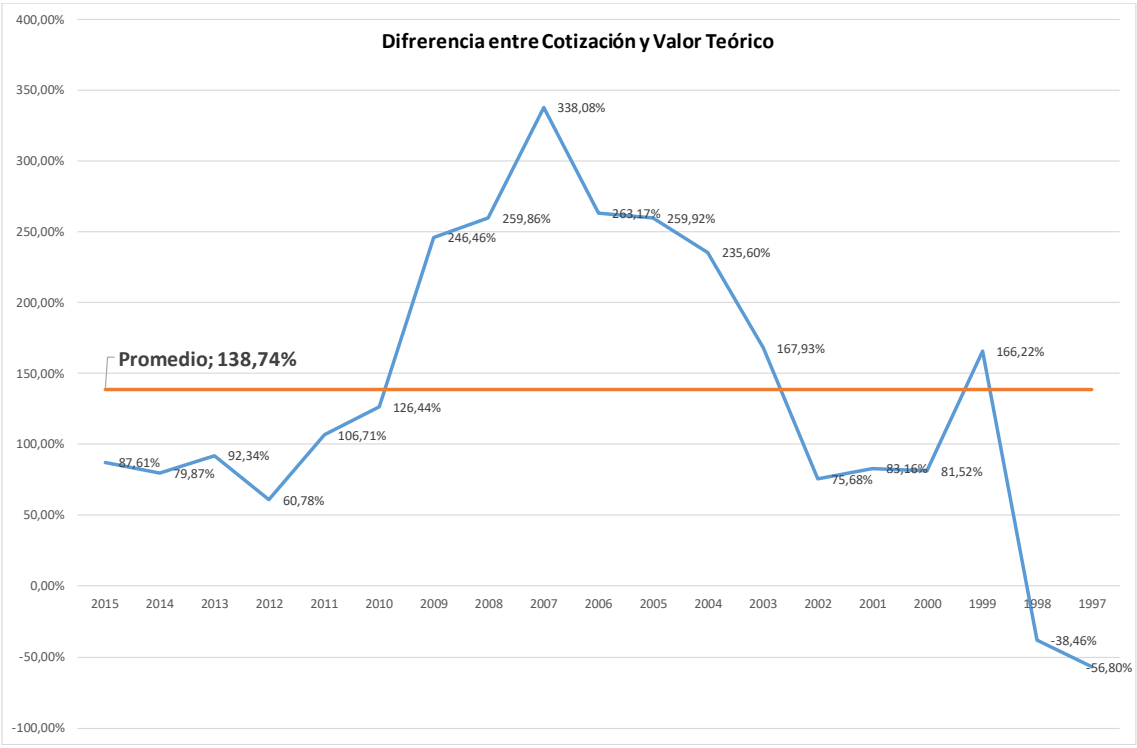



Fig. 6. Diferencia entre Cotización y Valor Teórico. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

## 8.4. ESTRATEGIAS A SEGUIR EN LOS PRÓXIMOS CINCO AÑOS Y PLANIFICACIÓN FINANCIERA

Nuestra propuesta metodológica de valoración requiere proyectar los estados financieros para los próximos ejercicios, una vez que previamente han sido analizados los datos históricos de Telefónica. Para ello, desarrollaremos un proceso de planificación financiera, donde estructuraremos la información disponible en los bloques siguientes:

- *Estrategia de Capital*, relacionada con las decisiones de inversión y financiación.
- *Estrategia Financiera*, basada en la forma de distribuir los recursos generados por la propia compañía. Aquí atenderemos a la política de mantenimiento (amortización activos), crecimiento (reservas) y rentabilidad (dividendos).
- *Estrategia de Circulante*, relacionadas con las políticas de circulantes en relación a activos corrientes y pasivos circulantes corrientes.
- *Mercado*, hace alusión a las previsiones de costes, precios y demanda.

Por ello, primero definiremos las distintas estrategias para pasar a desarrollar el plan financiero y, finalmente, valorar.

### 8.4.1. ESTRATEGIAS A SEGUIR

Antes de proceder a la valoración del negocio de Telefónica y sus intangibles debemos definir el escenario sobre el que vamos a valorar y que va a ser la base para el cálculo del valor de Telefónica y sus Intangibles.

Normalmente, para definir este escenario utilizamos las principales empresas del sector que sean similares en actividad y tamaño. No obstante, al ser Telefónica la empresa referente del sector, vamos a utilizar su histórico para proceder a su valoración.

Así, la estrategia la podemos definir en los siguientes puntos:

- Vamos a suponer que Telefónica va a mantenerse en la situación actual, esto quiere decir que las inversiones futuras que tenga que hacer Telefónica van a estar compensadas exactamente con la financiación necesaria y, por tanto, esta situación no va a afectar al valor.
- La amortización del activo intangible y del inmovilizado material la fijamos en 5 y 15 años, respectivamente.
- La devolución de la deuda antigua se hace por término medio en 15 años a un interés de un 5%.
- Anualmente consigue mantener una póliza de crédito como mínimo de mil millones de euros a un interés de un 5%.
- El objetivo de ventas a conseguir en cinco años va a ser un 20% superior a las ventas actuales, volumen de ventas que está entre las máximas conseguida por Telefónica en 2011 y 2012. A continuación, adjuntamos la distribución de las ventas de Telefónica de los últimos años, una distribución uniforme.

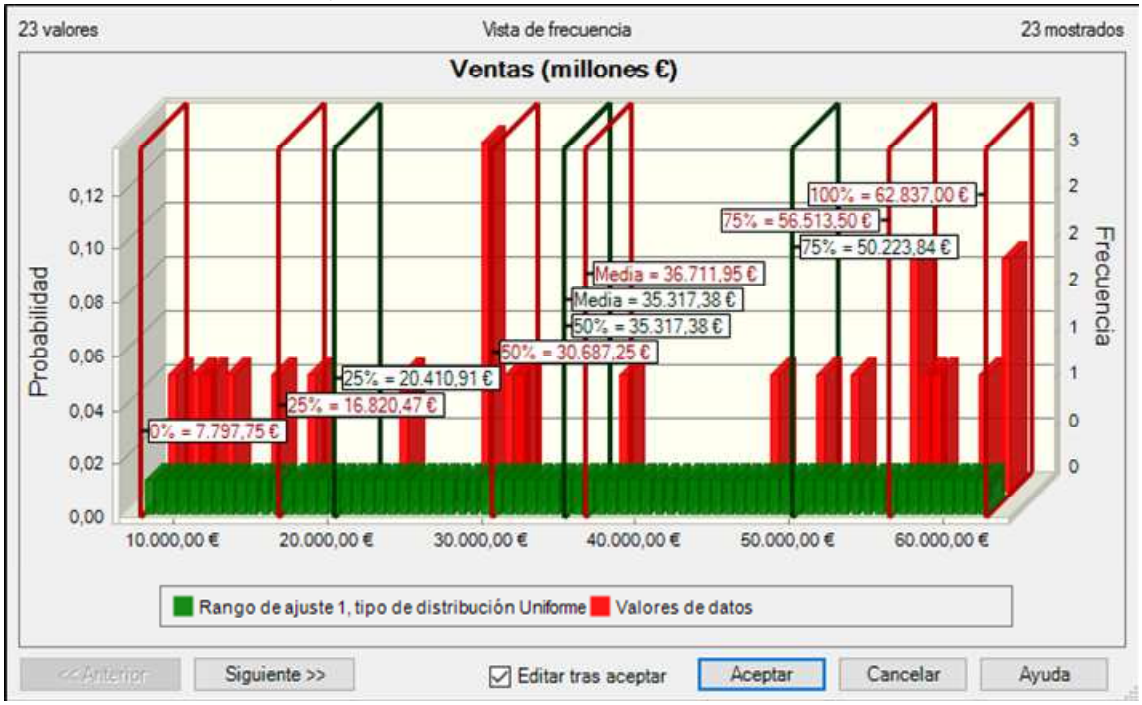



Fig. 7. Ventas Telefónica. Fuente: Jiménez Naharro, F., Sánchez Montañés, C.(2017)

La evolución de las ventas para los próximos cinco años las definimos en el siguiente gráfico.

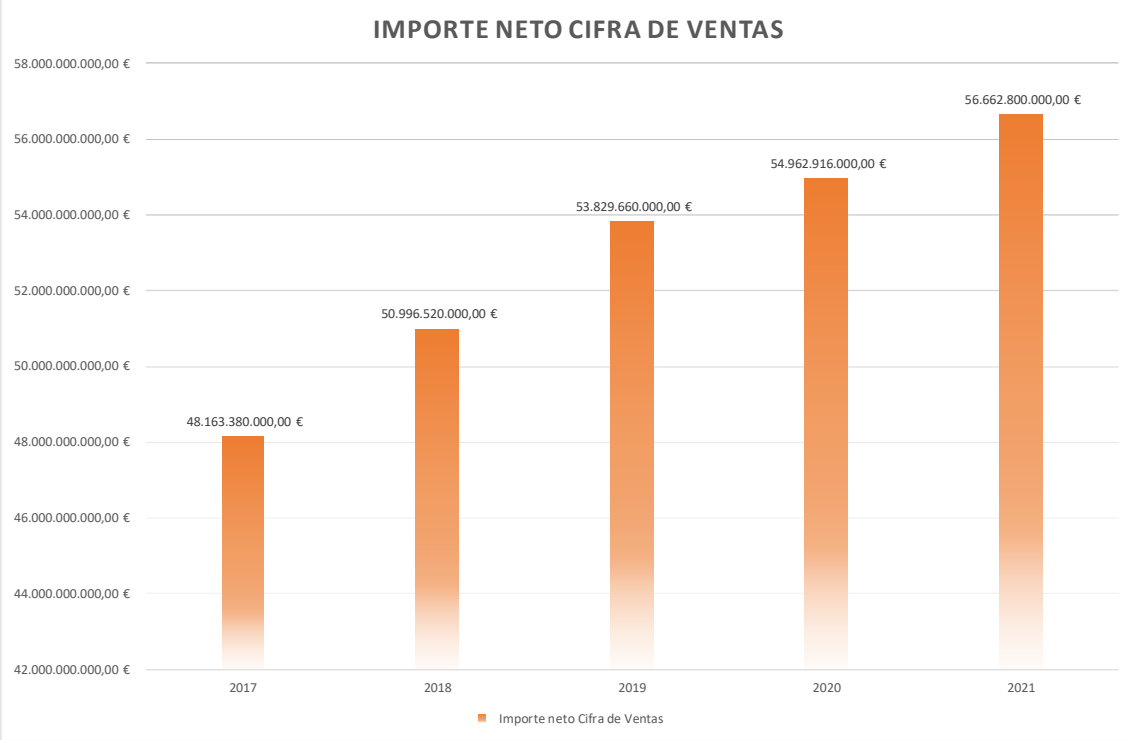



Fig. 8, Importe neto cifra de negocio. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

- A continuación, vamos a fijar los costes de explotación, en primer lugar, la plantilla de trabajadores la mantenemos en la actual con un coste anual por empleado de 77.845 euros con un crecimiento anual de un 3%. El número de empleados asciende a 125.892.
- La relación entre los costes de aprovisionamiento y ventas sigue una distribución de extremo mínimo, consideramos un objetivo razonable un 27,34%.

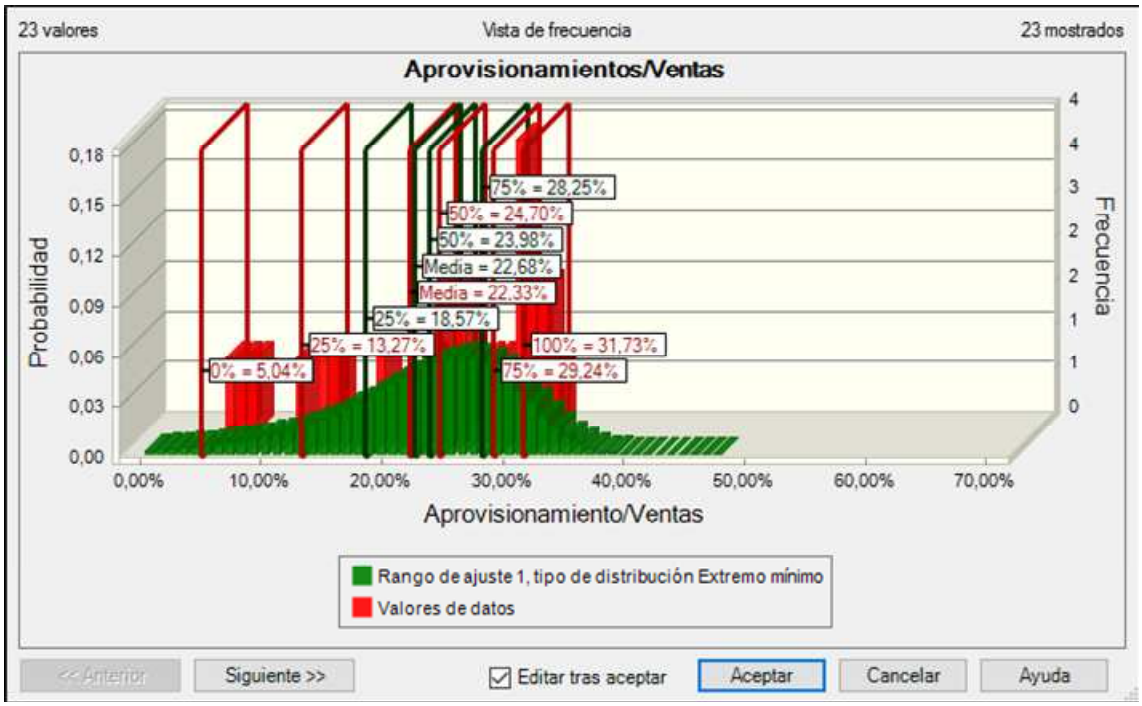



Fig. 9. Aprovisionamiento. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

- La relación entre otros gastos de explotación y ventas también sigue una distribución de extremo mínimo, considerando un objetivo razonable un 31,52%.

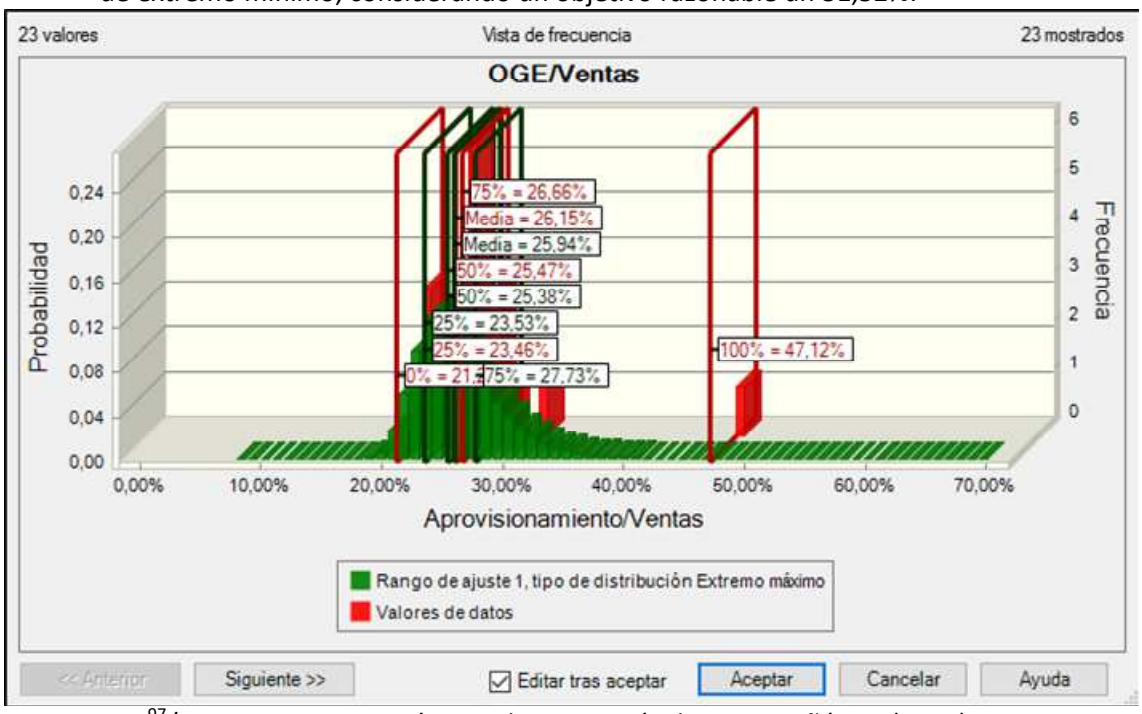



Fig. 10. OGE[97]/Ventas. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

- Vamos a considerar que la política de activación de intangibles se va a mantener en 784 millones de euros anuales.
- La política de circulante la vemos resumida en el siguiente cuadro:

| | **2017** | **2018** | **2019** | **2020** | **2021** |
|---|---|---|---|---|---|
| Política de Cobro | 50 días | 50 días | 50 días | 50 días | 50 días |
| Política de Existencia | 2 días | 2 días | 2 días | 2 días | 2 días |
| Política de Pago | 200 días | 200 días | 200 días | 200 días | 200 días |

## 8.4.2. PLANIFICACIÓN FINANCIERA

El objetivo que perseguimos es valorar y calcular los Flujos de Caja Libre previsionales, cálculo que haremos gracias a la obtención de Cuadros del proceso de planificación financiera (Cuadro de Cash Flow, el Cuadro de Circulante, el Presupuesto de Capital y el Balance previsional), con la información que vimos anteriormente.

En este apartado vamos a determinar los distintos cuadros presupuestarios que nos van a servir para determinar la valoración de la misma. Por ello, comenzamos con el último balance y cuenta de resultado de Telefónica aprobado que va a ser nuestro punto de partida.

[97] Otros gastos de explotación.

| Balance de situación | Telefónica España |
|---|---|
| | |
| **Inmovilizado** | **91.398.000.000,00 €** |
| Inmovilizado inmaterial | 40.307.000.000,00 € |
| Inmovilizado material | 30.549.000.000,00 € |
| Otros activos fijos | 20.542.000.000,00 € |
| | |
| **Activo circulante** | **31.576.000.000,00 €** |
| Existencias | 1.360.000.000,00 € |
| Deudores | 9.152.000.000,00 € |
| Otros activos líquidos | 21.064.000.000,00 € |
| | |
| **Total activo** | **122.974.000.000,00 €** |
| | |
| **Fondos propios** | **27.556.000.000,00 €** |
| Capital suscrito | 4.975.000.000,00 € |
| Otros fondos propios | 22.581.000.000,00 € |
| | |
| **Pasivo fijo** | **60.549.000.000,00 €** |
| Acreedores a L. P. | 47.117.000.000,00 € |
| Otros pasivos fijos | 13.432.000.000,00 € |
| Provisiones | - € |
| | |
| **Pasivo líquido** | **34.869.000.000,00 €** |
| Deudas financieras | 3.284.000.000,00 € |
| Acreedores comerciales | 7.187.000.000,00 € |
| Otros pasivos líquidos | 24.398.000.000,00 € |
| | |
| **Total pasivo y capital propio** | **122.974.000.000,00 €** |

| Cuentas de pérdidas y ganancias | Telefónica España |
|---|---|
| Ingresos de explotación | 48.747.000.000,00 € |
| Importe neto Cifra de Ventas | 47.219.000.000,00 € |
| Otros Ingresos Explot | 744.000.000,00 € |
| TRPPI | 784.000.000,00 € |
| Consumo de mercaderías y de materias | 12.910.000.000,00 € |
| Gasto de Personal | 9.800.000.000,00 € |
| Otros gastos de explotación | 14.882.000.000,00 € |
| **EBITDA** | **10.371.000.000,00 €** |
| CAT | 8.517.000.000,00 € |
| **BAIT** | **2.638.000.000,00 €** |
| Ingresos financieros | 2.085.000.000,00 € |
| Gastos financieros | 4.671.000.000,00 € |
| **Resultado financiero** | **- 2.586.000.000,00 €** |
| **Result. ordinarios antes Impuestos** | **52.000.000,00 €** |
| Impuestos sobre sociedades | - € |
| **Resultado Actividades Ordinarias** | **52.000.000,00 €** |
| Ingresos extraordinarios | |
| Gastos extraordinarios | |
| **Resultados actividades extraordinarias** | **2.582.000.000,00 €** |
| **Resultado del Ejercicio** | **2.634.000.000,00 €** |

Fig. 11 Balance y Cuenta de Resultado. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

Si tenemos en cuenta los objetivos relacionados con el mercado de ventas y costes obtenemos las cuentas de resultados previsionales para los próximos cinco años.

| Cuentas de pérdidas y ganancias | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|
| Ingresos de explotación | | | | | |
| Importe neto Cifra de Ventas | 48.163.380.000,00 € | 50.996.520.000,00 € | 53.829.660.000,00 € | 54.962.916.000,00 € | 56.662.800.000,00 € |
| Otros Ingresos Explot | | | | | |
| TRPPI | 784.000.000,00 € | 784.000.000,00 € | 784.000.000,00 € | 784.000.000,00 € | 784.000.000,00 € |
| Consumo de mercaderías y de materias | 13.168.200.000,00 € | 13.942.800.000,00 € | 14.717.400.000,00 € | 15.027.240.000,00 € | 15.492.000.000,00 € |
| Gasto de Personal | 10.094.000.000,00 € | 10.396.820.000,00 € | 10.708.724.600,00 € | 11.029.986.338,00 € | 11.360.885.928,14 € |
| Otros gastos de explotación | 15.179.640.000,00 € | 16.072.560.000,00 € | 16.965.480.000,00 € | 17.322.648.000,00 € | 17.858.400.000,00 € |
| **EBITDA** | 9.721.540.000,00 € | 10.584.340.000,00 € | 11.438.055.400,00 € | 11.583.041.662,00 € | 11.951.514.071,86 € |
| CAT | 10.254.800.000,00 € | 10.411.600.000,00 € | 10.568.400.000,00 € | 10.725.200.000,00 € | 10.882.000.000,00 € |
| **BAIT** | 250.740.000,00 € | 956.740.000,00 € | 1.653.655.400,00 € | 1.641.841.662,00 € | 1.853.514.071,86 € |
| Ingresos financieros | | | | | |
| Gastos financieros | 2.405.850.000,00 € | 2.248.793.333,33 € | 2.091.736.666,67 € | 1.934.680.000,00 € | 1.777.623.333,33 € |
| **Resultado financiero** | - 2.405.850.000,00 € | - 2.248.793.333,33 € | - 2.091.736.666,67 € | - 1.934.680.000,00 € | - 1.777.623.333,33 € |
| **Result. ordinarios antes Impuestos** | - 2.155.110.000,00 € | - 1.292.053.333,33 € | - 438.081.266,67 € | - 292.838.338,00 € | 75.890.738,53 € |
| Impuestos sobre sociedades | - € | - € | - € | - € | 18.972.684,63 € |
| **Resultado Actividades Ordinarias** | | | | | |
| Ingresos extraordinarios | | | | | |
| Gastos extraordinarios | | | | | |
| **Resultados actividades extraordinarias** | | | | | |
| **Resultado del Ejercicio** | **- 2.155.110.000,00 €** | **- 1.292.053.333,33 €** | **- 438.081.266,67 €** | **- 292.838.338,00 €** | **56.918.053,90 €** |
| **Autofinanciación** | 7.315.690.000,00 € | 8.335.546.666,67 € | 9.346.318.733,33 € | 9.648.361.662,00 € | 10.154.918.053,90 € |

Fig.12. Cuenta de resultado, información histórica. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

La evolución de los costes de explotación la vemos en el siguiente gráfico.

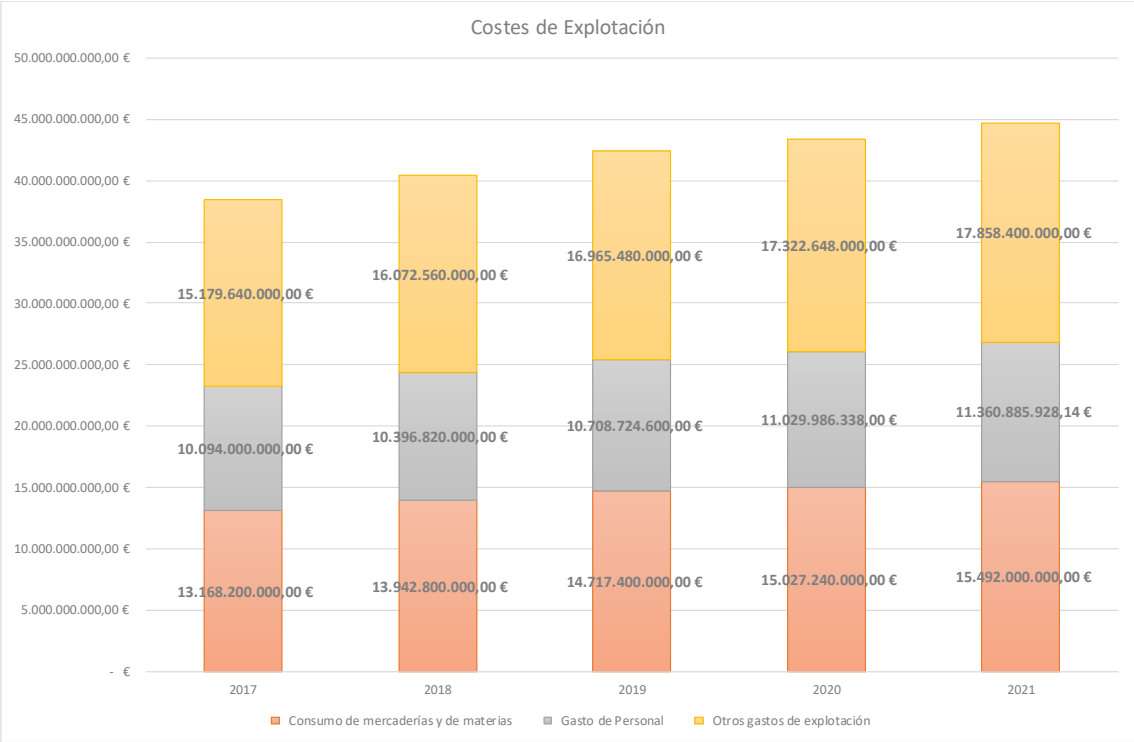


Fig. 13, Costes de Explotación. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

Si observamos la cuenta de resultados previsionales, vemos como la autofinanciación o la renta que genera y se queda en Telefónica está siempre por encima de nueve mil millones de euros anuales.

A continuación, teniendo en cuenta la política de circulante desarrollamos el cuadro de circulante para los próximos cinco años.

| | | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|
| Existencias | 1.360.000.000,00 € | 210.640.219,18 € | 221.436.602,74 € | 232.282.764,93 € | 237.697.941,58 € | 244.993.347,55 € |
| *Variación* | | *- 1.149.359.780,82 €* | *10.796.383,56 €* | *10.846.162,19 €* | *5.415.176,65 €* | *7.295.405,97 €* |
| Deudores | 9.152.000.000,00 € | 6.597.723.287,67 € | 6.985.824.657,53 € | 7.373.926.027,40 € | 7.529.166.575,34 € | 7.762.027.397,26 € |
| *Variación* | | *- 2.554.276.712,33 €* | *388.101.369,86 €* | *388.101.369,86 €* | *155.240.547,95 €* | *232.860.821,92 €* |
| Otros activos líquidos | 21.064.000.000,00 € | 687.923.000,00 € | 687.923.000,00 € | 687.923.000,00 € | 687.923.000,00 € | 687.923.000,00 € |
| *Variación* | | *- 20.376.077.000,00 €* | *- €* | *- €* | *- €* | *- €* |
| **Activo Corriente** | **31.576.000.000,00 €** | **7.496.286.506,85 €** | **7.895.184.260,27 €** | **8.294.131.792,33 €** | **8.454.787.516,92 €** | **8.694.943.744,81 €** |
| **Variación** | **- €** | **- 24.079.713.493,15 €** | **398.897.753,42 €** | **398.947.532,05 €** | **160.655.724,59 €** | **240.156.227,89 €** |
| Deudas financieras | 3.284.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € |
| *Variación* | | *- 2.284.000.000,00 €* | *- €* | *- €* | *- €* | *- €* |
| Acreedores comerciales | 7.187.000.000,00 € | 21.064.021.917,81 € | 22.143.660.273,97 € | 23.228.276.493,15 € | 23.769.794.157,81 € | 24.499.334.755,15 € |
| *Variación* | | *13.877.021.917,81 €* | *1.079.638.356,16 €* | *1.084.616.219,18 €* | *541.517.664,66 €* | *729.540.597,34 €* |
| Otros pasivos líquidos | 24.398.000.000,00 € | - € | - € | - € | - € | 18.972.684,63 € |
| *Variación* | | *- 24.398.000.000,00 €* | *- €* | *- €* | *- €* | 18.972.684,63 € |
| **Pasivo Corriente** | **34.869.000.000,00 €** | **22.064.021.917,81 €** | **23.143.660.273,97 €** | **24.228.276.493,15 €** | **24.769.794.157,81 €** | **25.518.307.439,78 €** |
| ***Variación*** | | ***- 12.804.978.082,19 €*** | ***1.079.638.356,16 €*** | ***1.084.616.219,18 €*** | ***541.517.664,66 €*** | ***748.513.281,97 €*** |
| **CC** | **- 3.293.000.000,00 €** | **- 14.567.735.410,96 €** | **- 15.248.476.013,70 €** | **- 15.934.144.700,82 €** | **- 16.315.006.640,89 €** | **- 16.823.363.694,97 €** |
| **NNCC** | | **- 11.274.735.410,96 €** | **- 680.740.602,74 €** | **- 685.668.687,12 €** | **- 380.861.940,07 €** | **- 508.357.054,08 €** |

Fig. 14. Cuadro de Circulante. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

La política de circulante definida anteriormente supone una disminución progresiva del circulante cada año, esto supone una fuente de financiación adicional para Telefónica.

El siguiente cuadro es el que refleja los orígenes de recursos y necesidades de inversión de forma permanente para Telefónica en los próximos años, esto se refleja en el presupuesto de capital.

| | Previsiones | | | | |
|---|---|---|---|---|---|
| | **2017** | **2018** | **2019** | **2020** | **2021** |
| **NECESIDADES DE FONDOS** | | | | | |
| RECURSOS APLICADOS EN OPERACIONES | | | | | |
| Inversión inmovilizado intangible | - € | - € | - € | - € | - € |
| Inversión inmovilizado material | - € | - € | - € | - € | - € |
| INVERSIÓN INMOVILIZADO | 0,00 € | | | | |
| AUMENTO/DISMINUCIÓN FONDO MANIOBRA | - 11.274.735.410,96 € | - 680.740.602,74 € | - 685.668.687,12 € | - 380.861.940,07 € | - 508.357.054,08 € |
| CAF | 3.141.133.333,33 € | 3.141.133.333,33 € | 3.141.133.333,33 € | 3.141.133.333,33 € | 3.141.133.333,33 € |
| **TOTAL NECESIDADES** | **-8.133.602.077,63 €** | **2.460.392.730,59 €** | **2.455.464.646,21 €** | **2.760.271.393,27 €** | **2.632.776.279,26 €** |
| **ORÍGENES DE FONDOS** | | | | | |
| RECURSOS GENERADOS EN OPERACIONES | 7.315.690.000,00 € | 8.335.546.666,67 € | 9.346.318.733,33 € | 9.648.361.662,00 € | 10.154.918.053,90 € |
| PRÉSTAMOS | - € | | | | |
| CAPITAL SOCIAL | - € | - € | - € | - € | - € |
| PRIMA EMISIÓN | - € | - € | - € | - € | - € |
| **TOTAL ORÍGENES** | **7.315.690.000,00 €** | **8.335.546.666,67 €** | **9.346.318.733,33 €** | **9.648.361.662,00 €** | **10.154.918.053,90 €** |
| **EXCESO - NECESIDADES DE FONDOS** | 15.449.292.077,63 € | 5.875.153.936,07 € | 6.890.854.087,12 € | 6.888.090.268,73 € | 7.522.141.774,64 € |
| **EXCESO - NECESIDADES DE FONDOS ACUM** | 15.449.292.077,63 € | 21.324.446.013,70 € | 28.215.300.100,82 € | 35.103.390.369,55 € | 42.625.532.144,19 € |
| **EFECTIVO Y ACTIVOS LIQUIDOS** | 16.137.215.077,63 € | 22.012.369.013,70 € | 28.903.223.100,82 € | 35.791.313.369,55 € | 43.313.455.144,19 € |

Fig. 15, Necesidades de Fondos y Orígenes de Fondo. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

Para acabar el plan financiero y la información que vamos a utilizar para hacer la valoración presentamos los balances previsionales para los últimos cinco años.

| Balance de situación | ACTUAL | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|
| | | | | | | |
| **Inmovilizado** | **91.398.000.000,00 €** | **81.927.200.000,00 €** | **72.299.600.000,00 €** | **62.515.200.000,00 €** | **52.574.000.000,00 €** | **42.476.000.000,00 €** |
| Inmovilizado inmaterial | 40.307.000.000,00 € | 32.872.800.000,00 € | 25.281.800.000,00 € | 17.534.000.000,00 € | 9.629.400.000,00 € | 1.568.000.000,00 € |
| Inmovilizado material | 30.549.000.000,00 € | 28.512.400.000,00 € | 26.475.800.000,00 € | 24.439.200.000,00 € | 22.402.600.000,00 € | 20.366.000.000,00 € |
| Otros activos fijos | 20.542.000.000,00 € | 20.542.000.000,00 € | 20.542.000.000,00 € | 20.542.000.000,00 € | 20.542.000.000,00 € | 20.542.000.000,00 € |
| | | | | | | |
| **Activo circulante** | **31.576.000.000,00 €** | **22.945.578.584,47 €** | **29.219.630.273,97 €** | **36.509.431.893,15 €** | **43.558.177.886,47 €** | **51.320.475.889,01 €** |
| Existencias | 1.360.000.000,00 € | 210.640.219,18 € | 221.436.602,74 € | 232.282.764,93 € | 237.697.941,58 € | 244.993.347,55 € |
| Deudores | 9.152.000.000,00 € | 6.597.723.287,67 € | 6.985.824.657,53 € | 7.373.926.027,40 € | 7.529.166.575,34 € | 7.762.027.397,26 € |
| Otros activos líquidos | 21.064.000.000,00 € | 16.137.215.077,63 € | 22.012.369.013,70 € | 28.903.223.100,82 € | 35.791.313.369,55 € | 43.313.455.144,19 € |
| | | | | | | |
| **Total activo** | **122.974.000.000,00 €** | **104.872.778.584,48 €** | **101.519.230.273,97 €** | **99.024.631.893,15 €** | **96.132.177.886,47 €** | **93.796.475.889,01 €** |
| | | | | | | |
| **Fondos propios** | **27.556.000.000,00 €** | **25.400.890.000,00 €** | **24.108.836.666,67 €** | **23.670.755.400,00 €** | **23.377.917.062,00 €** | **23.434.835.115,90 €** |
| Capital suscrito | 4.975.000.000,00 € | 4.975.000.000,00 € | 4.975.000.000,00 € | 4.975.000.000,00 € | 4.975.000.000,00 € | 4.975.000.000,00 € |
| Otros fondos propios | 22.581.000.000,00 € | 20.425.890.000,00 € | 19.133.836.666,67 € | 18.695.755.400,00 € | 18.402.917.062,00 € | 18.459.835.115,90 € |
| | | | | | | |
| **Pasivo fijo** | **60.549.000.000,00 €** | **57.407.866.666,67 €** | **54.266.733.333,33 €** | **51.125.600.000,00 €** | **47.984.466.666,67 €** | **44.843.333.333,33 €** |
| Acreedores a L. P. | 47.117.000.000,00 € | 43.975.866.666,67 € | 40.834.733.333,33 € | 37.693.600.000,00 € | 34.552.466.666,67 € | 31.411.333.333,33 € |
| Otros pasivos fijos | 13.432.000.000,00 € | 13.432.000.000,00 € | 13.432.000.000,00 € | 13.432.000.000,00 € | 13.432.000.000,00 € | 13.432.000.000,00 € |
| Deuda Nueva | | - € | - € | - € | - € | - € |
| | | | | | | |
| **Pasivo líquido** | **34.869.000.000,00 €** | **22.064.021.917,81 €** | **23.143.660.273,97 €** | **24.228.276.493,15 €** | **24.769.794.157,81 €** | **25.518.307.439,78 €** |
| Deudas financieras | 3.284.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € | 1.000.000.000,00 € |
| Acreedores comerciales | 7.187.000.000,00 € | 21.064.021.917,81 € | 22.143.660.273,97 € | 23.228.276.493,15 € | 23.769.794.157,81 € | 24.499.334.755,15 € |
| Otros pasivos líquidos | 24.398.000.000,00 € | - € | - € | - € | - € | 18.972.684,63 € |
| | | | | | | |
| **Total pasivo y capital propio** | **122.974.000.000,00 €** | **104.872.778.584,48 €** | **101.519.230.273,97 €** | **99.024.631.893,15 €** | **96.132.177.886,47 €** | **93.796.475.889,01 €** |

Fig.16, Balance de situación. Información histórica. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

Antes de continuar con la valoración, debemos señalar que los modelos de negocio de las empresas de la nueva economía se deben basar en dos pilares fundamentales y con la misma importancia: innovación y mercado.

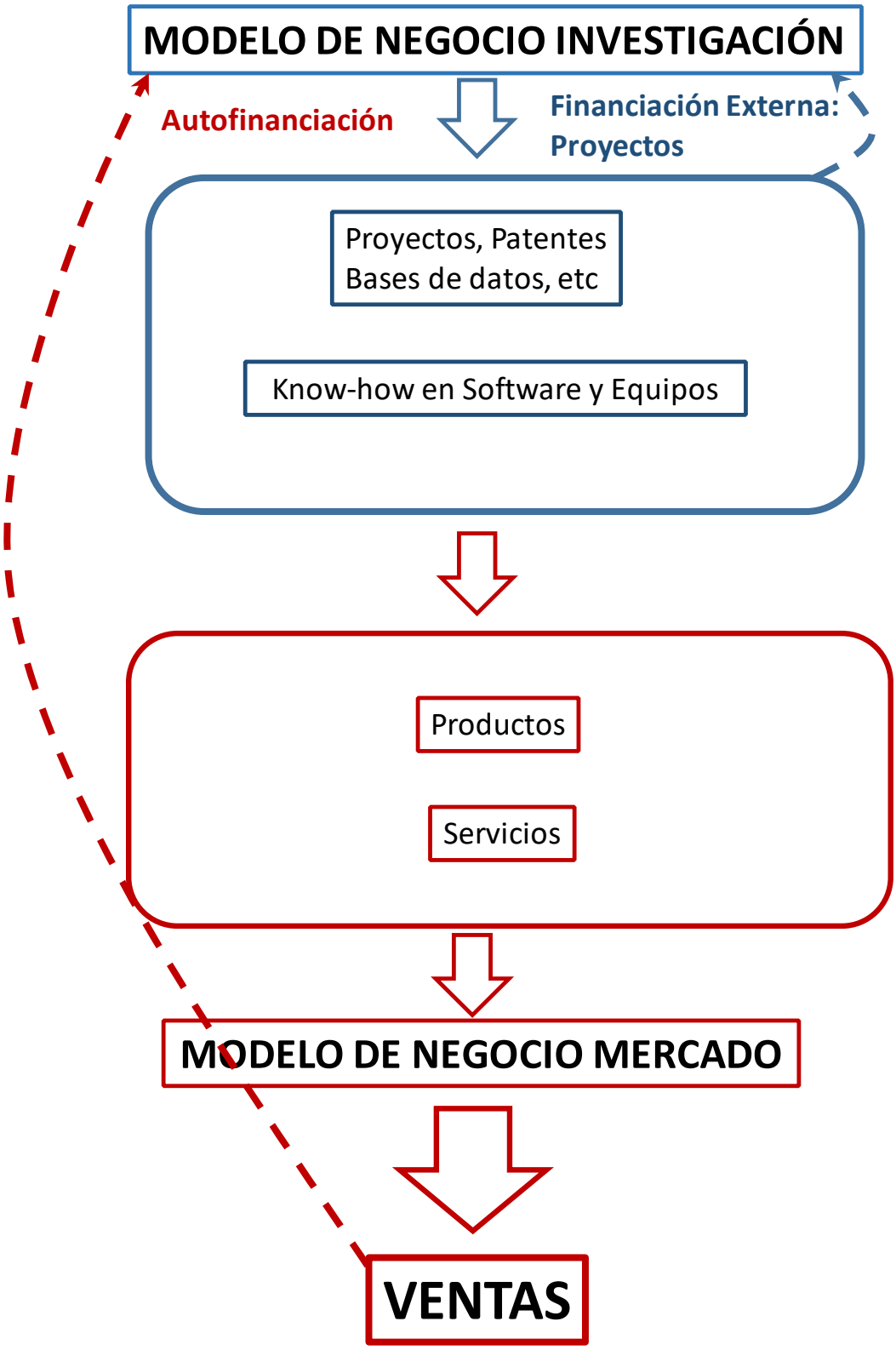
**Modelo de negocio basado en la investigación**: Telefónica es una empresa generadora de investigación. Esta investigación es la materia prima clave para el desarrollo del producto y/o servicio generado por Telefónica. No toda la investigación acabará en el mercado (hay muchos proyectos que se pierden por el camino; sin embargo, aquellos que consiguen posicionarse en el mercado, por muy pocos que sean, genera la renta suficiente para cubrir todas las necesidades creadas). Sin embargo, tanto en el caso de Telefónica como otras empresas del sector parte de sus proyectos y patentes acaban con el desarrollo de productos y/o servicios que actualmente son los que comercializan y los que constituyen el valor de su negocio. Por otro lado, hay proyectos y patentes que, aunque ahora no están dando resultados, en un futuro no muy lejano, pueden constituirse en una fuente potencial muy importante de recursos, entre éstos están los relacionados con la seguridad de la información como puede ser la cadena de bloques.[98]

El modelo basado en investigación se consigue gracias a un equipo con un nivel de investigación y profesionalidad bastante alto, dirigido por investigadores y profesionales de reconocido prestigio, a la financiación externa (financiación pública y privada) conseguida.

**Modelo de Negocio basado en el mercado**. Una vez que Telefónica ha desarrollado su labor investigadora, Telefónica cuenta con un equipo de profesionales que han conseguido concienciar a sus investigadores de la importancia del mercado para Telefónica, consiguiendo

[98] Blockchain es la espina dorsal del protocolo Bitcoin y una tecnología que ha cambiado todo para siempre. Base dedatos distribuida, formada por cadenas debloques diseñadas para evitar su modificación una vez que un dato ha sido publicado usando un sellado de tiempo confiable y enlazando a un bloque anterior. Es especialmente adecuada para almacenar de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión. Se aplicó por primera vez en 2009 como parte de Bitcoin.

acercar la investigación al mercado y buscando nuevos nichos que le permiten acceder a mercados que hace unos años eran impensables. Esto se consigue gracias a gestores con capacidad de motivación y dirección y en algunas ocasiones, como lo exige el sector en el que está enmarcado, con un nivel de riesgo controlado, ya que sin esta actitud se hubiesen perdidos muchas oportunidades.




**OBJETIVO: AUTOFINANCIACIÓN FINANCIE INVESTIGACIÓN PROYECTOS SEAN UN SUPLEMENTO Y NO CONDICIONE LA ACTIVIDAD**

## 8.5.- VALORACIÓN DE TELEFONICA MEDIANTE DESCUENTO DE FLUJOS Y OPCIONES REALES.

Siguiendo a Ruíz Martínez. R.J. y Jiménez Naharro, F. (1999), las técnicas clásicas de valoración, desarrolladas dentro del marco del Análisis Fundamental, adolecen de una serie de lagunas o limitaciones que, en muchas ocasiones, no son advertidas por los profesionales en su complicada tarea de valorar empresas. En trabajos anteriores, mi Director advertía qué había quedado de válido y qué métodos clásicos, por sus limitaciones, resultaban insuficientes para aplicarlos, en determinadas situaciones, a ciertos títulos.

Antes de continuar, debemos advertir que este apartado lo hemos circunscrito al área desarrollada por el análisis dinámico y, más concretamente, por el Análisis Fundamental. Al valorar un título debemos tener presente dos premisas fundamentales:

- La empresa se debe valorar en función de sus expectativas futuras, principalmente. Estas se miden a través de la renta generada en un futuro más o menos previsible.
- El inversor o accionista debe prever la liquidez que potencialmente puede recibir de su inversión, en un horizonte de valoración más o menos prolongado, como nos recuerda el principio fundamental de valoración.

Así, por todo lo estudiado hasta ahora, nos decantaremos por el análisis dinámico, y dentro de éste se convierte en un punto de inflexión, marcando un antes y un después, en la teoría de la valoración, el enfoque del Discounted Cash-flow o Flujos de Caja Descontados.

Este se erige como un modelo de análisis dinámico por excelencia, y más concretamente de Análisis Fundamental. Dicho enfoque completa gran parte de las lagunas sufridas por las principales técnicas clásicas de valoración:

- Las expectativas de los títulos deben quedar penalizadas por un cierto coste de oportunidad, coste que no está claramente presente en los modelos anteriores.
- Los distintos modelos no asumen con claridad el concepto de riesgo y, sobre todo, los distintos niveles del mismo y su cuantificación.
- Sobre todo, se utiliza una "liquidez previsional" y no la que realmente interesa, es decir, la liquidez potencial.

De esta manera, con nuestro trabajo describimos una técnica que desarrolla la problemática del valor de forma real y operativa para el inversor, dando las directrices oportunas para salvar estas limitaciones. De tal forma que éste sepa cuándo, ante qué situaciones y sobre qué títulos puede aplicar dicha metodología y, en caso contrario, aportar algunas alternativas.

La consecución del objetivo anteriormente citado lo fundamentaremos en la estructura del propio modelo, analizando con detenimiento el comportamiento de cada una de sus variables. Así, el valor de la sociedad determinado por la utilización de los flujos de caja descontados, se define a través de la siguiente función:

$$V = \sum_{t=1}^{n} \frac{FCD_t}{(1+K)^t} + \frac{VC_n}{(1+K)^n}$$

V = Valor de la empresa.
FCDt = Flujos de caja descontados para el período t.
VCn = Valor de continuidad en el momento n.
K = Tasa de actualización.
N = Horizonte previsional de valoración.

## 8.5.1. FLUJO DE CAJA LIBRE DESDE EL PUNTO DE VISTA DEL ACCIONISTA O EQUITY FREE CASHFLOW (EFCF)

Se entiende por cash flow libre desde el punto de vista del accionista al conjunto de fondos generados por la empresa y susceptibles de ser extraídos de la misma sin alterar su estructura óptima de capitales. O sea, el conjunto de recursos generados y disponibles directamente por parte del empresario y que potencialmente, con el paso del tiempo, pueden llegar a manos de los accionistas. Con tal propósito, la renta generada por la empresa la debemos minorar en función de sus necesidades de inversión y aumentar por su capacidad de endeudamiento.
La ***necesidad de inversión*** procede tanto del ***activo fijo (activo no corriente)*** como del ***circulante (corriente),*** debiendo estar financiada con recursos a largo plazo, recursos ajenos y propios. De esta forma, para llegar a la liquidez que puede ser utilizada directamente por el empresario, y potencialmente por el accionista, debemos añadir la parte que va a ser financiada por recursos ajenos - ***capacidad de endeudamiento***. La capacidad de endeudamiento se define como el conjunto de fondos, en términos netos (financiación nueva – devolución de la deuda), que obtiene la empresa procedente de la deuda. Una capacidad de deuda positiva significa que las renovaciones son superiores a las devoluciones de la deuda. La autofinanciación es el sumatorio de reservas, amortizaciones y provisiones.
En función de lo visto anteriormente, el cálculo del cash flow libre se sintetiza en el siguiente cuadro:

| | | |
|---|---|---|
| **+** Beneficio Neto | | **+** Autofinanciación |
| **+** Amortizaciones | **ó** | **+** Dividendos |
| ***CASH FLOW*** | | |
| **-** Inversiones Activo no Corriente | | |
| **-** Inversiones Capital Corriente (NOF o NNCC) | | |
| **+** Capacidad de endeudamiento | | |
| ***CASH FLOW LIBRE ACCIONISTA*** | | |

Fig. 17, Estimación del CFL para el accionista. Fuente: Jiménez Naharro, F., Sánchez Montañés C. (2017)

Comprobamos cómo el cash flow o renta generada por la empresa, no representa la liquidez disponible que puede ser utilizada directamente por el empresario o potencialmente por el accionista. Para llegar al cálculo del CFL o liquidez potencial, debemos deducir las necesidades de inversión y sumar la capacidad de endeudamiento.
Al analizar el proceso de cálculo anterior, se observa que la correcta aplicación de este método exige que la empresa posea o pueda desarrollar un proceso de planificación financiera donde defina y cuantifique cómo quiere implantar las estrategias y políticas previamente elaboradas. En definitiva, debe contar con una serie de cuadros presupuestarios, siguiendo a Ruíz Martinez, R.J. (1990):
Cuadro de Cash Flow.
Cuadro de Circulante.
Presupuesto de Capital.
Presupuesto de Tesorería.
Balances Previsionales. Los dos últimos balances y cuentas de resultados se obtienen mediante el desarrollo de los anteriores cuadros presupuestarios

De esta manera, utilizando el cuadro de cash flow, de circulante y presupuesto de capital, desarrollados en el proceso de planificación financiera, podemos conseguir el Cash Flow Libre o liquidez potencial.

## 8.5.2. VALOR DE CONTINUDAD

La principal fuente de información sobre la que se desarrolla el método de los flujos descontados, el proceso de planificación financiera, divide el horizonte de valoración en dos partes bien diferenciadas: horizonte previsible y horizonte no previsible. El horizonte previsible (desde "0" a "n") se construye sobre la información facilitada por los cuadros presupuestarios del proceso de planificación financiera. Esta parte del proceso de valoración ha sido analizada en los epígrafes anteriores, sobre todo a través de la definición del cash flow libre. Por otro lado, el horizonte no previsible (a partir de "n", en nuestro caso a partir de 2021) se caracteriza por la falta de información disponible en él. Dicho período comienza el año siguiente al que finaliza el proceso de planificación financiera o el horizonte previsible.

El valor que toma la empresa en ese horizonte se conoce con el nombre de valor de continuidad. La estimación de esta variable adolece de algunos inconvenientes, debido a la falta de información, fundamentalmente. Nosotros vamos a proponer que el cashflow libre a partir de 2021 se mantenga anualmente como el promedio de los cashflows libres entre 2017 y 2021.

Así, teniendo en cuenta lo analizado en los apartados anteriores y la información vertida en el plan financiero el cuadro con los distintos cashflow libre lo podemos ver en la siguiente figura.

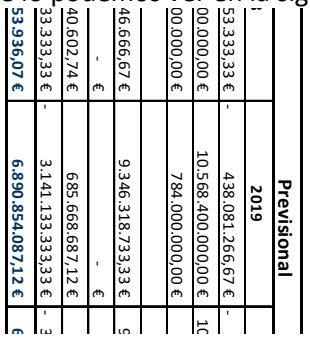



Fig. 18, 19, Horizonte previsional. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

## 8.5.3. VALORACIÓN

Por otro lado, si utilizamos como tasa de descuento el 6%, la calculada en el punto 2, el cuadro de valoración quedará como el que sigue.

| | Previsional | | |
|---|---|---|---|
| | 2018 | 2019 | 2020 |
| | - € | - € | - € |
| | 1.292.053.333,33 € | 438.081.266,67 € | 292.838.338,00 € |
| | 10.411.600.000,00 € | 10.568.400.000,00 € | 10.725.200.000,00 € |
| | 784.000.000,00 € | 784.000.000,00 € | 784.000.000,00 € |
| | 8.335.546.666,67 € | 9.346.318.733,33 € | 9.648.361.662,00 € |
| | - € | - € | - € |
| | 680.740.602,74 € | 685.668.687,12 € | 380.861.940,07 € |
| | - 3.141.133.333,33 € | - 3.141.133.333,33 € | - 3.141.133.333,33 € |
| | 5.875.153.936,07 € | 6.890.854.087,12 € | 6.888.090.268,73 € |
| | 0,89 | 0,84 | 0,79 |
| | 5.228.866.087,64 € | 5.785.693.968,11 € | 5.456.012.653,67 € |

De esta manera, comprobamos como el valor de telefónica según el descuento de flujos y el escenario definido asciende a 142 mil millones de euros o 29 euros la acción, 18 euros por encima de casi los 11 euros actuales que se pagan en Bolsa.

Para que nuestro método alcance los 11 euros de la Bolsa, tendríamos que descontar los flujos futuros a una tasa de un 16%, lo que supone aplicar una prima de riesgo de un 166% sobre la tasa del 6% utilizada por nosotros.

Esta prima de riesgo se puede estimar si utilizamos esta tabla de parámetros, suponiendo que el máximo de la prima de riesgo asciende a un 200%, 0 puntos sería un 0% y 5 puntos un 200%.

| | | | | | Riesgo | | |
|---|---|---|---|---|---|---|---|
| | | | bajo | normal | notable | alto | muy alto |
| Ponderación | | | 1 | 2 | 3 | 4 | 5 |
| 20% | | Negocio: sector / producto ... | | | | | |
| 5% | | Tamaño | | | | | |
| 10% | | La seguridad la lleva la propia empresa, una sola empresa o varias empresas | | | | | |
| 5% | | Exposición a otros riesgos (divisas...) | | | | | |
| 4% | | Riesgo país | | | | | |
| 5% | | Flujos. Estabilidad. | | | | | |
| 15% | | Endeudamiento asignado | | | | | |
| 10% | | Formación de los Directivos en temas de ciberseguridad | | | | | |
| 10% | | El valor depende de los intangibles | | | | | |
| 8% | | Conocimiento Avances tecnológicos | | | | | |
| 8% | | La empresa tiene estrategias de ciberseguridad | | | | | |

Fig. 20, Ponderación/riesgo. Fuente: Jiménez Naharro, F. y Sánchez Montañés, C. (2017)

Si la Bolsa descuenta Telefónica a una prima de riesgo del 166.6% con respecto a sus datos fundamentales y el coeficiente de determinación de Telefónica, que equivale al riesgo sistemático (epígrafe 2), es de un 76%. Esto quiere decir que el 76% de la prima de riesgo se debe al mercado, o sea un 126% de la prima de riesgo se debe al mercado y esto no podemos eliminarlo, pero el resto un 40% de prima de riesgo mediante una buena gestión de mercados internacionales e intangibles si podríamos reducirlo.

Así, para que Telefónica valga 11 euros en función de sus datos fundamentales y de nuestro escenario definido se debería descontar a una tasa del 16%, con una prima de riesgo del 166%, esta prima de riesgo la podríamos reducir hasta un 126% (que es la que depende del mercado

y no la podemos eliminar), lo que supondría una tasa de actualización de un 13,5%, lo que supondría un precio de 13,5 €/acción, lo que supondría un 23% sobre la cotización actual.

O sea, si hacemos una buena gestión, sobre todo en los intangibles de la empresa, manteniendo el escenario definido podemos aumentar la cotización de las acciones y el valor de Telefónica en un 23%.

Entre estas medidas podríamos señalar:

- Diversificar razonablemente la cartera de productos y servicios ofrecidos por Telefónica.
- Gestionar los riesgos en los mercados internacionales.
- Maximizar las oportunidades y reducir los riesgos derivados de la gestión de los intangibles de Telefónica (marcas, productos, servicios, bases de datos, información, seguridad de la información, etc.)

El cuadro que añadimos presenta el valor de Telefónica ante distintos volúmenes de venta, y tasas de riesgo:

- Las ventas de Telefónica para que el precio de la acción sea su valor teórico.
- Las ventas de Telefónica para que el precio de la acción este próximo a su valor mínimo en Bolsa.
- Las ventas de Telefónica para que el precio de la acción esté a un valor próximo al actual como 11€/acción.
- Las ventas de Telefónica para que el precio de la acción sea el valor estimado en nuestro escenario, 28€/acción
- Las ventas de Telefónica para que el precio de la acción sea próximo a su valor máximo en los últimos años 30€/acción.

| Ventas en 5 años | Tasa de Riesgo | P acción | Valor |
|---|---|---|---|
| **40.213.041.901,76 €** | 6,00% | 5,5 | 27.363.594.500,00 € |
| | 13,50% | 2,62 | 13.035.021.380,00 € |
| | 16,60% | 2,21 | 10.995.189.790,00 € |
| **42.693.560.245,05 €** | 6,00% | 9 | 44.776.791.000,00 € |
| | 13,50% | 4,18 | 20.796.331.820,00 € |
| | 16,60% | 3,48 | 17.313.692.520,00 € |
| **44.110.999.298,36 €** | 6,00% | 11 | 54.727.189.000,00 € |
| | 13,50% | 5,08 | 25.274.010.920,00 € |
| | 16,60% | 4,2 | 20.895.835.800,00 € |
| **56.159.231.251,51 €** | 6,00% | 28 | 139.305.572.000,00 € |
| | 13,50% | 12,66 | 62.986.019.340,00 € |
| | 16,60% | 10,4 | 51.742.069.600,00 € |
| **57.585.039.202,66 €** | 6,00% | 30 | 149.255.970.000,00 € |
| | 13,50% | 13,55 | 67.413.946.450,00 € |
| | 16,60% | 11,11 | 55.274.460.890,00 € |

Fig. 21, Venta, Tasa de riesgo, Precio acción, Valor. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

A continuación, vamos a definir tres posibles escenarios (optimista, normal y pesimista), calcular las probabilidades de ocurrencia de cada uno de ellos y mediante la aplicación de las

opciones reales determinar un nuevo valor para Telefónica y, finalmente, aplicando los múltiplos comparativos estimar un valor para los intangibles de Telefónica.

El escenario pesimista es aquel cuando el precio de la acción es inferior a la cotización mínima de 9€/acción, el escenario normal está comprendido entre 9€ y 30€ la acción, nosotros vamos a tomar como representativo el estimado por nosotros, 28€/acción y el optimista es cuando el precio de la acción está por encima de 30€ la acción.

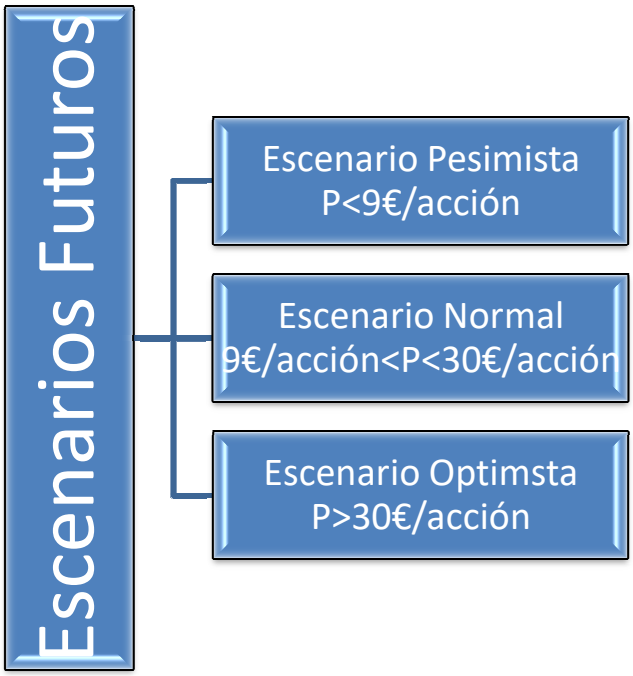
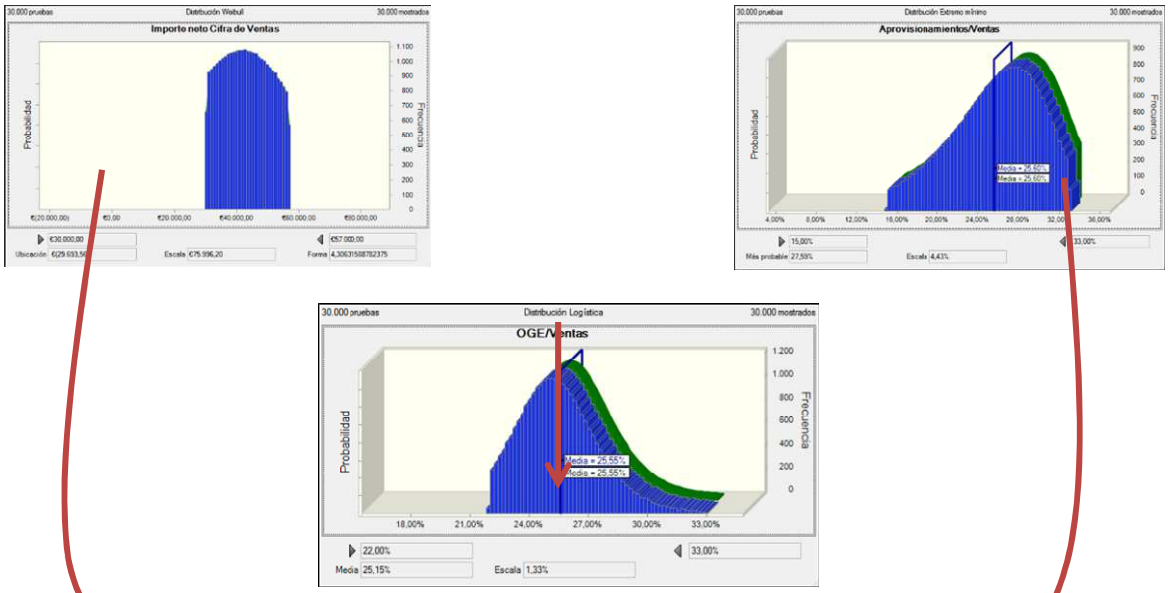



Fig. 22, Escenarios Futuros. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

Así, después de aplicar la Simulación de Montecarlo a nuestro escenario estimado con la herramienta Crystal Ball y realizar 30.000 iteracciones los resultados obtenidos aparecen en las siguientes figuras:

Variables de Entrada: Ventas, OGE/Ventas y Aprovisionamientos/Ventas. Variables de salida o decisión: Valor Total y Precio de la Acción.



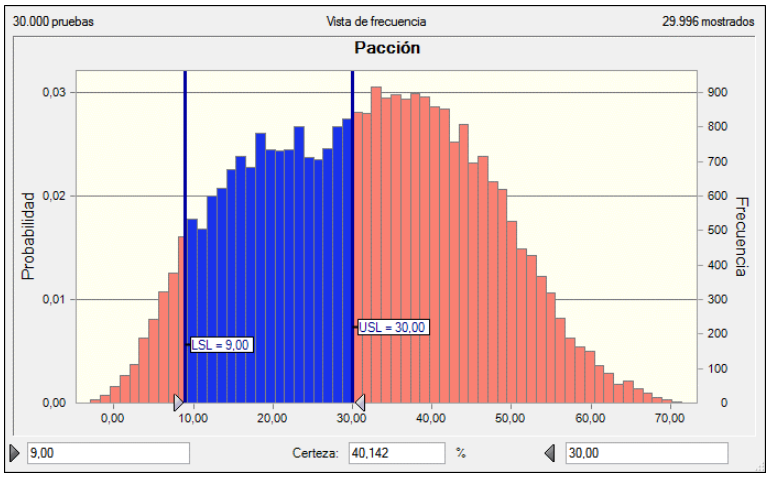



Fig. 23, Precio por acción. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

Una vez realizadas las simulaciones las probabilidades de ocurrencia son las que se presentan a continuación.

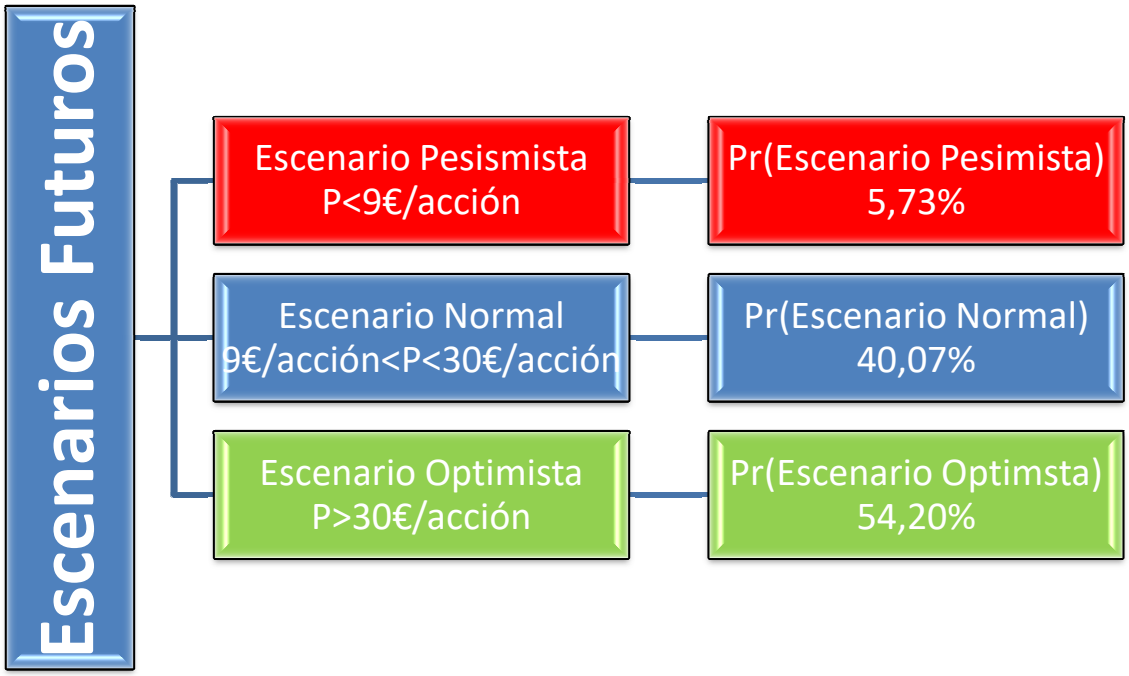



Fig. 24. Escenarios futuros, precios. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017).

A continuación, pasamos ponderar cada uno de los valores:

| Escenario Pesimista | | | | |
|---|---|---|---|---|
| **Ventas en 5 años** | **Tasa de Riesgo** | **P acción** | **Valor** | **Valor Ponderado** |
| **42.693.560.245,05 €** | 6,00% | 9 | 44.776.791.000,00 € | **44.776.791.000,00 €** |
| | 13,50% | 4,18 | 20.796.331.820,00 € | |
| | 16,60% | 3,48 | 17.313.692.520,00 € | |
| **Escenario Normal** | | | | |
| **Ventas en 5 años** | **Tasa de Riesgo** | **P acción** | **Valor** | **Valor Ponderado** |
| **56.159.231.251,51 €** | 6,00% | 28 | 139.305.572.000,00 € | **139.305.572.000,00 €** |
| | 13,50% | 12,66 | 62.986.019.340,00 € | |
| | 16,60% | 10,4 | 51.742.069.600,00 € | |
| **Escenario Optimista** | | | | |
| **Ventas en 5 años** | **Tasa de Riesgo** | **P acción** | **Valor** | **Valor Ponderado** |
| **57.585.039.202,66 €** | 6,00% | 30 | 149.255.970.000,00 € | **149.255.970.000,00 €** |
| | 13,50% | 13,55 | 67.413.946.450,00 € | |
| | 16,60% | 11,11 | 55.274.460.890,00 € | |

Fig. 25, ponderación de los factores. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

El valor ponderado en función de las distintas opciones ascenderá a:
Valor Telefónica = (44.776.791.000,00 € * 5,73%) + (139.305.572.000,00 € * 40,07%) + (149.255.970.000,00 € * 54,20%) →**Valor Telefónica = 139.278.705.925,40 €**
Por otro lado, si vemos la distribución que sigue la ratio Inmovilizado Inmaterial/Activo Total comprobamos que la ratio medio se sitúa en un 24%.

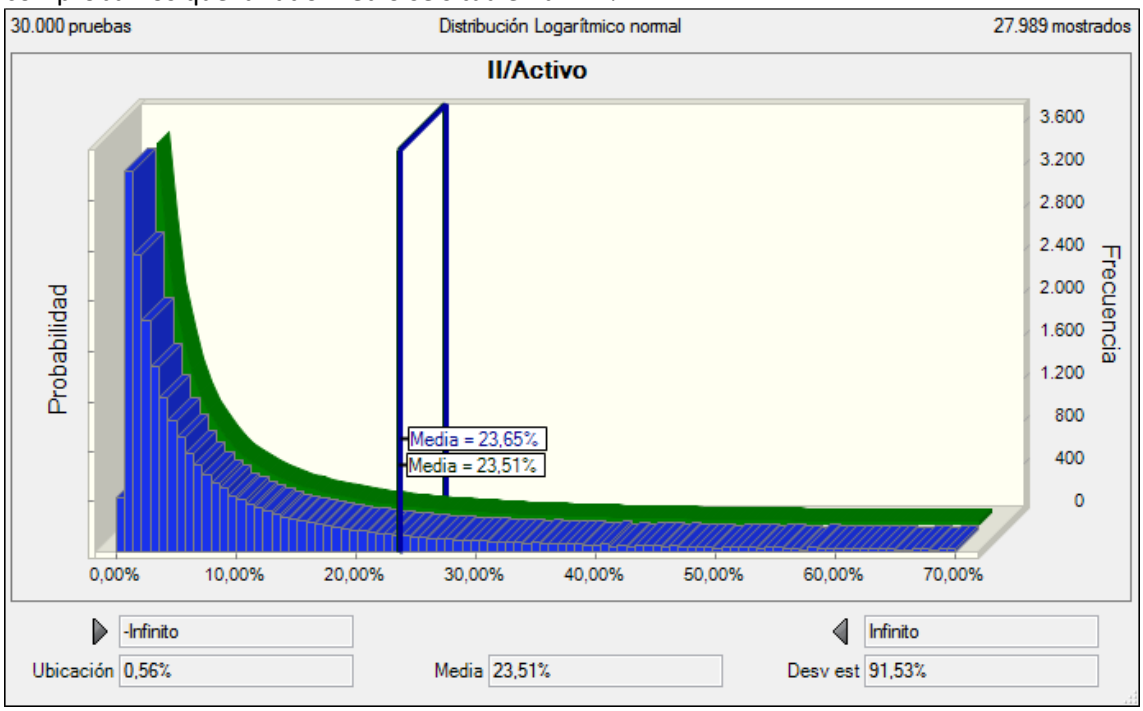



Fig. 26, II/Activo. Fuente: Jiménez Naharro, F., Sánchez Montañés, C. (2017)

Así, si aplicamos este indicador al valor de Telefónica, podemos estimar el valor del intangible de Telefónica en sus distintos escenarios y ponderado.

| **Escenario Pesimista** | | | | |
|---|---|---|---|---|
| **Ventas en 5 años** | **Tasa de Riesgo** | **P acción** | **Valor** | **Valor Intangible** |
| **42.693.560.245,05 €** | 6,00% | 9 | 44.776.791.000,00 € | 10.746.429.840,00 € |
| | 13,50% | 4,18 | 20.796.331.820,00 € | 4.991.119.636,80 € |
| | 16,60% | 3,48 | 17.313.692.520,00 € | 4.155.286.204,80 € |
| **Escenario Normal** | | | | |
| **Ventas en 5 años** | **Tasa de Riesgo** | **P acción** | **Valor** | **Valor Intangible** |
| **56.159.231.251,51 €** | 6,00% | 28 | 139.305.572.000,00 € | 33.433.337.280,00 € |
| | 13,50% | 12,66 | 62.986.019.340,00 € | 15.116.644.641,60 € |
| | 16,60% | 10,4 | 51.742.069.600,00 € | 12.418.096.704,00 € |
| **Escenario Optimista** | | | | |
| **Ventas en 5 años** | **Tasa de Riesgo** | **P acción** | **Valor** | **Valor Intangible** |
| **57.585.039.202,66 €** | 6,00% | 30 | 149.255.970.000,00 € | 35.821.432.800,00 € |
| | 13,50% | 13,55 | 67.413.946.450,00 € | 16.179.347.148,00 € |
| | 16,60% | 11,11 | 55.274.460.890,00 € | 13.265.870.613,60 € |

## 8.6. BIBLIOFRAFÍA:

BASE DE DATOS SABI: SISTEMA DE ANÁLISIS DE BALANCES IBÉRICOS, CONSULTADA LA UNIVERSIDAD PABLO DE OLAVIDE.https://www.upo.es>biblioteca>detalle-az

http://www1.upo.es>detalle-noticias>F

BOLSA DE MADRID: www.bolsamadrid.es

BOLSA DE BARCELONA: www.borsabcn.es

BOLSA DE NEWYORK: www.nyse.com

EUROSTOXX50: http://www.bsmarkets.com

MARKETLINE RESEARCH REPPORTS-MARKETRESEARCH.COM

JIMENEZ NAHARRO, F y DE LA TORRE GALLEGOS, A (2017): Manual de valoración de empresas y análisis bursátil. Editorial Pirámide.

RUIZ MARTÍNEZ, R. J. La viabilidad financiera de la empresa. Ed. Hispano Europea. Barcelona 1990.

TELEFÓNICA: https://www.telefonica.com
Historia de Telefónica.

# CONCLUSIONES

Se puede observar a lo largo de esta investigación que:

Vivimos en un entorno caracterizado por una transformación digital, pero con ciberamenazas y vulnerabilidades cada vez más sofisticadas en la medida en la que estamos más interconectados.

La transversalidad de la seguridad de la información, relacionada con fintech y insurtech, economía colaborativa, nuevas aplicaciones tecnológicas, competencia desleal, consumo, publicidad, propiedad industrial, propiedad intelectual, etc.

La persona es cada día más digital (con huella digital propia y con posible herencia digital de sus antepasados) y diferente a un ser cibernético que pueden convivir junto a esa persona.

Las empresas que están más implicadas en ciberseguridad y seguridad de la información: Telefónica, Banco de Santander e Inditex presentan información integrada, Integrated Reporting, IIRC (International Integrated Reporting Council) respecto al resto de las empresas estudiadas.

Telefónica está considerada una de las entidades más influyentes en la seguridad de la red. Además, la filial Eleven Paths fue creada como la unidad de ciberseguridad de Telefónica, liderada por el hacker Chema Alonso. Que el informe integrado de Telefónica está más en línea con una actitud proactiva ante estos casos.

La ciberseguridad y la seguridad de la información conlleva: cambios oganizacionales. Hay corporaciones a nivel mundial que están reformando áreas claves como la seguridad interna poniendo al frente de esta responsabilidad a un director, CISO (Chief Information Security Officer), con altos conocimientos en materia de seguridad de la información. Este puesto de CISO ha ganado importancia.

Existe un gap amplio entre el incremento continuo, a gran velocidad, de las nuevas tecnologías y la falta de implicación y actitud proactiva en algunas empresas, donde todavía no han tomado conciencia del problema de la ciberseguridad.

Sin seguridad de la información no hay negocio dado el principio de empresa en funcionamiento está en entredicho.

Toda valoración de empresas responde a la necesidad específica de quien la solicita y de quien la lleva a cabo, esto nos permite afirmar la no existencia de unanimidad en la utilización de los distintos modelos y que en el empleo de éstos se está sujeto a juicios de carácter subjetivo, como las estimaciones sobre el comportamiento futuro de diversos aspectos del desarrollo del negocio y de su entorno económico.

Algunas compañías estudiadas están implicadas en operaciones de ciberseguros. Telefónica es precursora en seguridad de la información, colaborando en el primer informe elaborado conjuntamente con THIBER, sobre la transferencia de riesgos cibernéticos a través de las ciberpólizas en España, participando en la elaboración del informe algunas de las más

importantes compañías del sector asegurador: AIG, AON, K2 INTELLIGENCE, MARSH, MINSAIT con la colaboración del INSTITUTO DE EMPRESA.

Existe falta de liderazgo en materia de ciberseguridad en la mayoría de los casos.

Falta preparación en los directivos de las compañías en general en materia de ciberseguridad y seguridad de la información en base a la trayectoria de sus miembros.

Falta de información sobre la actualización de los curriculums de los miembros de los consejos de administración de las compañías en materia de ciberseguridad y seguridad de la información.

Falta aprendizaje en esta materia en las empresas que hemos analizado.

La mayoría de las empresas analizadas no están en los foros a nivel nacional e internacional en esta materia.

No se percibe una actitud solidaria nacional e internacional con otras empresas para la resolución de problemas de ciberseguridad.

La ciberseguridad y la seguridad de la información no han calado en la conciencia interna de la empresa.

Falta información sobre la existencia de un presupuesto en materia de seguridad y seguridad de la información.

Tampoco se tiene información sobre la actitud e implicación de los stakeholders en el presupuesto.

Las cuentas anuales individuales y consolidadas no hacen alusión a la ciberseguridad en muchos casos, tampoco se hace alusión a la información expuesta y a sus riesgos.

No existe información sobre posibles pérdidas por deterioro en esta materia con respecto a los clientes online.

No existe información segmentada de las ventas en base a las operaciones online de las que no lo son.

No se da información sobre las bases de datos como activos intangibles. Se debe considerar el valor estratégico de las bases de datos en el futuro de las empresas.

No existe información sobre el grado de cumplimiento de la ley orgánica de protección de datos y auditorías bianuales.

El modelo de negocio se puede venir abajo como consecuencia de una conciencia laxa o poco escrupulosa ante estos temas.

No aparece información en las empresas estudiadas sobre las consecuencias de la digitalización en el derecho de los trabajadores, toda vez que muchos puestos de trabajo tradicionales van a desaparecer como consecuencia de la digitalización. Tampoco aparece información sobre “el compliance Laboral y el uso de las nuevas tecnologías en el trabajo.

No se da información sobre el gasto por impuesto sobre beneficios procedentes de operaciones online de las que no lo son, tampoco se da información sobre activos y pasivos por diferencias temporarias del impuesto sobre beneficios en base a las operaciones online del resto de las operaciones. Ni aparece el estado de conciliación de las distintas cuentas anuales que afectan al impuesto sobre beneficios en base a las trasacciones online.

Los activos de información son vitales para las compañías. En sus cuentas anuales deben aparecer en el inmovilizado tangible e intangible.

En el informe reputacional esta información también es clave para la empresa.

Una correcta valoración de empresas requiere conocer la actividad a la que se dedica la compañía objeto de la valoración; el entorno económico en el que se actúa; la futura evolución de la economía; la estructura, capacidades y recursos disponibles en la organización y considerar el modelo más adecuado en cada valoración. Falta más información relacionada con los intangibles, prestar más atención al capital intelectual en base a la teoría de recursos y capacidades que hemos visto en el capítulo 4 y su valoración.

Entendemos que la actividad de valorar empresas debe ser el resultado de un proceso bien estructurado y de la aplicación de unas fórmulas probadas, que permitan llegar a un intervalo de valor posible y, sobre todo, que impere el sentido común. Lo más importante no es establecer un valor,sino un camino que nos permita valorarla empresa y sus intangibles, así como saber qué hacer cuando se producen desviaciones con las estimaciones realizadas. Este el caso del capítulo 8 sobre la valoración de los intangibles de la Compañía Telefónica, precursora en materia de seguridad de la información, teniendo en cuenta los distintos escenarios (optimista, normal y pesimista) y los estados contables previsionales consecuencia de los distintos escenarios, así como las distintas variables previsionales del modelo aplicado, considerando el riesgo sistemático y los riesgos específicos (riesgos cibernéticos, riesgos relacionados con la seguridad de la información).

En el ámbito académico hay una especial predilección por los modelos basados en el descuento de flujos de caja, ya que son considerados como las técnicas más completas y las más utilizadas en los procesos de valoración empresariales. Sin embargo, en muchas ocasiones los recursos intangibles, como elementos generadores de resultados económicos empresariales son ignorados en la elaboración de los cash flows.

Además, este modelo tampoco tiene en cuenta las posibles opciones de que el plan no se cumpla, tanto por las desviaciones positivas como negativas. Estas dos limitaciones hacen que el modelo de flujos descontados “penalice” el valor de la empresa. Los modelos de las opciones reales surgen como complemento del modelo de flujos descontados, para resolver el problema de la rigidez del plan financiero, ya que incorporan flexibilidad al mismo, valorando la opción de poder tomar un nuevo camino al no cumplirse los objetivos establecidos en el mismo.

La información contable no es suficiente para valorar las fuentes de valor, los futuros beneficios y los cash flows de las empresas; información estrechamente relacionada con aspectos tales como el liderazgo, la innovación, la excelencia de la dirección o la imagen de marca de la empresa.

Las limitaciones de la información económico-financiera y el papel fundamental que desempeñan los intangibles como fuente de creación de valor en las empresas han dado lugar a numerosos esfuerzos y propuestas para proporcionar un marco de referencia para la gestión

y medición del valor del capital intelectual de la empresa a través de la identificación de sus distintos componentes.

En la actualidad no se dispone de una definición generalmente consensuada del término intangibles, a pesar del tremendo esfuerzo realizado y constatado en numerosas investigaciones en materia contable, financiera y de gestión, en general (tanto a nivel nacional como internacional, fundamentalmente). Existe un amplio debate acerca de los activos que deben considerarse de esa naturaleza. Entre las diversas definiciones propuestas parece existir cierto acuerdo en que los activos intangibles son fuentes generadoras de probables y potenciales futuros beneficios, carentes de sustancia física, controlado por la empresa, como resultado de previos sucesos o transacciones.

La problemática relacionada con la ciberseguridad es una de las áreas con mayor potencial de crecimiento dentro de la economía nacional. Las características anteriormente analizadas nos pueden hacer ver que este sector se puede convertir en una importante fuente de diversificación con la que aumentar la riqueza de la economía nacional.

Por último, y por ello no menos importante, consideramos que es fundamental que las empresas relacionadas con la problemática de la ciberseguridad desarrollen el modelo de negocio basado en la investigación, para una vez consolidado éste poder desarrollar un modelo de negocio basado en el mercado, orientado en la obtención de ventas, la generación de ventajas competitivas sostenibles y en la obtención de una autofinanciación que le permita crecer.

**PROPUESTA DE MÍNIMOS DESEABLES INFORMATIVOS POR ENCIMA DE LOS MINIMOS NORMATIVOS ESTABLECIDOS, RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN, EN UN ENTORNO DIGITAL. EN BASE A LAS ENCUESTAS REALIZADAS, HOJAS DE TRABAJO SOBRE MÉTRICAS DE INTANGIBLES Y LITERATURA CONSULTADA.**

Proponemos tener integrados junto al sistema de gestión de seguridad de la información, distintos sistemas de gestión que añadirían valor a los intangibles de la empresa (aumento de las ventajas competitivas) y por ende a la empresa en su conjunto e igualmente a su entorno. En concreto, proponemos que los mínimos normativos actuales desarrollados en las ISO 27.001 y 27.002 estén en concordancia con la contabilidad como sistema de información útil para la toma de decisiones por los distintos stakeholders y usuarios en general.

1.- Los activos de información de la empresa (aplicaciones informáticas, propiedad industrial, propiedad intelectual, bases de datos, software en general, equipos para procesos de información, hardware, instalaciones técnicas relacionadas con la seguridad de la información, sistemas de gestión implantados de la seguridad de la información, drones, robots, etc.) son sensibles a ataques por su grado de importancia e interés y deben tener presencia para su seguimiento y control en el balance de situación, con un apartado específico en cada masa patrimonial.

Información en la cuenta de resultados sobre los gastos en formación del personal dedicado a la seguridad de la información, primas por operaciones de ciberseguro, pérdidas por deterioro de activos de información e igualmente reversión por deterioro, amortización de los inmovilizados materiales o inmateriales de información, gastos por asistencia técnica en materia de seguridad de la información. Deslindar las ventas online del resto de las ventas. Pérdidas extraordinarias por ataques cibernéticos, beneficios o pérdidas por enajenación de los inmovilizados de información.

Presentación de la información segmentada online: por mercados geográficos, por productos, redes sociales, dado que hoy muchas operaciones de compraventa se realizan por redes sociales.

Información en la memoria, como cuenta anual, de los efectos de las pérdidas relacionadas con los riesgos cibernéticos.Información de todas las aplicaciones informáticas relacionadas con la seguridad de la información, uso y control de todas las bases de datos. Informar a los propietarios y responsables en cada momento del uso de las bases de datos y del efecto multiplicador de las mismas por operaciones finacieras online o tradicionales, que realice la empresa. Ejemplo: las que nacen de los procesos de fusión por absorción, nueva creación, combinaciones de negocios, consolidación, etc.

Información en el estado de flujo de efectivo de los flujos de tesorería por operaciones de explotación relacionado con los aprovisionamientos y ventas online, operaciones de inversión desinversión de activos de información por operaciones online, operaciones de financiación desfinanciación por operaciones online.

Información en el estado de cambio en el patrimonio neto relativa al uso de distintas reservas: obligatorias y de libre disposición, como consecuencia de operaciones relacionadas con los riesgos cibernéticos.

En el informe de gestión, información relativa a los presupuestos en materia de ciberseguridad y seguridad de la información, número de proyectos de investigación, información sobre planificación en materia de ciberseguridad.

En el informe de auditoría externa e interna, información específica en párrafo propio sobre los riesgos cibernéticos y las consecuencias para la empresa. Detalle sobre los protocolos de control interno. Igualmente, debe existir concordancia entre el informe de auditoría interna y externa en base a las normas de control interno.

Se propone una comisión de tecnología y ciberseguridad en conexión con la comisión de auditoría interna. Entre las funciones importantes estarían: supervisión del riesgo tecnológico, incluidos los riesgos sobre seguridad de la información y ciberseguridad, así como los procedimientos adoptados por el área ejecutiva para el seguimiento y control de estas exposiciones; revisar las políticas y sistemas de evaluación, control y gestión de los riesgos e infraestructuras tecnológicas, incluyendo los planes de respuesta y recuperación frente a ciberataques; ser informada (la comisión) sobre los planes de continuidad del negocio en lo que respecta a cuestiones tecnológicas; ser informada, según corresponda, sobre los riesgos de cumplimientos asociados a las tecnologías de la información; los procedimientos establecidos para identificar, valorar, supervisar, gestionar y mitigar estos riesgos; la comisión debe ser informada de los eventos relevantes que se hubieran producido en materia de ciberseguridad, entendiendo por tales, aquellos que, aisladamente o en su conjunto, puedan tener un impacto o daño significativo en el patrimonio, resultados o reputación.

2.- Deslindar los activos intangibles relacionados con la seguridad de la información del resto de los intangibles. Información sobre los activos intangibles relacionados con el capital humano (aptitudes, formación, entorno, crecimiento, flexibilidad, compromiso, motivación); estructura interna (innovación, cultura de seguridad de la información, calidad, eficiencia, tecnología, seguridad); relaciones externas en materia de seguridad de la información (imagen, marca, reputación, compromiso social, compromiso medioambiental, transparencia, clientela).

Con mediciones a través de indicadores no financieros de estructura externa, de estructura interna y de recursos humanos, a pesar de las dificultades prácticas.

3.- Información sobre los costes de formación a empleados y concienciación, para incrementar la cultura de la seguridad de la información. Las acciones de formación para empleados serán las adecuadas al puesto de trabajo que desarrolle, conocimiento de la ley orgánica de protección de datos, implicaciones organizativas e infracciones legislativas, amenazas de ingeniería social, seguridad versus comodidad y confianza.

4.-Información sobre los costes en acciones de formación para el personal técnico: proceso de formación continua, proceso de la seguridad perimetral (firewalls, antivirus, antimalware, etc.); supervisión del sistema operativo y software; herramientas de seguridad (cifrado, autenticadores, contraseñas, etc); políticas de seguridad (medios extraíbles, copias de seguridad, etc.).

5.- Información sobre políticas y procedimientos de seguridad: definir el procedimiento de alta de empleados (ley orgánica de protección de datos, confidencialidad, privilegios, etc.), definir procedimientos de actuación (qué se puede o no se puede hacer), normas de uso de recursos, definir los procedimientos disciplinarios y sanciones por incumplimiento.

6.- Información sobre la cultura de la seguridad de la información: las medidas y buenas prácticas deben ser adoptadas y asimiladas por los usuarios, conciencia del peligro y amenazas latentes que dependen de nuestros actos y decisiones, responsabilidad de acceder al ciberespacio, conocimiento.

7.- Información sobre los recursos disponibles para probar si la cultura de la seguridad está instaurada: existencia de simuladores o responsables (toma de decisiones sobre políticas, evaluadores de costes, ámbitos de impactos, efectos producidos, etc.), entrenadores o empleados (aprendizaje de amenazas, vulnerabilidades, intrusiones, navegación segura, evita fhishing, evitar rasomwere, uso BYOD, Bring your Own Device, etc.), gamificadores (ataques simulados, trampas, pruebas de intrusión, circunstancias anormales, evaluación de respuesta, etc.), otros (evaluadores sicológicos y de comportamientos).

8.- Información sobre protección del puesto de trabajo: es el primer punto de contacto y la zona más amenazada para el usuario, fomentar hábitos saludables en seguridad de la información, el puesto y la estación de trabajo son el punto de conexión al ciberespacio, es, por tanto, la puerta de entrada y debe estar asociada al usuario, ningún elemento debe permitir la autenticación de otro usuario en la estación de trabajo.

9.- Información sobre protección del puesto de trabajo, autenticación: nunca dejar contraseñas escritas en post-its, libretas, folios, u objetos en el escritorio, nunca dejar Smartcards, tokens, ni dispositivos de identificación en el puesto, nunca pronunciar, escribir o enviar la contraseña a otros individuos (política de seguridad de la información), destruir cualquier documento de forma segura sobre todo aquellos que contengan información confidencial.

10.- información sobre el puesto de trabajo, dispositivos desatendidos: nunca abandonar el puesto de trabajo sin bloquear la estación (ordenador, portátil, etc.), no dejar dispositivos móviles sin vigilancia en lugares de tránsito, no dejar dispositivos de almacenamiento sin vigilancia, ni siquiera conectados a la estación, dispositivos maliciosos (keyloggers, stealers, etc.).

11.- Información sobre protección del puesto de trabajo, BYOD (Bring your Own Device): el usuario accede a los recursos de la empresa empleando sus dispositivos personales, riesgo severo para los activos de la empresa, el puesto de trabajo se transforma y los riesgos de seguridad de la información se multiplican y agravan, MDM (Mobile Device Management), concienciación de los límites para millennials (emprendedores y digitales, talento digital), constante amenaza malware vía mensajería instantánea y tiendas de aplicaciones.

12.- Información sobre protección del puesto de trabajo, navegación y malware: la navegación y acceso a sitios en la red son un foco constante de malware y código maliciosos: por lo general los sitios de índole profesional suelen poseer un certificado y cifrado seguro; sitios de descarga ilegal suelen ser origen de descargas malware y scripts maliciosos; rasomwere, rogue software, adware, hijacking, phishing, spyware, etc.

13.- Información sobre protección del puesto de trabajo, almacenamiento online: el almacenamiento online se ha alzado como una opción cómoda y poderosa para almacenar información tanto profesional como privada. Activos corporativos quedan protegidos por el mecanismo de autenticación del usuario, almacenamiento en la nube suele padecer ataques masivos para revelar contraseña.

14.- Información sobre protección de puesto de trabajo, redes sociales y foros: relacionar empleado y puesto de trabajo puede abrir la puerta a la ingeniería social maliciosa, no utilizar la cuenta de correo profesional en foros y redes sociales, no publicar información laboral en las redes, no publicar fotografías del puesto ni del interior o exterior del centro de trabajo, no difundir información sobre los proyectos o actividades laborales bajo ningún concepto.

15.- Información sobre buenas prácticas del empleado: la cultura de la seguridad sólo se puede lograr a través de la plena involucración del trabajador, pequeños gestos y una atención especial puede suponer la diferencia entre salvación y debacle, el usuario debe ser consciente de los riesgos, el impacto y las consecuencias, pero además la imagen que transmitirá según el suceso, incluso como víctimas todavía hay tiempo para responder adecuadamente y reducir el impacto.

16.- Información sobre buenas prácticas del empleado, software: sistema operativo, herramientas, extensiones y antivirus actualizados por la vía oficial y estándar, usuario sin privilegios de administrador, nunca instalar aplicaciones descargadas de internet ni redes P2P[99] (política de empresa), no entorpecer (acción u omisión) la labor del software de seguridad ni las políticas de control, nunca habilitar servicios propios como P2P, correos, FTP[100], web, bases de datos, etc.

17.- Información sobre buenas prácticas de los empleados, spam y fhishing: el spam es un método de publicitación de productos o servicios que incluye código malicioso a través de sus adjuntos, enlaces o simplemente para confirmar como activa la cuenta de correo víctima. Nunca abrir ficheros adjuntos, acceder a enlaces, reenviar, responder, acceder a datos bloqueados, confirmar recepción, guardar, etc.

[99] Peer to Peer, red de pares, red entre iguales. Es en la actualidad una de las formas más importantes y populares de compartir todo tipo de material (video, audio, programas y literatura, entre otros) entre usuarios de internet, sin importar la plataforma de software utilizada ni el lugar o momento en que se encuentren.

[100] File Transfer Protocol, es un protocolo de transferencia de archivos. En informática es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCT (Transmission Control Protocol) basado en la arquitectura cliente-servidor.

Notificar al departamento de la recepción para que actualicen los filtros anti-spam.

18.- Información sobre buenas prácticas de los empleados, notificación de sucesos: los empleados deben conocer los mecanismos, instrucciones y detalles a registrar para notificar sucesos de seguridad que afecten a los activos. Gestor de tickets e incidencias. El empleado debe ser capaz de describir el suceso y deseablemente proporcionar logs. La reincidencia del empleado(s) en fallos similares o idénticos deberá iniciar mecanismos de reeducación y formación en seguridad.

19.- Información sobre buenas prácticas de los empleados, configuración: Los usuarios deben ser capaces de configurar o comprobar la configuración válida del equipo.

- ¿Cómo se conecta a la red? (Wifi o LAN)
- ¿Qué antivirus usa la empresa?
- ¿Qué software debe iniciarse con el equipo?
- ¿Qué dispositivos debo tener conectados?
- ¿Qué navegador es el que uso?
- ¿Qué extensiones tiene mi navegador?
- ¿Qué software es de mi empresa y cuál no?

20.- Información sobre buenas prácticas de los empleados, autenticación: El sistema de autenticación es individual e intransferible ya sea un token físico, una huella biométrica o una contraseña (memorizada).

- Todo sistema sensible de duplicación debe ser renovado periódicamente (política de empresa)
- Nunca comunicar nuestras credenciales.
- Nunca cambiar sin recibir notificación de la empresa nuestro mecanismo de autenticación, ya sea credencial o parámetro biométrico.

21.- Información sobre buenas prácticas de los empleados, información compartida: los empleados normalmente deben compartir información con otros trabajadores, pero es fundamental obedecer ciertas directrices.

- Compartir siempre los documentos específicos y nunca carpetas completas por comodidad.
- Nunca revisar o ejecutar archivos inesperados en una zona compartida de libre acceso.
- Definir plantillas y jerarquías de ficheros que permitan detectar anomalías en la estructura.

22.- Información sobre buenas prácticas de los empleados, sentido común: Los usuarios deben de conocer el plan y procedimiento a seguir en caso de acontecer algún suceso que afecte a la seguridad de los activos. Los empleados deben entrenar su capacidad para no ser víctimas de engaños por ingeniería social, como recibir llamadas que se identifican como el departamento de IT o correos electrónicos simulando ser compañeros de trabajo.

23.- Información sobre protección de la información, el control de acceso: El control de acceso lógico a los activos de la empresa debe comenzar en los sistemas y dispositivos que definen el ecosistema informático de la compañía.
El sistema de control, debe registrar y permitir la traza desde los usuarios que acceden a los sistemas hasta los recursos que consulten o visiten. Esta cadena de custodia de la información es esencial para la gestión de riesgos de seguridad. El control de acceso es esencial para definir los privilegios y las políticas de seguridad que rigen sobre el usuario.

El control de acceso por capas: física, lógica, políticas de seguridad, IDS[101]/FIREWALL, monitorización.

24.- Información para gestionar el Control de acceso es fundamental:

- Definir el tipo de información de la empresa según las áreas, la importancia, el grado de privacidad que requiere, el volumen, etc.
- Establecer quién puede acceder a cada tipo de información mediante permisos de acceso individuales o de acuerdo a alguno de los modelos de gestión de privilegios disponibles.
- Definir quién puede y cómo debeautorizar el acceso.

25.- Información sobre el control de acceso, modelos: Existen distintos modelos para definir los privilegios y derechos de los usuarios para acceder a los activos de información de la empresa, atendiendo a la granularidad o propiedad que lo gestionan.

26.- Información sobre el control de acceso, gestión de la identidad y autenticación: Son herramientas destinadas a verificar la correcta identidad de un usuario, realizando la autenticación y autorización a los sistemas y recursos bajo una adecuada identificación de una organización y habilitando el proceso de auditoría y contabilización (Accounting) de sus acciones.

27.- Información sobre control de acceso a red: Son herramientas destinadas a proporcionar mecanismos para administrar y controlar el acceso de usuarios a una red. Aplican configuraciones y soluciones de seguridad para aumentar la disponibilidad de red y el cumplimiento normativo.

28.- Información sobre control de acceso, tipos: sign-on[102], autenticación compartida.

29.- Información sobre control de acceso, tipos: certificado digital, firma digital, certificado y firma digital

30.- Copias de seguridad. Las copias de seguridad se han convertido en un factor críticopara las empresas con base tecnológica debido a las amenazas de seguridad y al impacto que pueden tener sobre los activos de información de la empresa. Debe formar parte de la política de seguridad.

31.- Información sobre el cifrado. El cifrado representa el mecanismo más importante para proporcionar confidencialidad de la información. Esto es evitar el acceso a los datos mediante la ofuscación de la información mediante técnicas de codificación. Simétrica y asimétrica.

32.- Información sobre almacenamiento en la nube. Servicios de almacenamiento ofrecidos por distintos proveedores de Internet y que funcionan de manera similar a un disco duro en red. No se debe confundir con cloud computing que es computación en la nube.

33.- Información sobre protección de dispositivos personales, BYOD, MDM.

---

[101] Sistema de detección de intrusiones, es un programa de detección de accesos no autorizados a un computador, con sensores como un sniffer, o una red, muy poderoso ya que se une la inteligencia del IDS y el poder de bloqueo del firewall.

[102] Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación (validación única). Hay distintos modelos de single sign-on.

34.- Información sobre cumplimiento legal, LOPD, LPI, LSSI, recomendaciones de seguridad, contrato de acceso y compartición de datos personales, fraude y gestión de la identidad. Categorizar los datos personales, declarar los ficheros, medidas de seguridad, derechos sobre información, tratamiento internacional, Reglamento General de Protección de Datos, valor de la información, ley de servicio de la sociedad de la información y de correo electrónico. Ley de propiedad intelectual (derechos de autor, derechos morales), ley de propiedad industrial.

35.- Información sobre protección de los clientes, responsabilidad como proveedor de servicios: comercio electrónico, transparencia, comunicación y satisfacción, contrato de confidencialidad, acuerdo de nivel de servicio (SLA[103]).

36.- Plan director de seguridad. La información es el activo clave de la empresa, el plan director consiste en poner las prioridades de la empresa en claro, lo más importante de la empresa y lo más esencial y crítico de ésta, y así afrontar la seguridad de ella y sus accesos. ¿Qué hay que conocer?: la fiabilidad del sistema, el sistema de identificación de usuarios. La protección de la información como pagos, reservas, datos de solicitud, etc. Reducir riesgos al mínimo, como por ejemplo el uso de antivirus en los ordenadores, sistemas de autenticación biométricos, análisis de estrategia corporativa de la organización, el potencial decrecimiento y los servicios que se usan para alinearlos con la estrategia de seguridad, dado que las medidas de seguridad aislada no resuelven nada, identifica los servicios que más interés hay en la empresa y con estos datos observar qué es lo que más necesita de seguridad para acceder a ellos.

37.- Auditoría de Sistemas de Gestión de seguridad de la Información. Estas auditorías nos permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad. Enumerar y posteriormente describir las vulnerabilidades que pudieran presentarse y una revisión exhaustiva de las estaciones de trabajo.

Respecto a las fases de la Auditoría, destacamos: enumeración de redes, topología (mapa físico o lógico de una red, nodos interconectados) y protocolos; verificación del cumplimiento de los estándares internacionales ISO; identificación de los sistemas operativos instalados; análisis de servicios y aplicaciones; detección, comprobación y evaluación de vulnerabilidades; medidas específicas de corrección, recomendaciones de medidas preventivas.

Existen distintos tipos de auditoría: Auditoría de Seguridad Interna: privacidad de redes locales y corporativas de carácter interno; Auditoría de Seguridad Perimetral, el perímetro de la red local o corporativa es estudiado y el grado de seguridad en las entradas externas; Test de intrusos, es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento de la auditoría perimetral; Análisis forense, es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se llama postmortem; Análisis de páginas web, entendido como el análisis externo de la web, comprobando vulnerabilidades como inyección de código SQL[104],

[103] Service Level Agreement, es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

[104] Structured Query Language, es un lenguaje específico del dominio que da acceso a un sistema de gestión de bases de datos relacionales que permite especificar diversos tipos de operaciones entre ellos.

verificación de existencia y anulación de posibilidades de cross site, scripting (XSS)[105], etc.; Auditoría de Código de Aplicaciones, análisis del código tanto de aplicaciones de página web como cualquier otro tipo de aplicaciones independientemente del lenguaje empleado.

[105] Cross-site scripting, es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o cualquier lenguaje similar, evitando medidas de control.

**FUTURAS EXTENSIONES DE LA INVESTIGACIÓN**

Todo lo que vamos de exponer a continuación se fundamenta en el importante auge de la digitalización de cualquier ámbito o sector de actividad y todo este auge implica mayor grado de exposición de la información y de los datos. Por consiguiente, van a existir numerosas oportunidades de negocios en ciberseguridad.

Estamos viviendo, si le podemos llamar así, una revolución silenciosa, se está gestando en los hogares, en los coches, en la correspondencia, en las oficinas, en las comunidades. Mucho de lo que tenemos podemos compartirlo. El consumo colaborativo es un verdadero cambio de paradigma, que pone el acento en el acceso a las cosas más que en la posesión. Todo lo que no se usa totalmente, todo puede estar a disposición de otros (sharing economy, economía compartida o digital). Para Gabriel Lanfranconi, director del programa de Ciudades de Cippec, una ONG que estudia las políticas públicas. El consumo se horizontaliza, se pacta de persona a persona, se eliminan los intermediarios. Con todo lo que eso implica.

Los promotores del consumo compartido prefieren no hablar de revolución: dicen que no están para reemplazar a nadie. Se trata de un nuevo paradigma, que baja el precio de los bienes y, por ende, posibilita que muchas personas de ingresos más bajos tengan acceso a ellos.

Siguiendo a Albert Cañigueral, autor del libro “Vivir con menos” y fundador del sitio consumocolaborativo.com. "El modelo más eficiente del siglo veinte fue el industrial, el institucional, el del edificio con la tienda... resulta que ahora tenemos plataformas que nos permiten romper ese esquema y que van a coexistir".

El consumo colaborativo y la ciberseguridad puede ser una futura investigación y sus implicaciones en la valoración de las empresas.

Los modelos de valoración de empresas y de intangibles tienen cada vez más importancia, no sólo con motivos exclusivamente de valoración, en un contexto del corporate finance, sino cada vez tiene más importancia a la hora del management empresarial (estrategia, marketing, operaciones, etc.), ya que permiten gestionar mejor la creación de valor generada en el seno de las organizaciones, y especialmente a la que se refiere al accionista.

Esto nos induce a pensar que se debe seguir investigando en la construcción y consolidación de modelos de valoración de empresas, elevando la calidad de los procesos de tratamiento de la información, afinar en los resultados y conseguir aumentar la credibilidad, contribuyendo todo esto a mejorar en la gestión gracias a herramientas mejoradas por la introducción de estos tipos de modelos.

En un panorama digital como el que vivimos que ya hemos comentado (Big data, internet de las cosas, robotización de las cadenas de producción, etc.) y ante la problemática de ciberseguridad, cada vez es más importante la implementación de una estrategia que abogue por la transparencia, por el respeto a la privacidad de todos los stakeholders, con clara información del alcance en el informe de buen gobierno (comisión de auditoría interna), informe de responsabilidad social corporativa de las empresas (nivel de riesgo que afecta a la empresa) y un informe de auditoría externa que explicite con claridad el alcance y contenido de todos los riesgos de la empresa sobre todo las amenzas de ciberseguridad.

Sería conveniente, profundizar o investigar en el gobierno corporativo, en el nuevo entorno digital (en un mundo lleno de vulnerabilidades y ciberamenazas) que es el conjunto de procesos, costumbres, prácticas, leyes e instituciones que afectan en alguna medida a la forma en que una empresa (o institución) es dirigida, administrada o controlada. El gobierno corporativo incluye las relaciones entre las distintas partes implicadas en la empresa con diferentes objetivos. En particular se incluyen como partes implicadas a los accionistas, acreedores, ejecutivos y junta directiva de la empresa. En concreto se debería investigr en el recorrido, experiencia e implicación en ciberseguridad de todos los componentes que conforman el gobierno corporativo y así prevenir problemas de seguridad de la información.

Desde el punto de vista social no debemos olvidar el futuro de muchos puestos de trabajos tradicionales, por ejemplo, el caso de la empresa Foxconn que reemplaza en mayo de 2016 por robots a 60.000 trabajadores en una fábrica en China. No sólo se trata de esta empresa hay muchas más con esta política de sustitución. Para ello debemos de contar con el principal aval que lo hace posible con garantías: el sentido común y la experiencia que refuerza tal sentido.

La solución a las amenazas de ciberseguridad está relacionada también con el sector de empresas relacionadas con el ciberseguro y con profesionales de alta cualificación en esta materia. Es importantísimo medir los impactos negativos de las ciberamenazas y profundizar en la docencia de estas materias es fundamental. Para ello traemos a colación una web sobre el futuro de la educación: cómo formar a profesores de élite. Estamos en un estado de emergencia educativa en muchos países en concreto en la Unión Europea. El futuro comienza a describirse con el acrónimo VUCA (Vulnerabilidad, incertidumbre, complejidad y ambigüedad, en inglés). Los individuos, instituciones y sociedad en su conjunto vamos a tener que seguir aprendiendo continua y eficientemente. El premio nobel Joseph Stiglitz en su libro la creación de la sociedad del aprendizaje utiliza el término Learnability, o sea, capacidad para aprender. Las empresas necesitan gente capaz de aprender continuamente.

http://politica.elpais.com/politica/2016/05/26/actualidad/1464262077_904773.html

El desarrollo de la era del conocimiento nos ha llevado a la interconectividad y a un futuro cercano del Internet de las cosas, donde los datos y su tratamiento es imprescindible para el desarrollo y competitividad de cualquier país o empresa; en un mundo donde cada vez impera más el desarrollo del Big Data y las innumerables oportunidades que ofrece la analítica predictiva, hace presagiar que la valoración de intangibles sea un nicho de investigación y de aplicación a la industria a considerar. Ante esta nueva situación que se abre es fundamental ampliar las miras a la forma y métodos a emplear en los modelos de valoración, nos referimos a la Inteligencia económica y el desarrollo de la Inteligencia Artificial. Esto ya es una plena realidad en los mercados financieros mediante la tecnología de trading de alta frecuencia, aunque para valorar se requiere sentido común y sólo es propia de los humanos, por ahora.

Es fundamental que se siga ahondando en la investigación del Capital Intelectual (CI) y en aquellos indicadores de CI que permitan aproximar la teoría financiera y las teorías sobre el CI, para mejorar los instrumentos de predicción que gestionen el valor y la gestión de las empresas.

Ante el peso creciente que goza en los mercados financieros el activo intangible sobre el tangible de las compañías, se hace fundamental que las autoridades que velan por la transparencia y el buen funcionamiento del mercado se tomen en seria consideración la obligatoriedad de la valoración de intangibles, y por su puesto de la empresa, como parte de la información financiera obligatoria con el propósito de complementar la información contable

presentada a los mercados de capitales e inversores y como mecanismo para controlar y mejorar los modelos previsionales.

Tomando como referencia a INCIBE (Instituto Nacional de Ciberseguridad) en su mapa de tendencias contemplamos como oportunidad de negocio la ciberseguridad en sistemas de control industrial o la protección de redes industriales inteligentes y redes de distribución eléctrica inteligente; y la protección de coches inteligentes, de sistema de comunicación satelital y de vehículos aéreos no tripulados, drones. Otras oportunidades de negocio a investigar podrían ir asociadas a la detección de fraude en banca y seguros, la gestión de información de eventos de seguridad o la seguridad en servicios Fintech (empresas tecnológicas no bancarias).

Investigar en el ámbito de la sanidad y la farmacia, las oportunidades de negocios estarían vinculadasa la protección de dispositivos médicos conectados, el cifrado para la investigación médica y farmacéutica o el almacenamiento y ubicuo de datos médicos.

Investigar en el sector de la cibereducación (educación a través de software educativo) y los laboratorios y los laboratorios de ciberseguridad para combatir riesgos y prevenir vulnerabilidades con el objetivo de que empresas, ciudadanos e instituciones estén más segurosen la red. La distribución de ciberinteligencia y la simulación de incidentes y ciberejercicios para resolverlos.

Investigar en los servicios de seguridad en la nube, el cifrado, el hacking ético y la creación de confianza digital.

Investigar sobre los nuevos ataques basados en malware destinados a la filtración de información y datos, principalmente de empresas, instituciones y gobiernos; las denegaciones de servicio por motivos políticos, geográficos o empresariales; el hacktivismo social y nuevos ciberataques a infraestructuras y operadores críticos.

Investigar en el ámbito del derecho administrativo sobre organismos públicos nacionales e internacionales relacionados con la ciberseguridad, por ejemplo, INCIBE, organismo dependiente del Ministerio de Energía, Turismo y Agenda Digital, que tiene como uno de los objetivos principales apoyar el emprendimiento, la promoción del talento y el desarrollo de la industria nacional de ciberseguridad.

Investigar en base al Programa Europeo Horizonte 2020, las nuevas tendencias TIC en relación con la robótica y sistemas autónomos aplicados a la industria avanzada de automóviles, la salud y la logística; computación avanzada y computación en la nube(cloud computing), entre otras.

Investigar en ciberseguridad de drones y robótica en base a la nueva economía (economía colaborativa, consumo colaborativo) y también la agricultura. Para enfrentarse al desafío de la competencia mundial, los agricultores tienen que optimizar su rendimiento de la inversión. Las soluciones son basadas en tecnología y van desde los drones, robotización de algunas actividades a través de máquinas parcialmente o totalmente automáticas. Además, la tecnología ayuda cuando se trata de la compra de este tipo de máquinas. Es la llamada Agricultura 4.0.

Los Drones están conquistando la agricultura desde el cielo. Sobre todo, cuando se trata de monitorización del suelo y agua, hay muchas ventajas – con la velocidad como el valor añadido central.

Examinando por ejemplo la salud de las plantas desde el cielo es significativamente más rápido que desde la tierra, lo que hace que los drones sean una alternativa seria para los agricultores. Incluso el hecho que los resultados obtenidos con estas tecnologías son menos precisos que los métodos tradicionales, no es necesariamente un bloqueador – por la razón sencilla de que la precisión es un requisito clave de solo unas pocas aplicaciones. En otras palabras: Los drones son el método a elegir cuando se requiere eficiencia.

La eficiencia también es clave cuando se trata de la automatización – y por lo tanto otra tendencia tecnológica. Máquinas parcialmente o totalmente automatizadas trabajan de forma rápida y fiable y ayudan a la gente a trabajar donde su mano de obra es realmente necesaria. Esto tiene varias ventajas en muchos entornos agrícolas donde muchas veces solo un número limitado de trabajadores está disponible.

Sin embargo, la automatización es más que esto: Separando el hombre de las máquinas –por ejemplo, con la ayuda de la tecnología GPS– mejora la seguridad en el trabajo. Y como las máquinas automatizadas trabajan rápidamente, con precisión e independientemente, también ayudan a reducir el consumo de combustible y energía.

La revolución “cooperativa”: Maquinaria compartida

La industria de la maquinaria agrícola está por lo tanto modernizándose rápidamente. Sin embargo, no todos los agricultores pueden permitirse la inversión en nuevas tecnologías. La situación de las pequeñas y medianas cooperativas es complicada. Por un lado, tienen que permanecer en el juego tecnológico para poder sobrevivir. Por otro lado, una inversión razonable conduciendo rápidamente a un retorno de la inversión, es la clave.

Nuevos modelos de compra sirven para responder con ambos requisitos. Enfoques compartidos son una opción popular en el mercado tratándose de obtener acceso a las máquinas asequibles. Muchas máquinas son utilizadas por más de un agricultor siguiendo el modelo de las coopativas recientes.