METODOLOGÍA PARA CUANTIFICAR LAS PÉRDIDAS ECONÓMICAS Y FINANCIERAS DE UNA EMPRESA, TANTO A NIVEL NACIONAL O INTERNACIONAL, CUANDO ES AFECTADA POR CIBERATAQUES O ATAQUES INFORMÁTICOS.

METHODOLOGY TO QUANTIFY THE ECONOMIC AND FINANCIAL LOSSES OF A COMPANY BOTH AT THE NATIONAL OR INTERNATIONAL LEVEL, WHEN IT IS AFFECTED BY CYBER-ATTACKS OR COMPUTER ATTACKS.

"Atencia-Lalinde-Eafit-Co - (Versión 1.0)"

VICTOR RAFAEL ATENCIA URUETA

Proyecto de grado, requisito para optar por el título de MBA en Administración

Director, docente
Juan Guillermo Lalinde Pulido

UNIVERSIDAD EAFIT
ESCUELA DE ADMINISTRACIÓN
MAESTRÍA EN ADMINISTRACIÓN - MBA
MEDELLÍN
2021

CONTENIDO

LISTA DE FIGURAS

RESUMEN

En este trabajo se examinaron los costos financieros, económicos y reputacionales directos en que incurre una empresa al ser afectada por ciberataques, para lo cual se creó o estructuró una metodología soportada en estándares internacionales sobre ciberseguridad.

La metodología propuesta permite apoyar a las empresas, gobiernos, jueces y a las aseguradoras, para cuantificar las pérdidas económicas, administrativas, comerciales, financieras y reputacionales en que incurra una empresa en cualquier país, al ser víctima de ciberataques en sus operaciones, servicios, infraestructura y/o reputación.

La importancia y la pertinencia de este trabajo se sustenta en lo que viene presentándose en la cibersociedad en los actuales tiempos de pandemia y post pandemia por covid-19, donde el trabajo en línea, el trabajo en casa, los negocios electrónicos, el aprendizaje *on line*, e-Banking, los servicios de la industria 4.0, y en general, toda la transformación digital de las empresas llegó para quedarse como una necesidad o requerimiento obligatorio, en la sociedad y seguir generando valor y produciendo en las empresas.

Esta transformación digital empresarial e institucional viene con un sinnúmero de servicios, que facilitan el desarrollo de las actividades productivas, pero también aumenta la vulnerabilidad hacia ataques informáticos o ciberataques en contra las empresas, organizaciones, instituciones privadas y gubernamentales a nivel mundial. Tales ataques

afectan considerablemente los recursos, la economía, las finanzas y todo el valor de las empresas y de las naciones.

Palabras clave: Metodología, Ciberataques, Ciberespacio, Ataques Informáticos, Valor del daño informático, Riesgos, Ciberdelincuentes, Terroristas digitales, hacker, Afectaciones, Csirt, ColCERT, Ataques cibernéticos, Seguridad digital, Pestesting, Vulnerabilidades, Bia, Mtpd, Rto, Utilidad Neta, Ebitda, Eva, Roi, Roe.

ABSTRACT

In this work, the direct financial, economic and reputational costs incurred by a company when affected by cyberattacks were examined, for which a methodology supported by international standards on cybersecurity was created or structured.

The proposed methodology allows supporting companies, governments, judges and insurance companies, to quantify the economic, administrative, commercial, financial and reputational losses incurred by a company in any country, when being a victim of cyberattacks in its operations, services, infrastructure and / or reputation.

The importance and relevance of this work is based on what has been occurring in cybersociety in the current times of pandemic and post-pandemic by covid-19, where online work, work at home, electronic businesses, learning on line, e-Banking, industry 4.0 services, and in general, the entire digital transformation of companies is here to stay as a necessity or mandatory requirement, in society and continue to generate value and produce in companies.

This business and institutional digital transformation comes with a number of services, which facilitate the development of productive activities, but also increase vulnerability to computer attacks or cyberattacks against companies, organizations, private and governmental institutions worldwide. Such attacks greatly affect the resources, the economy, the finances and the entire value of companies and nations.

Keywords: Methodology, Cyber-attacks, Cyberspace, Computer attacks, Value of computer damage, Risks, Cyber criminals, Digital terrorists, hacker, Impacts, Csirt, ColCERT, Cyber-attacks, Digital security, Pestesting, Vulnerabilities, Bia, Mtpd, Rto, Net Profit, Ebitda, Eva, Roi, Roe.

INTRODUCCIÓN

Para iniciar vale la pena tener en cuenta las palabras de Moisés J. Schwartz - Gerente de Instituciones para el Desarrollo del BID, en el Reporte sobre ciberseguridad 2020 (BID – OEA), en el cual plantea lo siguiente: "La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida.

Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y el suministro de agua y energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales.

Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB" (OEA – BID, 2021).

Igualmente, tomar como referente las palabras de la secretaria de Comercio de estados Unidos Gina Raimondo, el domingo 06 de junio de 2021 a la cadena televisiva ABC, donde aseguró “Los ciberataques de – ransomware - están aquí para quedarse, advierto que probablemente se intensifiquen, por lo que insto a las empresas a que refuercen su seguridad tras los últimos episodios sufridos en el país. Remarco que lo primero, que hay que hacer respecto a los ciberataques es reconocer que esta es la realidad.

Debemos asumir, y las empresas deben asumir, que estos ataques están aquí para quedarse y, probablemente, se intensificarán, invito a apuntar a la necesidad del sector privado de reforzar la seguridad en este ámbito. Somos conscientes del problema, en la Casa Blanca se ha presentado un programa junto al Departamento de Energía para modernizar las defensas de ciberseguridad en (infraestructura esencial del país), ante la creciente amenaza.

Estados Unidos ha sufrido recientemente dos (2) importantes ciberataques de (ransomware), que bloquean sistemas informáticos que no son liberados hasta que compañías o instituciones pagan un rescate a los piratas informáticos.

Informo que, a final de mayo, la empresa JBS, la segunda mayor procesadora de carne de EE.UU., sufrió uno de estos ataques y se vio obligada a suspender temporalmente sus operaciones.

Pocas semanas antes la empresa Colonial Pipeline, propietaria de varios oleoductos en Estados Unidos sufrió uno similar. Esta vez lanzado por la organización criminal DarkSide con sede en Rusia, que afectó durante días al suministro de combustible en la costa este del país. Colonial Pipeline reconoció posteriormente que pagó a los piratas informáticos un

rescate de 4,4 millones de dólares porque no estaba segura del alcance del ataque ni de cuánto tiempo haría falta para restaurar el servicio" (ABC, 2021).

De igual manera, resaltar lo expuesto en el comunicado de la Unión Europea de julio de 2020, donde se dice: "La preparación cibernética de la UE es fundamental tanto para el Mercado Único Digital como para la Seguridad y Defensa de la Unión. Es imprescindible fortalecer la ciberseguridad europea y abordar las amenazas a objetivos civiles y militares. En este gran esfuerzo, contamos igualmente con el apoyo de nuestros socios globales. Solo juntos, siendo resistentes, capaces de proteger a nuestra población de manera efectiva al anticipar posibles ciberamenazas e incidentes de ciberseguridad, al construir una fuerte resiliencia en nuestras estructuras y defensa, al recuperarnos rápidamente de cualquier ciberataque y al disuadir a los responsables, podremos proporcionar un ciberespacio abierto, seguro y protegido para todos" (UE, 2020).

En términos generales, las afectaciones por ataques cibernéticos o delitos informáticos a nivel mundial según el Foro Económico Mundial en lo corrido del primer semestre del 2021 ascienden a US$ 6 Billones de dólares, que es una cifra parecida y promedio al PIB anual de Japón - tercera potencia económica mundial (FEM, 2021).

Para el caso de Colombia, según las palabras del señor Alberto Samuel Yohai - presidente ejecutivo CCIT, "el cibercrimen ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el país" (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT - Policía Nacional, 2020).

En el mismo sentido, y según el coronel (RA) Fredy Bautista García - Asesor Ciberseguridad TicTac, CCIT y Policía Nacional, “El Cibercrimen actúa de una manera coordinada y dispone de recursos económicos ilimitados provenientes de las ganancias derivadas de actividades criminales previas. El fraude BEC (Los Ataques BEC son una de las principales amenazas a la cadena de suministros, componente fundamental en la actividad diaria de una empresa. Las comunicaciones con proveedores externos y socios de confianza requieren de entornos seguros, que garanticen la integridad de correos electrónicos y servicios de mensajería instantánea utilizados.), los ataques de Ransomware, las oleadas de Malware, las ciberextorsiones, entre otras amenazas, vienen afectando la cadena productiva de las empresas, y por ello es importante conocer las tipologías y modalidades que utiliza el Cibercrimen en Colombia.

Es claro que para enfrentar una amenaza es importante conocer cómo actúa y cuáles son los puntos débiles internos de la organización. Es necesario identificar las vulnerabilidades oportunamente para corregir los fallos en la seguridad e infraestructura, y de esta manera, implementar planes de mejoramiento que abarquen desde los recursos tecnológicos, humanos y del proceso mismo afectado en el incidente presentado. Cuando se conocen las amenazas y los riesgos pueden ser gestionados oportunamente. Desafortunadamente, las organizaciones siguen siendo reactivas y su actuación ante una incidente resulta descoordinada, en parte porque no conocen la problemática o no han definido de manera adecuada, los roles a seguir en la cadena de responsabilidad organizacional establecida” (Tendencia de Cibercrimen en Colombia 2019–2020 – CCIT-Policía Nacional, 2020).

Figura 1. Tendencia del Cibercrimen en Colombia 2019-2020 (CCIT Policía Nacional, 2020)

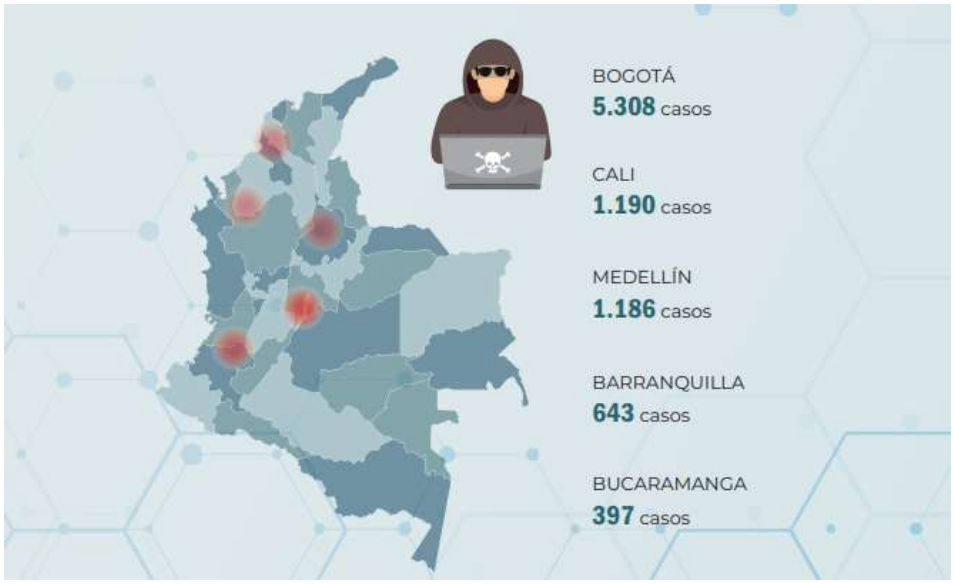


Figura 2. Delitos Informáticos reportados por ciudades - 2019 (Tendencias del Cibercrimen en Colombia 2019-2020 (CCIT Policía Nacional, 2020)

Para la vigencia 2019 se obtuvieron en Colombia los siguientes reportes y datos de afectaciones por delitos informáticos:

A. En los últimos meses el RANSOMWARE "SAMSAM" cobró relevancia en Colombia, porque permite al atacante el robo de contraseñas para el acceso remoto a los dispositivos a través del acceso a credenciales RDP (Remote Desktop Protocol), y de ese modo secuestrar la información de las compañías víctimas. Estos ataques estuvieron dirigidos a entidades o individuos con efectos altamente severos por la complejidad del ataque. SamSam elevó el monto de los rescates al situarlo entre 32 millones de COP hasta más 160 M por ataque. El Ransomware GandCrab mucho más común que SAM SAM exigió rescates a partir de 3 M COP. Todos los rescates se piden en Bitcoin (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT Policía Nacional,2020).

B. Las páginas y demás aplicaciones Web, son activos esenciales para el negocio de muchas empresas en Colombia, pues desde allí se atienden a terceros y clientes o se convierten en las principales plataformas informativas de sus productos y servicios online (eCommerce – Representa el 1,5% del PIB anual en Colombia). En 2019, según cifras del Centro Cibernético Policial, 170 empresas reportaron ataques DDoS que consiguieron interrumpir sus servicios de cara a sus clientes (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT-Policía Nacional,2020).

C. Según INTERPOL, “Acceder a las pretensiones de los cibercriminales sólo contribuye a que estas redes dispongan de más recursos para sofisticar sus ataques. (Interpol,2021).

D. En Colombia, el crecimiento de los ataques de Malware en 2020, fue de 612%. (Tendencia de Cibercrimen en Colombia 2019–2020 – CCIT Policía Nacional, 2020).

E. Millones de dólares es el estimado percibido por la criptominería ilegal al año en Colombia (Fortinet, 2021).

F. El 60% de las pequeñas y medianas empresas no pueden sostener sus negocios más de seis (6) meses luego de sufrir un ciberataque importante. Esto demuestra que los factores en torno a los ataques cibernéticos a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías (Tendencia de Cibercrimen en Colombia 2019–2020 – CCIT Policía Nacional, 2020).

G. Según la OCDE, el 99,5% de las empresas en Latinoamérica y el Caribe, corresponden a micro, pymes y medianas empresas (OCDE, 2021).

PLANTEAMIENTO DEL PROBLEMA

Formulación del Problema de Investigación:

I. Pregunta de Investigación:

¿Cómo cuantificar los efectos, afectaciones y los costos financieros, económicos, comerciales, organizacionales y reputacionales en las empresas que resultan siendo víctimas de ataques informáticos y ciberataques?

II. Antecedentes:

La literatura existente sobre investigaciones relacionadas con el Ciberdelito, es bastante amplia y prolífica. Sin embargo, se han seleccionado aquellas investigaciones de mayor actualidad, relevancia y pertinencia para los fines de este estudio.

1. Metodología para Identificación y valoración de Riesgos y Salvaguardas en una Mesa de Ayuda Tecnológica. Autor: Jeison Nicolás Ruge Pinzón – Universidad Piloto de Colombia (Facultad de ingeniería – Programa de Especialización de Seguridad informática, Bogotá D.C, 2011).

2. Los Delitos Económicos en Internet - Autora: Irene Rodríguez Rodríguez – Universidad Autónoma de Barcelona. (Facultad de Administración y Facultad de Derecho – Trabajo de Grado para Optar por los Títulos de Profesional en Administración y Dirección de Empresas y Profesional en Derecho, Barcelona - España, 2019).

3. The Social Engineering Framework para Aseguramiento de PYME. Autores: Alejandro Correa Sierra y Carlos Andrés Orrego Ossa – Universidad EAFIT (Departamento de Sistemas, Medellín - Antioquia, 2015).

4. El deber de mitigar el daño evitable por parte de la víctima en el ordenamiento jurídico argentino. (Tesis Doctoral) - Autor: Adrián Oscar Mórea – Pontificia Universidad Católica Argentina "Santa María de los Buenos Aires" (Facultad de Derecho y Ciencias Sociales del Rosario – Doctorado en Derecho, Buenos Aires - Argentina, 2015).

5. Los perjuicios inmateriales en la responsabilidad extracontractual del Estado en Colombia. - Autor: Andrés Ricardo Mancipe Gonzales – Pontificia Universidad Javeriana. (Facultad de Ciencias Jurídicas – Carrera de Derecho, Bogotá - Colombia, 2005).

6. Delito Informático: Estafa informática del Artículo 248.2 del Código Penal – (Tesis Doctoral) - Autor: Edmundo Ariel Devia González – Universidad de Sevilla. (Facultad de Ciencias Jurídicas – Doctorado en Derecho, Sevilla - España, 2017).

7. Investigación y Prueba del Ciberdelito – (Tesis Doctoral) - Autora: Josefina Quevedo González – Universidad de Barcelona. (Facultad de Derecho – Doctorado en Derecho y Ciencia Política "Derecho Procesal y Probatorio", Barcelona - España, 2017).

8. Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano – (Trabajo de Grado para Especialista Profesional) - Autores: Balvina Guerrero Lozano y Dirley Piedad Castillo Caicedo – Universidad Nacional Abierta y a Distancia UNAD (Escuela de Ciencias Básicas Tecnología e ingeniería – Especialista en Seguridad informática, Bogotá - Colombia, 2017).

9. Diseño de un nuevo esquema para el procedimiento de indagación de los delitos informáticos - Autores: Aracely del Rocío Cortez Díaz y Cindy Melina Chang Lascano – Universidad Politécnica Salesiana – Sede Guayaquil. (Facultad de Ingenierías Guayaquil Ecuador, 2012).

10. Delitos informáticos - Autora: Agustina Haarscher – Universidad Empresarial Siglo 21. (Facultad de Abogacía Córdoba Argentina, 2012).

JUSTIFICACIÓN

Esta investigación se planteó debido a la necesidad de contribuir a la consolidación, referenciación y la intención de ofrecer un apoyo técnico valido y basado en estándares internacionales que permitieran a todas las partes interesadas poder cuantificar las afectaciones que sufren las empresas por delitos informáticos o ciberataques, desde los puntos de vista económico, financiero, administrativo, comercial y reputacional.

Dada la inexistencia de este tipo de metodología, que valorara las afectaciones dificultaba el resarcimiento real del daño informático y complicaba la aplicación del derecho probatorio, el derecho penal. Es decir, era imposible y muy complicado realizar la cuantificación económica del daño informático ocurrido.

De la misma manera, afectaba y limitaba las aplicaciones, reclamaciones y los pagos de las pólizas de seguros que aseveran el patrimonio de las empresas, en cuanto a información, datos, metadatos, infraestructura, imagen corporativa y empresarial afectados por ciberataques en las empresas, a nivel nacional e internacional.

Igualmente, la proliferación de diferentes tipologías de ciberdelitos, dado el auge del uso del Internet y las Tics en todos los ámbitos de la sociedad global, pero también los vacíos teóricos y uniformes para castigar, prevenir y penalizar el delito informático, son razones que justifican esta investigación.

Lo anterior debido a que en el sector de la información y las comunicaciones (CiberSociedad), se vienen presentando cada vez nuevos y sofisticados ataques informáticos

o ciberataques. Una tendencia que aumenta como consecuencia de que muchas empresas a nivel nacional e internacional no son conscientes de lo que significa en términos económicos, financieros y de gastos ser víctima de estos ciberataques.

Algunas de las pocas organizaciones que están tomando conciencia de los graves riesgos y costos de estos ciberataques, se ven obligadas a hacer unos gastos altos la implementación de planes y políticas de seguridad informática para prevenir o mitigar los riesgos y las vulnerabilidades que puedan tener al interior de sus empresas e infraestructuras tecnológicas. No obstante, apoyados en algunos gastos económicos, tales planes no le permiten contar con una seguridad informática al cien por ciento por lo que siguen siendo víctimas de los ciberdelincuentes.

Al presentarse estos ciberataques, existen leyes a nivel nacional y algunas con aplicación internacional que permiten judicializar a los atacantes en caso de ser detectados y capturados, pero al momento de evaluar los daños causados y cuantificar las afectaciones económicas y financieras que sufrieron las empresas víctimas, no existía una metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa, tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos.

En este sentido, se realizó y se estructuró el presente documento, permitiendo suplir en el país, esa carencia de una metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos.

Viabilidad:

Esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, es de gran utilidad para todas las partes interesadas definidas en este proyecto. Se trata de una metodología posible de implementar, con gran aplicabilidad, pertinencia y requerimiento, es decir, posee una gran y pertinente viabilidad técnica, financiera, administrativa, de aplicación de justicia y para real resarcimiento del daño informático. De la misma manera, se convierte en una excelente guía para juristas, abogados, jueves, peritos de aseguradoras y para todas las empresas como tal, sobre todo para sus gerentes, juntas directivas, cisos y cios organizacionales, que deben velar por la productividad y la generación de valor institucional y corporativo, en sus empresas a cargo.

En resumen, este proyecto reúne y cumple, todas las características, condiciones técnicas y operativas que aseguran el cumplimiento de sus metas y objetivos.

Consecuencias del estudio:

Los efectos para la empresa, institución u organización afectada y atacada por delitos informáticos o ciberdelitos, pueden ser de diferente índole, impacto o gravedad. Y si se tiene en cuenta que no existen métodos, lineamientos o metodologías para cuantificar de manera científica, real y basado en estándares internacionalmente, tales afectaciones económicas, financieras y reputacionales pueden ser nefastas, como quiera que para algunas de estas empresas afectadas puede significar su desaparición o cierre total.

Esta metodología se creó para apoyar a todas las empresas, instituciones y corporaciones ~~a~~ con el fin de tener un apoyo técnico valido y así poder definir cuál es su real valoración de

las afectaciones y para de manera proactiva, conocer los valores reales por los cuales asegurar sus activos tangibles e intangibles en la organización.

Además, este proyecto y su producto llega y se pone a disposición de todas las partes interesadas para:

- Suplir la ausencia de criterios para valoras los bienes y activos tangibles y no tangibles de las empresas y organizaciones víctimas de ataques informáticos o ciberataques.
- Conocer previamente y de manera proactiva, cuáles serían los reales impactos y afectaciones desde el punto de vista económico, financiero, comercial y reputacional que pueden afectar a una empresa si llegase a ser víctima de ciberataques. Esto con el fin de asegurar sus bienes y activos tangibles e intangibles por los valores reales y por lo que apoya la valoración de la empresa u organización.

De igual manera podrá ser tenido en cuenta el producto de la aplicación de esta metodología para poder tomar decisiones sobre los montos y valores a invertir en protección de los niveles de seguridad y ciberseguridad en las organizaciones. Esto como información fidedigna para la toma de decisiones por parte de los gerentes y los encargados de la ciberseguridad en las organizaciones.

- Convertirse en una herramienta para peritos, jueces, fiscales, juristas, abogados litigantes, abogados corporativos que requieran que los daños y las afectaciones por

delitos informáticos, sean realmente resarcidas en el mismo grado de la afectación ocurrida y/o proporcionales.

- Ayuda a los peritos y profesionales de las aseguradoras a reforzar este producto de su mercado objetivo, para que den a conocer de manera real, valida y científica las afectaciones a las que se exponen las empresas si no cuentan con pólizas de seguros que respalden o salvaguarden sus bienes o activos en sus empresas y organizaciones.

En general, son varios los usos, utilizaciones y aportes que realiza este proyecto a la sociedad en general, sobre todo a las empresas, organizaciones, instituciones, Estado, y a los poderes judiciales de los países.

OBJETIVOS

GENERAL

Estructurar una metodología fundamentada en estándares internacionalmente reconocidos, para cuantificar las pérdidas económicas, financieras y reputacionales de una empresa, tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

ESPECÍFICOS

• Explicar el impacto empresarial, social, económico y financiero que se presentan en una empresa a nivel nacional e internacional, al ser víctima de un ataque informático.

• Describir los niveles y tipos de ataques informáticos que afectan a las empresas pública y privadas a nivel nacional e internacional.

• Diagnosticar el grado de conciencia en cuanto a ciberseguridad y seguridad informática, presentes en los directivos y empleados de las empresas publica y privadas a nivel nacional e internacional.

• Clasificar las afectaciones en que incurren las empresas y/o Instituciones empresa a nivel nacional e internacional afectadas por ciberataques.

MARCO TEÓRICO O MARCO CONCEPTUAL

La elaboración esquemática, la definición y creación de esta la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos es producto de la revisión, consulta y evaluación del acuerdo documental con sus correspondientes productos, los cuales se citan como núcleos del estudio. Como fundamentos base para la investigación de este trabajo de grado, se tuvieron en cuenta los siguientes conceptos:

METODOLOGÍA: Según la Universidad de Oxford y sus definiciones de Oxford Languajes, la metodología hace referencia al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos (Oxford, 2012).

La metodología (del griego μέθοδος de μετά metá 'más allá, después, con', οδως odós 'camino' y λογος logos 'razón, estudio'), hace referencia al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Con frecuencia puede definirse la metodología como

el estudio o elección de un método pertinente o adecuadamente aplicable a determinado objeto.

La metodología es una de las etapas específicas de un trabajo o proyecto que parte de una posición teórica y conduce una selección de técnicas concretas (o métodos) acerca del procedimiento destinado a la realización de tareas vinculadas a la investigación, el trabajo o el proyecto.

En la descripción de una metodología adecuada, la postura filosófica se orienta mediante términos como los siguientes:

Racionalismo: En oposición al empirismo, acentúa la función de la razón en la investigación

Pragmática: Es la manera en que los elementos del proyecto influyen en el significado.

Constructivismo o constructivismo epistemológico: En el que el conocimiento se desarrolla a partir de presunciones (hipótesis de partida) del investigador.

Criticismo: También de orden epistemológico, que pone límites al conocimiento mediante el estudio cuidadoso de posibilidades.

Escepticismo: Duda o incredulidad acerca de la verdad o de la eficacia de lo generalmente admitido como válido.

Positivismo: Derivado de la epistemología, afirma que el único conocimiento auténtico es el saber científico.

Hermenéutica: Que interpreta el conocimiento (Herrman, 2009).

ATAQUE INFORMÁTICO: De acuerdo con la aseguradora “Caser Seguros”, un ataque informático es un intento de acceder a los equipos informáticos o servidores, mediante la introducción de virus o archivos malware, para alterar su funcionamiento, producir daños o sustraer información sensible para la empresa.

Cuando se habla de un ataque informático se hace referencia a la realización de una tentativa de poner en riesgo la seguridad informática de un equipo o conjunto de equipos, con el fin de causar daños deliberados que afecten a su funcionamiento.

El desarrollo de estos ataques informáticos, o ciberataques, suele provenir de terceras personas, ajenas al negocio, mediante el envío de virus o archivos malware, diseñados específicamente para burlar las medidas de seguridad de tus equipos y/o servidores, para conseguir, alterar o dañar información sensible para la empresa (Caser, 2019).

Según “Global Finanz” (Consultora de riesgos y corredora de seguros), un ataque cibernético es una acción delictiva y malintencionada que se realiza para acceder a información privada, bien para apropiarse de ella o para inutilizarla y pedir dinero a cambio de liberarla.

Detrás de estos ataques cibernéticos están delincuentes informáticos, hackers, organizaciones criminales, entre otros, cuyo objetivo es apropiarse de la información o extorsionar a la empresa o persona atacada. Cualquier empresa que almacene, manipule o transmita datos se encuentra expuesta a un ciberataque (Global Finanz, 2018).

Según Evilfingers, un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático. Esto con el fin de obtener un beneficio, por lo general de índole

económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización (Evilfingers, 2009).

Los ataques informáticos son la principal fuente de robo de información. En este sentido, cuando un atacante decide realizar una acción puede elegir entre algunos métodos como:

- Interrupción: el ataque provoca un corte en la prestación de un servicio: el servidor web no está disponible, el disco de red no aparece o solo permite leer (no escribir), etcétera.
- Interceptación: el atacante logra acceder a comunicaciones y copia información que es transmitida.
- Modificación: el atacante accede, pero en lugar de copiar información, la modifica para que llegue alterada al destino y provoque alguna reacción anormal. Por ejemplo, cambiar las cifras de una transacción bancaria.
- Fabricación: el atacante se hace pasar por el destino de la transmisión, por lo tanto, conoce el objetivo de la comunicación, y engañar para obtener información valiosa, etcétera (Buendía, 2013).

SEGURIDAD INFORMÁTICA: Según Álvaro Gómez, en su obra Enciclopedia de la Seguridad Informática, define este concepto como: “Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos

puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema" (Ceupe, 2018).

Solamente cuando se es consciente de las potenciales amenazas, agresores e infecciones dañinas (directas o indirectas) en contra de una empresa u organización, se logra tener un control de los ataques. Para lograrlo es fundamental conocerlos y clasificarlos con el fin de tomar las medidas de protección adecuadas para evitar pérdidas o daños de recursos o pérdida de información valiosa.

La seguridad informática se encarga de proteger la confidencialidad, integridad, privacidad y disponibilidad de la información almacenada en un sistema informático.

- ✓ Confidencialidad: Asegura que únicamente puede acceder a la información y modificarla los usuarios autorizados comprendiendo la privacidad (protección de los datos personales).
- ✓ Integridad: Certifica que tanto la información como los métodos de proceso son exactos y completos asegurando que los datos no se han falseado.
- ✓ Disponibilidad: Acceso garantizado a la información en el momento en que sea requerida a los usuarios autorizados.

Algunos investigadores y autores especializados en el tema de seguridad informática comúnmente se centran solo en las tres características ya mencionadas. No obstante, de

acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de las tecnologías de la información de la empresa, las características además de la confidencialidad, integridad y disponibilidad son: efectividad, eficiencia y apego a los estándares.

Efectividad: Consiste en lograr que la información sea en realidad la necesaria para desarrollar cualquier tarea que la empresa u organización requiera. Además, debe ser adecuada para realizar los correctos procesos de la institución, proporcionándola de manera oportuna, correcta, consistente y accesible.

Eficiencia: Alude a que la información sea generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin.

Apego a estándares: Significa que en el procesamiento de la información se deberán acatar las leyes de uso general o reglamentos y acuerdos internos y contractuales a los cuales está sujeto el proceso de negocio.

Tipos de seguridad informática. Inicialmente hace referencia a dos tipos de seguridad teniendo en cuenta los recursos que se buscan proteger:

Seguridad física: establece la protección física del sistema ante amenazas como inundaciones, incendios, robos, entre otros.

Seguridad lógica: protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.

Existen también tipos de seguridad que hacen referencia al momento en que la

protección tiene lugar:

Seguridad activa: previene, detecta y evita cualquier incidente en los sistemas informáticos antes de que se produzcan (prevención). Por ejemplo, uso de contraseñas.

Seguridad pasiva: técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (corrección). Por ejemplo, copias de seguridad.

Así mismo, se tienen tipos de seguridad informática de acuerdo con los elementos

sobre los cuales se aplicará.

a. Seguridad de hardware: se refiere a la protección de computadoras o dispositivos frente a intromisiones o amenazas.

b. Seguridad de software: se encarga de la protección de las aplicaciones y el software de amenazas exteriores como ataques maliciosos, virus, etcétera.

c. Seguridad de red: se encarga de proteger toda la información que está accesible a través de internet (documentos, imágenes, datos bancarios) y que podrían ser usada de forma mal intencionada. Es quizás una de las más complejas de gestionar ya que un ataque a un equipo conectado a la red, propagará por la misma a otros equipos si la red no cuenta con los medios de protección necesarios.

CIBERESPACIO: La creación del término ciberespacio se atribuye a William Gibson, quien ~~la~~ utilizó por primera vez en un relato de 1981, haciendo alusión al conjunto de redes electrónicas, como un lugar de tránsito, hallazgos y encuentros. Utilizó el término en su novela Neuromante, la primera obra de su Trilogía del Ciberespacio, aunque en realidad, esta

palabra apareció por primera vez en un relato corto del mismo autor: Quemando Cromo. Sin embargo, el término no tiene verdadera importancia hasta que John Perry Barlow, que fue letrista de Grateful Dead y activista pro-derechos civiles en la red (fundador de EFF), empieza a utilizarlo para definir al espacio de relación virtual generado por Internet. Barlow pudo identificar lo que era imaginado como un metaverso con una realidad nueva por la que la sociedad y los medios de comunicación se preguntaban.

Se llama ciberespacio a un mundo no físico, el cual no tiene límites, donde cualquier persona puede estar interconectada únicamente con la red de tal manera que puede interactuar con el mundo entero sin barreras. El término ciberespacio no debe confundirse con Internet real, el cual se refiere generalmente a los objetos y recursos que coexisten en la misma red informática. Es decir, los hechos que ocurren en Internet, en el ciberespacio y no en los países donde los usuarios están, teniendo en cuenta que sí puede repercutir en los ideales sociales. Los usuarios que navegan por ciberespacio se llaman cibernautas y generalmente pasan varias de horas al día en esta actividad.

En la actualidad, el concepto de ciberespacio suele asociarse a Internet. Todo aquello que se desarrolla en Internet, a través de sitios web, correos electrónicos, redes sociales, entre otros, no tiene lugar en un país específico, más allá de la ubicación concreta de los servidores y de los usuarios. El ciberespacio, de todos modos, es más amplio que Internet.

Si se observa el aspecto de la legislación en el ciberespacio, esta regulación legal suele ser motivo de conflicto debido a las propias características virtuales de este ámbito. Los gobiernos tienen dificultades para imponer sus leyes y, de esta manera, los delitos que se cometen en este entorno son difíciles de perseguir y de juzgar. Pese a ello, muchos activistas

defienden la independencia y la autonomía del ciberespacio, exigiendo que las autoridades estatales no ejerzan controles ni cometan actos de censura.

Características: Falta de seguridad de la identidad- Es muy común en el ciberespacio utilizar identidades falsas para poder ejercer actos con los cuales no puedan ser reconocidos.

No tiene límites fronterizos, comunicación sincrónica o asíncrona. Se tiene la misma oportunidad de comunicación, dimensión más accesible económicamente que otros canales de difusión, toda sensación y percepción, está medida por aparatos (pantallas, altavoces, etcétera.), y presenta infinidad de posibilidades.

La importancia del ciberespacio radica en que se ha creado un ámbito donde la información se comporta libremente, siendo accesible un número de personas bastante mayor y donde existen canales de comunicación variados con distintas formas de ver todo. El ciberespacio ha desarrollado una enorme productividad desde el punto de vista económico, como también ha significado una enorme promesa para el futuro. En efecto hoy en día es posible trabajar desde muchos sitios y con toda la información necesaria al instante. El contacto inmediato a un costo bajísimo es otro de los factores por los cuales el mundo virtual ha cambiado el mundo real.

Muchos autores definen a su manera el ciberespacio, como se puede detallar a continuación:

“Nadie puede hacer el bien en un espacio de su vida, mientras hace daño en otro. La vida es un todo indivisible” (Mahatma Gandhi).

“El ciberespacio es una alucinación social consensuada. La matriz tiene sus raíces en las primitivas galerías de juego, en los primeros programas gráficos y en la experimentación militar con conexiones craneales” (William Gibson).

El teniente coronel del Ejército de Tierra destinado en el Mando Conjunto de Ciberdefensa, Manuel Saz, asegura que “no todo lo que ocurre en ciberespacio es ciberguerra, sino que muchas de las acciones van asociadas a cibercrimen, ciberespionaje o activismo”.

Lisa Mónaco, informó de la creación de la nueva agencia en un discurso en el Centro Wilson, en Washington, en el que alertó que las amenazas cibernéticas contra EE.UU. son cada vez más “diversas, sofisticadas y peligrosas”.

El ciberespacio hoy en día junto con el avance a grandes pasos de las nuevas tecnologías supone una amenaza para cualquier país y se ha convertido en un ámbito más donde las naciones pueden pelear por sus intereses, por tanto, deben estar preparados.

En España, la ciberseguridad se ha convertido en una de las grandes obsesiones de la seguridad del Estado. El crecimiento de la actividad criminal en la red va en aumento. Cada año las cifras se duplican o triplican. En el marco de la ciberdelincuencia, lo que más preocupa al Ministerio del Interior y al Ministerio de Industria es la seguridad de las denominadas infraestructuras críticas (infraestructuras estratégicas para el buen funcionamiento del Estado). La Secretaría de Estado de Seguridad, se detecta un potente crecimiento en los ataques localizados y rechazados contra estas estructuras, lo cual ha motivado la puesta en marcha de mecanismos con los cuales hacerle frente. La Oficina de Coordinación Cibernética ejerce permanentes labores de control ante estas amenazas.

En Estados Unidos tras los atentados del 11-S el Gobierno, anunció la creación de una nueva agencia centrada en las amenazas cibernéticas. Precisamente, una de las prioridades de seguridad nacional de la Casa Blanca, cuya tarea será reunir y analizar información de inteligencia para tratar de evitar ese tipo de ataques. La nueva entidad, denominada Centro de Integración de Inteligencia contra la Amenaza Cibernética (CTIIC, por sus siglas en inglés), no recolectará información de inteligencia, sino que reunirá y analizará la recopilada por otros servicios gubernamentales para detectar amenazas cibernéticas y prevenir ataques.

Internet igualmente se ha transformado en una nueva herramienta de socialización que puede ayudar a niños más tímidos, por ejemplo. Con este medio pueden hacer amigos de otras partes, mantener contacto con familiares o seres queridos que se encuentran lejos o pertenecer a grupos en los que se comparten intereses comunes. Hace mucho más rápido y entretenido el proceso de aprendizaje. Los escolares de hoy tienen acceso instantáneo a fuentes confiables y actualizadas con contenidos mucho más didácticos. Además, el espacio virtual permite que los niños estén conectados y hagan trabajos o tareas en línea o compartan información.

El ciberespacio sobrepasa los límites de cómo y cuándo interactuar y presenta las siguientes características:

Identidad, flexibilidad y anonimato: la falta de interacción física cara a cara causa un impacto en cómo la gente presenta su identidad, pues se tiene la oportunidad de expresar sólo alguna faceta de identidad o quizás quedarse en el anonimato, incluso puedes tener con una identidad imaginaria o falsa.

En el ciberespacio todos tienen la misma oportunidad de comunicación, por lo que algunos llaman a esto Democracia Net.

Trasciende los límites espaciales: Las distancias geográficas no limitan quién pueda comunicarse con quién. Alguien puede comunicarse con cualquier persona que esté en otro país.

Tiempo extendido y condensado: puede haber una comunicación con cualquiera vía internet, puede haber varias personas sentadas en su computadora al mismo tiempo. Este tipo de comunicación crea un espacio temporal donde el estar, como tiempo interactivo se extiende. Se tiene tiempo para pensar cosas y dar una respuesta (Ecured, 2018).

CIBERSOCIEDAD: La cibersociedad constituye un privilegiado escenario postmoderno en donde se puede visualizar la interconexión y fusión de ciertos componentes arquetípicos con las últimas manifestaciones de la cultura tecnológica. Efectivamente, es posible entender los medios de comunicación como prolongaciones del hombre.

La cibersociedad está comúnmente relacionada con la sociedad de la información, por lo que algunos autores definen a la cibersociedad o sociedad de la información como:

La idea de esta nueva sociedad que surge con el impulso de los avances tecnológicos tiene ya medio siglo de historia, de anticipaciones y estudios (un excelente resumen de esta arqueología de la "sociedad de la información" hecho por Armand Mattelart puede verse en Le monde diplomatique, edición española, número de setiembre de 2000).

Para algunos, el primer paso de esta nueva sociedad lo habría dado un estudiante de matemáticas en Cambridge, Alan Turing que en 1936 con 24 años publicaba un sonado

artículo donde explicaba las condiciones de una máquina teórica que pasaría de un estado a otro siguiendo un conjunto de reglas establecidas. Esta "máquina de Turing" condujo a un proyecto informático que presagiaba la estructura lógica de la "máquina inteligente" de Von Neuman de los años cuarenta, considerada por algunos como el primer ordenador de la historia e igualmente la de los modernos ordenadores digitales.

En la década de los sesenta las teorías de Marshall Mc Luhan sustentan lúcidas predicciones sobre la futura sociedad unificada de la aldea global. Por su parte, Alain Touraine en la sociedad postindustrial y Daniel Bell en el advenimiento de la sociedad postindustrial avanzan características ya propias de esta nueva sociedad que Zbniew Brzesinsky, consejero del presidente americano Carter, dando un paso más y apuntando al decisivo peso de las tecnologías, tipifica como la era tecnotrónica.

A finales de los setenta y comienzo de las ochenta otras voces surgidas en el campo de la sociología describen los contornos de la nueva sociedad. Por ejemplo, James Martin en la sociedad interconectada (1978) o Yonehi Masuda en la sociedad informatizada como sociedad post-industrial (1980) que predice una red del conocimiento que bien pudiera ser la actual Internet. Alvin Toffler, por su parte, divulga y populariza estas ideas con su best-seller La Tercera Ola (1978) que pone al alcance de los lectores los aspectos más brillantes de la nueva sociedad.

Es en ese tiempo también cuando importantes autores (Mattelart, Schiller o Chomski) presentan los primeros estudios y análisis que matizan críticamente el triunfalismo tecnológico de los cantores de la nueva sociedad. La UNESCO otorga su espaldarazo a tales críticas, avalando en 1990 el llamado "informe Mac Bride", (Un sólo mundo, voces múltiples.

Comunicación e información en nuestro tiempo) del premio nobel de la paz, el irlandés Sean Mac Bride. En su dossier se plantean serios interrogantes y la necesidad de construir un nuevo orden informativo, el NOMIC (Nuevo Orden Mundial de la Información y la Comunicación) que supere las desigualdades de los países y contribuya a un desarrollo verdaderamente humano. La UNESCO, sin embargo, no consigue imponer los valores del humanismo y de los objetivos sociales ante la avasalladora filosofía de mercado que, preconizada por Estados Unidos, se va a imponer por todo el mundo como pensamiento único (Ramonet, 1996, 1997).

En 1993 Washington lanza el "plan tecnológico americano" conocido como Plan Gore (encabezado por el vicepresidente Al Gore que acuña el término de "autopistas de la información", "information superhighway"). Europa, en la estela de los norteamericanos, apuesta abiertamente por ese tipo de sociedad en 1994 con el Libro Blanco de la Comisión Europea, del presidente Delors, crecimiento, competitividad, empleo, retos y pistas para entrar en el siglo XX refrendado y presentado al Consejo Europeo ese mismo año en Corfú por el llamado "Informe Bangemann" ("Europa y la Sociedad Global de la Información").

En esa última década del siglo, científicos y teóricos de Sillicon Valley, propagandistas y predicadores de la "sociedad de la información" ocupan tribunas de congresos y conferencias y protagonizan best-sellers de librerías. Nicholas Negroponte (El mundo digital) Bill Gates, (Camino al futuro), Dertouzos, Terceiro, Alvin Toffler y toda una pléyade de apologetas de las nuevas tecnologías, suscritas de forma entusiasta en amplios sectores académicos, refuerzan así el discurso de pensamiento único de los llamados global líderes que dominan el mundo.

Aun a riesgo de especular sobre algo tan complejo y en movimiento como las nuevas tecnologías es importante situarse ante ellas y su criatura predilecta, la "sociedad de la información", describiendo rasgos y características significativas de la misma. Estas podían ser:

-La información base de la economía.

-Cambios en la información.

-Un mundo digitalizado.

-El imperio de las redes y flujos.

-Una vida globalizada (fronteras y límites difusos con la economía de marcado a los mandos).

-Internet, corazón de la sociedad de la información.

-Una sociedad distinta (nuevo orden social).

Podrían resumirse en dos estas características; lo informativo (base de la economía, nuevo concepto de información) y lo digital (redes, globalización, internet) y como consecuencia, la nueva sociedad que surge, sociedad de la información o cibersociedad.

Algunos analistas van más allá de las cautelas de la UNESCO para poner la llaga en las sombras del brillante panorama que dibujan los globals líderes de la comunicación. Se trata de un pensamiento crítico que tiene sus puntas de lanza en autores como Mattelart, Schiller (Herbert y Dan), Dieterich, Chomsky, Sartori, Serge Halimi, Bourdieu, et. y en España Fernández Quirós, Bustamante, Murciano, entre otros. Muchos de ellos se agrupan en el

entorno de "Le Monde Diplomatique" que dirige Ramonet, donde publican con regularidad interesantes análisis críticos.

Señalan que ante las nuevas tecnologías se propaga un discurso de caracteres míticos que no se sostiene a la hora de comprobar la validez de los mismos. Denuncian, entre otros, los siguientes estereotipos atribuidos a las sociedades de la información:

- Que el fin de las desigualdades vendrá a través de la interdependencia en una globalidad en la que no existe centro, ni periferia y que la libre apertura al mercado de la información trae el fin de las desigualdades entre los países y entre las clases, proporcionando a toda igualdad de oportunidades y promocionando una verdadera democracia.
- Que las multinacionales son agentes revolucionarios en un mundo conservador y que en el mercado libre constituyen una potencia progresista ante la inercia de los estados, fuerza anti creadora y fuente de todos los problemas y conflictos.
- Que la tecnología, electrónica, la digitalización es capaz de cambiar el mundo y resolver todos los problemas y que la tecnología sería algo totalmente neutral.
- Que la abundancia y superabundancia de la información a través de los nuevos canales tecnológicos produce mayor cultura, mejor y mayor conocimiento.
- Que en las sociedades contemporáneas la gente se dedica cada vez más a tareas que tienen que ver con la información.
- Que la sociedad de la información produce automáticamente abundancia de bienes.
- Que las máquinas piensan como el ser humano (mito de la inteligencia artificial).

"A pesar de que hoy es bastante corriente escuchar a los teóricos de las relaciones internacionales que los modelos centro-periferia, la teoría de la dependencia o la teoría del imperialismo han quedado borrados del mapa por la realidad de la globalización, el perfil del sistema internacional tiene ahora diferencias todavía más lacerantes que en etapas anteriores. Eso sí, las diferencias pueden maquillarse mucho mejor gracias a la explosión de los nuevos medios de información". Esta dura reflexión del profesor Fernández Quirós (1998, 18) desmiente ese pretendido fin de las desigualdades o la potencialidad democratizadora que aportarían las nuevas tecnologías y la sociedad de la información. La realidad, en cambio, parece mucho más prosaica y remite a parámetros menos optimistas.

En realidad, en casi 20 años de revolución tecnotrónica:

- El sistema global de comunicaciones sigue teniendo un centro de poder principal: Estados Unidos, relacionado con los otros centros de poder económico mundial como la Unión Europea y Japón, al modo de los viejos imperios coloniales, jerarquizado por la propia tecnología.
- No son los grupos sociales los que controlan las redes de comunicación. Las grandes empresas transnacionales de la electrónica son las nuevas plutocracias de la aldea global. Como en la plutocracia clásica, son los más ricos los que gobiernan la nueva nación planetaria.
- El acceso al conocimiento está muy lejos de ser universal. Es precisamente la transferencia de la tecnología desde la plutocracia al conjunto del sistema, la que garantiza la existencia de varios escalones en el desarrollo tecnológico. Al eludir toda referencia al control de las redes de información, se esconde el hecho de que el acceso

al conocimiento y a la investigación no es universal. Se suman así a las viejas desigualdades, nuevas diferencias que se producen entre conectados y no conectados, entre emisores y no emisores etcétera.

- El Tercer mundo no sólo no ha iniciado despegue alguno, sino que se hunde cada vez más en la miseria. Se han incrementado las diferencias entre la opulencia y la precariedad informativa. Cuanto mayor es el poder económico, mayor es el poder informativo y viceversa.
- Cada etapa del proceso tecnológico ha producido un nuevo grado de concentración. Más que de consenso planetario habría que hablar de mercado planetario controlado por la plutocracia tecnotrónica.
- La concentración transnacional de la propiedad multimedia que controla toda innovación tecnológica hasta apropiársela es una característica fundamental de la sociedad de la información. La invasión de los mercados nacionales por las empresas transnacionales en países desarrollados intermedios reduce la democracia informativa pero la economía no se ve gravemente perjudicada. Sin embargo, en el Tercer Mundo han terminado por solaparse la revolución industrial y tecnológica, agravando el problema de la dependencia.

Por otra parte, hay que advertir que el pensamiento teórico de la sociedad de la información está construido en y desde la perspectiva de los países súper-desarrollados, ignorando y ocultando la real "aldea global" de cinco continentes con tres cuartas partes malviviendo en la incultura la miseria y el hambre e incluso las bolsas de pobreza y marginación de primeros

mundos como Estados Unidos. No se exime de culpa una perspectiva europea pretendidamente progresista que mientras denuncia agriamente la intrusión del mercado americano, pugna por introducir sus productos en el tercer mundo. Es el caso de los que se presenta como áreas y modelos de cultura, (francesa en África o castellano-española en América del Sur), pudorosas tapaderas del imperialismo empresarial de los estados (negocios en ultramar de Telefónica o France Telecom).

En cuanto al entusiasmo tecnófilo respecto a las virtudes democratizadoras de la globalización de lo digital no habría que hacerse demasiadas ilusiones. Serge Halimi (Le monde Diplomatique, septiembre, 2000) se pregunta si nos encontramos ante nuevos espacios de democracia o ante nuevas segregaciones y critica la euforia de algunos "cyberresistentes" y a propósito de Internet recuerda el viejo discurso de las "radios libres", "cuya génesis asociativa -dice- no resistió demasiado tiempo las tentaciones mezcladas de los ingresos publicitarios y la entrada en Bolsa".

Los críticos denuncian el uso y abuso de la palabra globalización, convertida en el concepto de moda en esta época y cuya cita se hace necesaria cuando se refiere a las características distintivas de la sociedad respecto a otros momentos históricos. Como todos los lugares comunes y tópicos, la globalización corre el peligro de querer explicarlo todo sin explicar, en el fondo, nada. Se le pone el nombre a una realidad (globalización) que no ayuda a aprehender lo que describe. En este caso, el lenguaje, más que ayudar a descubrir la realidad, lo que hace es encubrirla, volverla opaca, inaccesible, hacer pasar por obvio y conocido por todo el mundo lo que en realidad es complejo y requiere de una aproximación muy afinada.

En cuanto al último informe del Programa de Naciones Unidas para el Desarrollo (PNUD) de 1999, concluía de la siguiente manera: "Por el momento, Internet beneficia sólo a los individuos relativamente acomodados e instruidos: el 88% de los internautas vive en los países industrializados que, en su conjunto, apenas representan el 17% de la población mundial. Las personas que están "enganchadas" disponen de una ventaja aplastante sobre los pobres que no tienen acceso a esos medios o que, en consecuencia, no pueden hacer oír sus voces en el concierto mundial. Las redes mundiales enlazan a quienes tienen los medios y, silenciosamente, casi imperceptiblemente, excluyen a todos los demás" (PNUD, Rapport mondial sur le développement humain 1999. De Boeck Université, Paris-Bruselas, 2000).

Otro mito que no se tendría en pie según estos críticos es el referente a que la abundancia y superabundancia de información a través de los nuevos canales tecnológicos significa y produce mayor cultura, mayor y mejor conocimiento.

Ignacio Ramonet ha desarrollado extensamente el tema de la información de hoy en su obra La Tiranía de la Comunicación. Explica que la información se caracterizaría actualmente por tres aspectos: La superabundancia, el ritmo extremadamente rápido saltando tiempo y espacio y el cambio de criterios sobre el concepto de información entre los que ya no cuenta la veracidad o la verdad. Asegura que hoy se cuestiona la misma idea de la información. Hasta hace poco informar era, no solo proporcionar la descripción precisa -y verificada- de un acontecimiento, sino también aportar un conjunto de parámetros contextuales que permitieran al lector comprender su significado profundo. La información era conocimiento, responder a cuestiones básicas; ¿quién ha hecho qué?, ¿con qué medios?, ¿dónde?, ¿por qué?,

¿con qué consecuencias? En España el porcentaje de personas con acceso a Internet se situaba a finales del 2001 en el 21,2% de la población.

A este tipo de porcentajes, por lo demás no muy solventes estadísticamente, suele dársele un gran relieve cuando lo cierto es que el déficit principal y más grave viene por el flanco del conocimiento. Se trata de un conocimiento que tiene mucho que ver que, con Internet, con que el presupuesto total anual destinado a la investigación no llega al 1% del PIB, menos de la mitad de varios países europeos y sobre todo el poco aprecio y valoración en el que se tiene a la cultura.

Se daba por supuesto, por otra parte, que informarse era buscar y hallar la verdad. Hoy, sin embargo, se habría modificado ese concepto directamente relacionado con el conocimiento y lo que es más grave, con la veracidad. La ecuación información=verdad=libertad=democracia se habría venido abajo. Por el contrario, esos criterios habrían dejado de primar en beneficio de otros muy distintos. Actualmente, no se pregunta si la noticia es verdad o mentira. La información, en cambio, está marcada por el imperio del mercado, el de la imagen y de la emoción. La noticia vende. Es una pieza de la economía de mercado y se rige por sus normas. La información es una mercancía. Solo importa si emociona, si impacta, si vende.

Por otra parte, la información estaría cada día más supeditada a la inmediatez y a la plasticidad de la imagen. La optimización de los contenidos ahora es la instantaneidad (el tiempo real), el directo, que hasta ahora sólo podía ser ofrecido por la televisión y la radio.

Insidiosamente se han establecido así nuevas ecuaciones informacionales. Por ejemplo, la que se refiere al grado de emoción que puedan generar determinadas imágenes o sonidos.

Se funciona con la convicción de que basta ver para comprender. De esta forma informar es hacer asistir, si es posible en directo, al acontecimiento. La sociedad actual concede a la televisión el papel piloto en materia informativa ¿Cuál es la actualidad hoy? Lo que la televisión o la radio dicen que es actualidad. La prensa, desbordada, intenta seguir el paso de lo audiovisual en vez de buscar su sitio propio, acuciada por las presiones del mercado. Hay que vender. Este es la dura descripción y diagnóstico de Ramonet.

Lo cierto es que, en el nuevo orden de los más media, de la comunicación de masas, las palabras o los textos no valen lo que las imágenes. Es lo audiovisual lo que cuenta con toda su carga de distorsión, trivialización etcétera, tal como denuncian Sartori, Bourdieu, Gubern, Colombo, Baudrillard. Sin embargo, ver no es comprender. Querer comprender, informarse sin esfuerzo es una ilusión, dice el mismo Ramonet, director de Le monde diplomatique en cuya propaganda, se subraya significativamente; "Cuando todos los medios parecen dejarse llevar por la velocidad, la aceleración, la fascinación por la instantaneidad del "tiempo real", en Le Monde diplomatique se dice que lo importante, por el contrario, es reducir la velocidad, frenar un poco, darse el tiempo necesario para analizar, dudar, reflexionar. No aceptar que la "actualidad" nos sea definida por la televisión y los grandes medios en función de intereses puramente dramáticos".

La sobreabundancia de información, por otra parte, es una inquietante realidad. Hasta hoy se tenía como un axioma indiscutible que, a mayor información, mejor conocimiento. No obstante, la abundancia de información no sólo significa mayor y mejor información, sino

que esa abundancia funciona a veces como un biombo opaco que hace más dificultosa la búsqueda de la buena información. El ejemplo, ya clásico, de lo anterior se aprecia en la Guerra del Golfo, donde se ofreció una gran cantidad de imágenes, sometidas a estricto control de las autoridades militares norteamericanas, lo que provocó que los espectadores "creyesen" que estaban viendo la guerra; cuando en realidad solo veían los segmentos de la guerra que el Alto Mando Norteamericano quería que viesen.

Esta sobreabundancia de información, en vez de contribuir al conocimiento, se convirtió en auténtica desinformación. Y es que, ante la avalancha de informaciones, imágenes (emociones, impactos) se afianza la convicción de que se está informado.

Al hablar de las características de la sociedad de la información se señala que esta revolucionaria etapa se basaba fundamentalmente en lo digital por lo que muchos la denominan cibersociedad, sociedad digital o sociedad cibernética. Lo ciber adquiere carácter central mientras proliferan los ciber-campos, la ciber-tienda o el ciber-dinero, la ciber-cultura, el ciber-sexo, la ciber-economía, la ciber-sociedad o el ciber-espacio.

El ciberespacio, término acuñado por William Gibson en su novela Neuromancer, es invisible y artificial, pero existe en todas las facetas de la vida. La invisibilidad del ciber-espacio y su globalidad se aprecia cuando uno se introduce en Internet o se navega por la red. Yendo un paso más adelante adentrándose en el mundo virtual que sería el siguiente paso de rosca de la cibersociedad. De alguna forma la realidad virtual rebasa la sociedad de la información para dar paso a la sociedad de la post-información.

Queau define el entorno virtual como una base de datos de gráficos interactivos, explorable y visualizable en tiempo real, en forma de imágenes tridimensionales de síntesis, capaces de provocar una sensación de inmersión en la imagen. Se trata de un espacio de síntesis pues en el que uno tiene la sensación de moverse físicamente (P. Queau, 1995,15). Los mundos virtuales proporcionan una inmersión funcional dentro de representaciones tridimensionales con la ayuda de cascos visualizadores. De hecho, los mundos virtuales permiten volar en el espacio y de alguna forma liberar de las obligaciones de lo real.

Otro concepto y realidad más avanzada es la tele virtualidad que se podría definir como la simbiosis de las telecomunicaciones y las imágenes de síntesis, (videoconferencia). La tele virtualidad permite crear entornos virtuales que pueden compartir numerosos participantes conectados en una red, lo que posibilita, por ejemplo, la realidad de las comunidades virtuales y toda una serie de aplicaciones a la vida práctica como pueden ser la telemedicina, la teleeducación, el turismo virtual, el sexo virtual.

Sin embargo, en este documento, no se va a ahondar en este tema. El objetivo sigue siendo el expuesto desde el comienzo, tratar el tema del diario digital y según ello, partiendo del mundo digital, corazón de la cibersociedad.

CIBERSEGURIDAD: La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Según la multinacional rusa de seguridad informática kaspersky, la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes. La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.

La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.

La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause la suspensión de sus operaciones o haga que se pierdan datos. Las políticas de recuperación ante siniestros dictan la forma cómo la organización restaura sus operaciones e información

para volver a la misma capacidad operativa que se tenía antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización (kaspersky, 2021).

Las amenazas a las que se enfrenta la ciberseguridad son tres (3):

El delito cibernético incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.

Los ciberataques a menudo involucran la recopilación de información con fines políticos.

El ciberterrorismo tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.

VULNERABILIDADES INFORMÁTICAS: Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

AMENAZAS INFORMÁTICAS: Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento o activo de la organización. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

RIESGOS INFORMÁTICOS: El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus, entre otros. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El resultado de estos factores representa el riesgo.

Figura 3. Vulnerabilidades, Amenazas y Riesgos Informaticos (Incibe, 2021).

CIBERCRIMINALES o CINERDELINCUENTES o TERRORISTAS INFORMÁTICOS: Así como en la sociedad existen los delincuentes, en el mundo informático existen los ciberdelincuentes, que en líneas generales son personas que realizan actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

Los cibercriminales también conocidos como ciberdelincuentes o terroristas informáticos, pueden ser personas u organizaciones criminales o de Estados, que a través de múltiples formas de ataques en el ciberespacio pueden generar daños informativos y en contra de los activos de las organizaciones.

Pueden tener varias motivaciones, deseos o intenciones. En algunos casos por curiosidad, en otros casos por dinero, por aspectos religiosos, políticos o sociales.

Independiente de sus motivaciones, todos estos coinciden en afectar las disponibilidades, integridad y la disponibilidad de los activos, servicios o procesos en las organizaciones. De acuerdo con Oxford Languajes, un Ciberterroristas es una persona u organización criminal, que ha cometido o ha intentado cometer un cibercrimen.

Existen varios perfiles, entre ellos están:

HACKING/HACKERS

Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, también conocidos como delincuentes silenciosos o tecnológicos que les gusta indagar por todas partes y conocer el funcionamiento de los sistemas informáticos. Son aquellos que se dedican a este tipo de actividades como reto intelectual sin producir daño alguno, con la única finalidad de descifrar y conocer los sistemas informáticos.

Este tipo de personas, llamadas Hackers es algo así, como una versión virtual de un allanador de domicilios o casas, que, en el lugar de penetrar en domicilios ajenos, se dedican a entrar sin permiso en los equipos informáticos o redes de propiedad ajena.

CRACKING/CRACKERS

Son aquellos sujetos que se introducen en sistemas remotos con la finalidad de destruir datos, denegar el ingreso a servicio de usuarios legítimos, y por lo general, causar daños a los sistemas, procesadores o redes informáticos, conocidos como piratas informáticos.

Cabe señalar que los Cracking vienen a ser una versión violenta y refinada de los anteriores, ya que, si bien utilizan técnicas de hacking para ingresar sin el consentimiento y autorización a equipos y redes ajenas. Estos sujetos tienen una finalidad más peligrosa, por tratarse de ser delitos telemáticos, es decir, aquellos delitos que pueden cometerse a distancia sin la necesidad que el autor material e intelectual tenga que estar presente para ejecutar el acto.

Otro modus operandi que se presentan a diario, es la distribución dolosa de virus. Este tipo de delitos consiste en crear programas de cómputo para diferentes fines, pero siempre malignos, es decir, programas que apuntan a generar varios daños en los equipos y que sin el consentimiento de los propietarios han sido instalados. En algunas ocasiones, se han presentado virus que por medio de mecanismos de tiempo permanecen varios meses inactivos sin dar muestra alguna de su existencia y que en determinado tiempo o fecha desatan su poder destructivo sin que el usuario tenga una forma de evitarlo.

Una de las características principales que diferencian al hacker de los crackers, es que los segundos utilizan programas ya creados y que pueden adquirirlos por internet, mientras que los hackers, crean sus propios programas debido a que tiene muchos más conocimientos sobre programación y conocen muy bien los lenguajes informáticos. El director de negocios y alianzas estratégicas de Digiware, Andrés Galindo, afirma que el 50 por ciento de las bandas dedicadas al cibercrimen se componen de seis o más personas. De ellos, el 76% son hombres cuyas edades van desde los 14 años (8%) hasta los 50 (11%). Aunque la edad promedio de este tipo de delincuentes es 35 años (43%) (GALLO, 2016).

VUCA: El entorno VUCA, en el que se mueven las organizaciones en la actualidad, se caracteriza por la volatilidad, la incertidumbre, la complejidad y la ambigüedad. Este concepto se fraguó en la década de los noventa por los soldados norteamericanos y que responde al acrónimo inglés formado por los términos Volatility (V), Uncertatinty (U), Complexity (C) y Ambiguity (A).

En este escenario es en el que las empresas se ven obligadas a adaptarse a los continuos cambios que atacan su programación estratégica y sus rutinas profesionales.

El entorno VUCA está presente en infinidad de sectores profesionales como el de los servicios, industria, tecnología o banca en el que los avances tecnológicos o las fluctuaciones propias del mercado económico son los causantes de la inclusión de las organizaciones en este tipo de sectores.

Conocimiento y predecibilidad: claves para adaptarse al entorno VUCA

En definitiva, para hacer frente a estas dos premisas principales, es fundamental centrar la estrategia de negocio en el conocimiento y la predecibilidad abordándolo desde dos perspectivas:

Una formación constante en un entorno en el que los nuevos avances tecnológicos hacen necesaria una actualización casi inmediata de las condiciones del entorno.

Una correcta y eficaz capacidad para afrontar los cambios y hacer frente a los problemas y dificultades que se presentan, para lo cual se hace imprescindible trabajar valores como el esfuerzo y la perseverancia.

La figura del líder o cómo sobrevivir al entorno VUCA

Como se mencionaba anteriormente, en estos entornos VUCA es imprescindible adaptarse a los cambios e imprevistos que vayan surgiendo en el seno de su organización y, para ello, puede ser de gran utilidad, tal y como menciona Bob Johansen, experimentado consultor y ex CEO del reputado Instituto para el Futuro, en su libro Los líderes hacen el Futuro, utilizar otro entorno VUCA basado en las siguientes premisas:

Abordar la volatilidad con una correcta visión de futuro (V).

Afrontar la incertidumbre con conocimiento, formación, actualización constante, es definitiva con entendimiento (U).

Aportar claridad, simplicidad y sencillez en la ejecución de tareas y acciones dentro del seno de la organización (C).

Acabar con la ambigüedad con agilidad, con una rápida capacidad de reacción ante los imprevistos que sucedan y que atenten contra la planificación estratégica de la organización (A).

Para realizar este VUCA, en contraposición al primero, es fundamental la figura de un líder que ejerza un liderazgo positivo y que sea capaz de adaptarse a los continuos cambios con el conocimiento y perseverancia que se requieren pues, aquellas empresas que no sepan adaptarse con rapidez, agilidad y constancia a los cambios e imprevistos que van surgiendo, sus perspectivas de progreso y proyección se verán abocadas al fracaso ante la fuerza y estabilidad que ya están consiguiendo sus principales competidores y el resto de compañías del sector (APD, 2020).

Figura 4. Entorno VUCA – Definición (Vuca, 2020).

DERECHO PROBATORIO:

Ciencia que estudia los principios y normas reguladoras de la prueba judicial, tanto en su naturaleza, como en sus características, procedimientos y valoración. En consecuencia, tanto los principios filosóficos, políticos, históricos y sociológicos (parte general), como los medios de convicción o de prueba (parte especial).

Se ocupa de cuestiones generales como las siguientes:

- La noción de prueba - (qué es la prueba procesal)
- El objeto de la prueba - (qué se debe probar)
- La carga de la prueba - (quién debe probar)
- El procedimiento probatorio - (cómo se debe probar)
- La valoración probatoria - (cómo se evalúan las pruebas)

Se ocupa de los distintos medios probatorios. Art. 175 CPC: Declaración de Parte,

- Juramento,
- Testimonio,
- Dictamen Pericial,
- Inspección Judicial,
- Documentos, Indicios y otros.

Principios del Derecho Probatorio:

1. PRINCIPIO DE LA AUTORRESPONSABILIDAD: Art. 177 C.P.C. A las partes les incumbe probar los supuestos de hechos de las normas jurídicas cuya aplicación están solicitando. Las partes soportan las consecuencias de su inactividad, de su descuido. Si las pares no solicitan pruebas, si no hacen lo necesario para que se practiquen o no ejecutan las actividades necesarias para que estas se diligencien, sufren las nefastas consecuencias.

2. PRINCIPIO DE LA VERACIDAD: las pruebas deben estar exentas de malicia, de habilidad o falsedad. Los Art. 257, 289, 292, 274 del C.P.C. hacen relación a dicho tema, se sanciona a quien aporte documento falso, se permite la tacha de documentos, etcétera.

3. PRINCIPIO DE LA LIBRE APRECIACIÓN: el juez debe realizar un razonamiento teniendo en cuenta los hechos aportados al proceso por los medios probatorios y de acuerdo ~~a~~ con las reglas de la sana critica. El Art. 187 C.P.C. anota que las pruebas deben se apreciadas en conjunto, según las reglas de la sana crítica y sin perjuicio de las formalidades establecidas en la ley.

4. PRINCIPIO DE LA UNIDAD DE LA PRUEBA: los Art.187 C.P.C., Art. 238 C.P.P. consagran el método analítico y la apreciación en conjunto de las pruebas.

La valoración conjunta de las pruebas debe realizarse después del estudio individualizado de cada medio o elemento probatorio. Para estudiar la prueba en conjunto, no solo se recauda o aporta una prueba, sino que es normal que aparezcan varias, inclusive de la misma especie y el estudio que se realiza de estas se destina a buscar las concordancias y divergencias entre ellas.

5. PRINCIPIO DE LA IGUALDAD: Este principio tiende a lograr un equilibrio en el proceso. Por él, las partes tienen oportunidades iguales para pedir y obtener que les practiquen pruebas, para contradecir las del contrario, pero sobre todo apunta a obtener un equilibrio en cuanto al conocimiento de los hechos. La oportunidad para conocer la investigación penal que se ha iniciado debe ser inmediata para los sujetos procesales. Si no se hace la comunicación en el tiempo indicado se pierde la igualdad ya que mientras el Estado ejerce a plenitud su poder investigativo, el imputado no participa en la aducción de los medios probatorios que posteriormente se pueden usar en su contra.

6. PRINCIPIO DE LA PUBLICIDAD O SOCIALIZACIÓN: la prueba puede y debe ser conocida por cualquier persona; ya que proyectada en el proceso, tiene un carácter social puesto que hace posible el juzgamiento de la persona en forma adecuada y segura. Ejemplo de este principio es el que un tercero pueda reconstruir los hechos. Los hechos y la prueba de deben ser explícitos, de tal forma que cualquier persona pueda entender que sucedió desde el punto de vista fáctico y la manera cómo se probó.

7. PRINCIPIO DE LA FORMALIDAD Y LEGITIMIDAD DE LA PRUEBA: la prueba para ser aprehendida requiere el cumplimiento de formalidades de modo, tiempo y lugar, además

debe estar exenta de vicios como error, fuerza, violencia, entre otros. La prueba debe provenir únicamente de los sujetos legitimados para ello.

8. PRINCIPIO DE LA LIBERTAD DE LOS MEDIOS DE PRUEBA: Los medios probatorios sobre todo en materia penal deben estar taxativamente enumerados. El Art. 237 C.P.P. consagra que contiene el objeto de estudio de la investigación libertad de medios probatorios, pero existe taxatividad en el sentido de que no pueden violar derechos fundamentales.

9. PRINCIPIO DE LA SEPARACIÓN DE INVESTIGADOR Y JUZGADOR: el juez practicará prueba dentro de los supuestos hechos que han plasmado las partes, pero también podrá decretarlas de oficio dentro de esos límites. En materia penal el Estado es el más interesado en saber la verdad de los hechos. Por ello tiene una doble misión que es la de averiguar dónde está la información e informarse a su vez. O sea, el Estado debe buscar, escudriñar, exigir al funcionario que sea imaginativo, audaz a la hora de informarse y trabajar con hipótesis, es decir, hacer conjeturas imaginarias sobre la posible verdad. Puede a veces ocurrir que el juzgador cometa un error al hacer una mezcla entre lo realmente experimentado y sus hipótesis porque el juzgador es un ser humano. No obstante, debe tener presente que para obtener la verdad hay que acercarse a ella con la mente libre de intereses y perturbaciones. Por ejemplo, en Colombia (Art. 250 C.N.) el fiscal que investiga en un momento determinado se convierte en juez y valora la prueba para dictar medida de aseguramiento. No hay mucha objetividad en el hecho de que a un mismo funcionario se le den las funciones de buscar, capturar y evaluar. Se debe realizar separadamente la tarea de instrucción y de juzgamiento.

10. PRINCIPIO DE LA LICITUD DE LA PRUEBA: es prueba ilícita la que se obtiene violando los derechos fundamentales de las personas, ya sea para lograr la fuente de la prueba o el medio probatorio. La prueba ilegal es aquella que viola una norma legal. La prueba irregular viola el proceso. Se habla de la libre apreciación de prueba por lo que algunos autores se inclinan a pensar que es posible lavar las pruebas ilícitas ya que no se puede despreciar nada que pueda servir de prueba. La libre apreciación opera sobre pruebas aportadas en forma regular y sin violación a los derechos fundamentales. Se refiere únicamente a la apreciación de medios de prueba lícitos. No se puede argumentar que el fin justifica la búsqueda de la verdad a cualquier precio. El Art. 29 C.N. establece que es nula la prueba obtenida con violación al debido proceso. Esa nulidad comprende la prueba ilícita, ilegal o irregular. No debe admitirse ninguna de esta clase de pruebas. También se menciona la Teoría del árbol envenenado: (efecto de la prueba ilícita) donde se le resta mérito a la prueba ilegalmente obtenida, afectando a aquellas otras pruebas que sí fueron legalmente aportadas, llegándose a concluir que eses pruebas lícitas no pueden ser tampoco admitidas. Existe, además, el principio de la proporcionalidad que alude a sopesar los derechos fundamentales en conflicto y excepcionalmente admitir la aducción de pruebas, que en otras circunstancias serían ilícitas. En este sentido, en materia penal el funcionario debe rechazar las pruebas ilícitas e ilegales. Si la prueba ingresa al proceso cuando se haga la interpretación se percatará que no se debe tener en cuenta y no se valorará. Si se valora el recurrente deberá hacer lo siguiente en casación: -que la prueba fue obtenida ilegalmente – que los efectos reflejos de la prueba ilícita era la única manera de lograr otras pruebas legalmente obtenidas –que las otras pruebas no permiten sostener el fallo. Entre tanto, en materia civil si la prueba ilícita es valorada se puede casar por error de derecho.

11. PRINCIPIO DE LA INMEDIACIÓN: supone la percepción de la prueba por parte del juez y su participación personal y directa en la producción del medio probatorio. La inmediación subjetiva es la práctica de prueba llamada personal (interrogatorio a los testigos). La inmediación objetiva es en la cual el juez observa situaciones, circunstancias, objetos, documentos (inspección judicial).

12. PRINCIPIO DE LA NECESIDAD DE LA PRUEBA: la prueba es necesariamente vital para la demostración de los hechos en el proceso. El juez al dictar sentencia basará su decisión en las pruebas oportuna y legalmente recaudadas. Lo que no está en el mundo del proceso recaudado por los medios probatorios no existe en el mundo del juez.

13. PRINCIPIO DE LA COMUNIDAD DE LA PRUEBA O ADQUISICIÓN: no se puede pretender que las pruebas se aprecien en lo favorable a la parte que la peticionó o la aportó. En aplicación de este PRINCIPIO no se puede desistir de la prueba practicada.

14. PRINCIPIO DE LA CONTRADICCIÓN DE LA PRUEBA: la parte contra la cual se postula, se opone o aporta una prueba que no se conoce. Se debe tener en cuenta que la prueba no puede ser valorada o apreciada si no se ha celebrado con conocimiento de parte, es decir, que al proceso no pueden ingresar pruebas a escondidas o a espalda de la contraparte. La contradicción se da en tres momentos: 1) - Momento de asumirse el medio probatorio 2) - Momento de presentar alegaciones 3) - Momento de formulación de recursos.

15. PRINCIPIO DEL EMPLEO DE LAS REGLAS DE LA EXPERIENCIA: el juez en la valoración de la prueba debe emplear las reglas de la experiencia, o sea, la aplicación en concreto de la experiencia que tiene el funcionario.

• Regla de la experiencia: son definiciones o juicios hipotéticos de contenido general, desligados de los hechos concretos que se juzgan en el proceso, procedentes de la experiencia, pero independientes de los casos particulares de cuya observación se han inducido y que pretenden tener validez para otros nuevos. Las reglas de la experiencia cumplen con las siguientes funciones: -para hacer valoración de los medios probatorios –para indicar los hechos que están por fuera del proceso, por medio de otros (indicios) –en la formación de la sentencia –para integrar definiciones legales (buena fe).

• Las reglas de la experiencia debe ser conocida y adquirida por el aplicador y debe ser de conocimiento social.

• Errores en la apreciación de la prueba: en la apreciación de la prueba existen dos etapas: interpretación (- error de falso juicio de existencia cuando el juez no contempla o hace inventario de una prueba que no obra en el proceso –falso juicio de idoneidad cuando distorsiona el contenido objetivo, se cercena su o aumenta su contenido), y valoración (falso raciocinio cuando se aplica mal una regla de la experiencia o la lógica - falso juicio de ilegalidad –falso juicio de convicción).

16. PRINCIPIO DEL DERECHO A LA PRUEBA: el derecho a la prueba significa tenerlo con relación a pruebas lícitas que no sean obtenidas por medio de un delito. La C.N. consagra este principio en su Art. 29 al expresar que se pueden presentar y controvertir pruebas. Este derecho se manifiesta en:

• Derecho a asegurar la prueba (preconstituir la prueba, adelantarse a la recolección de la prueba.

• Derecho a que se admita la prueba • Derecho a que el medio probatorio sea practicado.

• Derecho a que el medio probatorio sea valorado.

• Obligación del funcionario a explicar los elementos de los medios probatorios.

Se debe estudiar la aplicación de los principios dentro de los procesos.

El objeto de la prueba radica en el conocimiento y reconstrucción de unos hechos. Son objeto de prueba judicial las relaciones susceptibles de ser probadas, sin relación con ningún proceso en particular. Son objeto de prueba:

• Conducta humana: los sucesos, acontecimientos, conductas presentes, pasadas o futuras, hechos o actos humanos, voluntarios o involuntarios, individuales o colectivos, son objeto de prueba.

• Hechos de la naturaleza: en los cuales no interviene el hombre, son casos fortuitos (terremoto, derrumbe, inundación).

• Cosas u objetos: que sean producto o no del hombre, puede ser objeto de prueba cualquier cosa que ocupe un espacio (armas, documentos).

• Persona física, su existencia y características, estado de salud (tatuajes, cicatrices, color rojo)

• Los estados y hechos síquicos internos del hombre: todos aquellos estados o atenuantes que conllevan a tener una conducta o a la realización de ciertos actos. (ira, trastornos mentales).

DERECHO PENAL: Según la Constitución de Colombia y del Código Penal, los derechos de las personas deben respetarse por encima de cualquier circunstancia. En este sentido, es muy importante que en esta publicación se hable del Derecho Penal, pues se trata de una rama del derecho que analiza, estudia y sanciona el comportamiento de una persona ante determinados actos. En otras palabras, se trata de un mecanismo o una herramienta utilizadas por los abogados para controlar la sociedad, o como ya se mencionó, el comportamiento de las personas para hacer justicia, defender a las víctimas y sancionar a los culpables del hecho ilegal; siempre dándole la oportunidad al señalado de defender sus derechos y su versión de los hechos.

El Derecho Penal, se rige por las normas expuestas en la Constitución y el Código Penal de cada país. En el caso de Colombia, el derecho penal determina, en esencia, cuáles hechos o actos son considerados como ilegales para presentar las sanciones correspondientes según la gravedad del caso.

El artículo 1 del Código Penal Colombiano (Ley 599, 2000) señala "el derecho penal tendrá como fundamento el respeto a la dignidad humana". Asimismo, en el artículo 6 establece "nadie podrá ser juzgado sino conforme a las leyes preexistentes al acto que se le imputa, ante el juez o tribunal competente y con la observación de la plenitud de las formas propias de cada juicio". Lo anterior quiere decir que, sin importar el motivo de señalamiento hacia el

culpable, la ley lo ampara y la persona debe ser tratado conforme lo indican las normas legales.

El libro segundo del Código Penal aclara que los delitos tratados en el derecho penal son:

Genocidio. El artículo 101 dice que los actos sancionados y penados entre 10 y 20 años de cárcel son "lesión grave a la integridad física o mental de miembros del grupo; embarazo forzado; sometimiento de miembros de grupo a condiciones de existencia que hayan de acarrear su destrucción física, total o parcial; tomar medidas destinadas a impedir nacimientos en el seno del grupo y traslado por la fuerza de niños del grupo a otro grupo".

Homicidio. El artículo 103 señala "el que matare a otro, incurrirá en prisión de 13 a 25 años". Los años de prisión aumentan hasta los 40 años para pagar la sanción si se trata de un delito que en el derecho penal se considera en "circunstancias de agravación".

Lesiones Personales. La norma 111 establece "el que cause a otro daño en el cuerpo o en la salud, incurrirá en las sanciones establecidas". Algunos de los daños que son sancionados en el derecho penal son "provocar incapacidad para trabajar o enfermedad, deformidad, perturbación funcional o psíquica, pérdida anatómica o funcional de un órgano o miembro, entre otros".

Aborto. El artículo 122 dicta "la mujer que causare su aborto o permitiere que otro se lo cause, incurrirá en prisión de 1 a 3 años". En el derecho penal, también se sanciona a la persona responsable que realizó el aborto con el consentimiento de la mujer. Además, la presente ley también determina sanciones que afecten al feto o le provoquen lesiones culposas.

Abandono de Menores y Personas Desvalidas. Según lo dispuesto en el artículo 127 "el que abandone a un menor de 12 años o a persona que se encuentre en incapacidad de valerse por sí misma, teniendo deber legal de velar por ellos, incurrirá en prisión de 2 a 6 años". Los años de prisión pueden aumentar según la gravedad del acto ilegal.

Actos Sexuales Abusivos. Los artículos 208, 209 y 210 aclaran "el que acceda carnalmente a una persona; realizare actos sexuales diversos del acceso carnal o acceda carnalmente a una persona en estado de inconsciencia incurrirá en prisión". Los años de sanción se deciden en el derecho penal según la gravedad del acto sexual sin el consentimiento de la víctima.

Contra las Personas. Delito de apropiación indebida, abuso de confianza, homicidio, concierto para delinquir, utilización indebida de información privilegiada, violación de derechos morales del autor, tráfico de personas, intimidad de víctima. Otros casos que atienden abogados especialistas en derecho penal son conducta indebida, violación de orden de restricción, violencia doméstica, usurpación de identidad y fabricación, tráfico o porte ilegal de arma de fuego.

Sexuales. Actos sexuales en sitios públicos, acceso carnal indebido, violación sexual de un menor, pornografía y pornografía infantil. Nuestros profesionales en derecho penal aplicarán las herramientas pertinentes para defender a la víctima.

Financieros. Extorsión, estafa, blanqueo de capitales, administración desleal, apropiación indebida, delitos societarios, robo, malversación de fondos, emisión o transferencia ilegal de cheques y lavado de activos.

Ambientales. Daños a los recursos naturales, contaminación ambiental, pesca ilegal, explotación ilícita minera y apoderamiento de hidrocarburos.

De la Competencia. Se aplica en casos de alteración de cantidad, calidad, peso o medida de productos, usurpación de marcas y patentes, y ejercicio ilícito de actividad monopolística.

Farmacéuticos. atendemos atiende casos de tráfico y comercialización de drogas y estupefacientes, fabricación de drogas o estupefacientes y posesión ilegal de sustancias ilícitas. (Jurídicos penales – 2020).

En términos generales el derecho penal es la rama del derecho público que regula la potestad punitiva del Estado y asocia a la realización de determinadas conductas, llamadas delitos, penas y medidas de seguridad como consecuencias jurídicas.

DERECHO PROCESAL: Cualquier sociedad está sometida a ciertas costumbres y reglamentada por normas jurídicas de imperativo cumplimiento por parte de sus asociados. Es, por lo tanto, normal y lógico que se presenten conflictos de intereses entre dichas personas y que el Estado, sea en primer lugar, el llamado o el encargado de darles solución y es por ello entonces que el derecho procesal surge como reacción a la forma primitiva de hacerse justicia por propia mano o privada.

El derecho procesal es un derecho independiente y autónomo con tres (3) elementos:

a. La Jurisdicción.

b. La Acción.

c. El Proceso.

NATURALEZA: El derecho procesal constituye hoy una rama propia e independiente del derecho, dotada de sus propios principios fundamentales con un extenso contenido doctrinario. De sus normas se derivan derechos y obligaciones de naturaleza especial. Se trata de un derecho público, formal, instrumental, autónomo y de principal importancia, así como de imperativo cumplimiento salvo las excepciones anotadas.

IMPORTANCIA: Regula la soberanía del Estado al aplicar la función jurisdiccional, estableciendo el conjunto de principios que deben encausar, garantizar y hacer efectiva la acción de los asociados (personas naturales, jurídicas) para lograr así la protección de todos sus derechos: vida, patrimonio, libertad, cuando estos se vean amenazados o perturbados.

PRINCIPIOS GENERALES DEL DERECHO PROCESAL:

- Del interés público o general en el proceso.
- Carácter exclusivo y obligatorio de la función jurisdiccional.
- Independencia de la autoridad judicial.
- Imparcialidad Rigurosa de los funcionarios judiciales.
- Igualdad de las partes ante la ley en el proceso.
- Necesidad de oír a la persona contra la cual va a surtirse la decisión y la garantía del derecho de defensa.
- Publicidad del Proceso.
- De la verdad procesal.
- De la Cosa Juzgada.

PRINCIPIOS FUNDAMENTALES DEL PROCEDIMIENTO:

- Obligatoriedad de los procedimientos establecidos en la Ley.
- Regla técnica Dispositiva – Inquisitiva.
- Valoración de la prueba por el Juez de acuerdo con las reglas de la sana crítica.
- De la Impulsión oficiosa del Proceso.
- De la Economía Procesal.
- Concentración del Proceso.
- De la eventualidad, y/o preclusión.
- De que las sentencias no crean derechos, se limitan a declararlos.
- Regla técnica de la Inmediación.
- Regla técnica de la oralidad y de la escritura.
- Del interés intervenir en el proceso.
- Del interés para pedir o contradecir una sentencia y de la legitimación en la causa.
- Regla técnica de la Impugnación.
- Regla técnica de las dos instancias.
- De la Motivación de las Sentencias.
- De la carga de la prueba.
- De la buena fe y de la lealtad procesal.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene lo que representa este tema para cada organización o entidad.

Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos. Requiere estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se necesite.

Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero.

La implementación de un sistema de seguridad debe estar complementado con las políticas de seguridad.

La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de las mismas, que pueden ser internas o externas a la organización. De nada valdría proteger la empresa de los usuarios del exterior si también existen amenazas internas. Por ejemplo, si un usuario utiliza un disquete que contiene un virus podría expandirlo a toda la intranet.

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ser dinámicos, es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon.

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles y deben tener el apoyo gerencial de la organización.

Las políticas de seguridad deben ser conocidos por todo el personal de una organización. Y en el contenido de los documentos deben estar claramente establecidos: El objetivo, los responsables del cumplimiento, las medidas que se aplicarán en caso de incumplimiento.

Entre los documentos pueden citarse los siguientes:

- Administración de usuarios que reglamentará el acceso a los recursos por el personal de la organización.
- Copias de respaldo: Describirá los pasos a seguir para asegurar una adecuada recuperación de la información, a través de las copias de respaldo.
- Tratamiento de la información: Definirá claramente los tipos de información que es manejada por las personas autorizadas dentro de la organización.
- Software legal: Definirá claramente el uso de software en la Empresa con licencias de uso legal.

- Uso del servicio de Internet y del correo electrónico: Describirá la protección de la información mediante el uso de correo electrónico y del servicio de Internet.
- Ambientes de Procesamiento: Define el uso de los ambientes de procesamiento de información.
- Seguridad en las comunicaciones: Describirá la protección de la información durante los procesos de transmisión y recepción de datos en las redes internas y externas.
- Auditorías de los sistemas: Que permitirá hacer un control de los eventos de seguridad de los sistemas.
- Continuidad del procesamiento: Se definirán y reglamentarán las actividades relativas a la recuperación de la información en casos críticos mediante una metodología adecuada.
- Protección física: Definirá la protección física de los equipos, de procesamiento, almacenamiento y transmisión de la información.
- Sanciones por incumplimientos: Este documento contemplará las medidas que se aplicarán por incumplimiento de las reglas definidas (Scielo, 2020).

PLAN DE SEGURIDAD DE LA INFORMACIÓN: El Plan de Seguridad de la Información (PSI), es un documento que tiene por objetivo trazar y planificar la manera cómo la entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Este documento deberá, cronograma, plazos, cuáles serán las labores que realizará la entidad con el objetivo de lograr el cumplimiento total de la implementación del MSPI al interior de todos los procesos de la entidad y debería contener como mínimo lo siguiente:

• REQUISITOS GENERALES

• ESTABLECIMIENTO Y GESTIÓN DEL MSPI

✓ Establecimiento del MSPI

✓ Implementación y operación del MSPI

✓ Seguimiento y revisión del MSPI

✓ Mantenimiento y mejora del MSPI

• REQUISITOS DE DOCUMENTACIÓN

✓ Generalidades

✓ Control de Documentos

✓ Control de Registros

• RESPONSABILIDAD DE LA DIRECCIÓN

✓ Compromiso de la Dirección

✓ Gestión de Recursos

✓ Provisión de Recursos

✓ Formación, toma de conciencia y competencia

• AUDITORÍAS INTERNAS DEL MSPI

• REVISIÓN DEL MSPI POR LA DIRECCIÓN

✓ Generalidades

✓ Información para la revisión

✓ Resultados de la revisión

• MEJORA DEL MSPI

✓ Mejora continua

✓ Acción correctiva

✓ Acción preventiva

• COMPATIBILIDAD DEL MSPI CON LOS OTROS SISTEMAS DE GESTIÓN

REQUISITOS GENERALES

Las entidades, a través de los comités de gestión y desempeño institucional, impulsarán la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, en el contexto de las actividades globales de la entidad y de los riesgos que enfrenta.

Para hacer realidad este propósito, se basará en el modelo PHVA.

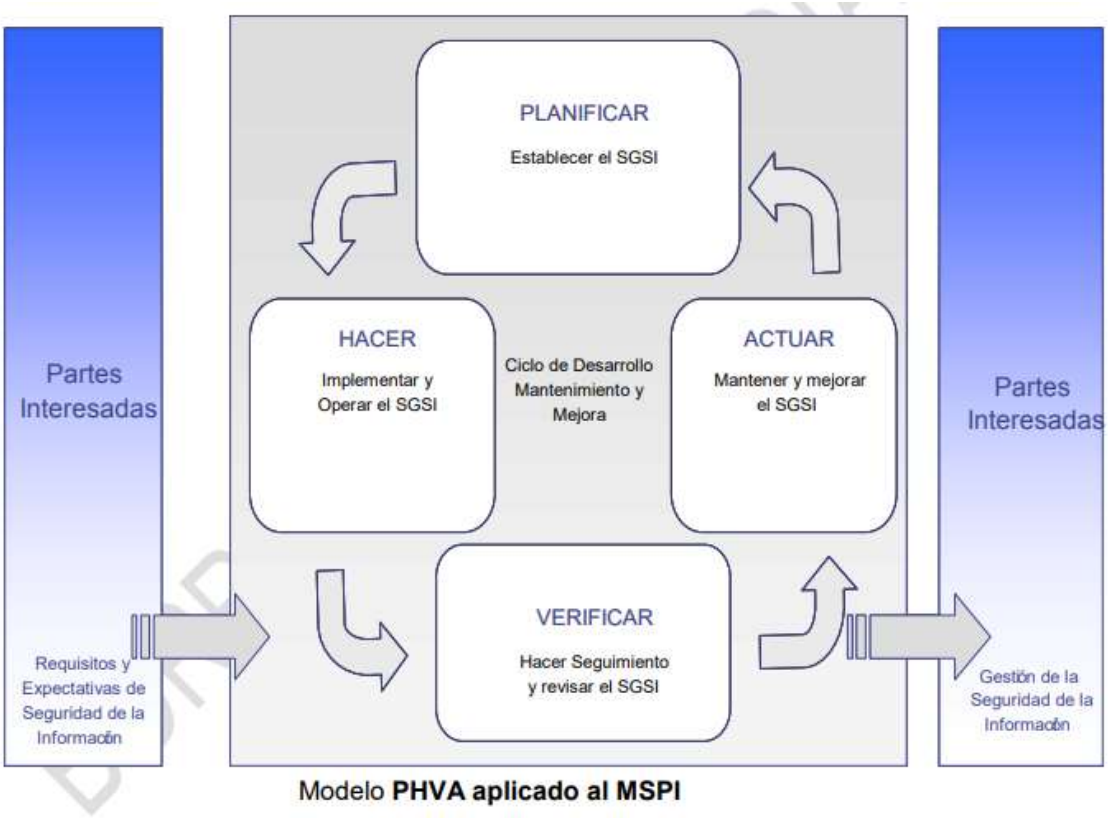


Figura 5. Plan PHVA aplicado al MSPI. (MinTic, 2019).

ESTABLECIMIENTO Y GESTIÓN DEL MSPI

Establecimiento del MSPI

La entidad debe:

• Definir el alcance y límites del MSPI en términos de las características del servicio que presta el organismo, su estructura interna, su ubicación, sus activos de información, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.

• Definir una política de MSPI en términos de las características del servicio que presta el organismo, su estructura interna, sus activos de información y tecnología; que:

- ✓ Incluya un marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información.
- ✓ Tenga en cuenta los requisitos del organismo, los legales o reglamentarios y las obligaciones de seguridad contractuales.
- ✓ Este alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del MSPI.
- ✓ Establezca los criterios contra los cuales se evaluará el riesgo.
- ✓ Haya sido aprobada por la dirección.

• Definir el enfoque organizacional para la valoración del riesgo.

- ✓ Identificar una metodología de valoración del riesgo que sea adecuada al MSPI y a los requisitos reglamentarios, legales y de seguridad de la información de la organización, identificados.
- ✓ Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables.

La metodología seleccionada para la valoración de riesgos debe asegurar que dichas valoraciones producen resultados comparables y reproducibles.

• Identificar los riesgos

- ✓ Identificar los activos dentro del alcance del MSPI y los propietarios de estos activos de información.
- ✓ Identificar las amenazas a estos activos.
- ✓ Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
- ✓ Identificar los impactos que la perdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

• Analizar y evaluar los riesgos.

- ✓ Valorar el impacto que podría causar una falla en la seguridad, sobre el organismo, teniendo en cuenta las consecuencias de la perdida de confidencialidad, integridad o disponibilidad de los activos.
- ✓ Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.
- ✓ Estimar los niveles de los riesgos.
- ✓ Determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios previamente establecidos.

• Identificar y evaluar las opciones para el tratamiento de los riesgos.

Las posibles acciones incluyen:

- ✓ Aplicar los controles apropiados.
- ✓ Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
- ✓ Evitar riesgos
- ✓ Transferir a otras partes los riesgos asociados con el negocio, por ejemplo, Firmar aseguradoras, proveedores, etcétera.

• Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos. Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos.

• Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.

• Obtener autorización de la dirección para implementar y operar el MSPI.

• Elaborar una declaración de aplicabilidad.

La declaración de aplicabilidad debe incluir;

- ✓ Los objetivos de control y los controles.
- ✓ Los objetivos de control y los controles que ya se hayan implementado.
- ✓ La exclusión de cualquier objetivo de control y controles y la justificación para su exclusión.

• Elaborar un plan de sensibilización y apropiación del MSPI para toda la entidad.

Implementación y operación del MSPI.

La entidad debe:

• Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

• Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.

• Implementar los controles seleccionados, para cumplir los objetivos de control.

• Definir cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.

• Implementar programas de formación y de toma de conciencia.

• Gestionar la operación del MSPI.

• Gestionar los recursos del MSPI.

• Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

Seguimiento y revisión del MSPI

La entidad debe:

• Ejecutar procedimientos de seguimiento, revisión y otros controles para;

- ✓ Detectar rápidamente errores en los resultados del procesamiento.

- ✓ Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
- ✓ Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
- ✓ Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.
- ✓ Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

• Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI, y la revisión de los controles de seguridad), teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

• Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

• Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en;

- ✓ La entidad
- ✓ La tecnología
- ✓ Los objetivos y procesos de la entidad

▪ Las amenazas identificadas

▪ La eficacia de los controles implementados

▪ Eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.

• Realizar auditorías internas del MSPI a intervalos planificados.

• Emprender una revisión del MSPI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de MSPI.

• Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.

• Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del MSPI.

Mantenimiento y mejora del MSPI

La entidad regularmente debe:

• Implementar las mejoras identificadas en el MSPI.

• Emprender las acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.

• Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.

• Asegurar que las mejoras logran los objetivos previstos. (MinTic, 2019).

PRESUPUESTO:

El presupuesto es una herramienta que le permite saber cuáles son sus ingresos y gastos en un tiempo determinado, conocer cuánto puede destinar al ahorro para el cumplimiento de sus metas planteadas, identificar en qué está gastando su dinero, cuánto necesita para cubrir sus necesidades, determinar en qué se está gastando más y tomar medidas cuando se requiera hacer un recorte de gastos.

Con un presupuesto puede organizar su dinero para usarlo de manera óptima, fijar prioridades, disminuir el riesgo de incumplir con sus obligaciones y comparar periódicamente sus consumos, identificar los gastos que puede ajustar y evaluar la gestión de sus recursos para determinar su estado financiero. Ajustar sus finanzas a tiempo, le permite tomar decisiones financieras acertadas y definir el mejor camino para alcanzar sus metas. (Saber más, 2018).

El presupuesto de una empresa es un plan que recoge todas las operaciones y recursos para lograr los objetivos marcados, expresado en términos monetarios. Se quiera o no, el presupuesto de una empresa es algo a tener muy en cuenta a la hora de realizar cualquier acción. Marcar un presupuesto es adelantarse al futuro para evitar contratiempos o problemas.

Cuando se hace un presupuesto se está planeando lo que se quiere en un futuro y el dinero que se va a invertir en ello. De esta manera se debe especificar cada gasto que va a producirse en cada acción establecida. Cuando, por ejemplo, se hace un viaje de empresa, no sólo se

debe especificar el coste del viaje en sí, sino también se ha de contemplar el alojamiento, las comidas, los desplazamientos, entre otros. De esta forma, desde el primer momento, se conoce el importe total de la acción y es posible hacer una previsión de lo que se puede y no se puede gastar en el resto (El País, 2017).

VALOR: El valor es una cualidad de un sujeto o un objeto. Los valores son agregados a las características físicas o psicológicas, tangibles del objeto. Es decir, son atribuidos al objeto por un individuo o un grupo social, modificando a partir de esa atribución su comportamiento y actitudes hacia el objeto en cuestión. El valor es una cualidad que confiere a las cosas comunes, hechos o personas una estimación, ya sea positiva o negativa.

Se puede decir que la existencia de un valor es el resultado de la interpretación que hace el sujeto de la utilidad, deseo, importancia, interés, belleza del objeto. Es decir, la valía del objeto es en cierta medida, atribuida por el sujeto, en acuerdo a sus propios criterios e interpretación, producto de un aprendizaje, de una experiencia, la existencia de un ideal incluso de la noción de un orden natural que trasciende al sujeto en todo su ámbito. "Puesto que los valores no son cosas, ni elementos de las cosas, entonces los valores son impresiones subjetivas de agrado o desagrado, lo que nos producen a nosotros y que nosotros proyectamos sobre las cosas. Se ha acudido entonces al mecanismo de la proyección sentimental; se ha acudido al mecanismo de una objetivación, y se ha dicho: esas impresiones gratas o ingratas, que las cosas nos producen, nosotros las arrancamos de nuestro yo subjetivo y las proyectamos y objetivamos en las cosas mismas y decimos que las cosas mismas son buenas o malas, o santas o profanas" (García Morente, 1992).

Valores tales como: honestidad, lealtad, identidad cultural, respeto, responsabilidad, solidaridad, amor, tolerancia, gratitud, laboriosidad, sociabilidad, entre otros, son fundamentales para convivir pacíficamente en la sociedad.

Sin embargo, como en muchos de los temas antropológicos se puede considerar que la libertad o la solidaridad, más que valores personales o sociales son sus fundamentos de valor, lo que delimita el ámbito axiológico. Como cualidades apreciadas por el sujeto solo adquieren el rango de valores en el momento en que son alcanzadas como prácticas personales y/o colectivas. En otras palabras, la libertad no es un valor por el contenido del concepto o por ser apreciada como una práctica deseable de un determinado grupo social. Se trata de un valor cuando es apreciada y ejercida por los sujetos, es decir, demanda situaciones praxeológicas, es el ejercicio de la libertad en una comunidad. Esto se conoce como dialéctica objeto-sujeto, relación recíproca entre el objeto considerado como valioso por el pensamiento y la práctica del sujeto hábitos virtuosos.

Los valores desarrollan virtudes que desplegados diariamente en el ambiente benefician al entorno y a la sociedad en general. Los valores se delimitan por una cultura, grupo, religión, hábitos o tradiciones. En línea con la dialéctica sujeto - objeto en los valores se producen los casos y controversias. Por ejemplo, el respeto a las mujeres en el Medio Oriente no es el mismo que se puede observar en otras partes del mundo. En una cultura y religión puede no considerarse vejatorio o intolerante (dimensión subjetiva del valor) (Universidad Pedagógica Nacional, 1995).

Para la corriente filosófica del materialismo, la naturaleza del valor reside en la capacidad del ser humano para valorar al mundo en forma objetiva.

El término valor puede tomar diferentes significados según se aplique. En general se define el valor como aquella cualidad buena o mala que se otorga a un suceso, un objeto o una persona. La valoración que se hace de algo o alguien puede ser positiva o negativa y depende de diferentes factores. Cuando se trata de un objeto el término valor puede tener dos posibles significados. Por un lado, se puede hablar del valor que cierto elemento tiene para una persona en particular. Esto puede relacionarse a un valor sentimental que relaciona a esa persona con el objeto haciendo que sea valioso para ella.

Por otro lado, en relación con un objeto, se puede hablar del valor monetario. En ese caso se apunta al costo que tiene cierto objeto por sus características. Esto se relaciona con el precio y la utilidad del elemento en cuestión. El valor de un objeto también puede relacionarse a la validez que tiene. Por ejemplo, en un juicio puede hablarse del valor que tiene una prueba o un testimonio en relación con lo que pueda aportar a la causa que se está analizando. Por ello el concepto de valor varía según la situación en que se utilice (Cao, 2012).

Muchas veces el valor monetario está asociado al dinero o cantidad de dinero que una persona está decidida a entregar por ese activo, bien, servicio o elemento. Es por ello, que se debe asociar el dinero también como una clasificación del valor. Dinero es todo activo o bien generalmente aceptado como medio de pago por los agentes económicos para sus intercambios y que además cumple las funciones de ser unidad de cuenta y depósito de valor Algunos ejemplos de dinero son: las monedas, las divisas y los billetes, las tarjetas de débito y crédito, y las transferencias electrónicas, entre otros.

El dinero tal como se conoce hoy (billetes y monedas sin valor propio), debe estar avalado o certificado por la entidad emisora. Para su aceptación necesita de la construcción de

mecanismos de legitimidad y de confianza. Actualmente son los gobiernos, a través de las leyes, los que determinan cuál es el tipo de dinero de curso legal. Pero son otras entidades, como los bancos centrales y las casas de la moneda (ceca), los que se encargan, primero, de regular y controlar la política monetaria de una economía, y segundo, de crear las monedas y billetes según la demanda y la necesidad de tener en circulación dinero físico. Desde un punto de vista de las Ciencias Sociales entra en juego el factor social ya que la moneda al ser «un bien público», en tanto que presta servicios de tal naturaleza, debe ser regulada por las autoridades públicas (mediante los bancos centrales) en cuanto representantes del interés público, y no solamente a través de los mecanismos de mercado.

Tipos

Dinero mercancía

A veces llamado dinero real, es aquella clase de dinero cuyo valor, a diferencia del dinero representativo y del dinero Fiat, proviene fundamentalmente del bien del cual se compone. El dinero mercancía consiste en bienes u objetos que tienen valor por sí mismos, además del valor de cambio al ser utilizado como moneda.

Dinero representativo

Tipo de dinero que, a diferencia del dinero mercancía, se basa en otro activo, como, por ejemplo, el dinero respaldado en oro, plata, petróleo u otra moneda, que tiene la cualidad de ser convertible al activo al cual representa, el cual puede ser una especie de dinero metálico.

Dinero fiat

También conocido como dinero por decreto, es una forma de dinero sin valor intrínseco. Su valor se basa en su declaración como dinero por el Estado. El término fíat frecuentemente se utiliza de forma intercambiable con el de dinero fiduciario, sin embargo, los términos no son equivalentes y el matiz puede ser considerable. El dinero Fiat es el tipo de dinero del dólar, euro, yen y principales monedas de curso internacional.

Dinero fiduciario

El dinero llamado fiduciario (del latín fiduciarĭus, de fiducĭa 'confianza' y ésta a su vez de fides 'fe'), es el que se basa en la fe o confianza de la comunidad, es decir, que no se respalda por metales preciosos ni nada que no sea una promesa de pago por parte de la entidad emisora. Es importante tener en cuenta que se entiende la confianza de la comunidad como el conjunto de la riqueza aparente que presenta la comunidad emisora de la moneda. Es el modelo monetario que predomina actualmente en el mundo, y es del dólar estadounidense, el euro y todas las otras monedas de reserva.

Moneda

La moneda es una pieza de un material resistente, de peso y composición uniforme, normalmente de metal acuñado en forma de disco y con los distintivos elegidos por la autoridad emisora, que se emplea como medida de cambio (dinero) por su valor legal o intrínseco y como unidad de cuenta.

Papel moneda

El billete de papel más antiguo conservado lo fabricó la dinastía Ming, hacia 1375 y equivalía a 1.000 monedas de cobre. Fue necesaria una evolución en la cual los Estados emitían billetes

y monedas, que daban derecho a su portador a intercambiarlos por oro o plata de las reservas del país. Los cambios en las dinámicas económicas durante el siglo XX dieron fin a la hegemonía de los metales en el dinero, el cual tomó otros aspectos (billetes, tarjetas, entre otros). La evolución del respaldo del papel moneda es el siguiente:

En los siglos XVIII y XIX, varios países tenían un patrón de dos metales, basado en oro y plata.

Entre 1870 y la Primera Guerra Mundial se adoptó principalmente el patrón oro, de forma que cualquier ciudadano podría transformar el papel moneda en una cantidad de oro equivalente.

En el periodo entre guerras mundiales se trató de volver al patrón oro, si bien la situación económica y la crisis o crac terminó con la convertibilidad de los billetes en oro para particulares.

Al finalizar la Segunda Guerra Mundial, los aliados establecieron un nuevo sistema financiero en los Acuerdos de Bretton Woods, en los cuales se establecía que todas las divisas serían convertibles en dólares estadounidenses y solo esta moneda sería convertible en lingotes de oro a razón de 35 dólares por onza para los gobiernos extranjeros.

En 1971, las políticas fiscales expansivas de los Estados Unidos, motivadas fundamentalmente por el gasto bélico de Vietnam, provocaron la abundancia de dólares, planteándose dudas acerca de su convertibilidad en oro. Esto hizo que los bancos centrales europeos intentasen convertir sus reservas de dólares en oro, creando una situación insostenible para los estadounidenses. Ante ello, en diciembre de 1971, el presidente de

Estados Unidos, Richard Nixon, suspendió unilateralmente la convertibilidad del dólar en oro para el público y devaluó el dólar un 10 %22. En 1973, el dólar se vuelve a devaluar otro 10 %, hasta que, finalmente, se termina con la convertibilidad del dólar en oro también para los gobiernos y bancos centrales extranjeros.

Desde 1973 el dinero utilizado en el mundo tiene un valor que está en la creencia subjetiva de que será aceptado por los demás habitantes de un país, o zona económica, como forma de intercambio. Las autoridades monetarias y bancos centrales no pretenden defender ningún nivel particular de tipo de cambio, pero intervienen en los mercados de divisas para suavizar las fluctuaciones especulativas de corto plazo, con el objetivo de mantener a corto plazo la estabilidad de precios, y evitar situaciones como la hiperinflación, que hacen que el valor de ese dinero se destruya, al desaparecer la confianza en el mismo, o como la deflación.

Dinero electrónico

El dinero electrónico (también conocido como e-money, efectivo electrónico, moneda electrónica, dinero digital, efectivo digital o moneda digital) se refiere a dinero que, o bien se emite de forma electrónica, a través de la utilización de una red de ordenadores, Internet y sistemas de valores digitalmente almacenados como el caso del Bitcoin, o es un medio de pago digital equivalente de una determinada moneda, como en el caso del Ecuador o Perú. Las transferencia electrónica de fondos y los depósitos directos son ejemplos de dinero electrónico (Revista Dinero, 2017).

BIENES PATRIMONIALES: Los bienes fiscales o patrimoniales, son aquellos que pertenecen a sujetos de derecho público de cualquier naturaleza u orden y que, por lo general,

están destinados al cumplimiento de las funciones públicas o servicios públicos, tales como los terrenos, edificios, fincas, granjas, equipos, enseres, acciones, rentas y bienes del presupuesto, entre otros. Es decir, afectos al desarrollo de su misión y utilizados para sus actividades, o pueden constituir una reserva patrimonial para fines de utilidad común. Su dominio corresponde a la República, pero su uso no pertenece generalmente a los habitantes, de manera que el Estado los posee y los administra en forma similar a como lo hacen los particulares con los bienes de su propiedad. Los mismos a su vez se pueden subdividir en bienes fiscales propiamente dichos y bienes fiscales adjudicables o baldíos. Estos últimos corresponden a los predios de la Nación que pueden ser adjudicados a las personas que reúnan las condiciones y requisitos establecidos en la legislación (Fallo 21699 de 2012 - Consejo de Estado, 2012).

Para el Código Nacional de Policía y Convivencia se entiende por bienes fiscales, además de los enunciados por el artículo 674 del Código Civil, los de propiedad de entidades de derecho público, cuyo uso generalmente no pertenece a todos los habitantes y sirven como medios necesarios para la prestación de las funciones y los servicios públicos, tales como los edificios, granjas experimentales, lotes de terreno destinados a obras de infraestructura dirigidas a la instalación o dotación de servicios públicos y los baldíos destinados a la explotación económica (Artículo 139 - Ley 1801 de 2016 Nivel Nacional, 2016).

Cuando se habla de bienes patrimoniales por lo general se hace un símil con bienes inmuebles porque refiere a cosas tangibles que forman parte de un patrimonio. Es decir, que dentro del conjunto de cosas que conforman al patrimonio se encuentran los bienes patrimoniales, con dos características principales:

Ser heredables.

Ser respaldo financiero.

Una vez heredado un bien patrimonial, éste pasa a ser derecho del patrimonio de quien recibe ese bien. Los bienes patrimoniales pueden ser utilizados para saldar algún adeudo o poner a la venta para adquirir dinero.

El capital representa el valor monetario de los bienes inmuebles que forman parte de un patrimonio. Para fines legales la clasificación y diferenciación de estos términos respalda el derecho civil de las personas para defender y mostrar que poseen o tienen derecho sobre un bien.

El patrimonio es todo aquello que te pertenece y puede ser vendido, por ejemplo, cosas materiales como:

Una motocicleta o automóvil.

Una casa o departamento.

Un terreno.

Pero también forman parte de él cosas intangibles como son:

Un contrato financiero de un fondo de inversión.

Acciones compradas.

Una herencia.

El potencial físico e intelectual –capacidades, talentos y habilidades– para desarrollar una actividad con la que se genere dinero.

Sin embargo, el patrimonio también se conforma de obligaciones como las deudas, hipotecas y en general todo pago pendiente, por lo que se restan de los derechos patrimoniales y da como resultado el patrimonio real de una persona.

Capital

Es aquí donde el término capital cobra lugar, se refiere a la parte del patrimonio que se puede representar o intercambiar por dinero. Todos los derechos que conforman el patrimonio pueden ser intercambiados por una ganancia.

En resumen, el patrimonio refiere a la posesión de cosas, entre ellas los bienes patrimoniales, bienes tangibles que pueden ser heredados e intercambiados por dinero, es decir, por recursos económicos por lo que son parte del capital de la persona.

ACTIVOS: Un activo es un recurso con valor que alguien posee con la intención de que genere un beneficio futuro (sea económico o no). En contabilidad, representa todos los bienes y derechos de una empresa, adquiridos en el pasado y con los que esperan obtener beneficios futuros.

Tienen en común que son resultado de sucesos pasados y son capaces de generar rendimientos económicos en el futuro. Todos los activos tienen el potencial de traer dinero a la empresa, ya sea mediante su uso, su venta o su intercambio. Son ejemplos de activo un local, una furgoneta, una patente, un ordenador, las materias primas, las inversiones financieras o los derechos de cobro, entre muchos otros (Economipedia, 2021).

Componentes del activo

El activo se divide en dos masas patrimoniales, que se distinguen por su función en el ciclo de explotación. Los activos que más rotan, como las materias primas para producir y el dinero de caja, forman el activo corriente, que compone los activos de mayor liquidez. Mientras que los activos más duraderos y menos líquidos forman el activo no corriente, que se convierten en liquidez mediante la amortización.

Activo corriente: Se hacen efectivos en un periodo inferior a un año. Por ejemplo, el inventario y la tesorería.

Activo no corriente: Tienen una vida útil superior a un año. Por ejemplo, los edificios, los vehículos y la maquinaria (Economipedia, 2021).

Los activos financieros son títulos o anotaciones contables que otorgan en el comprador derecho a recibir un ingreso futuro procedente del vendedor. Los pueden emitir las entidades económicas (empresas, comunidades autónomas, gobiernos…) y no suelen poseer un valor físico, como sí ocurre con los activos reales (un carro o una casa). Además, a diferencia de los activos reales, no incrementan la riqueza general de un país y no se contabilizan en el PIB, aunque impulsan la movilización de los recursos económicos reales, y contribuyen así al crecimiento de la economía. Gracias a estos activos, el comprador consigue una rentabilidad con el dinero que invierte, mientras que el vendedor se financia. Los activos financieros son, en resumen, derechos que adquiere el comprador sobre los activos reales del emisor, y el efectivo que estos generen. (BBVA, 2020).

Principales características de los activos financieros

En cuanto a las características que mejor definen a los activos financieros, habría que señalar principalmente tres (3).

Liquidez. Es la capacidad de transformar el activo en dinero sin sufrir pérdidas. El dinero es el activo más líquido, mientras que después se encuentran los diferentes tipos de depósitos y productos como bonos, fondos públicos u obligaciones.

Riesgo. Lo determinan tanto las garantías que ofrece el vendedor como su solvencia. A mayor probabilidad de que el vendedor cumpla con su compromiso, menor rentabilidad del activo.

Rentabilidad. Como contraprestación por aceptar el riesgo de la cesión de su dinero, el comprador obtiene un interés. Cuanto más elevado, mejor será la rentabilidad del activo.

Clasificación de activos financieros

La principal clasificación entre activos financieros distingue entre los que son de renta fija y los de renta variable.

Renta fija. Los activos de renta fija son aquellos que emiten administraciones públicas o empresas. Los primeros se caracterizan por su menor riesgo, debido al gran respaldo financiero de las entidades que los emiten. Estas se comprometen a devolver el capital invertido al cabo de un período de tiempo previamente establecido y una cierta rentabilidad. Como ejemplos, se pueden citar las letras del tesoro o los pagarés de empresas.

Renta variable. En este tipo de activos ni la rentabilidad ni la recuperación del capital invertido están garantizados, pudiendo incluso perderse la inversión. Su rentabilidad depende de diferentes factores como el balance de resultados de la entidad que vende el activo, o la

situación económica del mercado donde se opera. El principal ejemplo de este tipo de activos son las acciones.

Según su plazo de vencimiento

En función de su plazo de vencimiento, los activos financieros se pueden dividir entre los de corto y los de largo plazo.

Activos monetarios y a corto plazo. Su contrato se amortiza en un plazo de tiempo corto (generalmente menos de un año) y suelen ofrecer rentabilidades bajas.

Activos a medio y largo plazo. Se trata de activos con una duración superior a doce meses y que presentan más riesgos por la posibilidad de fluctuación del valor al ampliar su plazo de vigencia (BBVA, 2020).

Un activo intangible es un activo que no tiene forma física, no es algo material y, por tanto, no se puede ver ni tocar (Economipedia, 2021).

Los activos intangibles provienen de los conocimientos, habilidades y actitudes de las personas y empresas. Hay varios tipos de estos activos como las patentes, marcas, derechos de autor, fondo de comercio, dominios de internet, franquicias, etc. Lo contrario de un activo intangible es un activo tangible.

A pesar de no tener naturaleza física, los activos intangibles son recursos muy valiosos para las empresas, pues pertenecen a ella y pueden generar una gran ventaja competitiva si son correctamente gestionados.

Al conjunto de activos intangibles de los que dispone una empresa en un momento determinado se le conoce como capital intelectual, ya que generan un gran valor gracias al conocimiento y habilidades de los empleados y de la propia organización La mayoría de los activos intangibles no están reflejados contablemente en los estados contables tradicionales de las empresas, ya que resultan muy difíciles de cuantificar.

Características de los activos intangibles

Un activo intangible, como todos los activos, debe proporcionar beneficios económicos futuros razonablemente estimables y debe ser el resultado de una transacción previa (por ejemplo, una compra). La principal diferencia con los activos tangibles, es que no tienen forma física.

Según la norma internacional de contabilidad, "un activo intangible se caracteriza porque es un activo identificable, sin sustancia física y que se destina para ser utilizado en la producción o suministro de bienes o servicios, para arrendamiento a terceros o para fines administrativos".

Sin embargo, existen activos intangibles no identificables, que no puede adquirirse por separado de la empresa y que pueden tener una vida indefinida. El ejemplo más común de un activo intangible no identificable es el fondo de comercio, que es el saber-hacer de la empresa, la influencia de la marca, la fidelidad de los clientes, etcétera.

Ejemplo de activo intangible puede ser cuando una empresa que compra el derecho a explotar una patente durante cinco años que le permite fabricar unos envases que son mucho menos nocivos para el medioambiente a la par de que son más baratos de producir. Esta patente será

un activo intangible, que además se amortizará a lo largo de esos cinco años (Economipedia, 2021).

La gestión de activos de información es una tarea de las gerencias de seguridad o de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio.

Un activo de información en el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”.

Se pueden considerar como un activo de información ~~a~~:

- Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.
- El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.
- Los servicios utilizados para la transmisión, recepción y control de la información.
- Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.
- Personas que manejen datos, o un conocimiento específico muy importante para la organización (Por ejemplo: secretos industriales, manejo de información crítica, know how).

Bajo esta gestión se persigue dar cumplimiento a cuatro puntos claves:

Inventario de Activos: Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización.

Propiedad de los Activos: Todos los activos de información deben ser “propiedad” de una parte designada de la organización. En este sentido, el propietario del activo definirá y garantizará los controles para la adecuada protección del activo.

Directrices de Clasificación de Activos: La información debe clasificarse en términos de su valor, de los requisitos legales, de su sensibilidad y la importancia para la organización.

Tratamiento de Activos: A la información debe dársele un manejo adecuado. Se debe establecer con base en las mejores prácticas de seguridad, qué controles mínimos deben ser aplicados a los activos para su adecuado manejo, dependiendo del nivel de clasificación en el cual hayan sido catalogados (Iso 27001:2013 – Novasec, 2021).

Actualmente, el reto de los responsables de la seguridad de la información en las organizaciones es resolver el "cómo" de la gestión de activos, lo cual involucra el inicio de un proyecto con las siguientes fases mínimas, en resumen:

Figura 6. Gestión de Activos de Información (Iso 27001, 2013 – Novasec, 2021)

LEYES Y NORMATIVIDAD COLOBIANA DE DELITOS INFORMÁTICOS: En Colombia se puede utilizar como herramienta, apoyo y/o complemento en la aplicación del Código de Procedimiento Penal y la Ley 1273 de 05 de enero de 2009, "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Se trata de una normatividad para ser tenida en cuenta, utilizada y aplicada por parte de jueces, fiscales y partes interesadas en que se resarza real y completamente las afectaciones ocasionadas a las empresas en Colombia y/o las infraestructuras críticas del país, por parte de delincuentes informáticos o cibercriminales en el país o desde fuera de él contra las empresas nacionales. Siendo de esta manera consecuentes y respetuosos con la normatividad colombiana y los tratados jurídicos internacionales al respecto, como por ejemplo con el Derecho Internacional, el convenio de Budapest y/0 Ley 1928 de 24 de Julio de 2018, la Carta de las Naciones Unidas que son totalmente aplicados al ciber espacio y a todos los

delitos informáticos generados a nivel internacional, los cuales son delitos sin fronteras físicas o geográficas.

METODOLOGÍAS DE GESTIÓN DE RIESGOS INFORMÁTICOS: A nivel internacional son muchos los estándares que se tienen para gestionar y tratar los riesgos informáticos o cibernéticos en las empresas u organizaciones. Estos estándares y metodologías internacionales son:

• NIST.SP.800-207 y NIST - Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Originarias y aplicadas en EEUU).

• ISO 27001: 2013, ISO 27002: 2013, NTC-ISO-IEC- 27005: 2018, ISO 27007: 2011 ISO 27017: 2015, ISO 27018: 2019, ISO 22301: 2019, ISO 31000: 2018 (Aplicabilidad Internacional).

• MAGERIT NIPO-63012-171-8 (Originaria y aplicada en España, con vigencia también en algunos países de Europa y en países de habla hispana a nivel internacional).

• MEHARI: 2010 (Originaria y aplicada en Francia, reconocida a nivel mundial).

• GLOBAL RISKS REPORT (Originaria del Foro Económico Mundial y aplicado como además tenido en cuenta a nivel mundial).

• OCTAVE (Originaria de Estados Unidos de América, y aplicada en este país, reconocida y tenida en cuenta a nivel mundial).

• HTRA - Harmonized Threat and Risk Assessment Methodology: 2007 (Originaria de Canadá y aplicada allí mismo).

• CORAS: 2011 – CONTRUCT - Construct a platform for Risk Analysis of Security Critical System. (Originaria de Noruega y aplicada en la Unión Europea).

• CRAMM: 1987 (Originaria de Reino Unido (UK) y aplicada en Reino Unido (UK)).

• (Originaria de Francia y aplicada en este país y en la Unión Europea).

• AS / NZS 4360 (Originaria del Comité OB/7 de la Junta de Estándares de Australia y Nueva Zelanda, con aplicabilidad en estos países).

• UNE 71504: 2008 (Originaria de España y aplicada en la Unión Europea).

• RISK SAFE ASSESSMENT – ENISA (Originaria de la unión de Agencias Europeas de Ciberseguridad y aplicada en la Unión Europea).

• IT-GRUNDSCHUTZ-KOMPENDIUM EDITION 2021 – (Originaria en Federal Office for Information Security (BSI) de Alemania y con aplicación en este país).

SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO – ISO 22031-2018: Continuidad de negocio es el término que se acuña para referirse a las estrategias y planificación, mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos.

Un Sistema de Gestión de Continuidad de Negocio (SGCN o BCMS en sus siglas en inglés) certificado bajo la norma ISO 22301 – el estándar de mayor aceptación a nivel internacional- ayuda a las organizaciones a prepararse para las emergencias, a gestionar las crisis y mejorar

su capacidad de recuperación operacional, asegurar la cadena de suministro y protegerse, por ejemplo, su reputación ante una crisis, por el entorno cambiante que rodea a las organizaciones. En el actual contexto en el que ejecuta su actividad, todas las organizaciones pueden estar sujetas a interrupciones como fallos de la tecnología, inundaciones, incendios, interrupciones de servicios públicos o incluso u ataque terrorista.

Las consecuencias de las interrupciones del negocio inesperadas pueden ser de largo alcance y pueden implicar la pérdida de bienes y servicios, la pérdida de vidas humanas o la imposibilidad de entregar productos/servicios clave para la supervivencia de la organización. Un Sistema de Gestión de Continuidad de Negocio se caracteriza por la identificación proactiva de los efectos de la interrupción ya que reconoce aquellos procesos y productos/servicios que son cruciales para la existencia de la organización y establece las respuestas que serán necesarias en caso de que un incidente de gran alcance se produzca. La ISO 22301 proporciona a la organización la capacidad de reaccionar de forma adecuada.

Ventajas de un Sistema de Gestión de Continuidad de Negocio

Las organizaciones que apuestan por implementar y certificar un Sistema de Gestión de Continuidad de Negocio de acuerdo con la ISO 22301 se benefician de importantes ventajas: clientes más satisfechos.

La certificación de la ISO 22301 demuestra a los clientes y posibles clientes que el producto o servicio es fiable y, lo más importante, que lo seguirá siendo. Es una muestra de solidez empresarial. Una organización que cuenta con una estrategia y un plan para superar grandes adversidades estará mucho más preparada en el caso de emergencias y demuestra una gestión

eficaz de sus riesgos. Esta acción ayudará a la organización a recuperarse rápidamente en caso de crisis y a proteger su reputación. Aquí se tienen las credenciales de negocio probados, es decir, demostrar que la organización ha sido verificada por un organismo independiente frente a un estándar reconocido a nivel internacional, lo que se traduce en una calificación positiva de la organización ~~y~~ que refuerza su imagen de marca. Igualmente, aumenta su capacidad para conseguir más ventas, pues en muchas ocasiones, las especificaciones de los RFPs o pliegos de condiciones de las ofertas públicas o privadas requieren la certificación de la ISO 22301 para el suministro. De modo que, la obtención de la certificación abre puertas de negocio. De la misma manera otorga reconocimiento internacional, pues la organización será reconocida y valorada a nivel mundial. Certificar la ISO 22301 y mantener un Sistema de Gestión de Continuidad de Negocio ayudarán a la organización a comprender qué requisitos legales le afectan y debe cumplir y cómo afectan a su actividad y a sus clientes o destinatarios de la actividad que realizan. En el mismo sentido, se obtendrá ahorro de tiempo y costes, dado que la certificación de la ISO 22301 es la forma en que mejor se puede demostrar que se cumple con los requisitos de continuidad de negocio frente a proveedores, los que seguramente querrán tener certeza de la capacidad de respuesta ante una interrupción técnica. No obstante, a otros les preocupará la capacidad de reacción ante las emergencias y la gestión de las crisis. Es importante tener en cuenta que cada uno de esos requerimientos individuales conllevan tiempo y recursos para satisfacerlos, por lo que ser capaz de implementar un estándar es un mecanismo muy eficaz para hacer frente a todas estas obligaciones (ISO 22301, 2018).

DISEÑO METODOLÓGICO

En este trabajo y proyecto de investigación se trabajó con dos (2) enfoques, es decir, con un enfoque metodológico mixto, utilizando factores y fases de la investigación cuantitativa y cualitativa.

Es decir, se utilizó la recolección de datos para probar hipótesis del autor ~~del proyecto~~, con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento, probar y crear una nueva teoría o metodología (Hernández Sampieri, 2014, p. 4). De igual manera, se hizo la recolección y análisis de los datos para afinar las preguntas de investigación (Hernández Sampieri, 2014, p. 5).

Gracias a ello el autor, utilizando este diseño metodológico mixto logró:

•**Recolectar información pertinente y relevante:** Utilizando las fuentes de información primarias y secundarias existentes sobre el tema de estudio se analizaron muchos conceptos, teorías, métodos, estándares, metodologías, que sirvieron como base para esta investigación.

Realizado una estructurada y detallada revisión de toda la información existentes, tratando en lo posible, de utilizar y trabajar siempre con información reciente, verificada que asegurará la innovación, pertinencia y actualidad de los soportes requeridos.

De igual manera, a través de una encuesta respondida por empresarios, gerentes, ingeniero de sistemas, oficiales de seguridad de las organizaciones encuestadas, se pudo conocer información relevante, pertinente, actualizada que permitió hacer esta investigación y ayudar

a resolver el problema de investigación planteado, como, además, cumplir los objetivos específicos y el objetivo general de este trabajo.

•**Analizar toda la Información recolectada**: Se ejecutó este proceso o fase de la metodología a través de procesos rigurosos, que permitieron priorizar y clasificar toda la información obtenida de las fuentes primarias y secundarias utilizadas. Igualmente, consolidar los resultados de la encuesta aplicada en las organizaciones que apoyaron este proyecto de investigación.

Para ello se utilizaron métodos de clasificación priorización y consolidación de la información, que a la final sirvieron de base para crear la nueva metodología, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos.

•**Conocer, estudiar las estadísticas y casos históricos, sobre ataques informáticos o ciberataques en empresas y organizaciones nacionales e Internacionales**: Como parte de los datos y fuentes utilizadas y consultadas, se tuvo en cuenta por parte del autor toda la información nacional e internacional disponible para mirar y detallar los casos que sirvieron como antecedentes y pruebas de los ataques de han sufrido entidades colombianas y extrajeras que fueron víctimas de ciberataques o de ataques informáticos. Estos casos se pueden apreciar en mayor detalle en la sección de anexos de esta investigación.

• **Diseñar y estructurar una nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos**: Una vez

obtenida toda la información sobre el tema de estudio o investigación, una vez analizados todos los casos, luego de ser aplicadas, consolidadas y analizados los resultados de las encuestas se logró diseñar la nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos. Todo esto basado en fundamentos científicos universalmente conocidos y validados a nivel internacional.

• **Aplicar dos (2) pruebas pilotos en casos de ciberataques ocurridos contra empresas a nivel nacional e Internacional, utilizando la metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de estas empresas seleccionadas, esto en dos (2) empresas colombianas (Grupo Empresarial Matrix y el Servicio Nacional de Aprendizaje (SENA):** Una vez que se obtuvo el producto final de este trabajo de investigación "La nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos", se pudo probar su pertinencia, aplicabilidad, relevancia, validez en dos (2) empresas de Colombia.

A. Grupo Empresarial Matrix, con sede principal en Bogotá, subsede en la ciudad de Medellín y con cobertura en todo el país.

B. Servicio Nacional de Aprendizaje (SENA), con sede principal en la ciudad de Bogotá y que cuenta con 117 Centros de Formación en todo el país, en 33 regionales que corresponden a los 32 departamentos y la regional Bogotá Distrito Capital. Con cobertura y presencia en la totalidad de ciudades y municipios del país.

Nota: Los resultados de estas aplicaciones no se publican en este trabajo de grado, debido a los acuerdos de confidencialidad firmados entre el autor de este proyecto y las dos empresas. Esto para guardar su información, reputación y no poner el riesgo información sensible para estas dos organizaciones.

DESARROLLO DEL TRABAJO

De forma consecuente el desarrollo de este trabajo de grado se hizo de acuerdo con lo establecido en el diseño metodológico, es decir, se llevó a cabalidad y teniendo en cuenta las siguientes fases:

•Recolectar información pertinente y relevante: En esta fase se realizó lo siguiente:

A. Se revisó información documentada sobre delitos informáticos, leyes promulgadas para este tipo de delitos en Colombia y a nivel internacional, estándares de seguridad de la información, ciberseguridad, sistemas de gestión de seguridad de la información (ISO 27001, 2013 - ISO 31000, 2019), sistemas de gestión de la continuidad del negocio (ISO 22301, 2018 y Normas Cobit – UK, 2020). Además, se revisó toda la información existente y actualizada sobre metodologías para analizar y gestionar riesgos en las organizaciones en varios países a nivel mundial, algunas de estas con aplicación y cobertura internacional.

   Por otro lado, se revisó información relevante e importante de organizaciones como el Banco Mundial, Foro Económico Mundial, OTAN, OEA, ONU, entre otras entidades de relevancia en el tema de la ciberseguridad a nivel de Colombia, como la Superintendencia Financiera, Csirt Financiero, Csirt Policía Nacional, Centro Cibernético de Colombia, entre otros.

B. Se diseñó una encuesta sobre temas de ataques informáticos y ciberseguridad, la cual indagó sobre la recepción y aceptación de estas empresas y profesionales del área,

sobre la existencia de este tipo de metodologías que valoraran o cuantificaran el daño informático, económico, financiero y reputacional en las organizaciones. Así mismo, buscó verificar la aceptación, importancia o necesidad de esta metodología en las organizaciones y empresas colombianas.

•Analizar toda la Información recolectada:

Una vez recopilada toda la información primaria y secundaria requerida en este proyecto de grado, se prosiguió a organizar, priorizar, clasificar y analizar toda la información documentada, multimedial, entrevistas obtenidas.

De igual manera, una vez aplicadas las encuestas a ochenta (80) personas de diferentes empresas del país, se procedió a consolidar esta información y posteriormente a analizarla al detalle y así poder obtener los puntos de vista e información requerida del sector productivo nacional.

Este análisis de toda la información obtenida permitió al autor tener una sólida base documental y los aportes necesarios para responder al problema de la investigación y alcanzar todos los objetivos propuestos.

Como adicional a ello, el autor logró crear y diseñar una nueva metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos.

Logros según los objetivos:

- Conocer, estudiar las estadísticas y casos históricos, sobre ataques informáticos o ciberataques en empresas y organizaciones nacionales e Internacionales:

Parte de la información recopilada y analizada correspondió a ataques informáticos que afectaron a empresas de Colombia y a nivel internacional, lo cual ayudó a identificar los tipos de ataques más utilizados, los que se presentan con mayor frecuencia, los que más daños han producidos a estas empresas afectadas, y en general, obtener información valiosa que sirve de insumo importante para desarrollar la metodología y ese el trabajo de investigación.

• Diseñar y estructurar una nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa, tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos:

Una vez obtenida toda la información sobre el tema de estudio o investigación, y se analizaron los casos, así como la aplicación y consolidación de los resultados de las encuestas se logró diseñar la nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos. Todo ello basado en fundamentos científicos universalmente conocidos y validados a nivel internacional.

• Aplicar dos pruebas piloto en casos de ciberataques ocurridos contra empresas a nivel nacional e Internacional, utilizando la metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de estas empresas seleccionadas. Esto en dos empresas colombianas (Grupo Empresarial Matrix y el Servicio Nacional de Aprendizaje (SENA).

Una vez que se obtuvo el producto final de este trabajo de investigación “La nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y

financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos", se pudo probar su pertinencia, aplicabilidad, relevancia, validez en dos empresas colombianas:

A. Grupo Empresarial Matrix, con sede principal en Bogotá, subsede en la ciudad de Medellín y con cobertura en todo el país.

B. Servicio Nacional de Aprendizaje (SENA), con sede principal en la ciudad de Bogotá y que cuenta con 117 Centros de Formación en todo el país, en 33 regionales que corresponden a los 32 departamentos y la regional Bogotá Distrito Capital, con cobertura y presencia en la totalidad de ciudades y municipios del país.

Nota: Los resultados de estas aplicaciones no se publican en este trabajo de grado, debido a los acuerdos de confidencialidad firmados entre el autor de este proyecto con las dos empresas. Esto para guardar su información, reputación y no poner el riesgo información sensible para estas dos organizaciones.

RESULTADOS

Los hallazgos obtenidos en el desarrollo de esta investigación fueron:

1. Se logró diseñar y estructurar una nueva metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos. La idea es que esta metodología pueda ser aplicada a priori o antes de que las empresas sufran o sean víctimas de ataques informáticos, con la finalidad de conocer cuál sería su afectación en caso de que se materialicen las amenazas en las organizaciones, pero también apoyar sistemas y metodologías de análisis y tratamientos de los riesgos. Igualmente, se buscó determinar los niveles de inversiones a implementar en las empresas, de acuerdo ~~a~~ con la revisión de la relación costo-beneficio entre lo que se debe invertir-versus el impacto o la afectación total que puede llegar a sufrir una empresa si no implementa sistemas de gestión de la seguridad de la información y no establece los controles que desde la seguridad informática y la ciberseguridad se requieren.

   Los resultados de la aplicación de esta metodología en las empresas y en las organizaciones, permitirá a los gerentes o juntas directivas conocer cuáles son las afectaciones a las que se exponen y de esta manera, con base en cuantificaciones proceder a asegurar los activos y la empresa misma con pólizas de seguros o seguros contra riesgos informáticos de sus activos ya valorados o cuantificados por la metodología.

De igual manera, se podrá aplicar a posteriori, es decir, luego de que la empresa ya sufrió un ataque informático o ciberataque, para poder determinar con la mayor precisión posible cuál es la afectación ocurrida contra los activos organizaciones afectados y así dar a conocer a las autoridades, a gremios, a aseguradoras el daño total y el nivel de afectación que le produjo este ataque informático como tal.

Cabe anotar que esta metodología le sirve a:

A. Empresas, gerentes y juntas directivas para saber a qué se exponen, cuánto se están exponiendo, y en caso de materializarse uno o varios ataques informáticos contra ellos, cuál sería el costo financiero, comercial, económico y reputacional que pueden sufrir (futuro) o que sufrieron (pasado y presente).

   Determinar por cuánto asegurar los activos tangibles e intangibles de las empresas.

   Conocer el valor real de la afectación sufrida y proceder a reclamar a las aseguradoras, a través de sus abogados ante la justicia colombiana o internacional para que les resarzan el daño informático sufrido, entre otras aplicaciones más.

B. Entidades judiciales y de justicia del país, para que sepan darle real justicia y resarcimiento del bien y los activos afectados por las organizaciones que sufran este tipo de ataques informáticos o ciberataques.

C. Peritos o analistas de seguros contra delitos informáticos en las aseguradoras para saber de manera amplia, real y correcta por cuánto pueden ser valorados los ataques se sufran sus clientes y cuánto les correspondería resarcir en caso de que sus empresas clientes sean afectadas. Es decir, poder cubrir en sus pólizas de seguros ofrecidas la realidad de las afectaciones.

Además de las partes interesadas que se mencionan previamente existen otras empresas, academias, fuerzas de ley, instituciones comerciales y jurídicas, entre otras, donde resulta pertinente aplicar esta metodología.

2. La forma y fórmula recomendada para cuantificar las afectaciones en los activos tangibles afectados por ciberataque en las empresas debe recurrir a los principios técnicos de valoración, esto quiere decir, aplicar o tener en cuenta:

   a. Que no se debe valorar solo por lo que costo del gestor de bases de datos como tal, sino por lo que este contenía, aportaba a la empresa, lo imprescindible de ese activo para la organización y por el valor calculado que hasta el momento de la afectación tenía. Es decir, se debe sumar en la valoración de este activo lo siguiente:

   b. Valor propio del activo: Costo del instalador y la licencia. Acá no es el valor que tiene en facturas o en la contabilidad, luego de las depreciaciones, sino que se debe tener en cuenta el valor comercial actual, es decir, lo que vale hoy comprar el activo en el mercado productivo (Valor presente).

   c. Valor pagado por instalación y afinamiento del gestor de bases de datos. Este valor es doble, es decir, lo que ya se había invertido al inicio para poner en funcionamiento el activo + el valor de la nueva instalación y afinamiento posterior al ataque. (Reinicio de la continuidad del negocio) – (Valor presente).

Si el daño no fue total, sino parcial y se debió invertir tiempos en horas hombre o pago de servicio de mantenimiento correctivo, este se debe incluir como mano de obra para reestablecer el funcionamiento del bien afectado, en reemplazo del valor total si la afectación fuera total.

d. Valor actual y acumulado de los registros que tenían las bases de datos del Gestor de BD. (Valor Presente).

e. Valor de lo imprescindible para la empresa: Aquí se encuentran las pérdidas ocasionadas a la empresa por el tiempo que el Gestor de bases de Datos estuvo no operativo y las pérdidas operacionales en la empresa por esta para o detención. (Lucro Cesante) (Valor presente). (MTPD/MAO = Tiempo de reanudación total de los niveles normales de operación del Activo (ISO 22301, 2018))

f. En el caso de que sean Bases de Datos de procesos comerciales, mercadeo o ventas, se debe revisar el histórico de las ventas anteriores en el mismo volumen de tiempo sin operar. Es decir, cuánta utilidad de la operación real hubiera agregado al valor de la empresa si el gestor no hubiera sido atacado o afectado, valor que se debe sumar a la valoración (Valor presente y Utilidad Neta). (MTPD/MAO = Tiempo de reanudación total de los niveles normales de operación del Activo (Iso 22301, 2018)).

g. Si la afectación o suspensión del servicio ocasionó de igual manera multas, sanciones o pago de pólizas, ya sea por cláusulas contractuales o por incumplimientos de ley, estas deben ser tenidas en cuenta y sumar los valores a la valoración total del activo afectado (Valor presente y valor futuro).

h. Si este activo tiene dependencia relacionada con otro u otros activos requerido o requeridos para otro servicio u otros servicios en la organización, este valor o valores de pérdida por la detención en el funcionamiento del activo o servicio dependiente, se debe tener en cuenta, sumar y considerar la valoración total. Es decir, lo que dejó de recibir como utilidad neta la empresa por el tiempo que el servicio o los servicios dependientes dejaron de generarles utilidad o valor. Se deben tener en

cuenta los históricos de la organización en cuanto al tiempo y utilidades netas en ese tiempo de para y traer esos costos a valor presente. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios (MTPD/MAO = Tiempo de reanudación total de los niveles normales de operación del Activo (ISO 22301, 2018)).

Esta afectación cuantitativa total en formula, en las empresas que no coticen en bolsas de valores, sería:

Afectación cuantitativa por ataques informáticos o ciberataques en las empresas no cotizantes en Bolsa de Valores = CP+COI+COA+CRA+TINPMTPD+VRA+MSPPILC+COAADAM.

Si la empresa cotiza en bolas de valores se le debe adicionar la parte de VTPAMTPDPLDS (Valor Total de Pérdidas en Acciones por Tiempo de Afectación y Proyección de afectación futura Línea Directa Semestre siguiente), quedando la fórmula de la cuantificación cuantitativa de la afectación en empresas cotizantes en bolsas de valores así:

Afectación cuantitativa por ataques informáticos o ciberataques en las empresas cotizantes en Bolsa de Valores = CP+COI+COA+CRA+TINPMTPD+VRA+MSPPILC+COAADAM+ VTPAMTPDPLDS.

Nota 01: En las fórmulas anteriores estas siglas significan lo siguiente:

CP = Capex (Valor Presente)

COI = Costo Opex Inicial – Valor pasado traído a valor presente.

COA = Costo Opex Actual – Valor de nuevo Setup requerido.

CRA = Costo de Reparación del Activo – Incluye todas las reparaciones o mantenimiento correctivos requeridos.

TINPMTPD = Costo Total Imprescindible no percibido en para – Lucro cesante no recibido.

VRA = Valor de los registros informáticos o información afectada.

MSPPILC = Costos totales por multas, sanciones, pago de pólizas; incurridos por la empresa afectada o atacada, considerando los aspectos legales, administrativos, financieros y/o contractuales por incumplimientos a raíz de la afectación.

COAADAM = Costos derivados y asociados a las afectaciones de otros activos afectados que dependan del activo principal o de mayor afectación.

VTPAMTPDPLDS = Valor Total de Pérdidas en Acciones por el tiempo de las afectaciones y afectaciones proyectadas futuras lineales directas semestre siguiente.

El sumatorio total de estos valores, es lo que da o define el valor total final del activo afectado y es lo que se debe recuperar o pedir que resarzan económicamente hablando, ante las autoridades o el juez competente o ante la aseguradora previo acuerdo de los valores a asegurar.

Nota 02: Se debe ser muy detallado y precavido al momento de asegurar estos activos, pues las aseguradoras solo pagan o reconocen los valores propios del bien de acuerdo con las facturas en valores pasados, es decir, sin tener en cuenta el valor acumulado, o las variaciones o incrementos del IPC año a año, y el valor presente del activo afectado.

La situación se complica si es un activo que se debe importar, donde entra a jugar el valor pasado de la TRM al momento de la importación o compra anterior (Valor

pasado) o anterior vs el valor presente de la TRM a considerar en la nueva compra (Valor presente).

Nota 03: Al momento de asegurar o adquirir pólizas de seguros para los activos físicos y digitales de la empresa, se recomienda tener en cuenta estos valores definidos anteriormente, lo cual permitirá la recuperación y el lucro cesante de mejor manera en la empresa u organización.

Además, de hacer una correcta valoración del bien o el activo, antes de asegurarlo, en términos generales y a manera de resumen, se hace necesario tener en cuenta la salud o el nivel de salud y funcionamiento del activo.

3. La forma y fórmula recomendada para cuantificar las afectaciones en los activos intangibles afectados por ciberataque en las empresas ~~es~~ se centra en el activo que más está en riesgo es la reputación corporativa. Aquellas empresas que no saben gestionar correctamente un ataque y – en especial – su comunicación a clientes y accionistas, están en peligro de sufrir una caída de reputación. Un informe de Forbes Insights indica que el 46 por ciento de las organizaciones habían sufrido daños en la reputación y en el valor de su marca como resultado de un ataque.

   Además, la combinación de las consecuencias económicas y del daño reputacional, es a menudo fatal. Según datos de la National Cyber Security Alliance de Estados Unidos, el 60% de las PYME desaparece los seis meses siguientes a sufrir un ciberataque.

   Es por ello que para calcular y cuantificar estos ataques informáticos esta metodología propone y sugiere el siguiente método, procedimiento y formulas:

1. Tener en cuenta y a la mano las cifras de las utilidades netas de los últimos 24 meses.

2. Sumar estos valores de Utilidad Neta de los últimos 24 meses.

3. Este valor total de la sumatoria de las utilidades netas, dividirlo entre 720 días que corresponden a los 24 meses para obtener el Valor Ponderado de la Utilidad Neta diaria que ha tenido la empresa o compañía (PDUNeta).

4. Traer a valor presente el Valor Ponderado de la Utilidad Neta diaria que ha tenido la empresa o compañía (PDUNeta), para lo cual se debe revisar que el valor resultante no esté por debajo del valor reciente (mes anterior al ataque), en caso de estarlo se procede a trabajar con el valor actual (IPCUNeta).

5. A estos valores sumarle el valor del o los activos físicos afectados, dañados o destruidos en el ataque informático recibido. Para ello se puede tomar el valor que reposa en factura del bien o el activo y traer ese valor pasado a valor presente (VPAA = Valor Presente del o de los equipos, bienes y activos afectados por el ataque informático) (Capex). Si el Activo no fue destruido o afectado en su totalidad de recomienda tener en cuenta el CRA = Costo de Reparación del Activo – Incluye todas las reparaciones o mantenimiento correctivos requeridos.

6. Sumar el valor total o gasto acumulado pagado por la empresa para constituir su marca, buena imagen, good Will o reputación (Lo que ha permitido generar valor a la empresa). En este caso los valores al detalle que se deben tener en cuenta y sumar son:

A. Costo Acumulado pagado por Publicidad en la empresa en toda su historia. (CAPP).

B. Gastos acumulados pagado por Promoción y divulgación de la Marca y de la empresa, en toda su existencia (GAPPD).

C. Costos totales pagado para la creación de la empresa (CTPC), traído a valor presente.

D. Costos Totales pagados por el Registro y los registros históricos acumulados de la empresa. Estos valores pagados anualmente (CTPR).

E. Si la operación de la empresa está sujeta a licencias de cualquier tipo, se debe considerar y sumar el valor total de las licencias pagadas por la organización, desde su constitución hasta la fecha (VTLP).

7. Sumar el valor correspondiente al MSPPILC = Costos totales por multas, sanciones, pago de pólizas, incurridos por la empresa afectada o atacada, considerando los aspectos legales, administrativos, financieros y/o contractuales por incumplimientos a raíz de la afectación.

8. Sumar el valor correspondiente al COAADAM = Costos derivados y asociados a las afectaciones de otros activos afectados que dependan del activo principal o de mayor afectación.

9. Si la empresa comprometida, atacada o afectada cotiza en bolsas de valores se debe sumar la afectación negativa que sufran sus acciones, en este caso el VTPAMTPDPLDS = Valor Total de Pérdidas en Acciones por el tiempo de las afectaciones y las afectaciones proyectadas futuras lineales directas semestre siguiente.

Al sumar todos los anteriores valores implicados, es lo que da o define el valor total final del activo afectado y es lo que se debe recuperar o buscar que resarzan

económicamente hablando, ante las autoridades o el juez competente o ante la aseguradora previo acuerdo de los valores a asegurar.

Estos cálculos de las afectaciones reputacionales a tener en cuenta se definen en las siguientes fórmulas:

Afectación Reputacional Cuantificada por Ataques Informáticos o Ciberataques en las empresas no cotizantes en Bolsa de Valores = (((PDUNeta + IPCUNeta) * Números_de_Días_Afectados (No operados "MTPD") + VPAA + CRA + CAPP + GAPPD + CTPC + CTPR + VTLP + MSPPILC + COAADAM.

Si la empresa cotiza en bolas de valores se le debe adicionar la parte de VTPAMTPDPLDS (Valor Total de Pérdidas en Acciones por Tiempo de Afectación y Proyección de afectación futura Línea Directa Semestre siguiente), quedando la fórmula de la cuantificación reputacional cuantitativa de la afectación en empresas cotizantes en bolsas de valores así:

Afectación Reputacional Cuantificada por Ataques Informáticos o Ciberataques en las empresas no cotizantes en Bolsa de Valores = (((PDUNeta + IPCUNeta) * Números_de_Días_Afectados (No operados "MTPD") + VPAA + CRA + CAPP + GAPPD + CTPC + CTPR + VTLP + MSPPILC + COAADAM + VTPAMTPDPLDS.

4. Al aplicar las dos pruebas piloto en casos de ciberataques ocurridos contra empresas a nivel nacional e internacional, utilizando la metodología fundamentada en estándares, para cuantificar las pérdidas económicas y financieras de estas empresas seleccionadas, esto en dos empresas colombianas (Grupo Empresarial Matrix y el

Servicio Nacional de Aprendizaje (SENA), se pudo establecer su relevancia, aplicabilidad, pertinencia y la exactitud para ayudar a cuantificar los daños sufridos.

Ambas empresas pidieron seguir utilizando esta metodología y se ponen al servicio para futuras aplicaciones en caso de actualizaciones o mejoras.

Ambas empresas aceptaron que la metodología es correcta, real, que vela por el real resarcimiento y cuantificación de los activos y bienes atacados.

Nota: Los resultados de estas aplicaciones no se publican en este trabajo de grado, debido a los acuerdos de confidencialidad firmados entre el autor de este proyecto con las dos empresas. Esto para guardar su información, reputación y no poner el riesgo información sensible para estas dos organizaciones.

5. En cuanto a la encuesta aplicada en este proyecto de investigación, se pueden resaltar los siguientes resultados:
   A. El 100% de los encuestados laboran para empresas del país y multinacionales con presencia en Colombia.
   B. El 57.5% trabaja en empresas o instituciones públicas, el 36.6% trabaja en empresas privadas y el 5.5% trabaja en empresas de economía mixta.
   C. El 52.5% de las empresas encuestadas son empresas grandes, el 23.7% son empresas multinacionales, el 8.8% son empresas pequeñas y medianas, el 15% restantes pertenecen a otro tipo de clasificación de empresas.
   D. El 50% de las empresas encuestadas pertenece al sector educación, 18.8% a empresas del sector servicios, 4% al comercio al por mayor, 5% a empresas del gobierno, 2,5% al comercio al detal, 1.2% son aseguradoras, 2,5 % sector de

manufactura, 11,2% sector de tecnología y telecomunicaciones, 2,4% sector salud y 2,4% otras empresas.

E. Los niveles o cargos que ocupan las personas encuestadas son: 32.5% trabajadores, 13.8% directivos, 12,5% gerentes, 8.7% mandos medios, 7,5 % ejecutivos, 6,3% asesores, 1,3% consultores, 7,5% docentes o instructores y 9,9% otros cargos.

F. El 91,2% de las empresas encuestadas tiene u ofrece servicios en línea y el 8,8% no ofrece servicios en línea.

G. El 85% de los encuestados conoce los riesgos a los cuales se exponen las empresas y personas, al interactuar o utilizar servicios en línea en el ciberespacio o Internet, el 6,3% no los conoce y el 8,7% restantes dice que tal vez los conoce.

H. De las empresas encuestadas, el 58,8% han sido víctimas de ataques informáticos, el 28,7% no han sido víctimas de ataques informáticos y el 12,5% restantes dice que tal vez sí han sufrido ataques informáticos.

I. Las empresas que respondieron haber sido víctimas de ataques informáticos, respondieron que sus afectaciones fueron en: operación de la empresa, en los servicios ofrecidos por la empresa, robo de información, pérdida de confidencialidad o privacidad de la información, pérdida en la integridad o calidad de la información, pérdida de la disponibilidad de la información, reputacionales afectadas por noticias falsas, contra personas de la empresa, contra equipos, elementos o activos de la empresa, suplantaciones, secuestro de información o sistemas de la empresa, otro tipo de afectación o no conocían el detalle del ataque informático o ciberataque que los afectó.

J. Para el 100% de los encuestados o empresas encuestadas, es importante que las organizaciones estén protegidas contra ataques informáticos o ciber ataques.

K. El 73,8% de las empresas encuestadas consideran que es demasiado importante invertir en protecciones de ciberseguridad, 18,8% muy importante, 7,5% importante y 1,3% ligeramente importante.

L. De las personas encuestadas, el 46,3% en sus cargos tienen relación directa con el tema de ciberseguridad en sus empresas, el 46,3% no directamente y el 7,4% no conoce la relación.

M. En las empresas encuestadas, el 86,3% conoce sus vulnerabilidades en cuanto a seguridad informática o ciberseguridad, el 10% dice tal vez conocerlas y el 3,7% restantes no las conoce o no las tiene presente.

N. En las empresas encuestadas, el 62,5% ha implementado un sistema de gestión de la seguridad de la información (SGSI), el 26,2% no lo ha implementado y el 11.3% restante no sabe.

O. De las empresas encuestadas, el 45% no cuenta con certificaciones internacionales en seguridad de la información, el 32,5% sí cuenta con certificaciones internacionales en SI y el restante 22,5% no sabe o desconoce del tema.

P. El 52,5% de las personas encuestadas no sabe cómo cuantificar los daños informáticos que sufre una empresa, el 28,7% sí lo sabe hacer y el resto 18,8% no está seguro de saberlo.

Q. Se perciben bajo porcentaje de personas que conocieran si existían seguros contra delitos informáticos y el porcentaje de utilización de estos seguros es mucho menor, no están utilizando estas garantías o seguros y muchos los desconocen.

R. El 71,2% de las empresas encuestadas dicen desconocer las leyes y normas en el país, que definen y ayudan a resarcir el daño informático ocurrido por ciberataques. Solo el 17,5% dicen conocerlos y el resto no tienen la seguridad de conocerlas (11,3%).

S. Al 82,5% de las personas encuestadas le gustaría conocer y contar con una metodología que les permita a sus empresas, a los jueces, a las autoridades del país, a sus asesores jurídicos, como a las empresas auguradoras, poder cuantificar, valorar científicamente, de manera exacta y real, las afectaciones sufridas por ataques por delitos informáticos o ciberataques. Al 10% no les interesa en el momento relevante y el 8,5% tal vez le interesa.

CONCLUSIONES

De este trabajo de investigación y del diseño de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos, se puede concluir lo siguiente:

- ✓ Esta versión inicial de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, se ofrecerá y se aplicará en varias empresas en Colombia y a nivel internacional, con la finalidad de ir ajustándola cada día y se puede llegar a una versión plenamente reconocida en Colombia y a nivel Internacional. Los aportes y recomendaciones de las personas, empresas y autoridades que la pongan en práctica, enriquecerán esta metodología en favor de la sociedad y las empresas.
- ✓ Esta metodología se puede utilizar para valorar o cuantificar las afectaciones en cuanto a temas económicos, financieros, administrativos, comerciales y reputaciones en las empresas víctimas de Ataques Informáticos o Ciberataques a nivel internacional. Teniendo en cuenta los activos físicos, no físicos, tangibles e intangibles de las organizaciones y que le generan valor a estas empresas e instituciones públicas, privadas nacionales e internacionales.
- ✓ La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran

mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida (BID, 2021).

- ✓ Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y el suministro de agua y energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales (BID, 2021).
- ✓ Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB. (BID, 2021).
- ✓ En un sentido más general, en la última década, los ataques cibernéticos han aumentado en frecuencia e ingenio. El bajo costo y el riesgo mínimo que conllevan estos delitos han sido factores clave en su crecimiento. Con el simple uso de una computadora y el acceso a Internet, los ciberdelincuentes pueden causar daños enormes mientras permanecen relativamente anónimos. (OEA, 2021).

- ✓ Tanto las personas como las instituciones están expuestas a la incertidumbre y la impredecible naturaleza del delito cibernético. Por lo tanto, es imprescindible abordar estas amenazas. Los esfuerzos para hacerlo deben ser de naturaleza multidimensional, porque se requiere una variedad de factores para construir una cibersociedad resistente. Las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad civil, así como los sectores público y privado, deben trabajar para crear una cultura de ciberconciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad; por lo tanto, es un esfuerzo continuo y complejo (OEA, 2021).
- ✓ Dado el aumento de los ciberataques, la OEA y el BID han visto necesario implementar nuevamente el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés) a fin de poder medir el crecimiento y el desarrollo de las capacidades de nuestros Estados Miembros para defenderse de las crecientes amenazas del espacio cibernético.
- ✓ Los analistas apuntan que cerca del 90 % de los ciberataques que sufren las empresas en Colombia se deben a la ingeniería social, que obedece a técnicas de engaño para conseguir información confidencial, con la que luego suplantan identidades, falsifican correos, entre otras actividades maliciosas.
- ✓ En Colombia, el monto promedio de las cifras de pérdidas por ataque a empresas varía entre los 300 millones y 5.000 millones de pesos (Csirt Ponal y Csirt Financiero, 2020).

- ✓ De acuerdo con Flabio Rodríguez Correa, coordinador de Riesgos y Arquitectura de Claro, y quién participó en el estudio, “en el CSOC -Centro de Operaciones de Ciberseguridad de Claro, por sus siglas en español- ubicado en el Data Center Triara de Claro, se han gestionado en lo que va del año 2020, en promedio, más de cuatro millones de eventos de seguridad al mes, protegiendo servicios propios y de otras compañías, además de la confidencialidad de la información y datos personales de todos los clientes y usuarios”.
- ✓ En Colombia, el delito que mayores denuncias presentó fue la suplantación de sitios web para capturar datos personales con un crecimiento del 372% comparado con el 2019. Este delito tiene una relación directa con modalidades conocidas, tales como el Phishing, Spoofing y Pharming que sufrieron las empresas. Adicionalmente, hubo 3.800 casos denunciados donde este tipo de ataques fueron utilizados por los cibercriminales para capturar datos personales o dispersar malware en las redes corporativas.
- ✓ Estos ciberataques afectaron por igual diferentes sectores productivos del país, los métodos de propagación continúan siendo las campañas de phishing que contienen archivos adjuntos maliciosos. Las entidades de gobierno con mayor presencia de trámites en línea también se vieron afectadas, entre ellos, la Administración de Impuestos y Aduanas, la Registraduría Nacional del Estado Civil, la Fiscalía General de la Nación y las autoridades de tránsito que en su orden han sido las instituciones mayormente suplantadas.

- ✓ Evitar el cibercrimen es un trabajo que implica esfuerzos desde la empresa, las entidades de control, y por supuesto la Policía Nacional, que cuenta con el Centro de Capacidades para la Ciberseguridad de Colombia "C4" y hacen un constante seguimiento a este tipo de casos.
- ✓ Actualmente, resulta imposible crear un entorno informático inaccesible a delincuentes informáticos, aunque si se puede constituir un entorno preventivo que dificulte el acceso a los hackers.
- ✓ El momento en el que se detecta un incidente de fuga de información es un momento crítico en cualquier entidad. Una buena gestión de la fase de detección del ataque informático puede suponer una reducción significativa del impacto del ataque. Esta fase es muy importante, ya que muchas veces se tiene conocimiento de la irrupción una vez la información sustraída se revela al público o a la red, o el ciberdelincuente se pone en contacto con el despacho de abogados correspondiente, para revenderles la información, extorsionarles o amenazarles.
- ✓ A las empresas se les recomienda, apoyarse en terceros expertos independientes que puedan ayudarnos tanto en el desarrollo de todo el proceso, desde el desarrollo de políticas internas, como en la custodia de información, como a la hora de actuar ante alguno de los incidentes expuestos.
- ✓ Un ciberataque y la fuga de información, hoy por hoy, son uno de los más frecuentes dolores de cabeza de los empresarios en todo el mundo. Este tipo de acciones al margen de la ley, no solo generan significativos perjuicios económicos a las empresas, sino, que, a su vez, afectan negativamente su reputación, y generan cierto

grado de desconfianza entre los clientes y la sociedad que a diario consume este tipo de nuevas tecnologías que mueven el comercio y la economía digital a nivel mundial.

- ✓ Se espera que el costo global de los ataques informáticos pase de US$ 3 mil millones en 2015 a US$ 6 mil millones en 2021, según un estudio realizado en 2017 por el grupo CyberSecurity Ventures and Herjavec.
- ✓ No suele haber un inventario de los activos digitales de las empresas: sólo el 37% de los directores considera que la empresa identificó sus activos digitales más valiosos y sensibles.
- ✓ Las empresas tienen políticas de "higiene informática endebles: el 93% de los ataques podrían ser prevenidos con mejores políticas (actualizaciones de software, bloqueo de mails sospechosos, capacitación digital sobre phishing, etc.). Las amenazas a la seguridad informática están en todos lados y los ataques producen titulares cada vez más a menudo. También son muy costosos, tanto en dinero como en pérdida de reputación.
- ✓ Los costos de la "ciberdelincuencia incluyen daños y destrucción de datos, robo de dinero y propiedad intelectual, pérdida de productividad, malversación, fraude, daño a la reputación e interrupción del curso normal de los negocios. Su restablecimiento demanda normalmente de una investigación detallada ("forense"), restauración de datos y de sistemas atacados, y de una reorganización general de todas las áreas de la empresa.

- ✓ Además, la combinación de las consecuencias económicas y del daño reputacional, es a menudo fatal: Según datos de la National Cyber Security Alliance de EE.UU. el 60% de las PYME desaparece dentro de los seis meses siguientes a sufrir un ciberataque.

RECOMENDACIONES

Una vez alcanzado el objetivo del presente trabajo de investigación, de diseñar una metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos, y teniendo en cuenta los resultados obtenidos, el autor se permite hacer las siguientes recomendaciones:

1. Esta metodología se puede aplicar en cualquier orden de acuerdo con lo que se establezca en el plan de actividades del grupo de trabajo que decida aplicarla en la organización o empresa afectada por delitos informáticos o ciberataques.
2. Se recomienda aplicar la metodología en el orden que se presenta, la cual detalla el paso a paso y va desde lo más básico hasta lo más detallado los temas tratados. Esto para mejor comprensión, aplicación y efectividad en la empresa afectada por delitos informáticos o ciberataques.
3. Vale la pena destacar que esta metodología se puede aplicar en dos momentos:

a. El primero, cuando la empresa ya es víctima de un ataque informáticos o ciberataques y se necesita valorar o cuantificar la afectación económica, financiera, administrativa, comercial o reputacional.

b. El segundo, si se requiere hacer una valoración real de los riesgos en cuanto a ataques informáticos o ciberataques que pueda sufrir la empresa de acuerdo ~~a~~ con las vulnerabilidades y amenazas que tenga contra sus activos.

En este segundo momento se puede tomar el resultado para:

- Cuantificar las afectaciones que se puedan sufrir en la empresa, y con base en ese estudio, implementar planes de salvaguarda o mitigación de esos posibles ataques.
- Para adquirir una póliza de seguro contra este tipo de ataques, que realmente cubra todo lo requerido en la organización, y sea consecuente con el valor de la empresa y lo que esos activos tangibles e intangibles agregan valor a la organización.
- Para revisar y analizar la relación costo-beneficio entre los riesgos que se tienen en la empresa y el valor que se debe invertir para proteger y salvaguardar los activos. Es decir, si vale o no la pena la inversión en pro de la protección y la ciberseguridad de la empresa u organización.

4. Si lo que desea es cuantificar daños por delitos informáticos en la empresa en activos físicos y tangibles, es necesario tener en cuenta el "Anexo J: Etapa de Ciberataques Causantes de Pérdidas Económicas y Financieras Directas" y las fórmulas que allí se recomiendan y explican.
5. Si lo que desea es cuantificar daños por delitos informáticos en la empresa en activos no físicos o intangibles, es necesario tener en cuenta el Anexo K: Etapa de Ciberataques Causantes de Pérdidas o Afectaciones Reputacionales (Pérdidas Económicas y Financieras Indirectas y/o Colaterales).

6. Si se va a aplicar el Anexo J o el Anexo K, se sugiere de igual manera, observar el Anexo M: “Etapa de pérdidas por Leyes y Normas Nacionales e Internacionales”, donde se despejan las implicaciones jurídicas o sanciones a lugar.
7. Se sugiere que todas las empresas tengan implementado un Sistema Integrado de Gestión y particularmente, el Sistema de Gestión de la Seguridad de la Información (SGSI).
8. En lo posible toda empresa en Colombia y a nivel internacional, debe tener implementado y certificado al menos dos estándares de seguridad. Se recomiendan mínimo la Certificación en ISO 27001 - SGSI, 2013 y en ISO 22301 – SGCN, 2018.

   Todos los representantes legales, gerentes generales, CEO, miembros de Juntas Directivas y de las altas gerencias en todas las empresas, compañías o instituciones públicas y privadas, deben tener muy presente el tema de ciberseguridad y los riesgos a los cuales se enfrentan todos los días las organizaciones a su cargo. Se trata de uno de los riesgos más grandes y con mayor crecimiento que enfrentan actualmente las empresas, entidades públicas y los Estados en general. Incluso, se observa cómo los países han trasladado la guerra al ciberespacio afectando infraestructura, equipos de trabajo, sectores de la economía, entre otros.
9. Todas las empresas deben tener mecanismos de detección y/o contención contra estos ataques informáticos, pues estos crecen cada día. Según la

consultora PwC (2021), el costo de no identificar al agresor de los ciberataques será de US$ 6000 M en 2021.

10. Las empresas y sus directivos deben ser conscientes de que las amenazas a la seguridad informática no solo se mantienen, sino que van en aumento en cuanto a tamaño, sofisticación y costos. En consecuencia, surge la necesidad de implementar una estructura de administración y supervisión efectivas con un enfoque integrador, tal como lo señala Alejandro Rosa, socio de PwC Argentina de la práctica de Gobierno Corporativo.
11. Algunas áreas de foco que los directores, gerentes, administradores, deben incorporar a su agenda son:

a) Considerar como clave para el negocio los riesgos de ciberseguridad.
b) Tener un enfoque de supervisión que incluya la asistencia directa de expertos en seguridad informática y digitalización.
c) Discutir si la estrategia y los planes de defensa contra ataques informáticos son adecuados, incluyendo la definición del riesgo tolerable.
d) Establecer cuál es la información periódica o por excepción que necesitarán para monitorear la gestión del riesgo.
e) Monitorear la resiliencia de la organización ante los ataques, es decir, sus capacidades para resistir y recuperarse de los eventos.

12. Se recomienda establecer un programa efectivo y eficiente de gestión de riesgos, teniendo en cuenta que se trata de un camino que debe ser recorrido por la empresa, con el objetivo de mitigar los riesgos clave y lograr una organización resiliente a los ataques informáticos.

13. Se recomienda la concientización y educación a los usuarios de todas las empresas y a todo nivel por medio de la promulgación de políticas de seguridad y la continua capacitación en el uso de sus sistemas de modo seguro y prácticas que incluyan la prevención de los riesgos cibernéticos.
14. En todas las empresas como medida de prevención al acceso no autorizado a los sistemas y aplicaciones, se deben establecer políticas de control de acceso físico y lógico.
15. Es importante establecer un plan para estar preparados ante cualquier eventualidad. Se deben establecer responsabilidades y procedimientos.
16. Contratar ciberseguros o seguros contra delitos informáticos (Transferir el riesgo de la empresa), cuya finalidad es proteger a las entidades frente a los incidentes derivados de los riesgos cibernéticos, el uso inadecuado de las infraestructuras tecnológicas y las actividades que se desarrollan en dicho entorno. Vale la pena mencionar las principales garantías ofrecidas por el mercado asegurador:

- Responsabilidad civil frente a terceros perjudicados.
- Cobertura de los gastos materiales derivados de la gestión de los incidentes.
- Cobertura de las pérdidas pecuniarias ante la interrupción de la actividad derivada de un fallo de seguridad y/o sistemas.
- Cobertura de los gastos de asesoramiento legal en los que se debe incurrir para hacer frente a los procedimientos administrativos.
- Cobertura ante la denegación de acceso a otros sistemas.

- Acompañamiento en la gestión de la crisis.

Estos seguros suelen venir acompañados de servicios adicionales tales como son:

• El borrado de huellas e historial.

• La reparación de sistemas y equipos.

• La recuperación de datos.

• La descontaminación de virus.

Nota: Se recomienda cuantificar bien los activos de las empresas antes de asegurarlos, ya que de esta manera se traslada el riesgo de la empresa a la aseguradora y en los montos correctos.

17. Una vez detallada de forma muy general algunas de las diferentes responsabilidades en las que pueden incurrir los empresarios ante un ciberataque, es muy importante recomendar mantener las medias de seguridad y protección en materia de ciberseguridad, así como el cumplimiento estricto de la normativa legal y administrativa actual en materia de protección de datos y riesgos cibernéticos de las empresas, para evitar problemas legales que pueden generar mayores inconvenientes. Por último, es recomendable y de vital importancia contratar una adecuada póliza de ciberriesgos que contemple este tipo de riesgos y sus coberturas.
18. Dado a la impredecibilidad y a la constante evolución de los ataques cibernéticos, es imperativo la continua evaluación y gestión de riesgo. Dada su importancia se invita a:

● Analizar las áreas de negocio y los procesos de la empresa potencialmente expuestos.

● Identificar los riesgos y proponer los mecanismos de control y mitigación necesarios.

● Discutir las opciones disponibles con un ejercicio de costo-beneficio para transferir o asumir los riesgos identificados, según el apetito de riesgo y la capacidad de absorción disponible.

● Preparar la información necesaria para la transferencia, en los mercados nacionales e internacionales y por vías tradicionales o alternativas, si fuese necesario.

Ante este tipo de ciberataques, ya no sólo corresponde hablar de prevención o de aseguramiento. Éstos últimos son imprescindibles, pero no suficientes. Se requiere hablar de resiliencia, dando por hecho que el riesgo se va a manifestar y disponiendo de todas las estrategias a nuestro alcance para mitigarlo, gestionarlo y superarlo.

Se recomienda a todas las empresas estar preparadas y protegidas, pues se proyecta una DDoS total o mayoritaria a nivel mundial en menos de diez años, es decir, una “Pandemia Digital” de ciberataques, que solo las empresas protegidas y con sistemas de continuidad de negocios robustos podrán seguir operando.

REFERENCIAS

ALEMÁN NOVOA, Helena, RODRÍGUEZ BARRERA, Claudia, Fundación Universitaria Juan de Castellanos, Facultad de Ingeniería, Tunja, Boyacá, Colombia, (2018): Metodologías Para el Análisis de Riesgos en los SGSi, Methodologies for Analysis of Risks in the ISMS, https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874.

Almanza, A. (2016). Encuesta nacional de seguridad informática 2016. Desafíos de la cuarta revolución industrial. Sistema, 143, 18-36.

Análisis del caso Diginotar. http://www.computerworld.com/s/article/9233138/One_year_after_DigiNotar.

ÁNGEL MENDOZA, Miguel, (2020): Ciberataques: una de las principales amenazas para el 2020, De acuerdo una nueva edición del informe anual sobre riesgos que publica el Foro Económico Mundial, los ciberataques aparecen nuevamente como una de las principales amenazas que afrontaremos durante el 2020, https://www.welivesecurity.com/la-es/2020/02/13/ciberataques-principales-amenazas-2020/.

BECHARA PALACIOS, Yenifer Yirlesa, Universidad Cooperativa de Colombia, (2020): Análisis Jurídico del la Ley 1273 del 2009 y el Surgimiento y Expansión del Delito de Hurto y Semejantes por Medios Informáticos,

https://repository.ucc.edu.co/bitstream/20.500.12494/19788/3/2020_analisis_delitos_informaticos.pdf.

BORBÓN SANABRIA, Jeffrey Steve, Universidad Nacional Autónoma de México (2017): Lo que el Rumor se Llevó, Crónicas del Riesgo Reputacional.

https://revista.seguridad.unam.mx/numero-16/lo-que-el-rumor-se-llev%C3%B3-cr%C3%B3nicas-del-riesgo-reputacional.

Caro, M. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 49-82. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. IEEE Documento de opinión, 67, 1-16.

CCIT, Policía Nacional, INFORME TENDENCIAS CIBERCRIMEN en Colombia 2019 – 2020, (2021), https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf.

Convenio Internacional sobre Cibercriminalidad, Budapest, 23.XI. 2001, http://documentostics.com/documentos/convenio_cibercriminalidad.pdf.

Correa, M., & Cabezas, I. (2014). Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional - SIUN. 9 BUGARINI, L. F. (2007). Tesis propuesta de seguridad en la información, Escuela

Superior de Comercio y Administración. México D.F. Obtenido de http://tesis.ipn.mx/bitstream/handle/123456789/498/TESIS%20PROPUESTA%20SEGURIDAD.pdf? sequence=1 10 ESCRIVÁ GASCÓ, G., ROMERO SERRANO, R. M., & RAMADA, D. J. (2013). Seguridad Informática. Macmillan Iberia, S.A. Obtenido de https://ebookcentral.proquest.com/lib/ucooperativasp/detail.action?docID=3217398&query=segurid ad%20informatica#.

Corte Constitucional de Colombia, Sentencia C-344/17, (2017): DEMANDA DE INCONSTITUCIONALIDAD CONTRA EXPRESION "MATERIALES Y MORALES" CONTENIDA EN CODIGO PENAL SOBRE REPARACION DEL DAÑO POR RESPONSABILIDAD CIVIL DERIVADA DE LA CONDUCTA PUNIBLE-Perjuicios son indicativos y no excluyen la reparación integral de perjuicios a favor de las víctimas de delitos a través de diferentes instrumentos, https://www.corteconstitucional.gov.co/relatoria/2017/C-344-17.htm.

Club de la securite de lìnformation francais, mehari, [On line]. Disponible en: https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf.

Clusin, LES FONDAMENTAUX DE MÉHARI, (2019), https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/.

Clusin, LES MODULES DE MÉHARI, (2019), https://clusif.fr/services/management-des-risques/les-modules-de-mehari/.

De Tomas, S. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. ICADE, 92, 14-47.

Documento CONPES 3995, (2020): Política Nacional de Confianza y Seguridad Digital, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf.

Documento CONPES 3854, (2016): Política Nacional de Seguridad Digital, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

Escuela de Ciencias Jurídicas, España, (2020): ¿Cuáles son delitos informáticos más comunes?, https://escuelacienciasjuridicas.com/delitos-informaticos-mas-comunes/.

Enisa, European Union Agency for Cybersecurity, (2021): Risk Safe Assessment and Threat and Risk Management, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_risksafe-assessment.

Ero Security, Canada, (2021): Harmonized Threat and Risk Assessment (HTRA) Workshop Description, http://erosecurity.ca/en/harmonized-threatrisk-assessment-htra/.

Fairbrother, H., Curtis, P., & Goyder, E. (2016). Making health information meaningful: Children's health literacy practices. *SSM - Population Health*, *2*, 476–484. doi.org/10.1016/j.ssmph.2016.06.005

FERNÁNDEZ QUIRÓS, Fernando (1998). Estructura Internacional de la Información. Síntesis. Madrid.

SÁNCHEZ, Gabriel - URRUTIA, Román. IEEE España, (2020): Amenazas Persistentes Avanzadas (APT) como medida de disuasión en el ciberespacio. http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO12_2020GABSAN_Submarinos.pdf.

GATES, Bill. (1995). Camino al futuro. Mc Graw Hill. Madrid.

GIDDENS, Anthony. (2000). Un mundo desbocado. Los efectos de la globalización en nuestras vidas. Taurus. Madrid.

GIBSON, William (1999). Neuromante. Minotauro. Barcelona.

GRAY John. (2000). Falso amanecer. Los engaños del capitalismo global. Paidós. Barcelona.

Harmonized TRA Methodology (TRA-1), Canada, (2021): Canadian Centre for Cyber Security, https://cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1.

Hernández Sampieri, R., Méndez, S., Mendoza, C., & Cuevas, A. (2017). *Fundamentos de investigación*. México: McGraw-Hill.

Instituto de Gobierno de TI. COBIT 4.1. "Marco de Trabajo - Objetivos de control – Directrices Generales – Modelos de Madurez", 2007.

ISO (2012). ISO/IEC 27032:2012. Information technology - Security techniques -- Guidelines for cybersecurity. Ginebra: International Organization for Standardization.

ISO (2016). ISO/IEC 27000:2016 Preview. Information technology -- Security techniques -- Information security management systems - Overview and vocabulary. Ginebra: International Organization for Standardization.

ISO 27000.es, SGSI Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información, (2020), https://www.iso27000.es/sgsi.html.

IT Grundschutz: una herramienta para la seguridad de la información, Alemania, (2021): IT_Grundschutz_Kompendium_Edition2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6.

Joyanes, Luis. (1997). Cibersociedad. Los retos sociales ante un nuevo mundo digital. Mc Graw Hill. Madrid.

L. E. Sánchez, A. Santos-Olmo, V. Figueroa, D.G. Rosado, E. Fernández-Medina, (2020): Realizando una Revisión Sistemática de Metodologías ISRA orientadas a la Seguridad TIC. Periodo 2014-2019, https://editorial.urosario.edu.co/pub/media/hipertexto/rosario/anexos/proyecto-cibsi/11_F19_ok.pdf.

Legaltoday, Rosso Pérez, Manuel Enrique, (2019): Criterios de cuantificación del daño moral derivado de delito, https://www.legaltoday.com/practica-juridica/derecho-penal/penal/criterios-de-cuantificacion-del-dano-moral-derivado-de-delito-2019-10-23/.

Legis, Ámbito Jurídico, Rojas Quiñones, Sergio, Grupo de Investigación en Derecho Privado - Pontificia Universidad Javeriana (2019): ¿Cómo se debe cuantificar el daño según el Consejo de Estado y la Corte Suprema? (Parte I), https://www.ambitojuridico.com/noticias/columnista-online/administrativo-y-contratacion/como-se-debe-cuantificar-el-dano-segun-el.

Ley de Delitos Informáticos en Colombia, La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigente, Delta Asesores (2012), https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/.

López, Ramírez, Marxela, Universidad Piloto de Colombia, (2018): ANÁLISIS DE RIESGOS EN UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CON METODOLOGÍAS COMPLEMENTARIAS. http://polux.unipiloto.edu.co:8080/00004422.pdf.

Mac Bride et al. (1992). Un solo mundo, voces múltiples. Fondo de cultura económica. México.

Machín & Gazapo, 2016). La ciberseguridad como factor crítico en la seguridad de la unión europea. Revista UNISCI, 42, 47-68.

Metodología Coras (Construct a platform for Risk Analysis of Security critical system) [On line]. Disponible en: http://seguridades7a.blogspot.com/p/coras.html.

Ministerio de Hacienda y Administraciones Públicas, España, (2012). - NIPO: 630-12-171-8: MAGERIT versión 3 (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

NIST, information security, national Institute of Standards and Technology [On line]. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66,

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003.

Samper, Metodologías de evaluación del riesgo informático, 2014. http://metodevaluriesgos.blogspot.com/2014/03/metodos-para-realizar-evaluacion-de.html.

Pinari, Reglamentación AS/NZS 4360. (2021), AS/NZS 4360:1999 o Estándar australiano proporciona una guía genérica para la gestión de riesgos,

https://www.piranirisk.com/es/soluciones/reglamentaciones/asnzs-4360.

Presidencia de la República, Colombia, LEY 1928 DEL 24 DE JULIO DE 2018 (2018): LEYNo.1928 24 JUL2018 POR MEDIO DE LA CUAL SE APRUEBA EL «CONVENIO SOBRE LA Ciberdelincuencia», ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST,

http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf.

Reporte de Ciberseguridad 2020, OEA, BID, (2021): CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE, https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Risk4all, herramienta GRC que da soporte durante las distintas etapas del cumplimiento relacionado con la privacidad y en general con la seguridad de la información y el riego de seguridad o ciber-riesgo, (2019), https://www.risk4all.es/funcionalidades/.

ROA BUENDÍA, J. F. (2013). Seguridad Informática. Madrid: McGraw-Hill.24.

Salón, J. (2010). El ciberespacio y el crimen organizado. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 131-164. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Tangient LLC. (2014). EBIOS – Metodología Francesa Análisis y Gestión de Riesgos. Retrieved marzo 21, 2014, from EBIOS - Metodología Francesa Análisis y Gestión de Riesgos: [On line]. Disponible en: http://seguridadinformaticaufps.wikispaces.com/EBIOS+y+Metodologia+francesa+Analisis+y+Gesti%C3%B3 n+de+Riesgos.

Techtarget, ISACA (2019): CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia? ¿Qué hay en un nombre? Analice las verdaderas diferencias entre un CERT, un CSIRT, un CIRT y un SOC, antes de decidir qué es lo mejor para su organización, https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia.

T2B, (2021): ¿Cuáles son las consecuencias del ciberataque a una empresa?, https://t2b.tech/cuales-consecuencias-ciberataque-empresa/.

UNE – Normalización Española, UNE 71504, (2008): Metodología de análisis y gestión de riesgos para los sistemas de información, https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430.

Vallés, L. (2016). La ciberseguridad en el mundo actual. TINO, 50, 585-620.

Vargas, R.; Recalde, I. & Reyes, R. (2016). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 31-45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571.

ANEXOS

Anexo 01: Producto de la investigación: Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos “Atencia-Lalinde-Eafit-Co - (Versión 1.0)”.

Anexo 02: Encuesta aplicada a las empresas.

Anexo 03: Ponderación y resultados de la encuesta aplicada a las empresas.

Anexo 04: Casos reportados de Ciberataques a empresas en Colombia y a nivel mundial.

Anexo 01: Producto de la investigación: Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos “Atencia-Lalinde-Eafit-Co - (Versión 1.0)”.

ANEXO 01

Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

Atencia-Lalinde-Eafit-CO (versión 1.0)

Medellín - Colombia
2021

TÍTULO: *Atencia-Lalinde-Eafit-CO – versión 1.0. Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos. Libro I.*

Autor y coordinador de contenidos:
Víctor Rafael Atencia Urueta, Estudiante candidato al título de MBA en Administración, Universidad Eafit – Medellín (Colombia).

Director Proyecto de Grado:
PhD. Juan Guillermo Lalinde Pulido, Profesor Universidad Eafit – Medellín (Colombia)

Medellín – Antioquia (Colombia), junio de 2021.
Disponible esta publicación en la Biblioteca de la Universidad Eafit (Medellín – Colombia)

Edita:

Índice

Índice de Tablas

Índice de Figuras.

Prologo

La metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o ataques informáticos. Nace de la ausencia de mecanismos, procedimientos y estándares que ayuden a identificar, cuantificar cualitativa y cuantitativamente las afectaciones que sufren las organizaciones, las empresas al ser afectadas por este tipo de delitos.

En Colombia y algunos países se han adelantado acciones desde el Derecho Penal, particularmente en el derecho probatorio, aportando en sus procesos y legislación la responsabilidad de cuantificar estos impactos negativos y/o afectaciones (fruto de estos ciberataques o ataques informáticos). Esto ha servido particularmente a los jueces, fiscalías o entidades estatales que hagan las veces de fiscalías en los distintos países.

A pesar de que este avance es muy significativo, al querer igualar los delitos informáticos a delitos presenciales, civiles, comerciales, penales en sus respectivas leyes y procesos judiciales, todavía dista de una correcta y verdadera cuantificación y/o valoración de los activos afectados en las organizaciones.

Cabe anotar que la situación actual se agudiza al existir la necesidad de cuantificar las afectaciones por los ataques informáticos, a las empresas y/o personas naturales al interior de estas organizaciones, en temas considerados esenciales como principios, activos intangibles, derechos intangibles y/o reputaciones, derechos a la privacidad, derechos a la protección de datos personales o empresariales. A pesar de ser intangibles, sí afectan considerablemente el buen nombre, good Will, know-how, imagen corporativa de las organizaciones, llevándolas a pérdidas de sus clientes, reducción del valor en las acciones, pérdida de inversiones e inversionistas, pérdidas por reducción en volúmenes de ventas y/o servicios. Es decir, acciones que afectan considerablemente las utilidades, ebitda, eva, roe, roi, indicadores de liquidez, indicadores financieros, entre otros más.

La idea con esta primera versión de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos, es ofrecer una herramienta innovadora, pertinente, científica y basada en estándares internacionales, que ayude a los jueces, fiscales, jurídicos, gobiernos, poderes de Estado, aseguradoras, empresas, alta gerencia, juntas directivas y/o juntas corporativas, academia, entre otros más.

Además, que permita dar a conocer a todos los líderes corporativos, empresariales, gobiernos, poderes estatales, aseguradoras, y en general a todas las empresas y corporaciones públicas y privadas, los valores reales a los que están expuestos si no generan una especial atención a los temas de ciberseguridad. Resulta prioritario tener en cuenta los riesgos mencionados en sus estrategias comerciales, financieras, operativas, procedimentales a su cargo en sus empresas y/o países.

En esta misma línea viene trabajando la Organización de Estados Americanos (OEA), en alianza con el Centro Global de Capacidad en Seguridad Cibernética (GCSCC) de la Universidad de Oxford (UK) en la promulgación de un “Marco de Daño Cibernético” que al diseñarse, desarrollarse y aprobarse se pueda aplicar a todos los países miembros de la OEA (Reporte de Ciberseguridad OEA – BID – 2020).

En conjunto la OEA con la Alianza por la Seguridad de Internet (A.S.I), vienen trabajando en la creación de un “Manual de Supervisión del Riesgo Cibernético para las Juntas Corporativas”, desde el año 2019, con la finalidad de crear conciencia y ofrecer herramientas, indicadores a juntas directivas, juntas corporativas, alta gerencia, gobiernos, poderes estatales, académica, entre otros. Se busca en esencia tener empresas más seguras, crear ciber resiliencia empresarial, empresas más preparadas ante las ondas disruptivas de ciberataques, que les permitan seguir operando en la sociedad, en el ciberespacio y seguir siendo eficientes, eficaces y productivas (Reporte de Ciberseguridad OEA – BID – 2020).

En términos generales, esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos, está desarrollada y se puede aplicar modularmente debido a que tienen un prólogo, una descripción general tipo ejecutiva, una introducción, un resumen de gestión, una serie de dieciséis (16) anexos y una serie de apéndices que en conjunto le van a permitir al lector entender al 100 por ciento esta herramienta y considerar y/o aplicar en sus empresas y estados a cargos.

Descripción General de Tipo Ejecutiva.

La metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos es una herramienta que se pone al servicio y a consideración para su referencia y aplicación de personas jurídicas y naturales, en especial para todos esos profesionales con funciones y/o cargos de Ceo, Cios, Cisos, fiscales, jueces, asegurados, aseguradoras, analistas de seguros, peritos, abogados, gerentes, alta gerencia, juntas directivas, juntas corporativas y a todos los ejecutivos encargados de asegurar, velar por la estrategia, el patrimonio, buen nombre y los resultados operacionales, financieros; en sus empresas, organizaciones y/o estados.

Esta metodología les permitirá tener un punto de partida, de análisis, de apoyo en la valoración y/o cuantificación de las afectaciones sufridas por delitos informáticos. Adicionalmente, dará las pautas a tener en cuenta para mitigar los daños y las repercusiones negativas, así como conocer el detalle de costos y valores de estas afectaciones en sus empresas y/u organizaciones.

Se recomienda su utilización para:

- ✓ Cuantificar las afectaciones sufridas por empresas en Colombia y a nivel internacional, como parte de procesos jurídicos y de derecho penal, civil, en el cual abogados, jueces, fiscales, peritos deban asesorar, calcular la real afectación desde el punto de vista económico y financiero de la empresa afectada, teniendo en cuenta el derecho probatorio, la rigurosidad de estas afectaciones y/o procesos para todas las partes interesadas.

- ✓ En Colombia se puede utilizar como herramienta, apoyo y/o complemento en la aplicación del Código de Procedimiento Penal y la Ley 1273 de 05 de enero de 2009, "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

  Se buscar que la metodología sea tenida en cuenta, utilizada y aplicada por parte de jueces, fiscales y partes interesadas en que se resarza real y completamente las afectaciones ocasionadas a las empresas en Colombia y/o las infraestructuras críticas del país; por parte de delincuentes informáticos o cibercriminales dentro o fuera del país contra las empresas nacionales. Siendo de esta manera consecuentes y respetuosos con la

normatividad colombiana y los tratados jurídicos internacionales al respecto como por ejemplo con el Derecho Internacional, el Convenio de Budapest y/0 Ley 1928 de 24 de Julio de 2018, la carta de las naciones unidas y que son totalmente aplicados al ciber espacio y a todos los delitos informáticos generados a nivel internacional, los cuales son delitos sin fronteras físicas o geográficas.

- ✓ Aplicada en Colombia y a nivel internacional por aseguradoras y asegurados, peritos de seguros de protección contra delitos informáticos, peritos en evaluación y gestión de riesgos cibernéticos o de ciberataques; para que les permita evaluar y cuantificar de manera valida, real, adecuada y científica, bajo estándares internacionales las afectaciones económicas, financiera y reputacionales a que pueden verse involucradas las empresas que resulten víctimas de delitos informáticos o ciberdelitos.

- ✓ Ayudar en Colombia y a nivel internacional en todo lo referente a la Legislación Procesal del Delito Cibernético y/o Ciberdelitos.

- ✓ Ayuda a crear conciencia de ciberseguridad, resiliencia cibernética, ciberespacio seguro en las juntas directivas, alta gerencia, gerentes, directores de operaciones, directores de riesgos, directores económicos y/o financieros, directores estratégicos en las empresas y en general en todas las organizaciones públicas y privadas; teniendo a su alcance una herramienta que les muestre las reales afectaciones a las cuales se pueden ver abocados si llegan a ser víctimas de ataques informáticos o ciberataques, esto desde el punto de vista económico, financiero y reputacional.

  También permitirá a todas estas empresas, personas y roles poder tener claro, conocer el panorama de la ciberseguridad, los requerimientos para la estabilidad cibernética global, lo referente a la gobernanza de Internet y todo cuanto en sus empresas deben aportar e invertir para poder contar a nivel local, nacional y global con un ciberespacio abierto, libre y seguro, que les permita seguir operando y siendo representativos en sus nichos de mercados nacional y globales.

  Será posible conocer además cuáles son los niveles de inversiones que se deben realizar al interior de sus empresas y/u organizaciones para estar interconectados, operando y beneficiándose de manera segura en todos los servicios en línea, industrias 4.0, transformación digital y el ciberespacio como tal. Mirando y analizando la relación costo-beneficio de sus inversiones

y de esta manera estar protegidos en el mayor nivel posible contra ataques informáticos o ciberataques.

Lo anterior si se tiene en cuenta que se proyectaban aumentos de inversiones en ciberseguridad en las empresas a 2025 con un crecimiento del 88% promedio a los niveles actuales, pero factores como la recesión económica, la pandemia por covid-19 han mermados considerablemente estas inversiones; poniendo aún más en riesgos a todas las organizaciones y el ciberespacio como tal (Informes OEA – Foro Económico Mundial – ONU -2021).

Buscando en términos generales y como finalidad corporativa y/o empresarial eliminar las posibles afectaciones que le puedan ocasionar estos delitos informáticos en sus empresas y organizaciones.

Permite de igual manera mirar como si no se puede eliminar totalmente el riesgo de ser afectados por delitos informáticos, mirar con qué inversiones, tecnologías o acciones se pueden mitigar y/o mermar los daños y las afectaciones negativas en las empresas y organizaciones.

También en casos de no poder eliminar la totalidad de los riesgos de ser atacados por delitos informáticos, ni poder mitigarlos, mirar y tomar decisiones desde las juntas directivas y las altas gerencias o direcciones la idea de trasladar estos riesgos a empresas expertas o a aseguradoras que les permitan a estas empresas protegerse y/o que les puedan resarcir el daño en caso de llegar a ser víctimas de ciberdelincuentes.

- ✓ A las autoridades y organizamos nacionales e internacionales, poder tener herramientas y metodología estandarizada, les permitirá fomentar, crear y establecer políticas públicas basados en este tipo de recursos en pro de los beneficios de su sector productivo nacional, para que no resulten siendo afectados por delitos informáticos.

- ✓ En la academia se puede aplicar, considerar y tener en cuenta esta metodología, para las facultades de derecho, administración, economía, ingeniería, etcétera. A nivel de Pregrados y Postgrados esta metodología como herramienta se recomienda utilizarla para dar a conocer con mejores detalles sobre delitos informáticos, ciberdelitos, afectaciones, riesgos que representan los delitos informáticos para todas las organizaciones; básicamente fomentando la administración y/o gerencia ambidiestra,

innovadora, eficiente, productiva y segura para todas las partes interesadas e involucras en las empresas y/u organizaciones.

En resumen, esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos, les va a permitir a todas las personas jurídicas y naturales, como además a profesionales, gerentes, encargados de valoración de riesgos por delitos informáticos; contar y tener la información, cifras y cálculos reales para demandar, denunciar, asegurar, impartir justicia, pedir justicia y pedir resarcimiento real de los daños.

De igual manera, busca crear conciencia de ciberseguridad, que se tomen decisiones para invertir, prevenir, eliminar, mitigar, cubrir y/o trasferir a terceros todos estos riesgos; que pueden afectar a las organizaciones en cuanto a ciberdelitos o delitos informáticos.

Introducción.

Teniendo en cuenta las palabras de Moisés J. Schwartz - Gerente de Instituciones para el Desarrollo del BID, en el Reporte sobre ciberseguridad 2020 (BID – OEA), en el cual plantea lo siguiente *"La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida.*

Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y el suministro de agua y energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales.

Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB." (OEA – BID -2021).

Las palabras este domingo 06 de junio de 2021 en cadena televisiva ABC, de la secretaria de Comercio de EE.UU., Gina Raimondo, que aseguró *"Los ciberataques de – ransomware - están aquí para quedarse, advierto que probablemente se intensifiquen, por lo que insto a las empresas a que refuercen su seguridad tras los últimos episodios sufridos en el país. Remarco que lo primero, que hay que hacer respecto a los ciberataques es reconocer que esta es la realidad.*

Debemos asumir, y las empresas deben asumir, que estos ataques están aquí para quedarse y, probablemente, se intensificarán, invito a apuntar a la necesidad del sector privado de reforzar la seguridad en este ámbito. Somos conscientes del problema, en la Casa Blanca se ha presentado un programa junto al Departamento de Energía para modernizar las defensas de ciberseguridad en (infraestructura esencial del país), ante la creciente amenaza.

Estados Unidos ha sufrido recientemente dos (2) importantes ciberataques de (ransomware), que bloquean sistemas informáticos que no son liberados hasta que compañías o instituciones pagan un rescate a los piratas informáticos.

Informo que, a final de mayo, la empresa JBS, la segunda mayor procesadora de carne de EE.UU., sufrió uno de estos ataques y se vio obligada a suspender temporalmente sus operaciones.

Pocas semanas antes la empresa Colonial Pipeline, propietaria de varios oleoductos en EE.UU., sufrió uno similar, esta vez lanzado por la organización criminal DarkSide con sede en Rusia, que afectó durante días al suministro de combustible en la costa este del país. Colonial Pipeline reconoció posteriormente que pagó a los piratas informáticos un rescate de 4,4 millones de dólares porque no estaba segura del alcance del ataque ni de cuánto tiempo haría falta para restaurar el servicio." (ABC 2021).

Teniendo de igual manera en cuenta el comunicado de la Unión Europea en julio de 2020, donde dicen *"La preparación cibernética de la UE es fundamental tanto para el Mercado Único Digital como para la Seguridad y Defensa de la Unión. Es imprescindible fortalecer la ciberseguridad europea y abordar las amenazas a objetivos civiles y militares. En este gran esfuerzo, contamos igualmente con el apoyo de nuestros socios globales. Solo juntos, siendo resistentes, capaces de proteger a nuestra población de manera efectiva al anticipar posibles ciberamenazas e incidentes de ciberseguridad, al construir una fuerte resiliencia en nuestras estructuras y defensa, al recuperarnos rápidamente de cualquier ciberataque y al disuadir a los responsables, podremos proporcionar un ciberespacio abierto, seguro y protegido para todos."* (UE 2020).

En términos generales las afectaciones por ataques cibernéticos o delitos informáticos a nivel mundial según el Foro Económico Mundial en lo corrido del primer semestre del 2021 ascienden a US$ 6 billones de dólares, que es una cifra parecida y promedio al PIB anual de Japón - tercera potencia económica mundial. (FEM 2021).

Para el caso de Colombia, según las palabras del presidente ejecutivo CCIT, Alberto Samuel Yohai, *"El cibercrimen ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el País."* (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT, Policía Nacional – 2020).

De igual manera, según el CR (RA) Fredy Bautista Garcia - Asesor Ciberseguridad TicTac, CCIT y Policía Nacional *"El Cibercrimen actúa de una manera coordinada y dispone de recursos económicos ilimitados provenientes de las ganancias*

derivadas de actividades criminales previas. El fraude BEC (Los Ataques BEC son una de las principales amenazas a la cadena de suministros, componente fundamental en la actividad diaria de una empresa. Las comunicaciones con proveedores externos y socios de confianza requieren de entornos seguros, que garanticen la integridad de correos electrónicos y servicios de mensajería instantánea utilizados.), los ataques de Ransomware, las oleadas de Malware, las ciberextorsiones entre otras amenazas vienen afectando la cadena productiva de las empresas, y por ello es importante conocer las tipologías y modalidades que utiliza el Cibercrimen en Colombia.

Es claro que para enfrentar una amenaza es importante conocer cómo actúa y que puntos débiles internos de la organización aprovecha. Identificar las vulnerabilidades oportunamente permite entonces corregir los fallos en la seguridad e infraestructura e implementar planes de mejoramiento que abarquen desde los recursos tecnológicos, humanos y del proceso mismo afectado en el incidente presentado. Cuando se conocen las amenazas y los riesgos pueden ser gestionados oportunamente y las compañías desafortunadamente siguen siendo reactivas y su actuación ante un incidente descoordinada, en parte porque no conocen la problemática o no han definido de manera adecuada los roles a seguir en la cadena de responsabilidad organizacional establecida". (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT, Policía Nacional – 2020).

Figura 1- Tendencia del Cibercrimen en Colombia 2019-2020 (CCIT, Policía Nacional - 2020)

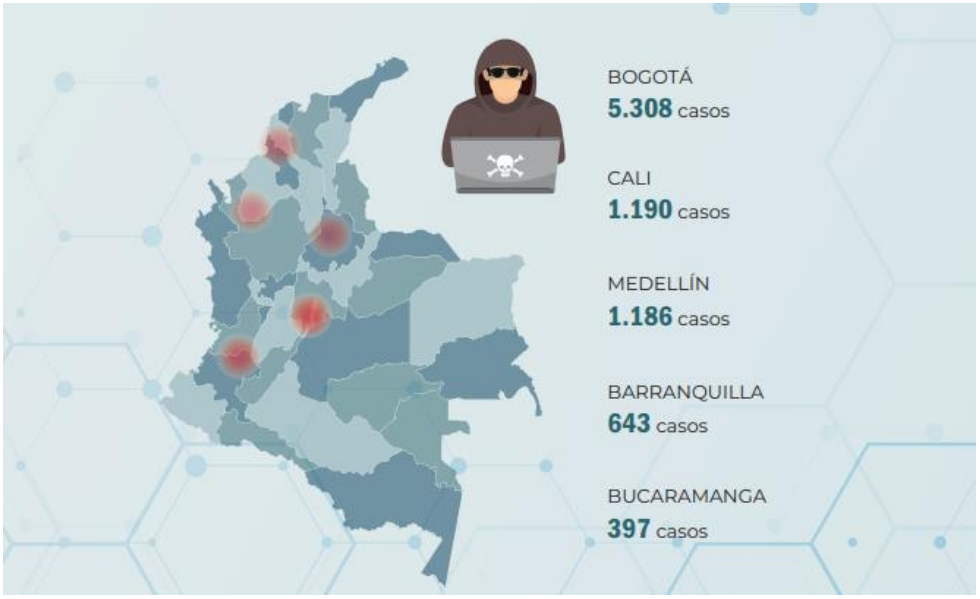


Figura 2- Delitos Informaticos reportados por ciudades - 2019 (Tendencias del Cibercrimen en Colombia 2019-2020 (CCIT, Policía Nacional 2020)

Para la vigencia 2019 se obtuvieron en Colombia los siguientes reportes y datos de afectaciones por delitos Informáticos:

A. En los últimos meses el RANSOMWARE “SAMSAM” cobró relevancia en Colombia, porque permite al atacante el robo de contraseñas para el acceso remoto a los dispositivos a través del acceso a credenciales RDP (Remote Desktop Protocol) y de ese modo secuestrar la información de las compañías víctimas. Estos ataques estuvieron dirigidos a entidades o individuos con efectos altamente severos por la complejidad del ataque. SamSam elevó el monto de los rescates al situarlo entre 32 millones de COP hasta más 160 M por ataque. El Ransomware GandCrab mucho más común que SAM SAM exigió rescates a partir de 3 M COP. Todos los rescates se piden en Bitcoin. (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT, Policía Nacional – 2020).

B. Las páginas y demás aplicaciones Web, son activos esenciales para el negocio de muchas empresas en Colombia, pues desde allí se atienden a terceros y clientes o se convierten en las principales plataformas informativas de sus productos y servicios online (eCommerce – Representa el 1,5% del PIB anual en Colombia), en 2019 Según cifras del Centro Cibernético Policial, *170 empresas reportaron ataques DDoS que consiguieron interrumpir sus servicios de cara a sus clientes.* (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT, Policía Nacional – 2020).

C. Según INTERPOL, “Acceder a las pretensiones de los cibercriminales sólo contribuye a que estas redes dispongan de más recursos para sofisticar sus ataques. (Interpol 2021).

D. En Colombia 612%, Fue el crecimiento de los ataques de Malware en el país en el último año 2020. (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT, Policía Nacional – 2020).

E. Millones de dólares es el estimado percibido por la criptominería ilegal al año en Colombia (Fortinet -2021).

F. El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis (6) meses luego de sufrir un ciberataque importante. Esto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías. (Tendencia de cibercrimen en Colombia 2019–2020 – CCIT, Policía Nacional – 2020).

G. Según la OCDE el 99,5% de las empresas en Latinoamérica y el caribe, corresponden a micro, pymes y medianas empresas. (OCDE 2021).

Como parte fundamental de la Introducción de esta metodología se pueden presentar y compartir lo siguiente:

Objetivos.

Flexibilidad:

La nueva metodología debe ser escalable que permita crecer el alcance de aplicación, ir tomando procesos de mejora continua y escalar para poder de manera pertinente, manejar y tener en cuenta todos los activos físicos, lógicos, reputacionales de la empresa, sus procesos, sus negocios, sus operaciones, su misión, estrategia y generación de valor a su público objetivo y en toda su arquitectura de tecnología de la información y las comunicaciones.

Es decir que se pueda aplicar a grandes, medianos y pequeños activos de la organización, siempre conservando y aplicando un nivel de detalle adecuado que permita satisfacer los objetivos comerciales, financieros, operacionales en todas las empresas y/u organizaciones.

Es decir, debe admitir diferentes niveles de granularidad, clasificaciones, aplicabilidad contando siempre con una capacidad de enrollado o cobertura, que permitan niveles de pertinencia y análisis detallados de las vulnerabilidades, amenazas, riesgos, valoraciones e impactos y cuantificaciones de dichos impactos en todos los activos corporativos o empresariales, que permitan su valoración enfocados en visiones individuales, generales, muchos más amplias y dependiendo del riesgo, ambiente y el propósito de la evaluación.

Modularidad:

La nueva metodología debe permitir el desglose, tratamiento, evaluación y valoración de todos los activos en las organizaciones y/o empresas en la cual se aplique, es decir, que permita aplicarlo en micro, pymes, medianas y grandes empresas, como además tener en cuenta todos los activos, procesos, operaciones y reputaciones en las organizaciones.

Debe contemplar los activos más grandes y complejos, como también en la misma proporción y rigurosidad los activos más pequeños, tener en cuenta todos componentes y situaciones manejables en dichas empresas, en conclusión, la nueva metodología debe soportar el análisis modular con vínculos adecuados entre elementos relacionados directa, indirecta y colateralmente.

Simplicidad:

Es importante resaltar que la lógica subyacente de la metodología debe ser intuitivamente satisfactoria y simplemente establecida, con la única finalidad de permitir una fácil, completa y pertinente aplicación por parte de los gerentes de los programas, líder de proyectos, Cios, Cisos, jefe de Sistemas, Lideres de Seguridad

y/o cargos similares o de los mismos niveles, así como, además por parte de practicantes de seguridad.

Para permitir esta aplicación y mejorar la facilidad de uso, los principios fundamentales y los procesos de la metodología armonizada estarán bien definidos, detallados e ilustrados con gráficos extensos, diagramas, ejemplos, tablas y plantillas de aplicación y pruebas.

Coherencia:

La nueva metodología debe permitir lograr una mayor y mejor coherencia entre las evaluaciones de riesgos, amenazas, riesgos, impacto y la cuantificación de dichos impactos por parte de delitos y ataques informáticos en las empresas y organizaciones, esto concluyendo de igual manera y de manera coherente así sea aplicada por diferentes personas en diferentes empresas, estamentos gubernamentales, aseguradoras o agencias estatales, privadas o de ley.

Esto se logra básicamente, debido a que esta nueva metodología se soporta y tiene como base y antecedente muchas normas, estándares y metodologías de análisis de riesgos internacionales, como además algunas de estas con aplicación en Colombia, estas son:

- NIST.SP.800-207 y NIST - Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Originarias y aplicadas en EEUU).

- ISO 27001: 2013, ISO 27002: 2013, NTC-ISO-IEC- 27005: 2018, ISO 27007: 2011 ISO 27017: 2015, ISO 27018: 2019, ISO 22301: 2019, ISO 31000: 2018 (Aplicabilidad Internacional).

- MAGERIT NIPO-63012-171-8 (Originaria y aplicada en España, también aplicada en algunos países de Europa y en países de habla hispana a nivel internacional).

- MEHARI: 2010 (Originaria y aplicada en Francia, como además reconocida a nivel mundial).

- GLOBAL RISKS REPORT (Originaria del Foro Económico Mundial y aplicado como además tenido en cuenta a nivel mundial).

- OCTAVE (Originaria de Estados Unidos de América y aplicada en EEUU y reconocida y tenida en cuenta a nivel mundial).

- HTRA - Harmonized Threat and Risk Assessment Methodology: 2007 (Originaria de Canadá y aplicada en Canadá).

- CORAS: 2011 – CONTRUCT - Construct a platform for Risk Analysis of Security Critical System. (Originaria de Noruega y aplicada en la Unión Europea).

- CRAMM: 1987 (Originaria de Reino Unido (UK) y aplicada en Reino Unido (UK)).

- EBIOS: (Originaria de Francia y aplicada en Francia y países de la Unión Europea).

- AS / NZS 4360 (Originaria del Comité OB/7 de la Junta de Estándares de Australia y Nueva Zelanda, con aplicabilidad en Australia y Nueva Zelanda).

- UNE 71504: 2008 (Originaria de España y aplicada en la Unión Europea).

- RISK SAFE ASSESSMENT – ENISA (Originaria de unión de Agencias Europeas de Ciberseguridad y aplicada en la Unión Europea).

- IT-GRUNDSCHUTZ-KOMPENDIUM EDITION 2021 – (Originaria en Federal Office for Information Security (BSI) Alemania y con aplicación en Alemania).

En síntesis, esta nueva metodología establece un vocabulario común con muchas definiciones sencillas, para todos los aspectos de la gestión de las vulnerabilidades, los riesgos, las amenazas y por ende del impacto y la cuantificación de todos los ataques y delitos informáticos en las empresas y organizaciones; aplicables en Colombia y a nivel internacional.

Adicionalmente tiene en cuenta variables y métricas solidas de los impactos de esos riesgos y las cuantificaciones de sus afectaciones en las empresas, específicamente los valores de los activos, de las amenazas y de las vulnerabilidades, que en esencia son vitales y requeridas para los análisis comparativos y los resultados replicables en todas las organizaciones.

Esta metodología es crucial para el riesgo informado, impacto y cuantificación de los riesgos y de las afectaciones de los delitos informáticos en las organizaciones, en los temas de activos, información, comunicaciones y en la reputación de las empresas.

Busca esta metodología, crear conciencia de la interoperabilidad de todos los actuales sistemas de información y comunicaciones, en la actual sociedad de la información, como además busca mostrar a todo lo que se exponen estas empresas en el ciberespacio; motiva también a mirar soluciones de seguridad de la información que sean rentables, protegiendo siempre los activos, la imagen, el patrimonio, la continuidad del negocio en empresas y organizaciones.

Generalidad:

Esta nueva metodología debe aplicarse por igual a todas las empresas sin importar su tamaño, número de empleados, procesos, tipo, tecnología medular y/o presupuesto.

Adicionalmente es aplicable para todos los activos físicos, lógicos, reputacionales de una empresa y por ende también en pro de la protección de los empleados, directivos, partes interesadas, información personal y empresarial.

Automatización:

Se debe tener en cuenta que, aunque la metodología armonizada de evaluación de riesgos, amenazas, vulnerabilidades, riesgos y la cuantificación de los impactos producidos por los delitos y ataques informáticos en las empresas es una herramienta manual, se ha desarrollado con miras a la automatización.

Para de esa manera poder simplificar de manera considerable, su aplicación y apoyo al interior de las empresas, aseguradoras, servicios de peritajes en procesos legales que tengan que ver con afectaciones por delitos informáticos contra personas naturales y jurídicas en Colombia y en el exterior.

Principios.

Es importante destacar que esta nueva metodología tiene en cuenta unos principios que son supremamente importante para la perfecta y pertinencia aplicación de la metodología en busca de cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

En esta metodología de evaluación y cuantificación del impacto de un ataque informático en una empresa, incluye los siguientes principios:

Compatibilidad:

Esta nueva metodología se puede utilizar para procesos comerciales, de garantías, de resarcimiento de daños, como evaluación en procesos penales y legales que involucren afectaciones por delitos informáticos no solo en Colombia sino a nivel internacional.

Esto se logra porque esta nueva metodología es totalmente compatible y toma en consideraciones aspectos legales internacionales, como además normas, estándares y metodologías totalmente válidas y reconocidas a nivel internacional; para la gestión de amenazas, vulnerabilidades, riesgos y sus respectivos impactos en personas naturales y jurídicas.

Estas normas, estándares y metodologías compatibles con la nueva metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos son:

- NIST.SP.800-207 y NIST - Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Originarias y aplicadas en EEUU).

- ISO 27001: 2013, ISO 27002: 2013, NTC-ISO-IEC- 27005: 2018, ISO 27007: 2011 ISO 27017: 2015, ISO 27018: 2019, ISO 22301: 2019, ISO 31000: 2018 (Aplicabilidad Internacional).

- MAGERIT NIPO-63012-171-8 (Originaria y aplicada en España, también aplicada en algunos países de Europa y en países de habla hispana a nivel internacional).

- MEHARI: 2010 (Originaria y aplicada en Francia, como además reconocida a nivel mundial).

- GLOBAL RISKS REPORT (Originaria del Foro Económico Mundial y aplicado como además tenido en cuenta a nivel mundial).

- OCTAVE (Originaria de Estados Unidos de América y aplicada en EEUU y reconocida y tenida en cuenta a nivel mundial).

- HTRA - Harmonized Threat and Risk Assessment Methodology: 2007 (Originaria de Canadá y aplicada en Canadá).

- CORAS: 2011 – CONTRUCT - COnstruct a platform for Risk Analysis of Security Critical System. (Originaria de Noruega y aplicada en la Unión Europea).

- CRAMM: 1987 (Originaria de Reino Unido (UK) y aplicada en Reino Unido (UK)).

- EBIOS: (Originaria de Francia y aplicada en Francia y países de la Unión Europea).

- AS / NZS 4360 (Originaria del Comité OB/7 de la Junta de Estándares de Australia y Nueva Zelanda, con aplicabilidad en Australia y Nueva Zelanda).

- UNE 71504: 2008 (Originaria de España y aplicada en la Unión Europea).

- RISK SAFE ASSESSMENT – ENISA (Originaria de unión de Agencias Europeas de Ciberseguridad y aplicada en la Unión Europea).

- IT-GRUNDSCHUTZ-KOMPENDIUM EDITION 2021 – (Originaria en Federal Office for Information Security (BSI) Alemania y con aplicación en Alemania).

Como se puede apreciar son muchas las normas, metodologías y estándares válidos y relevantes internacionalmente hablando, que se utilizaron como referencias para el diseño de la nueva metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

Todos estas referencias y la nueva metodología se deben tener en cuenta y utilizar como estándares de seguridad operacional relevantes, pertinentes, aplicables, universalmente validos sobre todo para todo lo que tiene relación con la identificación de activos, gestión de riesgos de seguridad, gestión de tecnologías de la información, planificación de seguridad de la información, seguridad física y continuidad del negocio; adicionalmente sobre todo esta nueva metodología debe

ser utilizada para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

Esta nueva metodología, debe estar supremamente vinculada e integrada con otras políticas relacionadas, especialmente las relativas a la gestión de riesgos, acceso a la información y privacidad de la misma, y de igual manera asociada a la gestión integrada de riesgos y marcos de responsabilidad gerencial, administrativos y financieros que tengan que ver con afectaciones por delitos informáticos en las organizaciones.

Transparencia:

Esta nueva metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; satisface de una manera alta y pertinente las necesidades que tienen:

Gerentes generales, gobiernos corporativos, juntas directivas, aseguradoras, Cios, Cisos, Jefe de Sistemas, Jefes de Departamentos de Calidad y Seguridad en las empresas, Lideres de SOC (Centro de Operaciones en Ciberseguridad), jueces, abogados litigantes, entidades de ley y entes jurídicos en Colombia y a nivel nacional; para conocer exactamente el valor y el coso del impacto por afectaciones a la que ha sido sometida una empresa atacada por delincuentes informáticos y/o terroristas informativos.

Permitiendo que se pueda conocer, cuantificar el real daño o impacto económico, administrativo, financiero, comercial, reputacional y operativo por dicho ataque informático; de igual manera que se puedan tener evidencias en derecho probatorio en casos judiciales y/o penales que ameriten o se tengan afectaciones por ataques informáticos contra personas naturales y/o jurídicas en Colombia o a nivel internacional y que se requieran cuantificar las implicaciones del ataque para demandas, pagos de pólizas de seguros, tipificar el delito, considerar la gravedad del delito, etc.

Es por esta razón que, en el diseño y desarrollo de esta nueva metodología, se utilizó apoyo, asesorías, conocimientos, recomendaciones de personas naturales y jurídicas públicas y privadas, como además de una gran cantidad y variedad de sectores para que se tuviera una amplia consulta interdepartamental, intergremiales, a muchas áreas, muchas empresas con enfoques y diferentes, que permitiera dar un mayor principio de universalidad y trasparencia a la metodología.

Todas estas personas, entes, estamentos, organizaciones, empresas, sectores públicos y privados; fueron esenciales durante el proceso de desarrollo.

Cambio Evolutivo:

Dado que esta es la primera versión de esta nueva metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos se adopta el principio de cambio evolutivo, debido a que entre más aplicaciones y utilización tenga la metodología en las empresas y por más autores, estos van a tener la posibilidad de retroalimentar la metodología para que siga creciendo, sea cada vez más reconocida y se amplíe tu nivel de aplicación y alcance en la sociedad.

Además de lo anterior también fundamentado en que la tecnología evoluciona considerablemente rápido y al llegar nuevas tendencias, tecnologías como Inteligencia Artificial (IA), BlockChain, Internet de la Cosas (IoT), Big Data, Computación Cuántica, Industrias 4.0, etcétera. Necesariamente la metodología tendrá que evolucionar para seguir siendo pertinente y utilizable en el tiempo.

La idea es dejarla en constante desarrollo, actualización, cambio y evolución.

Por lo tanto, lo que se pretende es aprovechar este conocimiento y experiencia, en la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, para siempre poner al servicio de la sociedad una herramienta válida, reconocida, pertinente, de apoyo que sea como una mejora incremental en lugar de una desviación radical de las prácticas establecidas.

Estructura y uso.

Esta metodología con la finalidad de cumplir con sus objetivos de simplicidad, pertinencia, innovación y flexibilidad de una manera integral, genera esta herramienta de propósito, una Metodología Armonizada de Cuantificación de las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, en síntesis esta metodología se ha estructurado en un formato altamente modular, de varios niveles de detalle, de clasificaciones por el tipo de impacto y/o afectación en las empresas.

Teniendo en ella desde resúmenes de alto nivel hasta descripciones cada vez más enfocadas de procesos y métricas específicas tenidas en cuenta para los análisis y las cuantificaciones financieras, económicas y reputacionales que pueden presentarse en las empresas afectada por Ciberataques o Ataques Informáticos.

En esta metodología la mayoría de los segmentos son limitados a unas pocas páginas de extensión, para que los usuarios puedan concentrarse rápidamente en aquellos aspectos de interés inmediato, de relevancia de acuerdo con la afectación sufrida o preocupación; sin tener que buscar en una narrativa extensa.

Este formato o la forma como se presenta la metodología también facilita las referencias cruzadas y pertinentes, para una fácil accesibilidad.

Los principales módulos de la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, incluyen:

- ✓ Un Prólogo para identificar el estado actual de la sociedad, el ciberespacio, las leyes y normatividades en Colombia y a nivel internacional, como además un consolidado de cómo se han incrementado los Delitos Informáticos en Colombia y en el mundo.

  Adicional que este documento proporcione un punto de análisis, percepciones y/o contacto para preguntas y mejoras sugeridas.

  De igual manera se tendrá la tabla de contenido que se acostumbra con sus respectivas listas de figuras y tablas.

- ✓ Una descripción general de tipo ejecutiva, para explicar la importancia de la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

Es decir, teniendo en cuenta la metodología como una herramienta para ayudar a las personas, Cios, Cisos, fiscales, jueces, asegurados, aseguradoras, analistas de seguros, peritos, abogados, gerentes y a todos los ejecutivos encargados de asegurar, velar por la estrategia, el patrimonio, buen nombre y los resultados en sus organizaciones.

Esta metodología les permitirá tener un punto de partida, de análisis, de apoyo en la valoración de las afectaciones sufridas por delitos informáticos, como además les dará las pautas a tener en cuenta para mitigar los daños, mitigar las repercusiones, conocer el detalle de costos y valores de estas afectaciones.

En resumen, les va a permitir a todos estos profesionales, gerentes y a los encargados de valoración, tener la información, cifras y cálculos reales para demandar, asegurar, impartir justicia, pedir justicia y pedir resarcimiento real de los daños, adicionar creará conciencia de ciberseguridad y que se tomen decisiones para prevenir, eliminar, mitigar, cubrir y/o trasferir a terceros estos riesgos que pueden afectar a sus organizaciones a cargo, teniendo total conocimientos de causas y afectaciones.

- ✓ Una Introducción que permite revisar algunos antecedentes, el porqué de la necesidad, aplicabilidad y pertinencia de la metodología, así como la justificación de esta nueva metodología, definiendo sus objetivos y los principios que rigen su desarrollo, como además la estructura adoptada para lograr estos objetivos.

- ✓ Un resumen de gestión, que se considera pertinente y necesario para describir todos los procesos a tener en cuenta en la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

  Esta información de un alto nivel para las empresas, empresarios, gerentes, profesionales jurídicos, profesionales judiciales y de aseguradoras, es decir para directivos y directores de proyectos con responsabilidades de gestión de riesgos, gestión de afectaciones y resarcimiento de daños o impactos negativos por delitos informáticos o ciberataques.

- ✓ Una serie de quince (15) Anexos, sobre las etapas sugeridas de aplicación de la metodología, de aplicación de acuerdo a los tipos de afectaciones que podría sufrir por ataques informáticos y/o Ciberataques una empresa, es decir, anexos para presentar, definir, asesorar, sugerir y aplicar en la práctica; cada paso del proceso de la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático; dependiendo del tipo de afectación a la cual se vea comprometida la empresa.

  En esta serie de anexos se tienen:

  - ❖ **Anexo A:** Etapa de Preparación.
  - ❖ **Anexo B:** Etapa de Identificación y Valoración de Activos.
  - ❖ **Anexo C:** Etapa de Valoración de Vulnerabilidades.
  - ❖ **Anexo D:** Etapa de Valoración de Amenazas.
  - ❖ **Anexo E:** Etapa de Valoración de Riesgos y Riesgo Residual.
  - ❖ **Anexo F:** Etapa de Ciberataques Internos.
  - ❖ **Anexo G:** Etapa de Ciberataques Externos.
  - ❖ **Anexo H:** Etapa de Ciberataques a la Información.
  - ❖ **Anexo I:** Etapa de Ciberataques contra Los Recursos, La Infraestructura, Funcionamiento y Operación de las empresas.
  - ❖ **Anexo J:** Etapa de Ciberataques Causantes de Pérdidas Económicas y Financieras Directas.
  - ❖ **Anexo K:** Etapa de Ciberataques Causantes de Pérdidas o Afectaciones Reputacionales (Pérdidas Económicas y Financieras Indirectas y/o Colaterales).
  - ❖ **Anexo L:** Etapa de Ciberataques a las Personas.
  - ❖ **Anexo M:** Etapa de pérdidas por Leyes y Normas Nacionales e Internacionales.
  - ❖ **Anexo N:** Etapa de Recomendaciones.
  - ❖ **Anexo O:** Etapa de Conclusiones.

- ✓ Una serie de apéndices exclusivos con material bastante pertinente y aún más detallado en forma de diagramas, descripciones técnicas, listas de verificación, diagramas de flujo, tablas y plantillas para ilustrar cada aspecto del proceso aplicado con la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

Buscando facilitar y hacer mucho más sencillo y comprensible la aplicación práctica de la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático en los procesos afectados en las organizaciones y detalladas en los quince (15) anexos de procesos definidos anteriormente.

- ✓ Un Décimo sexto (16º) anexo, que contiene de manera detallada material de apoyo adicional y pertinente sobre los temas, conceptos, información que se tratan o se tienen en cuenta en esta metodología, como por ejemplo Glosario, lista de acrónimos y referencias actualizadas.

    - ❖ **Anexo P:** Documentación y Referencias Adicionales.

Toda esta estructura y formato se ilustra en la Figura 03.

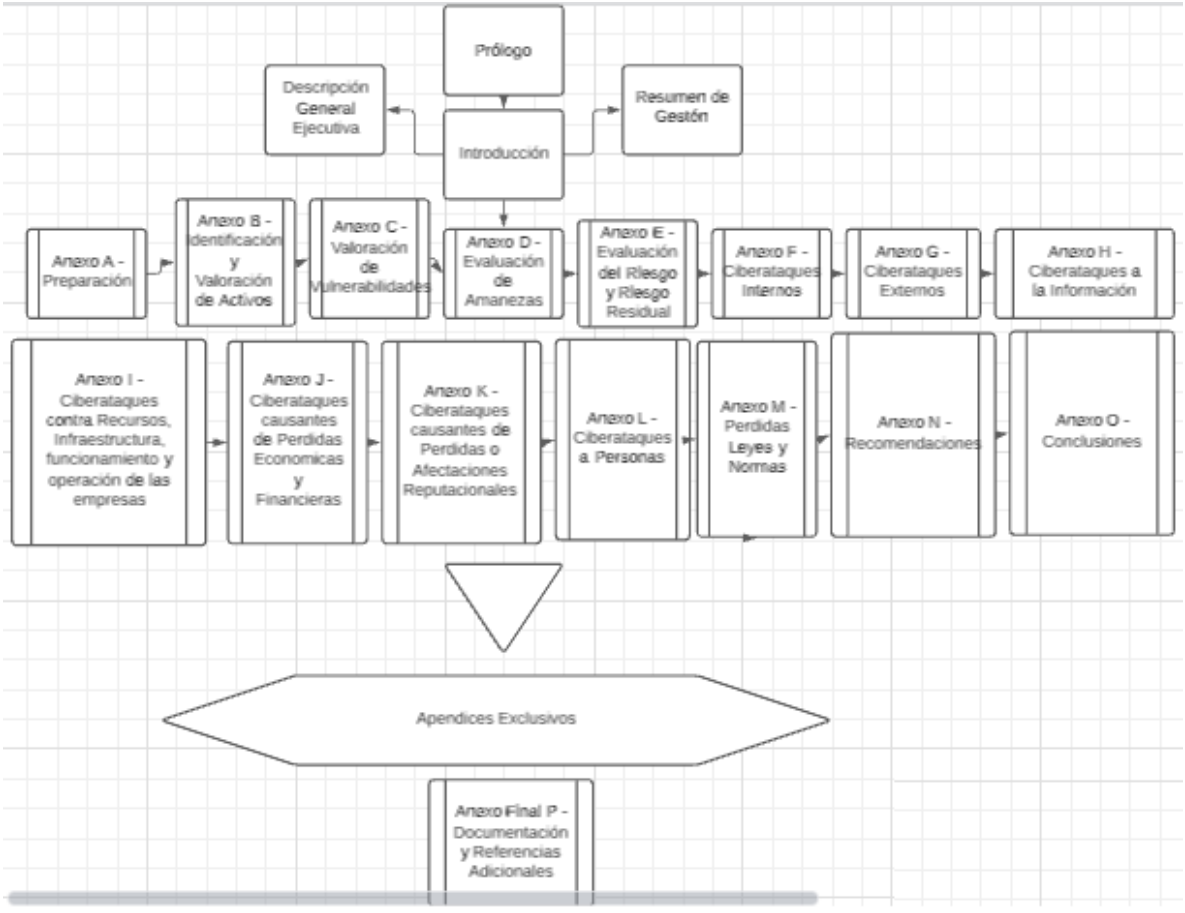


Figura 3- Estructura y uso de la Metodología. (Autoría Propia)

Se debe tener en cuenta y considerar que cualquiera que conozca y vaya a tener en cuenta por primera vez la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático o se acerque al documento por primera vez, se le recomienda navegar inicialmente por la Introducción, luego leer el Resumen de Gestión.

Posterior se le recomienda prestar mucha atención y comprender la Descripción General Ejecutiva.

Paso siguiente se le recomienda leer, analizar, comprender y aplicar las etapas definidas en los Anexos (15) del proceso general.

Tenga en cuenta que los anexos y apéndices más detallados están destinados a ayudar a todas las personas (Personal del programa o proyecto de seguridad, profesionales de la seguridad, gerentes, fiscales, abogados, jueces, peritos, aseguradoras y personas en general que están realmente encargados de la preparación, aplicación, interpretación y toma de decisiones que tengan que ver con el tema de cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

Cada uno de los anteriores temas, partes, etapas o pasos de la metodología, debería ser estudiado y analizado a fondo antes de comenzar las sucesivas fases de un proyecto con la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

Muchas de las preguntas e inquietudes normales se responderán específicamente en el cuerpo de estos segmentos o anexos, a menudo con ejemplos prácticos para ilustrar diferentes usos, soluciones e interpretaciones.

Además de este completo conjunto de herramientas, la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático; también comprende temas y/o productos estructurados de formación y sensibilización para garantizar accesibilidad y mayor utilidad para los gestores de riesgos departamentales, profesionales de la seguridad, gerentes, fiscales, abogados, jueces, peritos, aseguradoras y personas en general que están realmente encargados de la preparación, aplicación, interpretación y toma de decisiones que tengan que ver con el tema de cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

Se sugiere adicional, antes de hacer uso práctico de esta metodología:

• Tener socializaciones en grupos primario, grupos de decisiones sobre esta metodología y realizar ejercicios prácticos para explicar la guía del usuario y reforzar la experiencia de aprendizaje y aplicación de esta metodología en las empresas.

• Sesiones informativas complementarias para todas las personas y/o partes interesadas como directores superiores de programas, gestores de riesgos departamentales, profesionales de la seguridad, gerentes, fiscales, abogados, jueces, peritos, aseguradoras y personas en general que están realmente encargados de la preparación, aplicación, interpretación y toma de decisiones que tengan que ver con el tema de cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático. Esta recomendación para que se pueda conocer, entender, aprobar, aplicar y situar toda esta metodología dentro del Marco Integrado de Gestión de Riesgos general y en los Sistemas de Gestión de Seguridad de la Información (SGSI) en las compañías e instituciones públicas y privadas

Como se indica y se hace referencia en el Prólogo, las partes interesadas del sector productivo nacional e internacional (Empresas Publica, Privadas, Gobiernos, Entes Jurídicos, Entes Judiciales, Aseguradoras, los directores de proyectos y programas departamentales, etcétera).

Pueden obtener asesoramiento y orientación sobre la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático en contacto con el autor y el director del proyecto de grado para optar por el título de MBA en Administración (Universidad EAFIT sede Medellín).

Ingeniero Víctor Rafael Atencia Urueta – Email: vratenciau@eafit.edu.co y vatencia@sena.edu.co (Autor).

Ingeniero Juan Guillermo Lalinde Pulido – Email: jlalinde@eafit.edu.co (Director del Proyecto de Grado).

De Igual manera con la Universidad EAFIT sede Principal (Medellín – Colombia).

Resumen de Gestión.

Se considera pertinente y necesario este resumen de gestión para describir todos los procesos a tener en cuenta en la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

Esta información de un alto nivel para las empresas, empresarios, gerentes, profesionales jurídicos, profesionales judiciales y de aseguradoras, es decir para directivos y directores de proyectos con responsabilidades de gestión de riesgos, gestión de afectaciones y resarcimiento de daños o impactos negativos por delitos informáticos o ciberataques.

Esta metodología para lograr dar a conocer y que se pueda aplicar en su totalidad para cuantificar cualquier tipo de afectaciones ocurridas en las empresas al ser víctimas de ataques informáticos tiene en cuenta los siguientes procesos:

- ✓ Una serie de quince (15) Anexos, sobre las etapas sugeridas de aplicación de la metodología, de aplicación de acuerdo a los tipos de afectaciones que podría sufrir por ataques informáticos y/o Ciberataques una empresa, es decir, anexos para presentar, definir, asesorar, sugerir y aplicar en la práctica; cada paso del proceso de la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático; dependiendo del tipo de afectación a la cual se vea comprometida la empresa.

  En esta serie de anexos se tienen:

  - ❖ **Anexo A:** Etapa de Preparación.
  - ❖ **Anexo B:** Etapa de Identificación y Valoración de Activos.
  - ❖ **Anexo C:** Etapa de Valoración de Vulnerabilidades.
  - ❖ **Anexo D:** Etapa de Valoración de Amenazas.
  - ❖ **Anexo E:** Etapa de Valoración de Riesgos y Riesgo Residual.
  - ❖ **Anexo F:** Etapa de Ciberataques Internos.
  - ❖ **Anexo G:** Etapa de Ciberataques Externos.
  - ❖ **Anexo H:** Etapa de Ciberataques a la Información.
  - ❖ **Anexo I:** Etapa de Ciberataques contra Los Recursos, La Infraestructura, Funcionamiento y Operación de las empresas.
  - ❖ **Anexo J:** Etapa de Ciberataques Causantes de Pérdidas Económicas y Financieras Directas.

- **Anexo K:** Etapa de Ciberataques Causantes de Pérdidas o Afectaciones Reputacionales (Pérdidas Económicas y Financieras Indirectas y/o Colaterales).
- **Anexo L:** Etapa de Ciberataques a las Personas.
- **Anexo M:** Etapa de pérdidas por Leyes y Normas Nacionales e Internacionales.
- **Anexo N:** Etapa de Recomendaciones.
- **Anexo O:** Etapa de Conclusiones.

✓ Una serie de apéndices exclusivos con material bastante pertinente y aún más detallado en forma de diagramas, descripciones técnicas, listas de verificación, diagramas de flujo, tablas y plantillas para ilustrar cada aspecto del proceso aplicado con la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático.

Buscando facilitar y hacer mucho más sencillo y comprensible la aplicación práctica de la Metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informático en los procesos afectados en las organizaciones y detalladas en los quince (15) anexos de procesos definidos anteriormente.

✓ Un Décimo sexto (16º) anexo, que contiene de manera detallada material de apoyo adicional y pertinente sobre los temas, conceptos, información que se tratan o se tienen en cuenta en esta metodología, como por ejemplo Glosario, lista de acrónimos y referencias actualizadas.

- **Anexo P:** Documentación y Referencias Adicionales.

Teniendo en cuenta todos los anteriores procesos de la metodología lo que se busca es poder cuantificar exactamente o lo más real posible cuáles son esas afectaciones, económicas, financieras y reputacionales en que incurre y se ve perjudicada una empresa y/u organización al ser víctima de delitos informáticos o ciberataques a su infraestructura, procesos, operaciones, finanzas, reputación, etc.

Les va a permitir además conocer cuánto invertir en tecnologías y medidas de ciberseguridad para poder proteger los activos que pueden ser atacados en sus organizaciones.

Podrás conocer en cuanto tiempo deben resolver y seguir operando o seguir en continuidad del negocio, antes de sufrir pérdidas irreparables o la quiebra como tal de todo su negocio. (ISO 22301:2018).

Podrán saber, que, cuáles y como cumplir los requerimientos de ley en Colombia y a nivel internacional en cuanto a legislación procesal del delito cibernético y los derechos de las personas y de las empresas en cuanto a la privacidad de los datos personales y empresariales. Con la finalidad de evitar tener que pagar multas y sanciones al respecto.

De igual manera sabrán por qué es necesario hacer divulgación responsable de información y evitar Fake News, como además como estas Fake news o divulgaciones irresponsables pueden afectar a las empresas en su reputación y en sus objetivos y metas empresariales. Como por ejemplo lo sufrido por el Grupo Empresarial Éxito a raíz de una noticia de que en sus almacenes se torturaban jóvenes que protestaban en Colombia en los paros y marchas adelantadas en 2021.

Lo cual ocasiono rabia, indignación, ataques, sabotajes, robos, daños reputacionales a los almacenes Éxito solo por una falsa publicación y/o Fake News.

Procurará crear conciencia de ciberseguridad en las empresas y organizaciones, sobre todo en los grupos primarios, juntas directivas y directores que son los encargados de asegurar los activos y el patrimonio de las empresas y organizaciones, para ello la metodología busca que las empresas conozcan y establezcan “Resiliencia Cibernética” y “Gobernanza de Internet y del Ciberespacio” en todos sus procesos y acciones.

En resumen, se refuerza la idea que todos deben velar por una ciberespacio seguro, libre y abierto, donde todas las empresas y personas puedan interactuar, que las empresas tengan resiliencia cibernética, conocer los riesgos, protegerse de ellos y tener una visión de seguridad informática; eso no es Paranoia, eso es ser consiente de los riesgos que se tienen y responsable al tratar de evitarlos.

Tener esta conciencia de ciberseguridad, tener claro los riesgos que enfrentan las empresas y contar con mecanismos que ayuden a la Resiliencia cibernética y continuidad del negocio, hace que la empresa esté preparada, consiente, como además con los conocimientos y predecibilidad: claves para adaptarse al entorno VUCA. (El **entorno VUCA**, en el que se mueven las organizaciones en la actualidad, se caracteriza por la volatilidad, la incertidumbre, la complejidad y la ambigüedad. Este concepto se fraguó en la década de los noventa por los soldados norteamericanos y que responde al acrónimo inglés formado por los términos *Volatility (V), Uncertatinty (U), Complexity (C)* y *Ambiguity (A).) (Agenda APD 2021.)*

ANEXOS:

Anexo A: Etapa de Preparación.

Aspectos Generales y Aplicabilidad:

Teniendo en cuenta que las empresas, las organizaciones, la administración pública y en general toda la sociedad, depende de forma creciente del ciberespacio, los sistemas de información, las redes convergentes, las telecomunicaciones; para poder alcanzar sus objetivos, misión y cumplir con sus estrategias empresariales. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para todos los ciudadanos a nivel mundial; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios (Magerit 2012) (ISO 38500).

De igual manera se debe tener en cuenta que esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, es una herramienta que se pone al servicio y a consideración para su referencia y aplicación de personas jurídicas y naturales.

Esta aplicación se puede hacer previo a cualquier ataque sufrido y poder medir, proyectar el impacto y las afectaciones que se pudiesen llegar a sufrir en las empresas y/u organizaciones en caso de llegar a ser víctimas de ataques informáticos o ciberataques, es decir, de manera proactiva y previa; para saber que inversiones se deben hacer para proteger a la organización y de igual manera para saber que montos y activos asegurar contra ataques de delitos informáticos ante aseguradoras (trasferir el riesgo).

De igual manera se puede aplicar posterior a la afectación, por aseguradoras, peritos forenses, fiscales, jueces, fuerzas de ley, etcétera. Para conocer la afectación sufrida y poder determinar de una manera científica, bajo estándares internacionales cual es el monto total y/o parcial de las afectaciones ocurridas en una empresa por esos delitos informativos o ciberataques.

Para cualquier que sea la aplicación o independiente del momento en que se aplique esta metodología se debe tener en cuenta lo siguiente:

La planificación cuidadosa, los detalles, respetar las cadenas y procedimientos de custodia de la información y la previsión, son cruciales para lograr resultados efectivos en cualquier proyecto y en la aplicación de esta metodología no es la excepción.

Compromiso de gestión:

Al hablar sobre delitos informáticos y/o Ciberataques, siempre en todos los proyectos, en las empresas y en las organizaciones, para tomar decisiones informadas sobre la aceptabilidad de cualquier riesgo, riesgo residual, afectaciones financieras, económicas y reputacionales; los ejecutivos, juntas directivas, CEO y directores en general; requieren una sólida comprensión de estos temas, afectaciones, de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos y su papel dentro de los programa de gestión de riesgos, estrategia empresarial, misión y visión empresarial.

Es por ello que el compromiso y el apoyo de la dirección también son necesarios para establecer un mandato claro, movilizar los recursos necesarios y facilitar la recopilación de datos necesarios para una evaluación equilibrada, pertinente, real y consistente.

Reglas al aplicar esta metodología de cuantificación de las afectaciones por Delitos Informáticos y/o Ciberataques en las empresas:

En las empresas y organizaciones, sin importar su clasificación o tamaño, la mayoría de las veces los altos directivos normalmente asignan la responsabilidad de realizar y estar al frente de estos temas que se cubren en la metodología, a una sola oficina o funcionario con suficientes conocimientos sobre la empresa, los riesgos, estrategia empresarial y del negocio en general, pero que también conozca o tenga experiencia de la aplicación correcta de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

La oficina, oficinas y/o funcionarios designados, lo primero que se les recomienda tener presente y suficientemente claro; es el propósito, alcance y pertinencia del proyecto de dirigir la aplicación de la metodología, para confirmar tanto la viabilidad del ejercicio como la necesidad de esta evaluación.

Una vez estos aspectos han sido analizados, revisados y aceptados, deben especificarse las funciones y responsabilidades relativas de las partes involucradas e interesadas, especialmente para la autoridad de aceptación de riesgos, los impactos de estos riesgos en las empresas y organizaciones.

Otros temas supremamente importantes que se deben tener en cuenta, es considerar todas las prioridades del proyecto, expectativas de gestión e informes, debidos procesos de notificaciones a las autoridades y a las partes interesadas cuando las políticas de la empresa y las leyes del país así lo dicten o especifiquen.

Todo lo anteriormente expresado debe registrarse en el Plan de Trabajo, del proyecto de aplicación de la metodología para cuantificar las pérdidas económicas

y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, tal como se indica a continuación en la siguiente sección.

Alcance de un proyecto de aplicación metodología de cuantificación de las afectaciones por Delitos Informáticos y/o Ciberataques en las empresas:

En general, muchas metodologías de análisis de riesgos y proyectos de cuantificación del impacto de estos riesgos y afectaciones fallan porque al determinar y aplicar el alcance de la evaluación; esta no está claramente definido desde el comienzo de los proyectos como tal.

Casi inevitablemente, esto puede conducir y llevar a aplicar un esfuerzo y recursos de manera inútil y presentar retrasos innecesarios, por lo que es importante como además recomendado, determinar el propósito de la evaluación, el nivel de detalle requerido y los límites del ejercicio desde el principio.

Como regla general, a nivel internacional se tiene que las metodologías más eficaces en su aplicación son aquellas que son lo más breve posible en consonancia con la necesidad de una toma de decisiones informada. Es por ello que para lograr este ideal esta metodología recomienda que, para proyectos más grandes, de mayor alcance o en proyectos con activos complejos, a menudo es preferible realizar varios proyectos más pequeños y más evaluaciones modulares en lugar de un proyecto masivo, es decir, es mejor segmentar el proyecto de aplicación de esta metodología cuando son proyectos, empresas u organizaciones muy complejas en sus estructuras o son demasiados complejos los activos a los cuales se les deben cuantificar sus afectaciones.

Por supuesto, un proyecto puede cambiar si así lo deciden y/o requieren, el alcance en cualquier momento, básicamente para hacer frente de manera más pertinente a todas las circunstancias cambiantes que se pueden llegar a presentar, como además debido también al descubrimiento de impactos, riesgos, amenazas y vulnerabilidades previamente desconocidas. Teniendo esto en cuenta, algunos factores que se deben considerar al determinar el alcance de la aplicación de la metodología en empresas tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, incluye:

- ✓ Existencia, apoyo de sistemas de gestión y certificaciones de las mismas, en las empresas y organizaciones a analizar: Si las empresas que se van a analizar y se les va a aplicar esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos tienen implementados y/o están certificadas en sistemas de gestiones como ISO 27001, ISO 9001,

ISO 3100, ISO 22301, etcétera. Esto será un apoyo supremamente importante debido a que se tendrán avances en formatos, inventarios de activos, matrices, análisis de riesgos que permitan adelantar parte de trabajo requerido. Pero no debe para nada preocuparse si la empresa a analizar no cuenta, no tiene existencia de implementaciones o certificaciones de estos sistemas de gestión y/o estándares internacionales, dado que esa no existencia; para nada afecta el desarrollo o análisis al aplicar la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

- ✓ La etapa en el ciclo de vida del plan del proyecto para la aplicación de la metodología: Se requerirá y se tendrá una mayor precisión en todos los aspectos del análisis al aplicar la metodología, a medida que los proyectos avancen y evolucionen, esto desde la definición de los requisitos iniciales, los diseño, el desarrollo hasta la implementación final.

- ✓ El entorno de los riesgos y afectaciones en las empresas y organizaciones: Por lo general, se requiere un análisis más extenso y profundo en toda la organización a analizarlas, máximo dependiendo de su estructura, composición, tecnología medular, áreas existentes y procesos a tener en cuenta; la mayoría de las veces se requieren estos análisis para empleados, activos y servicios catalogados como en mayor riesgo o que si de llegarse a confirmar el riesgo en ellos, su impacto sería súper significativo negativamente para las empresas y/u organizaciones (mayor impacto).

  Teniendo en cuenta lo anterior, en algunas ocasiones puede ser necesario un escaneo superficial al principio, caracterizar el entorno de riesgo y luego si, proceder a indagar en mayor proporción o complejidad sobre estos activos, servicios o recursos de la organización sujeto de análisis con la metodología.

  El análisis de los riesgos y de las afectaciones, considera los siguientes elementos:

- Activos: Que son los bienes de la empresa, elementos de la empresa, los elementos del sistema de información de la empresa (o estrechamente relacionados con este) que soportan la misión de la Organización.

- Amenazas: Que son cosas, acciones que les pueden pasar a los activos causando un perjuicio a la Organización.

- Salvaguardas, protecciones, Garantías o Contra Medidas: Que son medidas de protección desplegadas para que aquellas amenazas no causen tanto daño (mitigar), como además las acciones que toma la organización para trasferir los riesgos a los cuales están expuestos sus activos (Magerit 2012) (ISO 38500).

  Con estos anteriores elementos se puede estimar:

  - El impacto: Lo que podría pasar.
  - El riesgo: Lo que probablemente pase.

  Siempre debemos tener presente, que el análisis de riesgos y de afectaciones, contemplados en esta Metodología, permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a las fases de tratamiento, reclamaciones, demandas, etcétera.

  Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión (Magerit 2012) (ISO 38500).

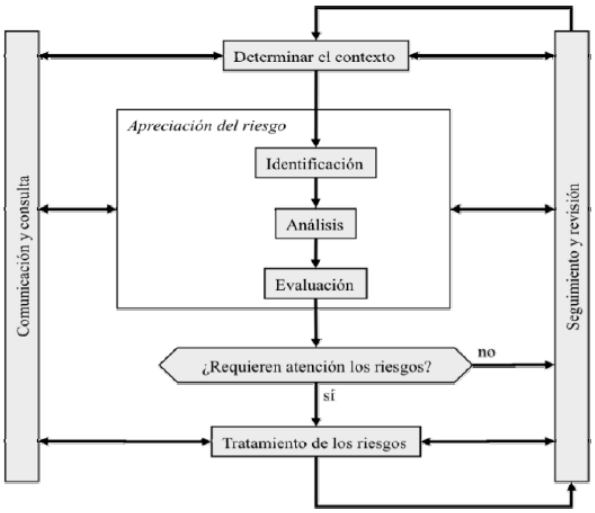


Figura 4- Proceso de Gestión de Riesgos. (Iso 31000)

✓ El propósito del proyecto de aplicación de la metodología: Las evaluaciones por áreas en las organizaciones analizadas, suelen ser de alto nivel y de base muy amplia, mientras que los de los principales proyectos de cima o de estamentos directivos de las empresas y/u organizaciones; suelen ser bastante detallados, en cambio y como recomendación al aplicar esta metodología en segmentos específicos, breves, delimitados e identificados;

son ideales para abordar problemas de seguridad específicos, sus afectaciones e impactos.

- ✓ Restricciones de tiempo y costo: En algunas ocasiones y/o análisis, debido a la necesidad; las consideraciones prácticas requeridas, las políticas empresariales y/o por requerimientos normativos, jurídicos y/o legales, puede llegarse a limitar el alcance de la aplicación de esta metodología en la empresa u organización afectada por delitos informáticos o ciberataques.

  Estas razones que son válidas y legítimas, se deben tener en cuenta y respetar en pro del éxito de todo el proyecto, como además para evitar posibles multas y sanciones.

Conformación del equipo de trabajo para aplicar la Metodología:

Se debe considerar que al aplicar esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos en microempresas, pymes o en procesos empresariales afectados que no sean tan complejos, se podría pensar y completar que este trabajo y/o aplicación sea realizado por una sola persona, sin embargo en la gran mayoría de los casos se requerirá un esfuerzo de equipo interdisciplinario que pueda aportar y ayudar a reunir la información y sobre todo que los miembros del equipo conformado realmente cuenten con los conocimientos y la experiencia necesarias para una evaluación eficaz.

En general, muchos más miembros para este equipo de trabajo, son necesarios para proyectos muchos más grandes y complejos, pero a pesar de que algunos proyectos sean menos complejos; se recomienda crear ese equipo de trabajo con personal con diferentes conocimientos y habilidades.

En términos generales se puede decir que, para asegurar una adecuada, real y pertinente información para la evaluación, los siguientes perfiles, roles y/o autoridades normalmente deben participan directamente como miembros del equipo de trabajo o en el peor de los casos si no pueden hacer parte; si deben ellos proporcionar la información requerida para la correcta aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

Estos roles, autoridades son:

• Los directores, gerentes, subgerentes o coordinadores de programas o negocios de la empresa u organización, los cuales comprenden la importancia operativa de los empleados a cargo, activos a su cargo, procesos que lideran y los servicios que prestan, así como las lesiones, afectaciones y valoraciones, que pudieran surgir en caso de un compromiso, por lo que su aporte es crucial para las fases de identificación y valoración de activos de la evaluación o aplicación de la metodología en sus áreas a cargo.

• Los gerentes de proyecto y todo su personal a cargo, los cuales representan, conocen y traducen los requisitos funcionales, operativos, legales o comerciales en soluciones técnicas, para que puedan contribuir significativamente tanto a la identificación de activos, procesos y la evaluación de vulnerabilidades y afectaciones subsiguientes.

• Los gerentes de instalaciones, jefes de Sistemas, jefes de Infraestructuras, los directores de información, administradores de plataformas, los DBA, gerentes de mesas de ayudas, directores de Help Desk, Gerente de NOC y todo su personal, analistas, profesionales a cargo. Este personal en general, pueden proporcionar valiosa, importante información sobre alojamientos compartidos, contratos de servicios, acuerdos de servicios con clientes y proveedores, como además ofrecer información puntual y requerida de las infraestructuras técnicas tanto para el proceso de identificación de activos, evaluación de vulnerabilidades explotadas, impactos, valoración de las afectaciones, entre otros.

• Autoridades y roles de seguridad informática en las empresas, áreas, departamentales, etcétera. También el oficial de seguridad departamental (DSO), CISO, CIO, Gerentes de SOC, Coordinador de seguridad en IT (ITSC), Analistas de SOC, profesionales y analistas de riesgos, profesionales de Calidad, Coordinadores de planificación de continuidad del negocio (BCPC), entre otros roles de seguridad informática o cibernética que existan en las empresas u organizaciones.

Todo este personal, puede ofrecer asesoramiento y orientación sobre el entorno de amenazas, riesgos, trazabilidad y alcance de las afectaciones sufridas y las opciones de protección requeridas.

• Profesionales jurídicos, profesionales del derecho en sus diferentes ramas o especializaciones, personal con conocimiento normativo y legal que aporten sus asesorías en cuento a los requerimientos legales, normativos, afectaciones, derecho penal, derecho civil, derecho comercial, derecho administrativo, pólizas, acuerdos de niveles de servicios, derecho informático, derecho forense, etc.

• Directores financieros, directores administrativos, directores comerciales, directores de operaciones, directores de innovación, contadores, entre otros

directores de la organización y de igual manera todo su personal a cargo como almacenistas, compras, contratación, inventarios, etcétera.

Todo este personal posee información y conocimientos administrativos, financieros, económicos, inventarios, garantías, entre otros más; que pueden ser supremamente importantes para poder llegar a una cuantificación real y pertinente de las afectaciones sufridas en la organización por delitos informáticos y/o ciberataques.

Otros recursos:

Dependiendo del alcance, la magnitud y la complejidad de los ataques y de las afectaciones sufridas, puede ser necesario adicionar a todos los perfiles, roles, personal interno en la organización, anteriormente descritos, nuevas personas que pueden apoyar y aportar al interior de la organización y que pertenezcas a áreas responsables y pertinentes para la empresa y para el cumplimiento de las metas, estrategia corporativa o empresarial.

Adicional a ellos, las empresas se pueden apoyar en profesionales y personal externo, los cuales en muchos casos pueden ser de mucha utilidad para dar soporte a las empresas en estos casos o proyectos.

Estos perfiles, personal pueden ser: Asesores técnicos, asesores legales, asesores financieros económicos o comerciales, consultores técnicos, consultores legales, consultores administrativos, financieros, auditores internos, auditores externos, peritos de computación forense, peritos de aseguradoras o independientes, peritos o analistas financieros y/o Comerciales, salud ocupacional, etc.

Todas estas personas pueden proporcionar detalles útiles para complementar material recopilado por los miembros del equipo central.

En algunos casos entidades nacionales e internacionales, privadas y públicas, como también organismos de ley, pueden apoyar en estos proyectos, casos o incidentes; por ejemplo, Csirt Financiero Colombia, Csirt Américas, Csirt Europa, ColCERT, Csirt Ponal, CCOC (Comando Conjunto Cibernético de Colombia), CCP (Centro Cibernético Policial), entre otros más.

Estos roles y perfiles externos a las empresas, como además organismos nacionales e internacionales de apoyo en ciberseguridad, se pueden apreciar en el Apéndice A.

Plan de trabajo para la aplicación de la metodología de cuantificación de las afectaciones por Delitos Informáticos y/o Ciberataques en las empresas:

Es supremamente importante y pertinente poder asegurar contar con el esfuerzo coordinado al aplicar esta metodología y sobre todo que satisfaga las necesidades operativas, financieras, jurídicas, comerciales, administrativas, reputacionales y estratégicas de la organización afectada, como además de los directores de programas, juntas directivas, ceo, gerentes y en general de los ejecutivos departamentales relacionados con estas afectaciones a la empresa por delitos informáticos y/o ciberataques.

Es perentorio y un deber, que el equipo encargado del proyecto de aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; prepare un plan de trabajo integral como su primera tarea importante. Este plan debe ser aprobado por la autoridad de aceptación de riesgos en las empresas u organizaciones, como además por parte de la Junta Directiva y/o representante legal y/o CEO de la Organización.

Estas autoridades son la última instancia, que deben revisar las recomendaciones (Técnicas, Financieras, Legales, Administrativas, etcétera) entregadas y con base en ello, proceder a aceptar, rechazar, informar, denunciar, reportar para resarcimiento de patrimonio; todas las afectaciones sufridas, los riesgos totales y riesgos residuales proyectados e identificado en el Informe final de la metodología aplicada.

Si bien el nivel real de detalle variará según el alcance y la magnitud de la evaluación, el plan debe registrar como mínimo:

• Las reglas, propósitos, alcance y todos los términos de referencia establecidos y a tener en cuenta para la aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos en la empresa u organización.

• Descripción del equipo central de trabajo y listado de todos los otros recursos a su disposición, con términos de referencia o descripción breves para cada uno.

• Aportaciones relevantes al proyecto, como registros anteriores, antecedentes, registros de anteriores de ataques y/o afectaciones, evaluaciones de impacto en la privacidad, integridad, disponibilidad de la organización (PIA), Análisis de impacto empresarial (BIA – ISO 22301), documentación de diseño, planos de planta de las instalaciones afectadas, resúmenes de gestiones, listas de inventario de activos

afectados, información de inventarios y recursos físicos sobre los valores de activos afectados, facturas e informe desde el área contable de los valores actuales de los activos afectados, informes de depreciaciones de los productos afectados, copia de las pólizas y/o garantías constituidas y vigentes de los activos afectados, así como cualquier información que el equipo de trabajo considere importante y pertinente de agregar.

De igual manera se debe tener soportar de cualquier memorando de entendimiento (MOU) relevante para el intercambio de información u otros activos, ya sea con proveedores, aseguradoras, partes interesadas, accionistas, entidades de ley del país u organismos nacionales e internacionales de apoyo.

• Un cronograma con fechas, objetivos para cada entregable, desde la Fase de identificación de activos hasta las cuantificaciones, conclusiones y recomendaciones finales del Informe; producto del análisis a través de la aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos en la empresa u organización.

• Arreglos, detalles y requerimientos logísticos relevantes, como controles de seguridad, apoyos administrativos, manejo de la información con las partes interesadas, informes presentados a las autoridades pertinentes, necesidades de recursos, incluida la fuente de fondos para cualquier gasto relacionado, como contratos de consultoría, asesorías de toda índole.

Anexo B: Etapa de Identificación y Valoración de Activos.

Luego de haber completado todo lo referente a la fase de preparación, el equipo de trabajo para la aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; puede comenzar la identificación de activos, revisión de matrices de riesgos, verificar el BIA (Iso 22301), verificar inventarios y valores de los activos afectados en la organización e iniciar la evaluación puntual en los dos (2) momentos que lo permite esta metodología:

1. Cuánto cuesta (presente afectación) desde el punto de vista económico, financiero y reputacional para la empresa toda la afectación ocurrida por delitos informáticos o ciberataques (manera reactiva o posterior a los ataques), pasado el hecho.

2. Cuánto costaría (posible o futura afectación) desde el punto de vista económico, financiero y reputacional para la empresa toda la afectación en caso de ocurrir o ser víctimas de delitos informáticos o ciberataques (manera proactiva – preventiva), es decir, posibles proyecciones, cuantificación de afectaciones y análisis de las afectaciones en caso de que la empresa llegue a ser atacada; esto para toma posterior de decisiones con datos más reales y con conocimiento de causa y efectos para la organización).

Esta fase del proyecto de aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, en realidad involucra cuatro (4) diferentes, pero estrechamente relacionados procesos.

Estos procesos son:

A. En primer lugar, todos los empleados, activos y servicios dentro del alcance de la evaluación deben ser identificado con el mayor nivel de detalle posible y apropiado, para determinar quién y qué podría requerir protección, como además cuál de estos eran o no sujetos de protección; pero que fueron atacados o son víctimas de ciberataques.

B. A continuación, se debe identificar el nivel de lesión (sufrido o que puede llegar a sufrir) cada uno de los activos involucrados de la organización, es decir, en este caso que podría esperarse razonablemente que surja en caso de que se comprometa o que ya este comprometido.

En este caso se sugiere tener en cuenta para todos los activos de la organización, los temas de comprometimiento en cuanto a su confidencialidad, disponibilidad, integridad, apoyo a la continuidad del negocio; para ello se recomienda hacer esta evaluación teniendo en cuenta y con base a estándar de seguridad operacional de identificación de activos.

C. Entonces, basado en esta evaluación, que debe ser detallada, completa, relativa, real y muy aterrizada; los valores se asignan para categorizar activos, procesos y servicios en particular. Hay que tener en cuenta que todos los activos tienen uno o más valores económica, financiera y de reputación, los cuales están estrechamente relacionados con su confidencialidad, disponibilidad, integridad y su aporte a la continuidad y eficiencia del negocio.

D. Para el caso de las afectaciones y/o valores determinados o clasificados como reputacionales se deben tener en cuenta, la afectación al buen nombre, Good Will y reputación en general de la empresa al ser víctimas de ataques informáticos o ciberataques; esto debido a que estos ataques pueden dañar y afectar considerablemente la imagen de la empresa, la confianza de las partes interesadas de la empresa, además toda su operación comercial y financiera como tal.

   Esto se masifica si tenemos en cuenta que estas afectaciones a la reputación de las empresas y de las organizaciones atacadas por delitos informáticos pueden ocasionar pérdidas en cuanto a:

   - Pérdidas de clientes fidelizados y/o registrados en la empresa.

   - Pérdidas en la consecución de nuevos clientes y/o ampliación del nicho de mercado.

   - Pérdidas por baja en los volúmenes de ventas, que van a incidir directamente en todo el rendimiento de la empresa como por ejemplo en flujos de caja, flujo de capital, utilidades, generación de valor empresarial, Ebitda, Eva, Roi, Roe, etc.

   - Pérdidas por retiro de inversionistas actuales.

   - Pérdidas por ausencia de financiación y/o apalancamiento financiero de nuevos inversionistas y del sistema de apalancamiento financiero y empresarial.

- Pérdidas por caída de las acciones en la bolsa, en caso de que la empresa cotice en Bolsas de valores.

- Pérdidas por terminación y pérdida de apoyo y apalancamiento por parte de sus proveedores, al perder la confianza o los intereses luego de estas afectaciones por ciberataques.

- Pérdidas por multas y/o sanciones impuestas por entidades públicas y del estado, como por ejemplo por superintendencias, ministerios, autoridades en general en el caso de perder o poner en riesgos información y datos personales de clientes y/o personas en general vinculadas o relacionadas con la empresa atacada.

- Pérdidas por multas y/o sanciones por incumplimiento de leyes, normas del país o de los países de sus partes interesadas.

- Pérdidas por sanciones y/o multas por pérdidas de información o comprometimiento de la información; esto en caso de que la empresa afectada y/o atacada, tenga vínculos comerciales, operativos, información sensible o de seguridad nacional, es decir, de entidades del estado, que al comprometerse pongan en riesgo al país afectado y su seguridad nacional.

- Pérdidas por resarcimiento o pago de pólizas en caso de presentarse incumplimientos y/o afectaciones en el cumplimiento de compromisos, acuerdos comerciales, incumplimiento de acuerdos de servicios, incumplimiento o faltas a clausulas firmadas en cuanto a confidencialidad, integridad y disponibilidad; en acuerdos o contratos con terceras partes, lo cual se agrava considerablemente si estos acuerdos y/o contratos son firmados con estados o países.

Se deben especificar, detallar y tener muy en cuenta todos estos aspectos que afectan la reputación de las empresas víctimas de ataques informáticos o ciberataques; pues pueden llegar a ser tan graves, que pueden ocasionarle la pérdida total, quiebra, cierre, liquidación o intervención por parte de las autoridades competentes del país sede o base.

Para facilitar la identificación y cuantificación de los activos, con un nivel de detalle adecuado, real y armonizado; la metodología recomienda e introduce una lista de activos jerárquica y completa. Para analizar activos y realizar evaluaciones uniformes, pertinentes y reales se permite el análisis comparativo entre diferentes

activos o diferentes valores para el mismo activo, la guía también contiene una tabla de lesiones complementaria con valores que van desde “Muy Bajo” hasta “Muy Alto”.

El resultado final de la fase de identificación y valoración de activos de un proyecto de aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, es conocido y se recomienda que se le llame “Declaración de Sensibilidad”, lo cual es simplemente una lista de empleados, activos, procesos y servicios con valores asignados de acuerdo con las lesiones o el impacto operacional derivado del compromiso; tenidos en cuenta desde el punto de vista económico, financiero y reputacional.

Para esta fase de Identificación y cuantificación de los activos se debe por favor tener en cuenta y presente lo siguiente:

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

a. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación, afectación o comprometimiento.
b. Determinar a qué amenazas están expuestos aquellos activos.
c. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
d. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
e. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se introducen los conceptos de “impacto y riesgo potenciales” entre los pasos b y c. Estas valoraciones son “teóricas”: en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso c, derivando estimaciones realistas de impacto y riesgo (Magerit 2012). La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

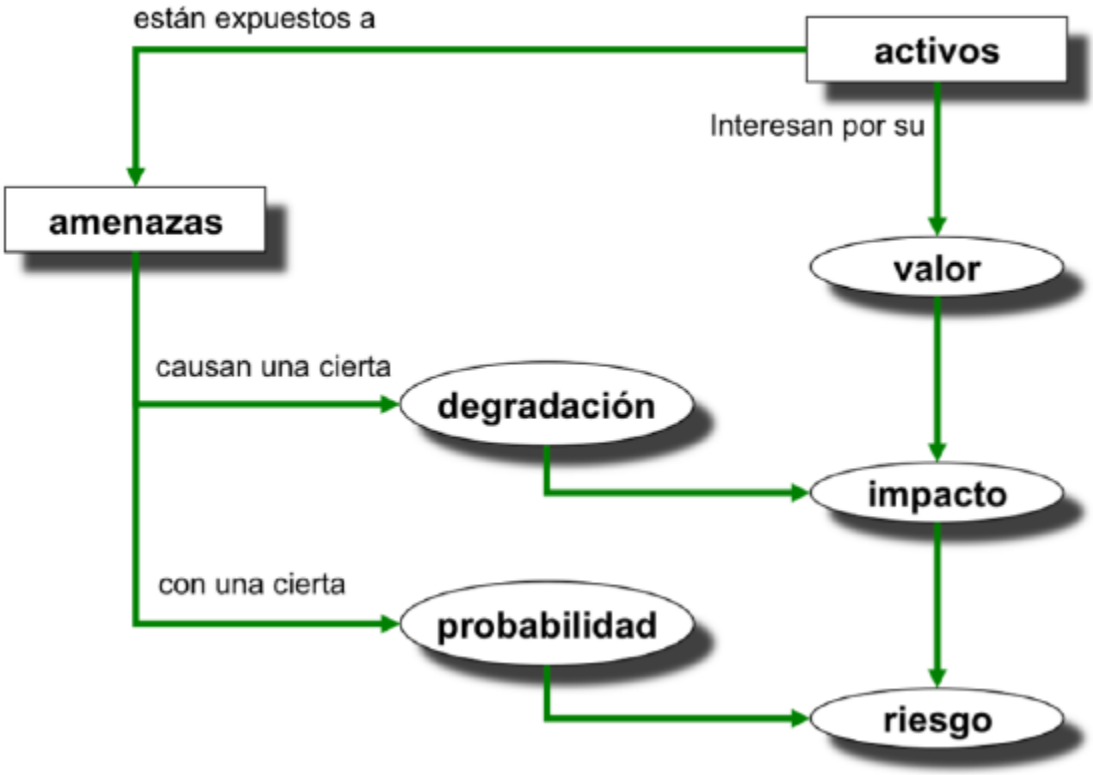


Figura 5- Elementos del Análisis de Riesgos Potenciales y sus Cuantificaciones. (Magerit 2012).

Los activos son los componentes o funcionalidades de un sistema de información, sistema empresarial, infraestructura corporativa susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, procesos, reputación, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos, recursos intangibles (reputacionales o licenciamientos) y recursos humanos. (UNE 71504:2008), (Magerit 2012).

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'.

Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño en caso de materializarse las amenazas.

Por ello aparece como importante el concepto de “dependencias entre activos” o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Aunque en cada caso hay que adaptarse a la empresa u organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores (Magerit 2012).

Activos esenciales:

Información que se maneja
Servicios prestados

servicios internos:

Que estructuran ordenadamente el sistema de información

El equipamiento informático:

Aplicaciones *(software)*
Equipos informáticos *(hardware)*
*C*omunicaciones
Soportes de información: discos, cintas, etcétera

El entorno: Activos que se precisan para garantizar las siguientes capas:

Equipamiento y suministros: energía, climatización, etc.
Mobiliario

Los servicios subcontratados a terceros:

Las instalaciones físicas:

El personal:

Usuarios:

Operadores y administradores
Desarrolladores
Otras Partes Interesadas

Reputación: Buen Nombre, Good Will, Confianza Organizativa:

- Clientes
- Inversionistas
- Partes Interesadas
- Gobiernos
- Estados
- Proveedores
- Acciones (Bolsa de Valores)
- Imagen Institucional o Corporativa
- Pólizas
- Multas y Sanciones
- Normatividad y Leyes
- Financiación
- Apalancamientos financieros y comerciales
- Acuerdos de servicios y niveles de servicios
- Cláusulas de Confidencialidad e Integridad en contrataciones
- Seguridad Corporativa
- Seguridad Nacional

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios (Magerit 2012) (UNE 71504 2008) (IT-GRUNDSCHUTZ-KOMPENDIUM EDITION 2021).

Se reconocen habitualmente como dimensiones básicas la confidencialidad, integridad, disponibilidad, autenticidad ligada al no repudio y la trazabilidad. En esta metodología se han añadido la cuantificación económica, financiera y reputacional. Que a efectos técnicos, económicos, financieros y reputacionales; se traducen en mantener la integridad, la

confidencialidad, la disponibilidad, la autenticidad, la trazabilidad y el valor real o que obtienen ciertos activos de las empresas y organizaciones.

¿Cuánto vale la “salud” de los activos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a la valoración, la cual es la determinación del costo que supondría recuperarse de una incidencia que destrozara el activo (Magerit 2012). Hay muchos factores a considerar:

- Costo de reposición: Adquisición e instalación.
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo.
- Lucro cesante: Pérdida de ingresos.
- Capacidad de operar: Confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos, propios o ajenos.
- Daño a personas.
- Daños medioambientales.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes para respetar son:

  - La homogeneidad: es importante poder comparar valores, aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.
  - La relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos (Magerit 2012) (Mehari 2010).

Ambos criterios se satisfacen con valoraciones económicas (costo en dinero requerido para “curar” el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente. Incluso es fácil ponerles precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos, por lo cual se pretende en esta metodología aportar a que esto sea cada día más fácil de identificar y que sea universalmente valido.

Valoración cualitativa:

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Esto es parte de lo que pretende resolver y aportar la Metodología y que sea un pazo de inicio o apoyo inicial para hacer que estas valoraciones cualitativas cada vez sean muchos más objetivas, entendidas y universalmente aceptadas en la sociedad.

Valoración cuantitativa:

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente “natural”. La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

¿Vale la pena invertir tanto dinero en esta protección o salvaguarda?

¿Qué conjunto de protecciones o salvaguardas optimizan la inversión?

¿En qué plazo de tiempo se recupera la inversión?

¿Cuánto es razonable que cueste la prima de un seguro? (Magerit 2012)

El valor de la interrupción del servicio:

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad, cierre o quiebra de las empresas (ISO 22301:2018).

Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias (Magerit 2012). En consecuencia, para valorar la interrupción de la disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en algún gráfico como los siguientes:

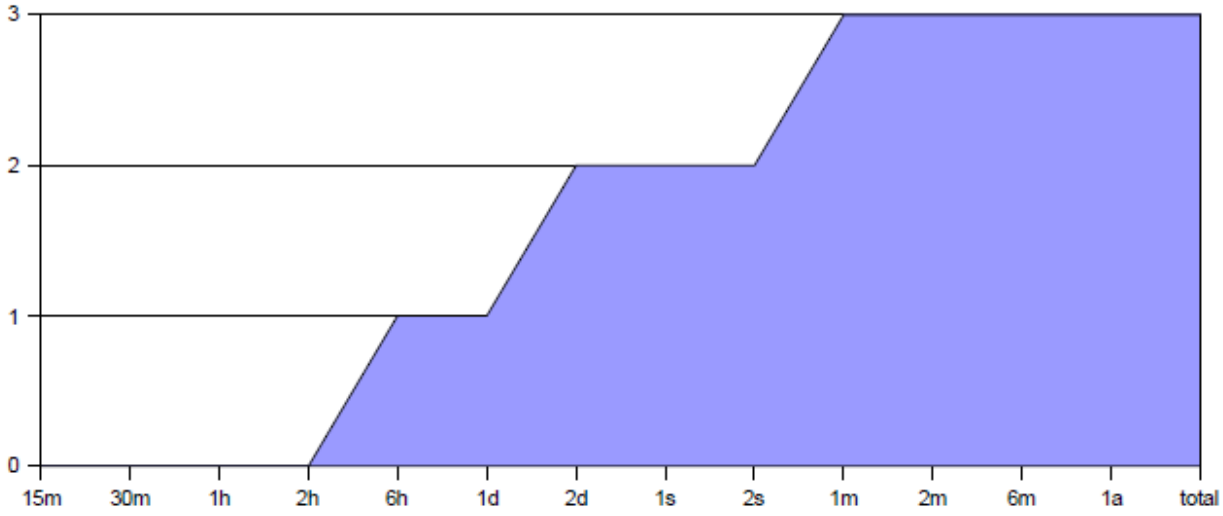


Figura 6- Costo de la Interrupción de la disponibilidad del servicio y/o Activo (Iso 22301:2019)

Figura 7- Recuperación - Tiempo vs Costos (Iso 22301:2018)

RPO (Punto de Recuperación Objetivo)

- Es el tiempo que existe entre las copias de seguridad de datos y respaldos de sistemas. Define la pérdida de datos máxima tolerable antes una interrupción.

RTO (Tiempo Objetivo de Recuperación)

- Es el tiempo de recuperación objetivo para tener, los sistemas y procesos operativos nuevamente.

MTPD (Período Máximo de Interrupción Tolerable)

- Es el tiempo máximo después del comienzo de una interrupción del negocio, dentro del cual se debe reanudar la operación a su normalidad. De no recuperarse la operación, el impacto se vuelve inaceptable.

Figura 8- Plan de Continuidad del Negocio. (Iso 22301:2019) (NFPA 1600:2016)

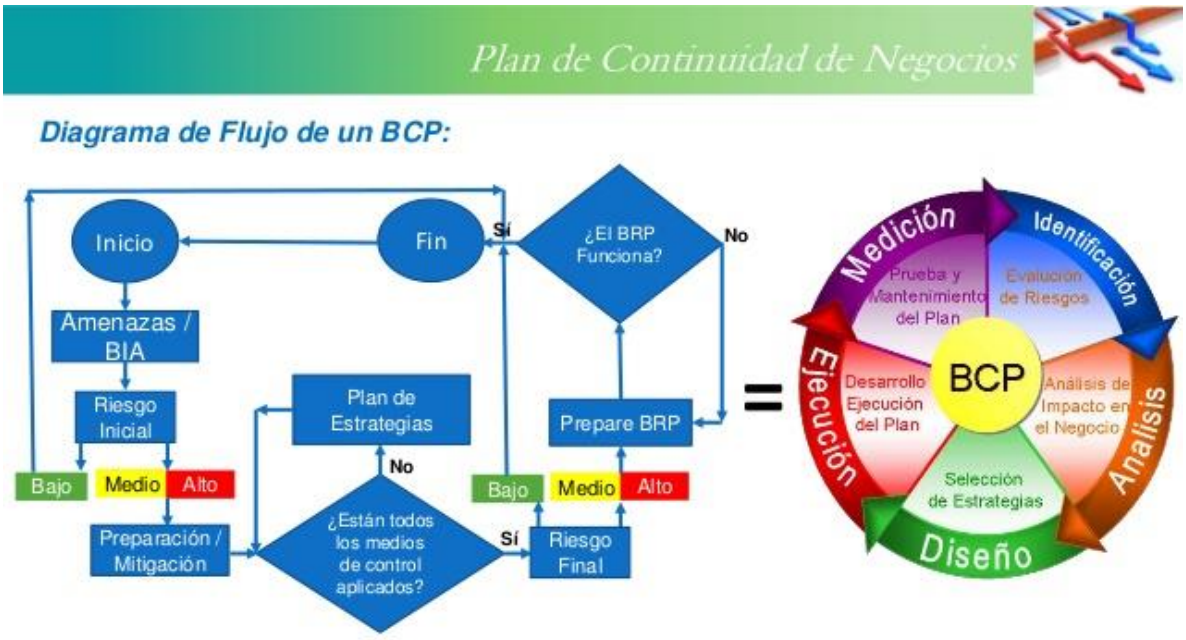


Figura 9- Diagrama de Flujo de Continuidad del Negocio. (Iso 22301:2019)

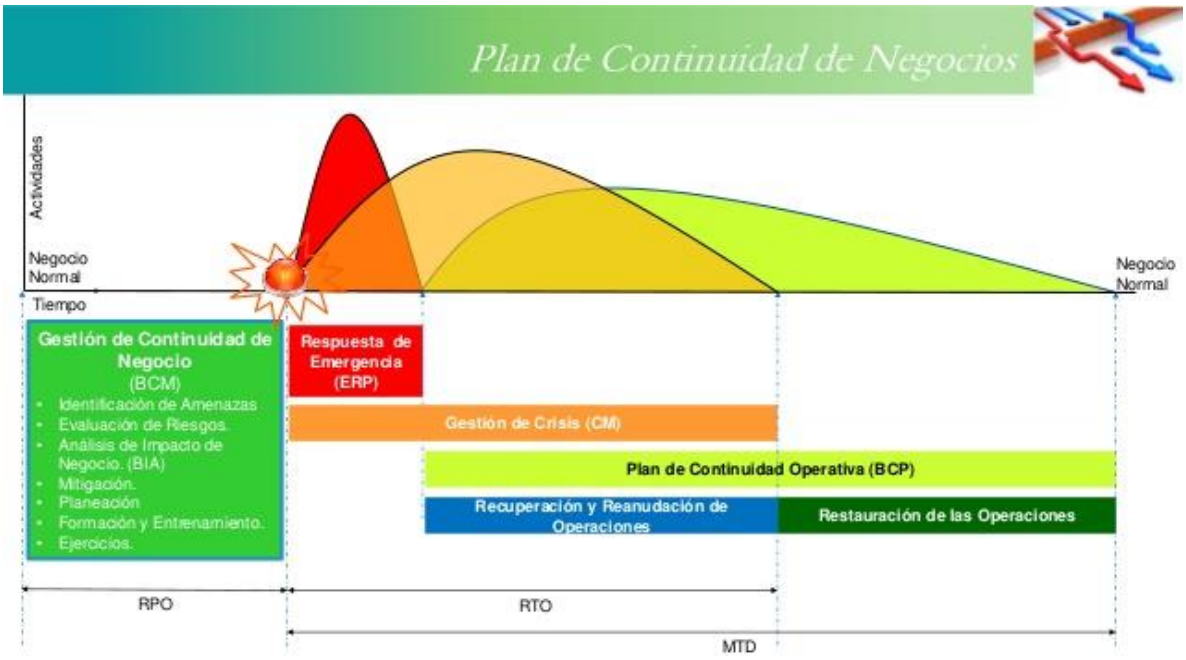


Figura 10- Gestión de afectaciones e Incidentes – (ISO 22301:2018)

Anexo C: Etapa de Valoración de Vulnerabilidades.

Antes de empezar a revisar, determinar y valorar las vulnerabilidades en las empresas y como estas pueden de una u otra manera permitir que se lleven a cabo los ataques informáticos o ciberataques, se sugiere por favor tener claro que son las vulnerabilidades.

Hoy en día todas las organizaciones y personas utilizan dispositivos inteligentes, computadoras, redes inalámbricas, etcétera. Y están expuestas a diferentes amenazas cibernéticas derivadas de la utilización de páginas web, apps, documentos, correos electrónicos, servicios de chat, redes sociales, etc.

La mayoría de estas amenazas están siendo creadas para extraer información personal o corporativa y con esto realizar ataques dañinos que vulneran nuestra capacidad para realizar transacciones, acceso a documentos, sistemas internos, etc.

Mientras que por un lado hoy tenemos a la disposición cientos de servicios de interconexión entre personas y organizaciones, por el otro estamos teniendo mucha mayor exposición de nuestra información personal y corporativa hacia personas no autorizadas que utilizan diferentes métodos para atacar y estos están siendo cada vez más complejos, más difíciles de prevenir y sobre todo más dañinos. Esto ha llevado a las organizaciones a poner mucho más énfasis en la ciberseguridad y los aspectos preventivos y correctivos ante un ataque.

Dentro de una correcta planeación de protección preventiva y correctiva se debe de considerar el análisis de vulnerabilidades como una actividad clave para asegurar que estamos al día ante la creciente ola de amenazas que día a día va creciendo de manera exponencial. (Cero Uno – 2020).

Se define vulnerabilidad como una debilidad de cualquier tipo que compromete la seguridad del sistema informático, es decir, sus servicios, procesos, información, infraestructuras y recursos a cargo. (U Distrital – 2016).

También se puede definir una vulnerabilidad, como un estado de un sistema (o conjunto de sistemas), que puede ser explotada por los ciberdelincuentes o atacantes de manera intencionada, no intencionada, por error y/o por desconocimiento, de tal manera que pueda:

- Permitir a un atacante acceder a información confidencial.
- Permitir a un atacante modificar información.
- Permitir a un atacante negar o denegar un servicio o todos los servicios de un sistema informático o de una red convergente.

Permitir a un atacante sustraer, robar información de las organizaciones y de las personas.

Permitir a los atacantes secuestrar la información de las organizaciones y pedir rescates o extorsionar económicamente a la empresa afectada.

Comprometer secretos industriales y/o empresariales.

Comprometer la seguridad y la disponibilidad de Infraestructura Criticas.

Comprometer la seguridad nacional de un país.

Entre otras afectaciones más.

Es perentorio que todas las organizaciones conozcan, analicen y traten en lo posible de erradicar estas vulnerabilidades en sus sistemas de información e interconexiones, máximo en lo que tiene que ver con sus interrelaciones con el ciberespacio.

Conocer el listado o contar con una matriz e vulnerabilidades permitirá a las empresas saber a qué se arriesgan, a que se exponen, saber que deben hacer para resarcir esa vulnerabilidad y de igual manera conocer que, cuáles y cuantas modificaciones e inversiones deben realizar para eliminarlas, corregirlas o mitigarlas.

De igual manera las empresas afectadas o atacadas por delitos informáticos o ciberataques, podrán determinar que vulnerabilidad fue explotada, si estaba esta vulnerabilidad en sus registros, conocer las posibles nuevas afectaciones a las que pueden verse expuestos; como además conocer el origen de las afectaciones y el modo operandi de los atacantes.

De igual manera si tiene matrices de relaciones entre sus debilidades, podrán determinar que otras afectaciones, servicios o procesos pueden estar afectados y así lograr una cuantificación y valoración efectiva, real y proporcional de los daños sufridos.

El objetivo principal de este Anexo C, es mostrar parte de esta metodología, dar a conocer otras metodologías existentes, mostrar procesos de determinación y análisis de vulnerabilidades en las redes convergentes de las empresas. Esto para que las empresas puedan tener en cuenta todas estas consideraciones, análisis y listado de vulnerabilidades para:

- Estudios previos para identificaciones de las vulnerabilidades, análisis de las mismas y mirar que inversiones e implementaciones realizar al interior de la empresa u organización para eliminarlas o mitigar el impacto de estas al llegar ser explotadas.

- Al momento de análisis y cuantificación, posteriores a los ataques informáticos o ciberataques ocurridos en una empresa u organización, en caso de que estas vulnerabilidades ya fueran explotadas. Esto se sugiere como un punto de partida del análisis de afectaciones en las que se incurre, pero también para mirar que otras vulnerabilidades tienen relación y/o dependencia con la vulnerabilidad explotada; para de esta manera rastrear otras afectaciones, otros ataques de no tal fácil detección y en general poder realizar estudios completos, pertinentes y eficaces en la empresa afectada.

  De igual manera el análisis de todas las vulnerabilidades, sus correlaciones con otras vulnerabilidades permitirán identificar completamente todo el daño o afectación, pero de igual manera permitirá conocer que otras afectaciones se sufrieron o pueden sufrir a futuro y que pongan en riesgo la estabilidad, incluso la existencia de la organización.

En términos generales estas vulnerabilidades se pueden presentar a nivel lógico, físico, procedimentales, en personas, en procesos, en políticas, en procedimientos; dentro de las empresas u organizaciones.

La metodología propuesta, a manera de guía, consiste en hacer un levantamiento de información para identificar puertos, servicios, procedimientos, fallas en los recursos o en general en todas las empresas en lo que tienen que ver con sus vulnerabilidades existentes y/o explotadas, como además revisar las correlaciones o interdependencias entre todas ellas, que puedan llevar al traste toda la operación, las finanzas y la reputación de las organizaciones.

Acto seguido, se recomienda hacer los análisis requeridos de cada una y de todas las vulnerabilidades de la empresa u organización, determinando el nivel de posibles explotaciones de estas vulnerabilidades, el impacto que pueda conllevar al interior de las organizaciones y determinar cómo suplir estas vulnerabilidades o de qué manera la utilizaron para atacar a las empresas como tal.

Se puede informar que los métodos propuestos para la identificación y análisis de vulnerabilidades, tienen un alto sentido práctico y es eficiente para todos aquellos involucrados en el área de seguridad, al utilizar herramientas de fácil acceso, herramientas propietarias o herramientas con cero costos y que entregan información valiosa, veraz de los componentes de las redes, como además de todas las redes convergentes e interconexión empresarial al ciberespacio de las empresas a analizar; que en sentido general, proporcionan una mejor visualización y compresión, apoyando la toma de decisiones para mitigar los riegos de seguridad y ayudar a cuantificar de manera completa y amplia las afectaciones reales ocurridas

o sufridas en las empresas u organizaciones, víctimas de ataques informáticos o ciberataques.

Existen en las infraestructuras, en los recursos y los procesos de las organizaciones y de las empresas como tal, muchas vulnerabilidades; acá se destacan, las que se consideran más importantes o las que a lo largo del tiempo vienen siendo más utilizadas y/o más explotadas, para afectar a las empresas, estas en resumen son:

- Vulnerabilidades de Diseños: En esta se tienen en cuenta las debilidades en el diseño de protocolos utilizados en las redes, sistemas informáticos, redes convergentes o en la operación de las empresas que en la mayoría de los casos están interconectados a internet o al ciberespacio. Esto en la gran mayoría de casos se presentan por políticas de seguridad deficientes o inexistentes, falta de implementación de políticas de seguridad en nuevos productos y/o servicios, errores de programación, existencia de "puertas traseras" en los sistemas informáticos, descuido de los fabricantes, descuido en los usos, mala configuración de los sistemas informáticos, desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática, gran existencia y alta disponibilidad de herramientas que facilitan los ataques, limitaciones empresariales y/o gubernamental de tecnologías de seguridad, vulnerabilidades del día cero – las cuales son el grupo de aquellas vulnerabilidades para las cuales no existe una solución conocida, pero se sabe cómo explotarla.

  Con el fin de protegerse contra este tipo de ataques informáticos, es importante desarrollar políticas, matrices, procesos, procedimientos, aplicaciones que utilicen lenguajes de programación avanzados; que permitan y garanticen una administración precisa de los recursos, las acciones, las operaciones seguras en todas las empresas y organizaciones.

  En la actualidad esto viene ocurriendo en sistemas de IoT (Internet de las Cosas), donde se tienen a nivel mundial más de 100 billones de dispositivos interconectados al internet y al ciberespacio, con nulas herramientas y protecciones, las cuales vienen siendo ampliamente atacadas, poniendo en riesgo las operaciones empresariales, los datos personales, los datos corporativos, privacidad de las empresas, organizaciones y hasta la seguridad nacional y empresarial.

- Vulnerabilidad de condición de carrera o (Race Condition): Este tipo de vulnerabilidad se presenta cuando múltiples procesos se encuentran en modo de competición, pues del resultado de la competencia dependerá el orden de ejecución de dichos procesos y nuevos nichos de mercados para

las organizaciones. Al encontrarse los procesos en este tipo de condición no estarán correctamente sincronizados, testeados, analizados y es aquí donde se manifiesta el riesgo de corrupción de datos, puertas traseras, problemas graves de vulnerabilidades en los productos y servicios, sacados al mercado sin todas las pruebas y validaciones requeridas.

Ejemplos de esto, pueden ser: Salida al mercado de productos no terminados o en modo beta, como además otro ejemplo de esta situación es cuando se presenta el interbloqueo: dos procesos están en espera de que el otro ejecute una acción y finalmente, ninguno de los dos se ejecuta como consecuencia de esta espera.

- Vulnerabilidad de Cross Site Scripting (XSS): Vulnerabilidad que se presenta en aplicaciones web, caracterizadas por la inyección de código VBScript, JavaScript u otros códigos maliciosos desarrollados con cualquier otro lenguaje de programación, que se evidencia en las experiencias de usuario final al ingresar a alguna página; es una de las vulnerabilidades más conocidas y de mayor de uso para ataques en el ciberespacio, siendo el phishing su forma más utilizada, en donde la victima cree que está ingresando a una página legítima a través de una URL valida y en la cual normalmente se sugiere en la barra de direcciones; sin embargo, accede realmente a una página totalmente diferente a la desea.

  El riesgo potencial de esta modalidad es que una vez la víctima ingresa sus credenciales son enviadas al atacante, esto quiere decir, que estas páginas la desarrollan para obtener datos personales, datos de tarjetas de créditos, información bancaria y en general datos que pueden utilizar para robar recursos económicos, hacer compras posteriores en internet en contra del real dueño de las tarjetas y de las cuentas bancarias.

- Vulnerabilidad de denegación del servicio: Su principal objetivo es imposibilitar la prestación de servicios empresariales, institucionales o corporativos; acá en este ataque de denegación de servicios, al contrario del ataque anteriormente definido (phishing), no se tienen como finalidad la captura datos personales, claves o datos en general, sino que su única finalidad de sabotear, buscar negar el acceso a servicios y recursos de una organización por un periodo de tiempo no definido.

  Esto afecta de forma considerable la reputación, la operación, la disponibilidad y toda la parte económica y financiera de las organizaciones, en resumen estas vulnerabilidades y los ataques que explotan esas

vulnerabilidades (DoS – Denegación de Servicios), va dirigido a empresas cuyo funcionamiento hace un uso robusto de los recursos de internet para impedirles su normal desarrollo, operaciones y generación de valor; un claro ejemplo de este tipo de ataques es la saturación de los Call Center (Centro de Llamadas) de las organizaciones, a través de peticiones excesivas, a tal punto que este servicio colapsa y deja de estar disponible para las personas o empresas que realmente requieren comunicarse con el centro de llamadas de la empresa afectada.

Existe una variante de este ataque que explota esas vulnerabilidades de las empresas y es lo que se conoce como Denegación de Servicios Distribuidas (DDoS), en la cual se opera de una manera muy similar a los ataques de DoS, pero en este caso se hace a mayor escala, mayor afectación, mayor impacto y de una manera más compleja y preparada. Es decir, de una manera más distribuida y afectando a muchos más recursos, servicios al tiempo en la misma organización o empresa víctima.
Estos dos (2) tipos de vulnerabilidades de este ítem (DoS, DDoS), presentados conjuntamente por su similar y parecida forma de atacar a las organizaciones, realizan ataque donde envían paquetes IP de tamaños y formatos no tradicionales que logran saturar los equipos objetivos, generando mal funcionamiento con la consecuente inestabilidad del servicio ofrecido en las organizaciones. De esta manera, se altera el normal funcionamiento de la prestación de servicios.

Las recomendaciones para que las empresas se mantengan, protegidas contra este tipo técnicas maliciosas, son: visitar regularmente las páginas que informan de nuevos ataques, monitorear todas las paginas, portales e infraestructura que soportan los servicios en las organizaciones, llevar de manera organizada y tabulada información estadística de todos los Monitoreos, tener grupos de trabajos contra estos incidentes, analistas de la infraestructura y los servicios, como de igual manera es supremamente importante tener parchados los sistemas operativos y/o Fireware (aplicar parches y actualizaciones informáticas generadas y distribuidas por los fabricantes de los equipos o servicios); de esta manera se puede una empresa proteger en parte y ayuda de una u otra manera a mitigar el riego en buena medida, de ser víctima o sufrir estos atacas que explotan las vulnerabilidades de la infraestructura para denegar los servicios empresariales.

- Vulnerabilidad de ventanas engañosas (Windows, ARP Spoofing, otras): Otras de las vulnerabilidades ampliamente utilizadas son estas que tienen que ver o

utilizan ventanas emergentes engañosas, mensajes engañosos, que de una manera u otra le dicen y dan a conocer al usuario víctima, que ha sido el ganador de algo o tal cosa, lo que realmente es totalmente invalido o una gran mentira.

Estas vulnerabilidades y/o ataques, buscan que el usuario proporcione información personal, financiera entre alguna otra información que realmente requiera el atacante o los patrocinadores de ese tipo de ataque.

Existen otros tipos de ventanas emergentes, que lo que hacen es una vez activadas, empiezan y siguen obteniendo datos del computador comprometido, para luego si realizar ataques informáticos contra esa persona u organización; su funcionamiento o modo de operación, en resumen, se basa en el envío de paquetes falsificados, generalmente banners, indicando que la víctima, es el ganador de un premio; donde de esta manera se buscan mínimo dos (2) objetivos:

i. Obtener la información del usuario o datos de identificación del equipo, como su dirección IP o MAC, con esto se logra asociar la dirección MAC de un equipo con la correspondiente dirección de IP de la puerta de enlace o Gateway del dispositivo conectado a la red de internet. De esta manera se obtiene o se logra que cualquier información que envíe el usuario no llegue a su destino real sino a la persona o atacante, que realiza el ataque.
ii. Una vez con estos datos se pueden llevar a cabo dos (2) tipos de ataques. El primer es un ataque “Pasivo”: Donde se deja pasar la información hacia el destino real y se escuchan los datos enviados (Sniffer o Escucha Electrónica) – (Perdida de Privacidad y/o Confidencialidad). El segundo ataque es el ataque “Activo”, donde los datos originales son modificados para su posterior reenvío (perdida de Integridad).
iii. Como medidas de contención de este tipo de ataques o explotación de estas vulnerabilidades, se recomiendan procedimientos técnicos como el uso de ARP estáticas, la utilización y activación de DHCP Snooping, Bpdu Guard, entre muchas más; que en síntesis permiten detectar la existencia de estas vulnerabilidades e identificar si existe una suplantación de ARP u otras posibles afectaciones.

Todas estas anteriores vulnerabilidades informáticas definidas, también las podemos organizar, agrupar en función de:

- ✓ Diseño e implementación de políticas de la seguridad perimetral o también con base a la seguridad en profundidad.
- ✓ Debilidades en el diseño de protocolos utilizados en las redes, productos, equipos, sistemas operativos y/o plataformas tecnológicas.
- ✓ Debilidades en los diseños de productos o servicios, por falta total o parcial, de conocimientos y de la cultura de ciberseguridad; la cual debe prevalecer y estar presentes en todas las áreas de las empresas u organizaciones.
- ✓ Políticas de seguridad deficientes e inexistentes en las empresas u organizaciones.
- ✓ Problemas o fallas asociados a las Implementaciones en las empresas y organizaciones.
- ✓ Errores de programación.
- ✓ Existencia de “puertas traseras” en los sistemas informáticos.
- ✓ Descuido de los fabricantes.
- ✓ Uso.
- ✓ Configuración inadecuada de los sistemas informáticos.
- ✓ Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- ✓ Alta y exagerada Disponibilidad de herramientas que facilitan los ataques.
- ✓ Limitación gubernamental de tecnologías de seguridad.
- ✓ Vulnerabilidad del día cero.

Previendo y siendo proactivos ante todos estos factores de riesgos, los más pertinentes controles, consisten en el análisis de vulnerabilidades; como un servicio por medio del cual se comprueban a través de herramientas de software, análisis y servicios de consultoría, la posible debilidad o fortaleza que posee una empresa u organización, ante el conjunto de amenazas conocidas al día de la evaluación tanto para elementos externos (Servicios SAAS, Servicios de Cloud Computing, Servicios BYOD, Usuarios no autorizados, sniffers, robots, IoT, IA, Blockchain, Data Analítica, etc.) como para elementos internos (Usuarios, sistemas implementados, estaciones de trabajo, dispositivos móviles, sistemas operativos, etc.)

Se debe tener en cuenta que un correcto, completo y pertinente análisis de vulnerabilidades; no solo detecta las áreas con vulnerabilidades, sino área con posibles soluciones de mejora a trabajar y a tener en cuenta. De igual manera esto también permite saber en qué invertir, cuánto invertir, y en general, proponer una correcta arquitectura necesaria para proteger la infraestructura de una organización y los diferentes cambios de políticas de seguridad que se requieran implementar para asegurar una continuidad de operación y del negocio.

Permite además conocer el nivel de asistencia que se debe proveer, cuando se ve comprometida la seguridad informática y la recuperación ante desastres por estas amenazas, intrusiones, delitos informáticos o ciberataques.

Como sugerencia para aplicar la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; establece y recomienda tener en cuenta y seguir como mínimo los siguientes pasos que se consideran necesarios y pertinentes.

Esto ayudaran al equipo de trabajo del proyecto a realizar un análisis de vulnerabilidades pertinente, real, optimo, completo y que se pueden resumir de la siguiente forma:

- Diagnóstico de Seguridad de la información, seguridad informática y ciberseguridad en la organización motivo de análisis:

  Escaneo de vulnerabilidades externas.

  Escaneo de vulnerabilidades internas.

- Revisión de la ausencia, existencia, aplicabilidad de las Políticas de Seguridad de la información en las empresas u organizaciones.

- Revisión de procesos, pólizas de soporte y configuraciones que comprometan la seguridad informática.

- Reforzamiento y afinamiento de las topologías de las redes convergentes de las empresas u organizaciones.

- Generación de documento de recomendaciones de buenas prácticas de seguridad informática, arquitectura ideal para la organización.

- Planeación ante eventos que comprometan la seguridad de la empresa u organización.

- Revisión de políticas de respaldos, sistemas de redundancia, planes de recuperación de desastres.

- Generación de documento recomendaciones ante eventos de seguridad.

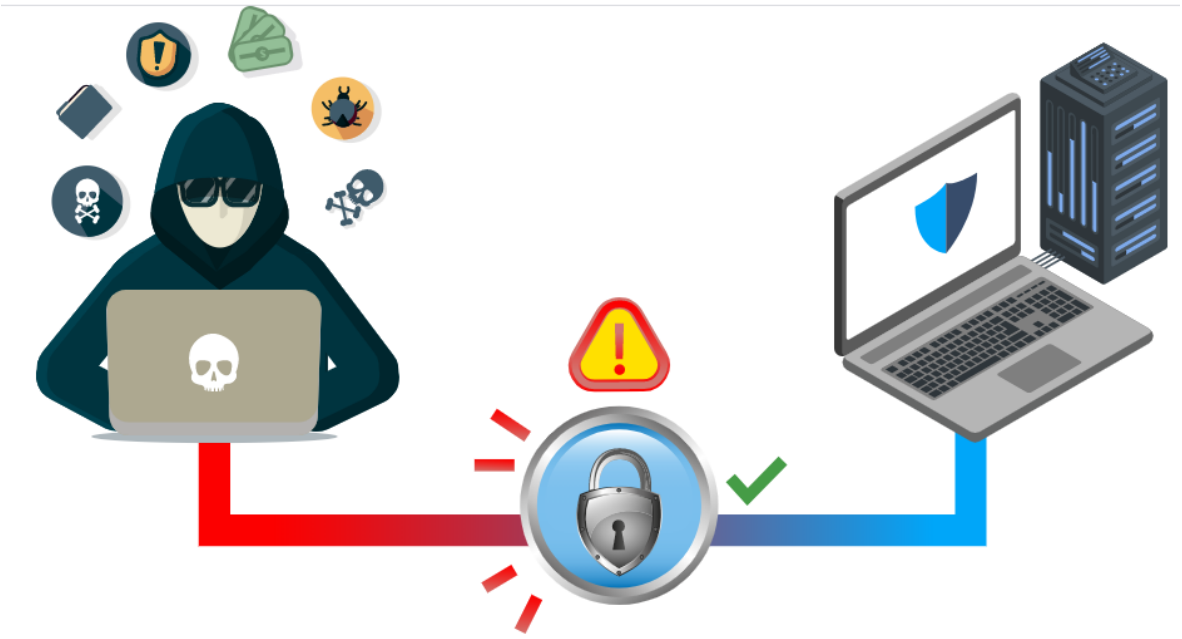


Figura 11- Representación gráfica de las vulnerabilidades informáticas y tecnológicas en las empresas u organizaciones (Azure and Fortinet - 2021).

Es supremamente importante que todos los esfuerzos realizados en las empresas u organizaciones posteriormente a la implementación o aplicación de un análisis de vulnerabilidades, se diseñen, implementen y realicen procesos de auditoría por lo menos semestralmente; esto se considera como un periodo de tiempo adecuado o mínimo que permite asegurar que todas las recomendaciones estén en funcionamiento y los procedimientos, como además las políticas adoptadas en seguridad de la información, seguridad informática y ciberseguridad; se encuentren acordes, sean pertinentes y suficientes a la situación actual de la organización, previéndole los niveles de seguridad y de continuidad del negocio que le permitan generar valor a la empresa y seguir siendo éxitos y vigentes en el tiempo.

Desde el punto de vista de la aplicación y de la implementación de los análisis de vulnerabilidades se recomienda minino tener y seguir los siguientes pasos y recomendaciones:

- Tener en cuenta que análisis de vulnerabilidades informáticas, es un complemento del proceso del análisis y valoración de riesgo informáticos, los cuales veremos en uno de los próximos anexos de esta metodología.

- El análisis de vulnerabilidades es una actividad fundamental con el fin de orientarnos hacia un sistema de gestión de la seguridad de la información (SGSI), el cual debería comprender como mínimo las siguientes actividades y/o fases:

a) Entendimiento de la Infraestructura y Topologías existentes: En esta fase se debe, identificar e inventariar; canales, conexiones, dispositivos de hardware o software existentes en la infraestructura que soportan los procesos y servicios del negocio. Esta selección debe iniciarse con los servicios prestados, continuar luego con los procesos asociados a estos servicios y de allí, determinar los activos o dispositivos que soportan estos procesos. (Canales con sus respectivos acuerdos de servicios, servicios se seguridad tercerizados, pólizas y garantías d servicios contratos, servidores, equipos terminales de datos, aplicaciones o plataformas, bases de datos, equipos activos de redes, equipos y plataformas de seguridad, dominios, cuentadantes y ubicación de todos estos equipos y elementos).

b) Pruebas: En esta segunda fase que se recomienda, se deben realizar una clasificación de activos o dispositivos con base en la confidencialidad de la información que guardan y la importancia del activo para la continuidad del proceso en estudio.

   Utilizando herramientas, comandos y metodologías para este proceso, se deben llevar a cabo todas las pruebas, estas desarrollados por expertos y personas autorizadas por escrito por el representante legal de la empresa u organización. Para ello se puede hacer uso de herramientas para la detección de vulnerabilidades GNU y licenciadas, se recomienda preferiblemente herramientas comerciales (no software libre) y soportadas debidamente por su fabricante.

   Adicional se recomienda y se requiere que, en la empresa u organización, exista y este aprobada una base de datos actualizada y completa de vulnerabilidades aceptadas por la industria (CERT, SANS) y con un criterio común de clasificación como el CVE (common vulnerabilities and exposure). Estas herramientas aplicadas en la empresa permiten poder identificar cualquier elemento activo presente en la red que tenga asociada una dirección IP (v4 o v6), con la finalidad de detectar en estos, sus vulnerabilidades presentes a nivel de software, Fireware y evitar futuros incidentes de seguridad, ataques informáticos o ciberataques.

c) Medidas preventivas a tener en cuenta antes de realizar un análisis de vulnerabilidades: Siempre antes de proceder a correr o aplicar un análisis de vulnerabilidades, esta metodología le recomienda determinar el alcance y universo de la prueba, una vez determinado el alcance o universo de la prueba, se deben tomar si o si, medidas preventivas adecuadas necesarias para la ejecución del análisis de vulnerabilidades, esto con la única finalidad

de prevenir efectos adversos, contrarios o no deseados, sobre la prestación, disponibilidad y operación de los servicios en la empresa u organización motivo de análisis; entre ellas, podemos resaltar:

1. Especificar ventana de tiempo o hora adecuada de pruebas – Se sugiere horas de inactividad o horas de poco tráfico

2. Realizar un análisis de riesgo cualitativo sobre la prueba, es decir, un análisis sobre la no disponibilidad de activos críticos de la prueba, esto estimando porcentaje de probabilidad y estimación del impacto si llegase a presentar algún riesgo no controlado.

3. Tomar algunas medidas de contingencia, en caso de presentarse resultados no deseados o no esperados, es decir, especificar estrategias de contingencia para activos críticos, involucrar al oficial de seguridad, coordinador BCP o DRP, realizar respaldos de la información de los activos involucrados y guardar en formato electrónico y físico configuraciones de equipos involucrados.

4. Realizar Monitoreos constantes de los servicios durante las pruebas, teniendo en cuenta y priorizando casos excepcionales como tiempos de respuesta excesivos, eventos o incidentes de seguridad.

5. Se debe contar con autorización por escrito del representante legal de la empresa u organización y de igual manera se debe informar a todas las personas de operaciones en la empresa, de la realización de las pruebas.

6. Se debe monitorear el tráfico de la red, priorizando los segmentos que se consideren críticos, utilización de los segmentos críticos, condiciones de error (CRC, Bad checksum, etc.), utilización de procesamiento en los servidores críticos, informar a los dueños, cuentadantes o responsables de los activos objeto de análisis.

d) Realización de las pruebas de vulnerabilidades: Para estas pruebas dependiendo de la cantidad de activos a analizar se van a requerir grandes tiempos de operación y desarrollo de la prueba, se estima que para un grupo de activos aproximadamente de 90 IPs, el tiempo de la prueba debe estar alrededor de tres (3) horas para el análisis completo y exhaustivo.

Es proporcional si quisiéramos extrapolar para otros rangos de direcciones y estimar otros tiempos de duración. Es importante considerar que si se tienen redes remotas protegidas por firewall, las cuales también quisieran ser

analizadas, el firewall debe permitir pasar el tráfico generado por la herramienta de análisis de vulnerabilidades. Por ello se debe tener en cuenta y conocer los puertos a utilizar y estos permitirlos en el Firewall o Corta Fuego. Por último, se recomienda utilizar con una herramienta tecnológica, que tenga la posibilidad de descubrimiento automático de dispositivos de red.

Estos análisis o pruebas se pueden clasificar como:

1. Internas (Sin conocimiento o Con conocimiento)
2. Externas (Sin conocimiento o Con conocimiento)

e) Pruebas de Explotación de las vulnerabilidades: Como parte primordial del proceso de análisis de vulnerabilidades, se realiza la clasificación de las vulnerabilidades más críticas, sobre estas se debe hacer una prueba tratando de realizar su explotación.

En la medida en que la herramienta sea más inteligente, más estructurada, más exhaustiva y por ende más estructurada el proceso será más corto y no requerirá un perfil tan sofisticado.

Se estima que en promedio el tiempo de explotación de al menos 20 vulnerabilidades, debe gastar al menos unas tres (3) horas, incluyendo la realización del informe que es la parte más importante de todo este análisis. El proceso de explotación debe incluir el escalar privilegios (tomar control del dispositivo como administrador) con el fin de tomar control total de los sistemas y de esta manera seguir de manera estricta la forma en que se llevan a cabo los ataques en la vida real (simular ciberataques).

f) Análisis de resultados: Cuando ya se obtengan los datos, producto del análisis de vulnerabilidades y el respectivo informe final, se debe con base en la información recolectada y obtenida; realizar una reunión técnica para informar de estos resultados y realizar una revisión general de las vulnerabilidades encontradas y la clasificación realizada por la herramienta.

Cuando la empresa ya fue afectada por delitos informáticos o ciberataques, este proceso se debe hacer teniendo en cuenta los lineamientos de computación forense y sin llegar a contaminar las pruebas o evidencias del caso. Allí se debe mirar que vulnerabilidad fue explotada, que otras vulnerabilidades tiene relación o conexión con la vulnerabilidad explotada y

de esta manera hacer un estudio mucho más completo, estructurado y que permita definir el impacto del ataque y cuantificar correctamente la afectación económica, financiera, operacional o reputacional en contra de la empresa u organización.

Una vez definidas estas correlaciones entre vulnerabilidades, se deben revisar la información, operación, funcionamiento o afectación de los procesos, activos o servicios que están asociadas a esas vulnerabilidades priorizadas.

En esta reunión de entrega de informe y resultados, mínimo debe estar:

1. CIO, CISO u oficial de seguridad.
2. Responsables o dueños de los procesos, servicios o activos ligados o asociados a las vulnerabilidades definidas.
3. Gerente o director del área o áreas afectadas.
4. Comité de seguridad o de riesgos en la empresa u organización.
5. Dueños o responsables de los activos implicados.
6. Coordinador del plan de contingencias y del proceso de continuidad del negocio.

g) Plan de corrección o tratamiento de vulnerabilidades: Una vez aplicado el análisis de vulnerabilidades, identificados los riesgos o vulnerabilidades explotadas y sus afectaciones o impacto, se debe proponer un plan de mejora o de corrección específico para las vulnerabilidades, este plan de igual manera podría hacer parte del Plan de Tratamientos de Riesgos de la Organización (ISO 27001 – ISO 31000 – ISO 22301).

Este plan de mejora, en resumen, clasifica con ayuda de las herramientas de vulnerabilidades y de explotación, la criticidad de cada una de las vulnerabilidades encontradas y sugiere cuales deben ser solucionadas en el corto, mediano o largo plazo. Esta decisión sobre el tiempo a implantar el control respectivo a la vulnerabilidad también debe contemplar costo del control, la inversión requerida, el daño ocasionado, el valor del esfuerzo perdido o la inversión perdida, la capacidad, administración y facilidad de implementar correctamente el plan de mejora al interior de la organización, empresa y todos sus procesos, activos y servicios.

A manera de conclusión de este anexo C, de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, se puede especificar lo siguiente:

Debe existir una matriz o listado de vulnerabilidades, organizadas de acuerdo con la criticidad e impacto de ellas en los procesos, servicios o activos de las empresas u organizaciones.

Esta matriz de vulnerabilidades se debe tener en cuenta al momento de definir los sistemas de gestión de seguridad de la información (SGSI), la matriz de riesgos, el plan de mejoramiento y tratamiento de los riesgos en las organizaciones.

Se deben analizar las vulnerabilidades y sus procesos asociados, pero de igual manera de sebe estudiar las relaciones entre las vulnerabilidades y los procesos, activos o servicios asociados a estas vulnerabilidades y que puedan resultar afectados.

Se recomienda que se utilice una herramienta de análisis de vulnerabilidades que cuente con un soporte adecuado de su fabricante y cuente también con una base de datos muy completa en cuanto a vulnerabilidades.

Se recomienda con la herramienta de prueba o de análisis de las vulnerabilidades, adicionándole que en lo posible sea una herramienta automatizada, para mejorar la efectividad, es decir, utilizar herramientas más inteligentes, más eficaces, más efectivas ojalá asociadas o trabajando en conjunto con IA, SIEM, etc.

Es necesario tener en cuenta y considerar la efectividad del plan de mejora de esas vulnerabilidades, que como tal es la salida principal de todo este proceso de análisis de vulnerabilidad, y en últimas lo que garantizará la confiabilidad de los procesos y servicios ofrecidos.

Anexo D: Etapa de Valoración de Amenazas:

Luego de terminar o completar las fases de identificación y valoración de activos, la fase de valoración de vulnerabilidades, el equipo de trabajo del proyecto de aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; deben como fase siguiente identificar cualquier amenaza que por razonablemente o irrazonablemente pueda o haya causado afectaciones o lesiones a recursos, empleados, activos o servicios en una empresa, esta es la entrega identificada en la metodología como tercera fase (Anexo D).

Todas las amenazas: provocadas por el hombre (deliberadas, por desconocimiento, por error o accidentales) y por peligros naturales: se consideran con un nivel de detalle acorde con el alcance de la evaluación. Para diferenciar entre diversas amenazas y determinar cuáles tienen más probabilidades de plantear preocupaciones serias o mayores impactos, cada una se debe evaluar por separado y de acuerdo con la probabilidad de ocurrencia y la gravedad del evento en caso de que surja dentro de una empresa afectada o víctima de delitos informáticos o ciberataques.

Dado todo el exponencial crecimiento y pluralidades de las incertidumbres que rodean a la mayoría de las amenazas en las empresas y las organizaciones, los profesionales de seguridad y todas las partes interesadas de la empresa, a menudo experimentan serias dificultades. Se puede utilizar para entender y analizar esta incertidumbre el modelo VUCA 2012.

Figura 12- Entorno VUCA (Vuca 2012).

¿Cuánto afecta el entorno al negocio? El término VUCA - Volatilidad, Incertidumbre, Complejidad y Ambigüedad, por sus siglas en inglés - es una herramienta para empezar a comprender en cómo abordar la complejidad de los fenómenos actuales y qué hacer para adaptarse. Habitualmente se lo utiliza para calificar entornos complejos donde las tareas pueden variar y cambiar tan rápido como su ambiente.

El término VUCA se empezó a utilizar en el ámbito empresarial luego de la crisis económica del 2008 y sobre todo en este período de tiempo donde los cambios tecnológicos avanzan con tanta rapidez que desconcierta cualquier planificación haciendo que las empresas se vean obligadas a realizar modificaciones en su gestión de forma más rápida y radical. Esto se ve en diferentes contextos, sin importar el rubro: servicios, industria, producción y tecnología. (Vuca 2012).

Para facilitar la identificación de amenazas en un nivel de detalle apropiado, la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, introduce una lista jerárquica de amenazas. Luego, para promover el análisis comparativo entre diferentes amenazas, esta guía también proporciona métricas simples para la probabilidad y la gravedad de la amenaza potencial dentro de los procesos, servicios y en contra de los activos y recursos de las empresas y organizaciones. De esta manera se va a llegar a los valores de amenaza con mayor relevancia y pertinencia, los cuales van desde muy bajo a muy alto.

El resultado final de esta fase de evaluación de amenazas de un proyecto de aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, es simplemente una lista de amenazas con valores relativos que reflejan su probabilidad de ocurrencia y la seriedad de su potencial impacto en la confidencialidad, disponibilidad, integridad de la información y en los activos o recursos corporativos.

Esta fase consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos, servicios, recursos, reputación y empresa u organización; causándole un daño y afectado los principios de confidencialidad, integridad, disponibilidad y continuidad del negocio.

La amenaza se puede definir coma la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (UNE 71504:2008).

Identificación de las amenazas:

Esta parte de la metodología presenta y explica cómo se deben caracterizar las amenazas y las evaluaciones de las mismas, es en resumen un "Repositorio de Elementos" en el cual se presenta una relación de amenazas típicas.

Amenazas de origen natural:

Hoy día y de manera más constante, como además creciente y por efectos del calentamiento global, se presentan mayores accidentes naturales (terremotos, inundaciones, Tsunamis, Pandemias, etc.). Ante todos estos avatares el sistema de información es una víctima pasiva, pero de todas formas se debe tener muy en cuenta y se tiene muy en cuenta para la continuidad del negocio y lo que a las empresas les pueda llegar a suceder y les pueda llegar a afectar.

Amenazas del entorno, en cuanto al origen empresarial e industrial:

Se vienen presentando cada vez más y con mayor repeticiones y complejidad, muchos desastres industriales (contaminación, fallos eléctricos), ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos (Magerit 2012).

Amenazas por defectos de las aplicaciones:

Muchos de los problemas identificados en las empresas y en las organizaciones, se ha demostrado que nacen directamente en el equipamiento propio por defectos en su diseño, desarrollo o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades, tal como se puede observar en el anexo anterior.

Amenazas causadas por las personas de forma accidental o por desconocimientos:

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error, por omisión o por total desconocimiento.

Amenazas causadas por las personas de forma deliberada:

El recurso humano con acceso autorizado (Insider) o no autorizados al sistema de información, pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Se debe tener en cuenta que no todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir. Es decir, las instalaciones pueden incendiarse; pero las aplicaciones, no. Las personas pueden ser objeto de un ataque bacteriológico; pero los servicios, no. Sin embargo, los virus informáticos afectan a las aplicaciones, no a las personas (Magerit 2012 – Octave).

En todo este análisis se debe precisar que, para hacer valoraciones de las amenazas, no se puede obviar que cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, esto visto desde dos (2) sentidos:

Degradación: Que determina cuán perjudicado resultaría el “Valor” del activo.

Probabilidad: Que determina, cuán probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. Pero de igual manera la degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. (AS / NZS 4360)

Cuando las amenazas no son intencionales, probablemente baste con conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna, pues el atacante puede causar muchísimo daño de forma selectiva (Magerit 2012).

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 1- Degradación del Valor (Magerit 2012)

De igual manera, a veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia, como una medida de la probabilidad de que algo ocurra, es decir, son valores típicos (ARO – Annual Rate of Occurrence – 2012):

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 2- Probabilidad de Ocurrencia. (Magerit 2012)

Es importante tener siempre presente, que la determinación del impacto potencial de una amenaza, se le denomina “impacto” a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios, Es decir que el valor que se debe tener en cuenta no es para nada el costo que tenga en el sistema de inventario de las empresas o según facturas emitida por el proveedor del activo, sino que debe ser tenido en cuenta por el valor de lo que representa, apoya y ayuda ese activo a cumplir la misión, la estrategia institucional y la generación de valor en la empresa y la organización.

En general, Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

Figura 13- Clasificación de las amenazas. (CRAMM).

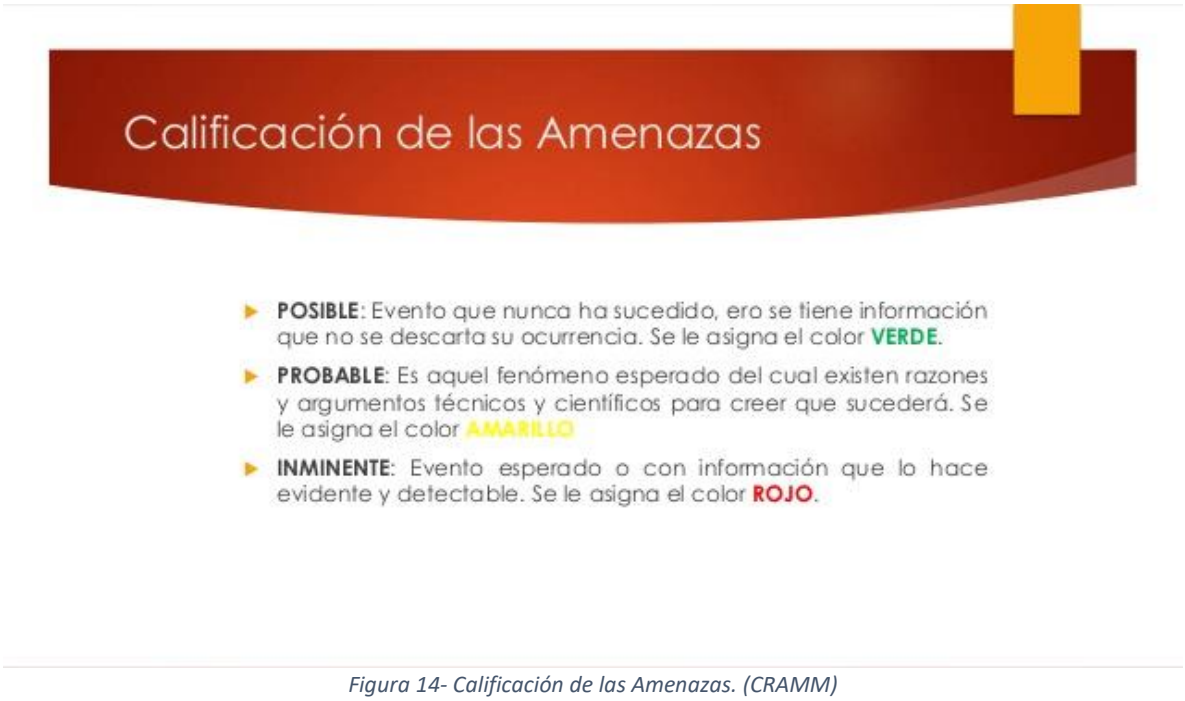


Figura 14- Calificación de las Amenazas. (CRAMM)

EVENTO	COMPORTAMIENTO	COLOR ASIGNADO	
POSIBLE	Es aquel fenómeno que puede suceder o que es factible porque no existen razones históricas y científicas para decir que esto no sucederá	VERDE	
PROBABLE	Es aquel fenómeno esperado del cual existen razones y argumentos técnicos científicos para creer que sucederá	AMARILLO	
INMINENTE	Es aquel fenómeno esperado que tiene alta probabilidad de ocurrir	ROJO	

Figura 15- Clasificación de las amenazas en color, de acuerdo a la probabilidad de ocurrencia. (Nist – Nist.sp.800-207).

VALORACIÓN	
PUNTAJE	CRITERIO
0	Se cuenta con suficientes elementos
0,5	Se cuenta parcialmente con los elementos o están en proceso de adquisición
1,0	Cuando no se cuenta con recursos

Tabla 3- Valoración de las Amenazas. (Mehari 2010)

PUNTAJE	ANÁLISIS	COLOR ASIGNADO
0,0 - 1,0	BAJO	
1,1 - 2,0	MEDIO	
2,1 - 3,0	ALTO	

Tabla 4- Puntajes, análisis y color asignado de acuerdo a la probabilidad de ocurrencia. (Mehari 2010)

Ver comentarios contienen explicación de llenado				
AMENAZA	FUENTE DE RIESGO	RANGO	CALIFICACIÓN	COLOR
PELIGRO				
	Describa que origino el peligro	0	Posible	
		0	Posible	
PELIGRO				
	Describa que origino el peligro	0	Posible	
		0	Posible	

POSIBLE	PROBABLE	INMINENTE
		

Tabla 5- Clasificación de las amenazas. (Mehari 2010)

A continuación, se muestra un resumen de un listado típico de amenazas:

- Ciberataques
- Manipulación de programas
- Denegación de servicios
- Robo de equipos
- Ataque destructivos
- Extorsión
- Ingeniería social
- Difusión de software dañino
- Errores de los usuarios
- Errores de administradores
- Vulnerabilidades de los programas
- Indisponibilidad del personal
- Desastres industriales
- Emanaciones electromagnéticas
- Contaminación medioambiental
- Avería de origen físico o lógico
- Corte de suministro eléctrico
- Fallo de servicios de comunicaciones
- Interrupción de servicios o suministros esenciales
- Desastres naturales

Anexo E: Etapa de Valoración de Riesgos y Riesgo Residual:

La comprensión de las prioridades y requisitos para la Continuidad del Negocio y los niveles de seguridad cibernética deseados en una empresa u organización, se logran mediante el análisis del impacto en el negocio (en inglés BIA) y la evaluación de los riesgos (en inglés RA). El BIA permite a la organización dar prioridad a la reanudación de las procesos y actividades de soporte a sus productos y servicios prioritarios.

La evaluación de riesgos promueve la comprensión de los riesgos para las actividades prioritarias y sus dependencias, y las posibles consecuencias de una disrupción. Este entendimiento permite a la organización seleccionar las estrategias y soluciones de continuidad de negocio apropiadas, tanto preventivas como correctivas y de recuperación.

Como además aplicando la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; le permitirá conocer exactamente que afectaciones económicas, financieras y reputaciones puede o sufrió una empresa al ser afectada por delitos informáticos o ciberataques.

Antes de profundizar en la sección, vamos a recordar los conceptos relativos al riesgo:

Riesgo: Efecto de la incertidumbre sobre los objetivos. Puede ser positivo o negativo. Un efecto es una desviación de lo esperado. Puede ser positivo, negativo o ambos, y puede abordar, crear o dar lugar a oportunidades y amenazas.

Los objetivos pueden tener diferentes aspectos y categorías, y pueden aplicarse a diferentes niveles. El riesgo suele expresarse en términos de fuentes de riesgo, eventos potenciales, sus consecuencias, y su probabilidad.

Evaluación de riesgos: Proceso general para identificar, analizar y evaluar los riesgos.

Apetito al riesgo: Cantidad y tipo de riesgo que una organización está dispuesta a afrontar o mantener. Aunque el concepto se mantiene vigente, el término ha sido eliminado de la última versión de la norma ISO 22301:2019, utilizándose en su lugar la propia definición cuando es requerido.

El riesgo residual: Los peligros que persisten después de haber implementado todos los controles y medidas de prevención respecto de los riesgos inherentes, se denominan riesgos residuales

El alcance aquí de riesgo, ahora sí, está relacionado con los riesgos disruptivos, y por lo tanto será expresado principalmente con consecuencias / impactos negativos.

La siguiente imagen muestra las fases de la evaluación de riesgos, en alineación con la norma NTC-ISO 31000:2018. Gestión del Riesgo. Directrices

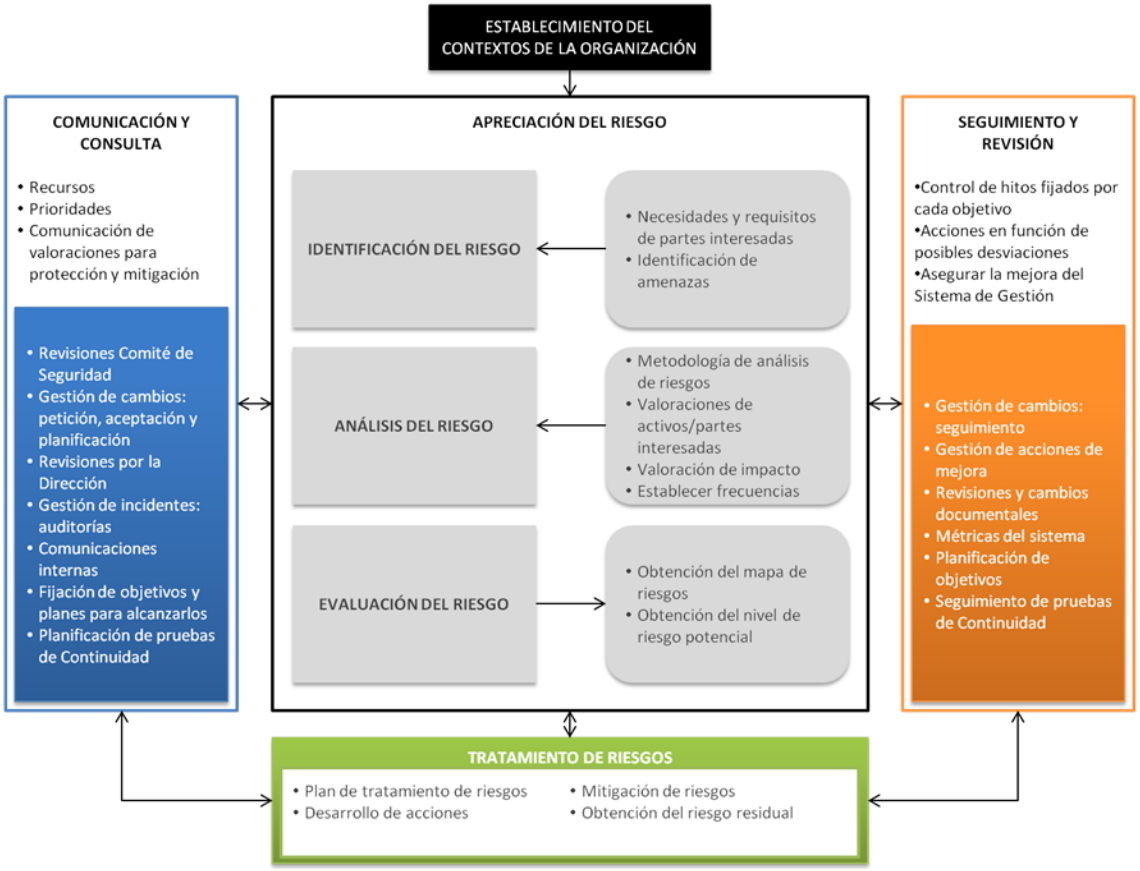


Figura 16- Apreciación del riesgo en una organización (ISO 22301:2019).

Se ha de garantizar que el proceso de evaluación de riesgos establezca y mantenga los siguientes criterios:

• Criterios de evaluación o de riesgo: Indica cuando la evaluación debe realizarse, normalmente a intervalos planificados y cuando hay un cambio relevante en la organización o alguno de sus recursos de soporte o infraestructura, por ejemplo, un proceso de negocio, un servicio, un sistema de información, un proveedor, etc.

• Criterios de aceptación de riesgo (apetito del riesgo): Indica la cantidad y tipo de riesgo que una organización puede aceptar ante interrupciones de las actividades priorizadas. Los criterios de aceptación del riesgo a menudo dependen de las políticas de la organización, las metas, los objetivos y los intereses de las partes interesadas. Una organización debe definir sus propias escalas para los niveles de aceptación del riesgo. El criterio de aceptación de riesgos debe establecerse teniendo en cuenta criterios comerciales o de negocio, aspectos legales y

reglamentarios, aspectos operacionales, tecnológicos, financieros, sociales, etcétera.

La fase de identificación se centrará en describir qué podría pasar, por lo que es importante detectar cualquier amenaza y vulnerabilidad que podría afectar a la continuidad del negocio, esto normalmente estará relacionado con los recursos de soporte, esto es, procesos, sistemas, información, personas, instalaciones, terceras partes y otros.

Dado lo heterogéneo de este estudio, es muy recomendable establecer un proceso de comunicación con las partes interesadas internas, que deberían colaborar en esta actividad, por ejemplo, RRHH, Tecnologías de la Información y las Comunicaciones, Organización interna, Áreas de negocio, Proveedores, Seguridad Física, Mantenimiento de instalaciones, Ciberseguridad, etc.

A continuación, se muestra un listado típico de amenazas:

- Ciberataque
- Manipulación de programas
- Denegación de servicio
- Robo de equipos
- Ataque destructivo
- Extorsión
- Ingeniería social
- Difusión de software dañino
- Errores de los usuarios
- Errores de administradores
- Vulnerabilidades de los programas
- Indisponibilidad del personal
- Desastres industriales
- Emanaciones electromagnéticas
- Contaminación medioambiental
- Avería de origen físico o lógico
- Corte de suministro eléctrico

- Fallo de servicios de comunicaciones
- Interrupción de servicios o suministros esenciales
- Desastres naturales

En la fase de análisis, se obtienen la probabilidad y las consecuencias o impactos, en el caso de que los riesgos identificados en la fase anterior se materialicen, y, por tanto, los riesgos disruptivos, en la forma:

Riesgo = Probabilidad x Impacto

Por ejemplo, si para el riesgo de Desastre industrial por accidente de incendio, se ha estimado una probabilidad de 2 y el impacto estimado es de 3, obtendríamos:

R = 2 x 3 = 6, lo que supone un riesgo de nivel 6 (Nivel medio), que requiere tratamiento (Consultar el ejemplo de metodología posterior).

En la fase de evaluación, se deberán comparar los riesgos obtenidos con los criterios de aceptación fijados por la organización, de tal forma que se puedan determinar qué riesgos requerirán tratamiento y cuáles no.

A continuación, se muestra un ejemplo didáctico, de metodología de evaluación de riesgos y de establecimiento del criterio de aceptación de riesgos:

Probabilidad		
1	**Baja**	Frecuencia baja inferior a un mes
2	**Media**	Frecuencia media entre 1 mes y 1 año
3	**Alta**	Frecuencia alta más de 1 año

Tabla 6- Probabilidad del Riesgo. (Iso 22301:2019)

Impacto		
1	**Bajo**	Económico menor a 3.000 Personal: Involucrados menos del 5% del personal Clientes: No implica a clientes o de forma individualizada a 1 ó 2 Legal: Las consecuencias no implican incumplimiento o sería muy leve
2	**Medio**	Económico entre 3.000-30.000 Personal: Involucrados entre un 50-30% del personal Clientes: Implica entre un 10-25% de clientes Legal: Las consecuencias implicarían incumplimiento de leve a moderado o una mejora sobre el cumplimiento notable
3	**Alto**	Económico: Mayor de 30.000 Personal: Involucrados más del 30% del personal Clientes: Implica a más del 30% de clientes Legal: Las consecuencias implicarían un incumplimiento grave o muy grave o una mejora sobre el cumplimiento excepcionales

Tabla 7- Impacto del Riesgo (Iso 22301:2019)

Riesgo resultante y criterio		
1	**Bajo**	Aceptar
2	**Bajo**	Aceptar
3	**Bajo**	Aceptar
4	**Bajo**	Aceptar
5	**Medio**	Aceptar
6	**Medio**	**Tratar**
7	**Medio**	**Tratar**
8	**Alto**	**Tratar**
9	**Alto**	**Tratar**

Tabla 8- Riesgo resultante y criterios del riesgo (Iso 22301:2019)

Un mapa de riesgos, también conocido como mapa de calor de riesgo, es una herramienta de visualización de datos para mostrar los riesgos obtenidos por una organización, ayudando a priorizarlos de acuerdo con sus criterios de aceptación.

Un mapa de calor para la metodología anterior sería el siguiente, donde el criterio de aceptación de riesgo es cinco (5), por lo que cualquier riesgo superior a cinco (5) debería ser tratado mediante medidas preventivas y de mitigación (correctivas):

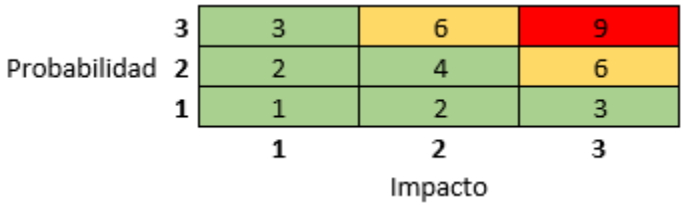


Tabla 9- Mapa de Riesgos y/o Mapa de Calor del Riesgo (Iso 22301:2019)

Las opciones de tratamiento de los riesgos se pueden clasificar en las siguientes opciones:

• **Aceptar:** En ese caso el riesgo no se modifica, y se acepta.

• **Tratar:** El riesgo se modifica, implementando salvaguardas, que podrán modificar probabilidad o impacto, o ambas.

• **Transferirlo:** El riesgo se transfiere a un tercero, por ejemplo, es el caso de las compañías de seguro, o la externalización de procesos, donde algún riesgo se transfiere al tercero a través de un contrato de prestación de servicio.

• **Evitarlo:** Esta opción está asociada a la eliminación de la actividad o proceso que origina el riesgo, por ejemplo, cesar una actividad, eliminar un sistema de información obsoleto porque ya no es operativo, etcétera. Lógicamente no siempre puede evitarse el riesgo, las actividades y recursos conllevan de manera inherente riesgos.

Cuando la organización decide tratar el riesgo, implementando salvaguardas, éstas pueden obtenerse de cualquier marco o estándar.

Por ejemplo, la norma GTC-ISO-IEC 27002:2015 incluye un total de 114 controles de seguridad, clasificados en 12 dominios y diversos subdominios de seguridad. Los dominios de seguridad son los siguientes:

Dominios GTC-ISO-IEC 27002:2015

A.5 Políticas de seguridad.

A.6 Aspectos organizativos de la seguridad de la información.

A.7 Seguridad ligada a los recursos humanos.

A.8 Gestión de activos.

A.9 Control de accesos.

A.10 Cifrado.

A.11 Seguridad física y ambiental.

A.12 Seguridad en la operación.

A.13 Seguridad en las telecomunicaciones.

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.

A.15 Relaciones con suministradores.

A.16 Gestión de incidentes en la seguridad de la información.

A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

A.18 Cumplimiento. (ISO 27002:2015).

De igual manera existen muchos otros estándares y metodologías que van a permitir toda este análisis y evaluación del riesgo en las empresas y organizaciones. Como, por ejemplo:

El NIST (Instituto Nacional de Estándares y Tecnología) en Estados Unidos, publicó el 16 de abril de 2018 la versión 1.1 del Marco para la mejora de la seguridad cibernética en infraestructuras críticas.

El Marco proporciona un lenguaje común para gestionar, identificar y priorizar el riesgo de ciberseguridad. El Núcleo del Marco proporciona un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación en cómo lograr dichos resultados, y consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas.

Figura 17- Marco para la mejora de seguridad cibernética. (NIST 2018)

Los elementos del Núcleo del Marco trabajan juntos en la siguiente manera:

• Las Funciones organizan actividades básicas de ciberseguridad en su nivel más alto. Estas funciones son Identificar, Proteger, Detectar, Responder y Recuperar. Estas ayudan a una organización a gestionar su riesgo de ciberseguridad, organizando información, habilitando decisiones de gestión de riesgos, abordando amenazas y mejorando el aprender de actividades previas.

• Las Categorías son las subdivisiones de una Función en grupos de resultados de ciberseguridad estrechamente vinculados a las necesidades y actividades particulares.

Los ejemplos de categorías incluyen "Gestión de activos", "Gestión de identidad y control de acceso" y "Procesos de detección".

• Las Subcategorías dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada Categoría. Algunos ejemplos de subcategorías incluyen "Los sistemas de información externos se catalogan", "Los datos en reposo se protegen" y "Las notificaciones de los sistemas de detección se investigan".

• Las Referencias Informativas son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría.

Las cinco (5) funciones básicas del Marco se definen a continuación:

• *Identificar:* Comprensión del contexto de la organización para administrar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades.

Los ejemplos incluyen: Gestión de activos, Entorno de negocios, Gobernanza, Evaluación de riesgos y Estrategia de gestión de riesgos.

• *Proteger:* Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.

Los ejemplos de categorías de resultados dentro de esta función incluyen: Gestión de identidad y control de acceso, Conciencia y entrenamiento, Seguridad de datos, Procesos y procedimientos de protección de la información, Mantenimiento y Tecnología de protección.

• *Detectar:* Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

Los ejemplos de categorías de resultados dentro de esta función incluyen: Anomalías y eventos, Monitoreo continuo de seguridad y Procesos de detección.

• *Responder:* Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de ciberseguridad. La función Responder respalda la capacidad de contener el impacto de un posible incidente.

Los ejemplos de categorías de resultados dentro de esta función incluyen: Planificación de respuesta, Comunicaciones, Análisis, Mitigación y Mejoras.

• *Recuperar:* Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad.

Los ejemplos de categorías de resultados dentro de esta función incluyen: Planificación de recuperación, Mejoras y Comunicaciones.

De igual manera a nivel de las empresas y las organizaciones, una vez que han identificados los riesgos, han realizado el respectivo análisis y la evaluación de estos, la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, recomienda tener a continuación en cuenta la “Evaluación de Impacto en el Negocio o más conocido como BIA (ISO 22301:2019).

Se define Análisis de Impacto en el Negocio (BIA, en inglés) como: Que es el proceso de análisis del impacto en el tiempo de una disrupción (Ataque Informático o Ciberataque), en la organización.

Antes de profundizar en esta sección, recordemos algunos de los conceptos claves que se deben tener en cuenta para aplicar correctamente la metodología:

• *MTPD/MAO (Maximum tolerable period of disruption:* Periodo Máximo Tolerable de Interrupción / Maximum acceptable outage – Interrupción Máxima Aceptable): Tiempo que llevaría para que los impactos adversos, que podrían surgir como resultado de no proporcionar un producto / servicio o realizar una actividad, se vuelvan inaceptables.

• *RTO (Recovery Time Objective – Tiempo Objetivo de Recuperación):* Periodo de tiempo que sigue a un incidente dentro del cual:

- Los productos o servicios deben ser reanudados, o
- Las actividades deben ser reanudadas, o
- Los recursos deber ser recuperados

- *RPO (Recovery Point Objective - Punto Objetivo de Recuperación o MDL - Maximum Data Loss / Máxima pérdida de datos):* Punto en el cual la información utilizada por una actividad debe ser restaurada para poder operar en la reanudación.

Este parámetro se refiere al tiempo, antes de una interrupción, que una organización debe garantizar su información. El tiempo en el que dicha información debe estar disponible se denomina, como se ha indicado anteriormente, RTO.

- *MBCO (Minimum Business Continuity Objective – Objetivo Mínimo de Continuidad de Negocio):* Nivel mínimo de servicios y/o productos que es aceptable para que una organización alcance sus objetivos empresariales durante una disrupción (ISO 22301:2019).

El siguiente gráfico muestra la relación entre los principales parámetros de la gestión de continuidad de negocio: RTO, MTPD/MAO y MBCO.

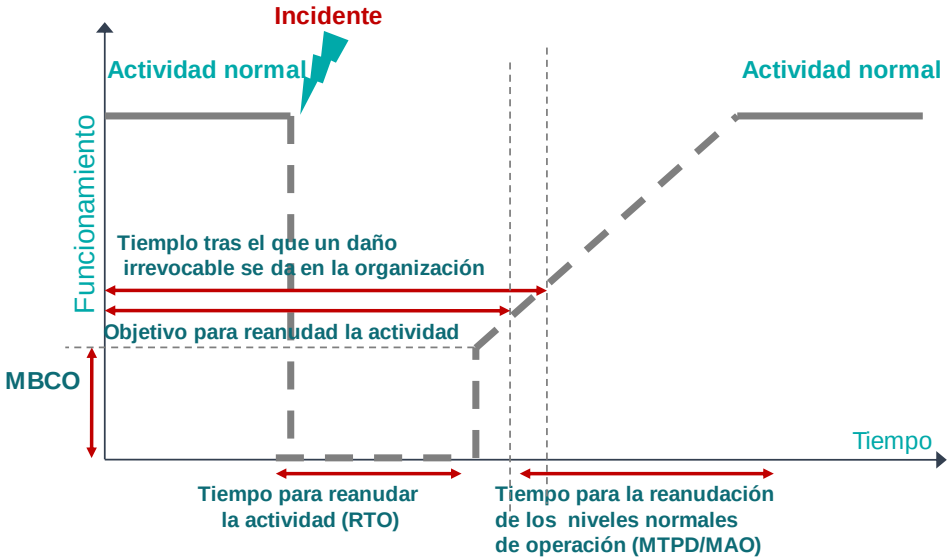


Figura 18- Parámetros de la GCN (ISO 22301:2019).

En caso de que una empresa u organización se vea afectada y ocurra en ella, un incidente que provoca una disrupción de las operaciones de negocio, afectando a la entrega de productos o servicios, los niveles de servicio pasan a ser inaceptables, bien porque son cero (0) o muy cercanos a cero (0).

El tiempo que hemos marcado como objetivo para recuperar dichas actividades, aunque sea a un nivel inferior (MBCO) al habitual, se denomina RTO. De hecho, una organización podría definir más de un punto objetivo de recuperación, desde que se inicia la recuperación de las actividades, hasta que se consigue una recuperación total de las mismas.

El tiempo que una organización considera que es inasumible para recuperar una actividad, aunque sea de forma degradada, se denomina MTPD o MAO. Se deduce

entonces, que RTO < MTPD, por lo que cuanto más cerca esté RTO de MTPD menos margen de error tiene la organización para la recuperación de las operaciones, y, por tanto, de poner en riesgo la viabilidad del negocio.

El parámetro RPO, aunque no se muestra en el gráfico, se situaría en un momento temporal antes del incidente, e indica cuánta información podemos asumir perder, es decir, dada una disrupción que haya afectado a la información, cuanta información podremos recuperar con los recursos disponibles.

El RPO marca las estrategias de copia de seguridad, por ejemplo, para una organización que realiza un Backup cada 24h, su RPO será de 24h, ya que con dicha estrategia está asumiendo, en el peor caso, que podría llegar a perder 24h de información si la disrupción que afecta a los datos se produjera justo antes de copiarse la información diaria. Existen de igual manera empresa y/u organizaciones que no pueden permitirse ninguna pérdida de información, como un banco, disponen de estrategias y soluciones de sincronización de datos en tiempo real que hacen que su RPO=0.

La organización debe desarrollar un proceso definido, apropiado para determinar el impacto de toda interrupción de las actividades de valor de la organización, necesarias para entregar productos y/o servicios. El proceso debería ser ejecutado a intervalos planificados y/o cuando haya cambios relevantes en la organización o el contexto en el que opera.

El propósito del BIA es:

• Obtener una comprensión de los principales productos y servicios de la organización y las actividades que los suministran.

• Determinar las prioridades y los plazos para reanudar las actividades.

• Determinar los recursos fundamentales que se necesitarán para la continuidad y la recuperación.

• Identificar las dependencias (tanto internas como externas).

El ciclo de vida del Análisis de Impacto en el Negocio (BIA) se pude ver en la siguiente imagen:

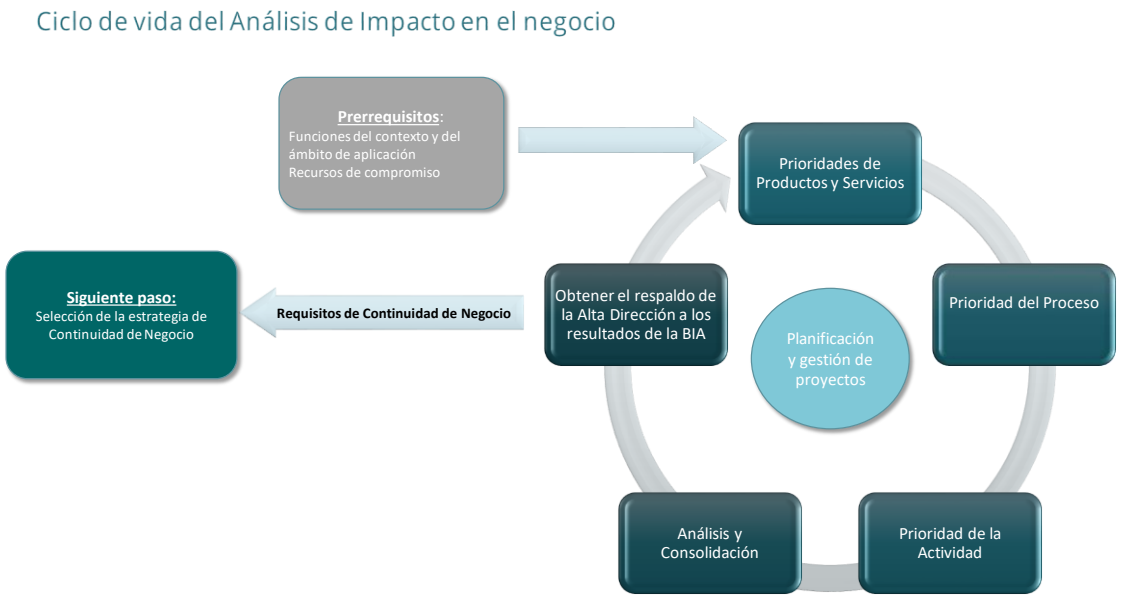


Figura 19- Ciclo de Vida del Análisis de impacto en el negocio. (ISO 22301:2019).

El objetivo del BIA es priorizar componentes organizativos, de tal forma que los productos y servicios puedan ser recuperados según un orden prestablecido después de una disrupción.

Se describen a continuación las fases:

- 1- Priorización de productos y servicios:

Como primer paso del proceso de BIA, la alta dirección debería priorizar los productos y servicios que tras una disrupción puedan amenazar el logro de los objetivos como organización.

Cuando una organización tiene demasiados productos y servicios para identificarlos individualmente, es posible agruparlos cuando tienen prioridades similares. Para cada grupo de productos y servicios, la organización debe comprender los impactos que puede causar una perturbación, identificando las expectativas de los clientes, las sanciones si no se cumplen esas expectativas, y los efectos que tendrán sobre la organización si se imponen las sanciones.

En las organizaciones que operan en un entorno no comercial, el "cliente" puede ser el público o una autoridad de supervisión, como el gobierno.

Otras partes interesadas y su impacto después de una interrupción en la organización pueden incluir:

- Organizaciones socios - su voluntad de seguir cooperando.
- Los medios de comunicación y la sociedad - valor de la marca y la opinión pública.
- Clientes potenciales - pérdida de la cuota de mercado actual y futura.
- Accionistas - efecto sobre el precio actual de las acciones y las inversiones futuras.
- Competidores - que pueden intentar aprovecharse de la situación.
- Personal - retención de personas.
- Los reguladores y el gobierno - sanciones y cambios en las normas.

Para cada grupo de productos y servicios la organización debe documentar:

- El tiempo transcurrido después del cual el incumplimiento continuado de los mismos se convierte en inaceptable para la organización porque los impactos mencionados anteriormente amenazan su supervivencia o hacen que sus objetivos ya no sean alcanzables (MTPO o MAO).
- La razón o razones por las que se ha identificado este período de tiempo en relación con los crecientes impactos a lo largo del tiempo.
- Los requisitos para la entrega de productos y servicios.

Los impactos más habituales son:

- Financiero: Pérdidas financieras debido a multas, penalizaciones, pérdida de beneficios o disminución de la cuota de mercado.
- Reputacional: Opinión negativa o daño de la marca.
- Legal y reglamentario: Responsabilidad por litigios y retirada de la licencia para seguir operando.
- Contractual: Incumplimiento de contratos u obligaciones entre organizaciones.
- Objetivos de la empresa: Incumplimiento de los objetivos o aprovechamiento de las oportunidades.
- Personal.
- Otros, que pueden incluirse.
- Personal o el bienestar público.
- Ambientales.
- Operacional.

- Entre otro más, dependiendo la misión o estrategia de la empresa.

Se debe tener en cuenta que los impactos aumentan con el tiempo, por lo que este estudio debe hacerse teniendo en cuenta dicha temporalidad, para determinar en qué grado aumentan los impactos.

• 2- Priorización de procesos:

Las empresas y organizaciones deben realizar una priorización a nivel de proceso para determinar las interrelaciones entre los procesos internos y la forma en que éstos suministran productos y servicios. También pueden, según su tamaño y complejidad, determinar las actividades que conforman esos procesos durante la tarea de priorización del proceso. Esto también será clave para poder priorizar la recuperación de los procesos y sus actividades.

Los resultados a obtener durante esta fase serán:

- Las relaciones entre productos y servicios, procesos y actividades.
- La evaluación de impactos de los procesos.
- La priorización de procesos a la hora de recuperar los productos y servicios.

• 3- Priorización de actividades:

En este nivel de actividades organizativas, el objetivo es entender los recursos necesarios para operar, después de cualquier disrupción.

El objetivo ahora es obtener una comprensión detallada de las necesidades de recursos habituales, lo que permitirá identificar los recursos necesarios para la recuperación. La información relacionada con los recursos incluye:

- Personas/habilidades/funciones.
- Instalaciones.
- Equipos.
- Registros.
- Financiación.
- Las tecnologías de la información y las comunicaciones, incluidas las aplicaciones, los datos, la telefonía y las redes.
- Proveedores, terceros y socios colaboradores.
- Dependencias de otros procesos y actividades.
- Herramientas especiales, piezas de repuesto y consumibles.
- Limitaciones impuestas a los recursos por la logística o los reglamentos.

Este ejercicio de detallar las necesidades de recursos deberá hacerse de manera alineada con los tiempos objetivos de recuperación (RTO) que la organización haya aprobado para la recuperación de los productos y servicios. Se debe tener en cuenta que, a veces, una organización, puede determinar más de un RTO, de forma que en las actividades se vayan recuperando gradualmente.

- 4- Análisis y consolidación:

Las empresas y organizaciones deberían realizar una consolidación de los análisis obtenidos. Ello supone examinar los resultados de las actividades priorizadas y sacar conclusiones que conduzcan a los requisitos de continuidad del negocio.

Los resultados esperados en esta fase son:

- ✓ Confirmación de los impactos a lo largo del tiempo
- ✓ Revisión y confirmación de las dependencias y necesidades de recursos
- ✓ Consolidación de las necesidades de recursos, cuando proceda
- ✓ Revisión y confirmación de las interdependencias de los procesos y actividades, y su relación con la entrega de productos y servicios

Aunque existen diversos métodos o técnicas para llevar a cabo un BIA, destacamos algunos de los más habituales:

- *Talleres:* Ofrecen resultados rápidos y favorecen el establecimiento de compromisos con gestión de continuidad de negocio, considerando una labor previa de concienciación a todos los departamentos y participantes mediante la cual hayan asumido la importancia de su participación para alcanzar los objetivos.

- *Cuestionarios:* Tanto en papel como con apoyo de herramientas software (p.ej. intranet) pueden aportar grandes cantidades de datos, pero existe el riesgo de incoherencias si no se han preestablecido en base a una estrategia sistemática que trate de resolver objetivos muy concretos.

- *Entrevistas:* Tanto en formato estructurado como no estructurado pueden aportar información relevante, pero hay que tener en cuenta el tiempo que se debe dedicar por los encuestados y que los datos logrados en las diferentes citas pueden corresponder a estructuras y formatos muy distintos.

Sobre la base de los resultados del BIA y la evaluación del riesgo, las empresas y las organizaciones, deberán identificar y seleccionar estrategias de continuidad de las actividades priorizadas para antes, durante y después de la interrupción. Las estrategias de continuidad de negocio se implementarán a través de una o más soluciones.

Es importante tener en cuenta que las estrategias se refieren, tanto a las de protección o preventivas (aquellas que vienen de la evaluación de riesgos y se implementan para antes de la potencial disrupción), como a las de mitigación o correctivas para limitar, bien los impactos en la disrupción, como el tiempo de la disrupción una vez que se haya producido.

Es muy recomendable compartir o balancear los recursos disponibles de la organización entre estrategias de protección y de mitigación, ya que apostar sólo por una de ellas no parece lo más razonable. Por ejemplo, un sistema de detección de incendios o un sistema antimalware son soluciones preventivas, en cambio, una arquitectura de alta disponibilidad de un sistema o unas oficinas alternativas son estrategias de mitigación o de recuperación.

Algunos elementos clave para seleccionar estrategias y soluciones adecuadas son:

- Debe tener como información de entrada lo resultados de los riesgos y del BIA (estrategias para antes del incidente, durante y después)
- Se debe tener en cuenta los costes asociados frente a los beneficios aportados.
- Se debe tener en cuenta el apetito de riesgo, así como los objetivos de continuidad de negocio para identificar, y seleccionar posteriormente estrategias y soluciones, para:
    - ✓ Reducir la probabilidad de disrupción.
    - ✓ Limitar el impacto de la disrupción.
    - ✓ Liminar el periodo de disrupción.
    - ✓ Proporcionar disponibilidad de los recursos

Los tipos de estrategias son las siguientes:

- De protección:
    - ✓ Reducir el riesgo (probabilidad) de la actividad (*)
    - ✓ Transferir la actividad a un tercero.
    - ✓ Finalizar o cambiar la actividad si es viable.

(*) Siempre se debe tener en cuenta que cuando el costo de la protección es extremadamente alto o la probabilidad de ocurrencia de la amenaza es extremadamente improbable, el riesgo puede ser aceptado y reevaluado como parte del proceso de mejora continua.

- De mitigación, respuesta y gestión de impactos:
    - ✓ Reducir el riesgo (impacto) de la actividad (*)

- ✓ Seguros para obtener una recompensa financiera (otros impactos no se pueden cubrir: cuota de mercado, consecuencia sobre las personas, etcétera).
- ✓ Restauración de activos: Incluye limpieza, reparación.
- ✓ Gestión de reputación.

• De estabilización, continuación, reanudación y recuperación:

- ✓ Reubicación de las actividades interna o externamente.
- ✓ Reubicación o reasignación de recursos, incluyendo el personal.
- ✓ Procesos alternativos y capacidad de reserva.
- ✓ Reemplazo de recursos y habilidades.
- ✓ Soluciones temporales.

• De recursos:

- ✓ Personas.
- ✓ Información y datos.
- ✓ Infraestructura física, como edificios, lugares de trabajo y otras ubicaciones y utilidades.
- ✓ Equipamiento y consumibles.
- ✓ Sistemas de Información.
- ✓ Telecomunicaciones.
- ✓ Transporte y logística.
- ✓ Finanzas.
- ✓ Suministradores y partners / colaboradores / socios.

• Estrategias para personas:

- ✓ Lista de especialistas de respaldo y plan de llamadas.
- ✓ Capacitación de personal y contratistas de múltiples habilidades.
- ✓ Separación de habilidades clave para reducir el impacto de un incidente.
- ✓ Teletrabajo.
- ✓ Utilización de terceras partes.
- ✓ Plan de sucesión.
- ✓ Documentación de procesos y otras formas de retención de conocimiento.

- ✓ Se deben tener en cuenta procedimientos de transporte del personal a ubicaciones alternativas, así como necesidades como acomodación, catering, cuestiones personales y familiares.

• Estrategias para información y datos:

- ✓ Tener en cuenta la seguridad de la información durante el proceso de recuperación y uso de la información.
- ✓ Formatos físicos.
- ✓ Formatos electrónicos.
- ✓ Copia de la información suficientemente lejos de las instalaciones habituales.
- ✓ Sincronización de datos.

• Estrategias para edificios, entornos de trabajo y otras ubicaciones:

- ✓ Ubicaciones alternativas dentro de la organización.
- ✓ Ubicaciones activo-activo dentro de la organización.
- ✓ Ubicaciones alternativas en otras organizaciones.
- ✓ Centros de control de emergencia.
- ✓ Ubicaciones alterativas proporcionadas por terceros especializados.
- ✓ Teletrabajo o lugares remotos.
- ✓ Uso de una fuerza laboral alternativa en un sitio establecido.

• Estrategias para Tecnologías de la información y Comunicaciones:

- ✓ Distribución geográfica de la tecnología.
- ✓ Reemplazos de emergencia o repuesto (spare, en inglés).
- ✓ Contrato de provisión de equipamiento o servicios de recuperación
- ✓ Rutas redundantes.
- ✓ Accesos remotos.
- ✓ Arquitecturas Activo-Activo / Activo-Pasivo.

Una vez se han seleccionado las estrategias en cada caso, se requiere que las empresas y organizaciones, implementen soluciones de continuidad de negocio, para activarlas cuando sea necesario.

En términos generales se puede decir que esta quinta fase del proyecto de aplicación de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, sobre la Evaluación de Riesgos, se lleva a cabo en mínimo dos (2) etapas secuenciales.

La primera que comprende cinco (5) procesos para evaluar las vulnerabilidades que afectan los activos de los empleados y servicios identificados en la tercera fase que podrían ser explotados por las amenazas catalogadas en la cuarta fase.

La segunda etapa de la Evaluación de Riesgos implica un solo proceso para calcular el riesgo residual que surge de cada combinación de activos con las amenazas y vulnerabilidades relacionadas.

Ampliando para la primera etapa, se puede complementar y sugerir que, para evaluar las vulnerabilidades, el equipo de trabajo de aplicación de la metodología debe medir la efectividad de las protecciones o salvaguardas y aquellos pendientes de implementación. El análisis de estos datos revelará cualquier atributo de empleados y activos o el entorno en el que operan que los hacen susceptibles a compromiso.

La evaluación de vulnerabilidades puede complicarse por una percepción errónea común que siempre son debilidades o fallas de seguridad. Si bien muchas vulnerabilidades son negativas (atributos), otros son cualidades positivas que simplemente tienen efectos secundarios potencialmente adversos.

Por ejemplo, la portabilidad de las computadoras portátiles es una característica deseable por la que se paga una suma Premium, aunque esto, también lo que los hace es más susceptibles al robo. Por lo tanto, para ayudar a lograr una evaluación equilibrada de las vulnerabilidades, la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; proporciona una amplia lista de Listado de vulnerabilidades con referencias cruzadas adecuadas al listado de protecciones o salvaguardas presentado en la fase de recomendaciones.

Al igual que con los valores de activos y amenazas, se establecen métricas simples para calificar diferentes vulnerabilidades desde “Muy Baja” a “Muy Alta”.

Ampliando para la segunda etapa, se puede complementar y sugerir que, una vez, habiendo identificado y asignado valores a los activos (incluidos empleados y servicios), amenazas y vulnerabilidades, es una cuestión simple calcular el producto de las tres (3) variables para producir una lista priorizada de riesgos residuales evaluados para su análisis durante la fase de recomendaciones de esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos.

Una vez que se han identificado los riesgos residuales evaluados, se asignan niveles relativos de “Muy bajo” a “Muy alto” y posteriormente priorizado, el equipo de trabajo de la aplicación de la metodología debe preparar recomendaciones

adecuadas para la autoridad de aceptación de riesgos en las empresas y organizaciones.

De igual manera si la aplicación de la metodología es posterior a la afectación por delitos informáticos o ciberataques en una empresa u organización, el equipo de trabajo deberá entregar un informe y reporte sobre los riesgos explotados y la cuantificación desde el punto de vista económico, financiero y reputacional (Pérdidas por afectaciones); en que se incurrió o se fue afectado la organización en general.

Cuando los riesgos residuales evaluados sean totalmente aceptables para el equipo ejecutivo (generalmente aquellos en los rangos “Muy Bajo”, “Bajo” y posiblemente “Medio”), debería ser suficiente recomendar la retención de las protecciones o las salvaguardas existentes y por ende definir la finalización de cualquier medida de seguridad pendiente de implementación, con seguimiento continuo de su eficacia.

En algunos casos, cuando los riesgos residuales evaluados se califican como “Muy bajos”, puede ser factible recomendar la eliminación de algunos mecanismos de protección con la aceptación de un poco elevados niveles de riesgo, para lograr economías deseables o mejorar la eficiencia operativa.

En los casos en que los riesgos residuales evaluados sean inaceptables (generalmente aquellos en “Muy Alto”, Rangos “altos” y posiblemente “medios”), generalmente se requiere alguna acción correctiva. Para ayudar a seleccionar una respuesta adecuada, la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, incluye una extensa lista de protecciones o salvaguardias, que tienen una referencia cruzada a las vulnerabilidades que corrigen, las amenazas que mitigan y los activos (o empleados y servicios) que protegen. Además, la selección de protecciones o salvaguardas explícita.

Los criterios se explican en detalle para facilitar el análisis comparativo de sus costos relativos y eficacia. Finalmente, los riesgos residuales evaluados de la Evaluación de Riesgos se revisan para reflejar cualquier mejora esperada una vez que las recomendaciones se implementen por completo y una vez se haya aplicado la metodología, generando un informe final de afectaciones, valoración de estas afectaciones, como además si aplica, se deben anexar y presentar en este informe final, los riesgos residuales proyectados.

Para todos los riesgos que sean priorizados y definidos como pertinentes en la aplicación de la metodología se debe considerar su impacto en caso de ser explotados o se hagan efectivos esos riesgos.

Determinación del impacto potencial:

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias (Magerit 2012).

Impacto acumulado:

Es el calculado sobre un activo teniendo en cuenta.

- Su valor acumulado (el propio más el acumulado de los activos que dependen de él)
- Las amenazas a que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las protecciones o salvaguardas que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etcétera.

Impacto repercutido:

Es el calculado sobre un activo teniendo en cuenta

- Su valor propio.
- Las amenazas a que están expuestos los activos de los que depende.

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de valores de impacto:

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

• Puede agregarse el impacto repercutido sobre diferentes activos.

• Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.

• No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores.

• Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque con-viene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.

• Puede agregarse el impacto de una amenaza en diferentes dimensiones.

Determinación del riesgo potencial:

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

• *Zona 1* – riesgos muy probables y de muy alto impacto.

• *Zona 2* – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.

• *Zona 3* – riesgos improbables y de bajo impacto.

• *Zona 4* – riesgos improbables, pero de muy alto impacto.

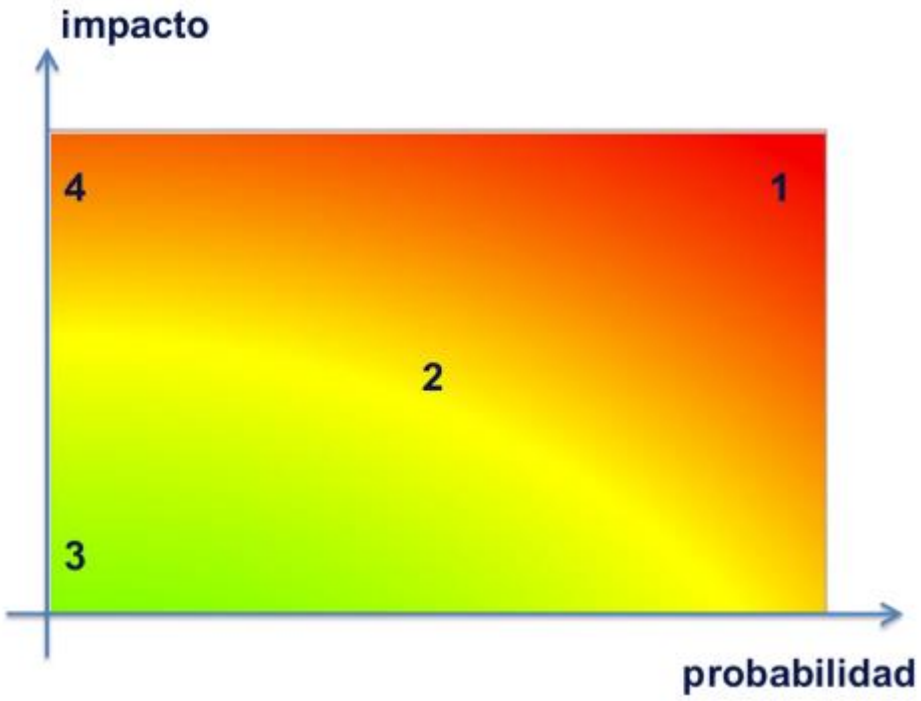


Figura 20- El riesgo en función del Impacto y la Probabilidad. (Magerit 2012).

Riesgo acumulado:

Es el calculado sobre un activo teniendo en cuenta

- El impacto acumulado sobre un activo debido a una amenaza, y
- La probabilidad de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza. El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las protecciones o salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etcétera (Magerit 2012).

Riesgo repercutido:

Es el calculado sobre un activo teniendo en cuenta

- El impacto repercutido sobre un activo debido a una amenaza y
- La probabilidad de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza. El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las

incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo (Magerit 2012).

Protecciones o Salvaguardas:

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las protecciones o salvaguardas presentes.

Se definen las protecciones o salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal (EBIOS – Octave 2018).

A continuación, esta metodología referencia un "Catálogo de Elementos" presenta una relación de salvaguardas adecuadas para cada tipo de activos.

Selección de salvaguardas:

Ante el amplio abanico de posibles protecciones o salvaguardas a considerar, es necesario hacer una reducción inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger.

En esta reducción, se deben tener en cuenta los siguientes aspectos:

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
2. Dimensión o dimensiones de seguridad que requieren protección.
3. Amenazas de las que necesitamos protegernos.
4. Si existen protecciones o salvaguardas alternativas.

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.
2. La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo).
3. La cobertura del riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos (2) tipos de declaraciones para excluir una cierta protección o salvaguarda del conjunto de las que conviene analizar:

• No Aplica – Se dice cuando una protección o salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración.

• No se justifica – Se dice cuando la protección o salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

Como resultado de estas consideraciones dispondremos de una “declaración de aplicabilidad” o relación de protecciones o salvaguardas, que deben ser analizadas como componentes nuestro sistema de protección.

Efecto de las protecciones o salvaguardas:

Las protecciones o salvaguardas entran en el cálculo del riesgo de dos (2) formas:

Reduciendo la probabilidad de las amenazas: Se llaman protecciones o salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

Limitando el daño causado: Hay protecciones o salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas protecciones o salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan (Mitigación).

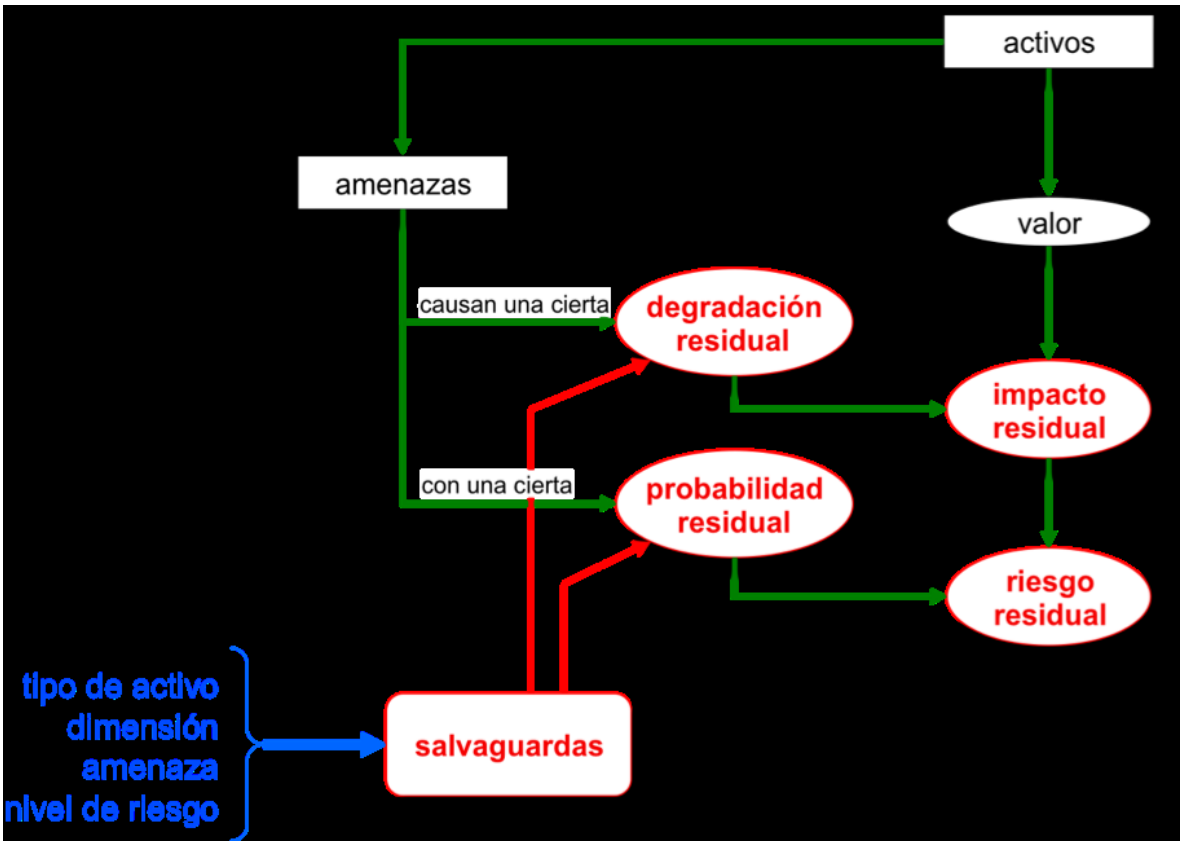


Figura 21- Elementos de análisis del riesgo residual. (Magerit 2012).

Tipos de protecciones o salvaguardas:

Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

> *[PR] Prevención*: Diremos que una protección o salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la protección o salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: Autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas, etcétera.
>
> *[DR] Disuasión:* Diremos que una protección o salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o lo piensan dos (2) veces antes de atacar. Son protecciones o salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados, en caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente, entre otros.

[EL] Eliminación: Diremos que una protección o salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son protecciones o salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños en el caso de que la protección o la salvaguarda no sea perfecta y el incidente llegue a ocurrir. Ejemplos: Eliminación de cuentas stándar, de cuentas sin contraseña, de servicios innecesarios, etcétera.

En general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información, armarios ignífugos, entre otros.

[IM] Minimización del impacto / limitación del impacto: Se dice que una protección o salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente. Ejemplos: Desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente.

[CR] Corrección: Diremos que una protección o salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son protecciones o salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños. Ejemplos: Gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes, etcétera.

[RC] Recuperación: Diremos que una protección o salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son protecciones o salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo. Ejemplos: Copias de seguridad (back-up)

[MN] Monitorización o Monitoreo: Son las protecciones o salvaguardas que trabajan monitoreando o monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de protecciones o salvaguardas de cara al futuro. Ejemplos: Registros de actividad, registro de descargas de web, correlacionadores de eventos (SIEM), etcétera.

[DC] Detección: Diremos que una Protección o salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños. Ejemplos: Anti-virus, IDS, detectores de incendio, etc.

[AW] Concienciación: Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los

errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las protecciones o salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación. Ejemplos: Cursos de concienciación, cursos de formación, etc.

[AD] Administración o Gobernanza: Se refiere a las protecciones o salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo. Ejemplos: Inventario de activos, análisis de riesgos, plan de continuidad, etcétera (Magerit 2012).

La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tabla 10- Tipos de Protecciones o Salvaguardas. (Magerit 2012- Coras 2018)

Eficacias de las protecciones o salvaguardas:

Las protecciones o salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina dos (2) factores:

- Desde el punto de vista técnico
  - Es técnicamente idónea para enfrentarse al riesgo que protege.

- Se emplea siempre.

❖ Desde el punto de vista de operación de la salvaguarda.

- Está perfectamente desplegada, configurada y mantenida.
- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos.

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Tabla 11- Eficacia y madurez de las protecciones o Salvaguardas. (Magerit 2012)

Anexo F: Etapa de Ciberataques Internos:

En todas las empresas, organizaciones o instituciones se pueden ver hoy día como vienen incrementando el número de ataques informáticos o ciberataques, muchos de estos ataques y las afectaciones que ello conlleva se están realizando al interior de las organizaciones; esto por descuidos, falta de cultura de ciberseguridad, desconocimiento de las políticas de seguridad de la información, errores humanos, empleados mal intencionados (Insider).

Los ataques en la red o ciberespacio son muy variados y pueden comprometer la seguridad de los usuarios y las organizaciones. Es algo que afecta a todo tipo de sistemas y dispositivos. Con el paso del tiempo los ciberdelincuentes o piratas informáticos, también perfeccionan esos ataques para lograr saltarse las medidas de seguridad y lograr así su objetivo, incluyendo en sus ataques muy altas tecnologías como IA, Blockchain, Data Analítica, etc.

Este anexo de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, nace de la ausencia de mecanismos, procedimientos, metodologías y estándares que ayuden a identificar, cuantificar cualitativa y cuantitativamente las afectaciones que sufren las organizaciones, las empresas al ser afectadas por ataques de delitos informáticos o ciberataques, específicamente en este anexo f; se presenta y se define la manera cómo los ataques informáticos internos han ganado terreno a los ataques externos en la red o ciberespacio y él porque es importante considerarlos. Se puede establecer que los ataques internos son más comunes que los externos.

Como se ha indicado a lo largo de esta metodología, son muchos los ataques informáticos o ciberataques que podemos sufrir en la red o en el ciberespacio en general. Estas amenazas pueden llegar a través de medios muy diversos. Podemos sufrir ataques mediante software malicioso que recibimos, programas modificados que instalamos y que pueden robarnos, ataques de suplantación de identidad, explotación de vulnerabilidad, entre otros listados de ataques informáticos.

Si tenemos en cuenta el informe presentado por Netwrix Cyber Threats a finales del año 2020 (Netwrix 2020), se trata de las conclusiones a una encuesta realizada a más de novecientos (900) profesionales TI a nivel mundial, para determinar cuáles son los principales incidentes en ciberseguridad que pueden afectar a los empleados. En este informe se pudo detectar que existen cuatro (4) puntos muy presentes:

- ✓ Errores de administración.
- ✓ Intercambio no consentido de datos confidenciales, incluidos datos financieros.
- ✓ Mala configuración de la nube, sistemas, plataformas y sistemas On Premise.
- ✓ Robo de datos.

Todo lo anteriormente expresado, indica que la mayoría de los ataques que afectan a un sistema son internos. Es decir, son errores que un usuario ha cometido, una mala configuración, etcétera. Este informe indica además que este tipo de ataques son más difíciles de detectar. Por ejemplo, pueden pasar semanas hasta detectar el robo de datos personales (Netwrix Cyber Threats 2020).

Esto se ha incrementado exponencialmente en los últimos meses, donde el trabajo en remoto ha tenido una gran importancia y ha sido la única opción posible por los largos y reiterativos periodos de cuarentenas y aislamientos sociales, en fin, con todo lo relacionado con la pandemia del Covid-19.

Lo cual ha traído consigo, cambios importantes al día a día de la sociedad, de las empresas y organizaciones en su forma de seguir operando en tiempos de pandemia, todo ello se ve reflejado en la manera en la que trabajamos. Muchos usuarios han comenzado a desempeñar sus funciones de forma remota. El problema es que en ocasiones utilizan equipos inadecuados, que no están actualizados, tienen vulnerabilidades o no están lo suficientemente protegidos. Incluso en algunas ocasiones, se trata de usuarios que no tienen experiencia previa en el uso de este tipo de equipos informáticos, plataformas, conexiones; para su día a día en las organizaciones.

Todo esto ha hecho, que los ataques internos ganen terreno, tengan un mayor abanico de posibilidades respecto a hace unos meses. Por ello fue incluido este apartado o anexo en la metodología, debido a que es esencial, pertinente y necesario prestar atención a cómo los empleados utilizan los datos confidenciales de ellos y de las empresas para las cuales laboran, teniendo en cuenta que muchas veces existen desconocimiento total de cómo operan las políticas de seguridad en la red o ciberespacio.

De igual manera, es necesario tener en cuenta los empleados inconformes o con algún grado de resentimiento contra las empresas u organizaciones, donde estos laboran, lo cual los convierte en potenciales ciberdelincuentes en las actuales situaciones y época. Estas amenazas crecen exponencialmente si estos empleados resultan siendo personas infiltradas en las organizaciones, que llevan propósitos claros, definidos para afectar la operación y los resultados de las empresas u organizaciones.

Estos ciberdelincuentes internos (Insider), tienen múltiples motivaciones personales, laborales, ideológicas, administrativas que pueden llevarlos a cometer estos delitos informáticos al interior de las organizaciones, teniendo ellos a su favor que ya se ganaron la confianza de la empresa, ya están al interior de la organización, tienen credenciales de seguridad corporativos, tienen acceso a muchos activos, equipos de la empresa y trabajan con una ventaja que es la sorpresa de poder crear caos y afectaciones, sin ser detectados e incluso sin sospechar de estas personas.

Si se piensas que allí afuera (ciberespacio), hay miles de hackers o cibercriminales que quieren vulnerar la seguridad informática de tu empresa, se tiene toda la razón, pero si se piensa que esa es la fuente principal de las incidencias en ciberseguridad de las empresas, esto resulta erróneo y alejado de la actual realidad.

Según Cow92, OTAN, NIST y ENISA (Risk Safe Assessment) en 202º y lo corrido de 2021, aproximadamente un 80% de todos los fraudes, robos, sabotajes o accidentes relacionados con los sistemas informáticos, tienen como únicos responsables a los empleados o ex empleados de las compañías a la que pertenecen dichos sistemas atacados y/o afectados. (Cow92 2020, OTAN 2021, Nist.SP 2020, Enisa 2021).

Dado este alto porcentaje de fraudes al interior de las empresas y organizaciones, es por ello que la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos; tiene muy en cuenta a los delitos informáticos internos y define un anexo para que se traten este tipo de amenazas, que cada día vienen adquiriendo mayor renombre, más afectaciones y las cuantificaciones por estas afectaciones económicas, financieras y reputacionales vienen en aumento.

Al hablar de ataques informáticos, ataques cibernéticos, podemos agrupar estos ciberataques en tres (3) categorías, por un lado, tenemos los ataques externos, ataques internos y estos últimos por su impacto y frecuencia de ocurrencia requieren que sean clasificados a su vez como ataques intencionados o no intencionados).

Ataques Informáticos, cibernéticos o ciberataques externos:

Los ataques Informáticos, cibernéticos o ciberataques externos, son los que se ejecutan por ciberdelincuentes, hackers o ciberorganizaciones de forma remota, en la gran mayoría de los casos, sin tener conocimientos algunos del funcionamiento de la red que están atacando; para ello estos cibercriminales ejecutan, utilizan y aplican una serie de herramientas, conocimientos, plataformas, protocolos y equipos con la única finalidad de vulnerar los activos de la empresa víctima.

Generalmente y dependiendo del nivel de experticia, tecnologías aplicadas y cantidad de ciberterroristas involucrados, estos ataques tomarán horas, días, semanas o meses; acá este tiempo de igual manera es proporcional y depende del tipo de seguridad, políticas, controles, protecciones o salvaguardas, con las que cuente la red empresarial, por así decirlo.

Ataques Informáticos, cibernéticos o ciberataques internos intencionados:

Teniendo en cuenta los ataques informáticos o ciberataques, que se pueden presentar y se vienen presentando al interior de las empresas u organizaciones, es pertinente y necesario tener en cuenta los ataques informáticos, cibernéticos o ciberataques internos intencionados; este tipo de ataque constituye en sí la mayor preocupación de las empresas, al darse no solo un abuso de confianza, sino al ser una amenaza constante en el ámbito de la seguridad informática empresarial, de la cual no se sabe con certeza cuándo sucederá, que tan grave será el impacto dado el nivel de privilegio y de acceso a los activos por parte de los empleados.

Si bien un hacker o ciberterroristas, no tiene contraseñas, accesos, ni conocimiento de ningún tipo acerca de la red a la que va a acceder, varios de los empleados de la empresa si lo tienen y más grave aún, muchos de ellos tienen súper privilegios o accesos como administradores de activos de la organización, sin conocer exactamente los riesgos y las amenazas a las que ese activo está expuesto; como además y más grave aún, muchos empleados, si conocen todo el daño que se puede hacer a la organización, si hacen mala utilización de esos privilegios y credenciales de seguridad.

Por todo anteriormente comentado, se sugiere por parte de esta metodología, tener presente que, en teoría, alguien con cualquier motivo, puede atacar la red y los activos de la empresa donde trabaja, de forma tan sencilla como lo es, ingresando un usuario, una contraseña y ejecutando determinados programas, comandos, herramientas o protocolos para hacer todo el daño que desee; desde el punto de vista económico, operacional, financiero y hasta reputacional.

Al respecto el analista Paul Foster de Talon Cyber Defense, de Sausalito California, relató a modo de ejemplo, el caso de una empresa de mensajería de alcance mundial, que, aunque es capaz de llevar paquetes al último rincón del mundo a tiempo, era estafada por empleados y exempleados que crearon una red paralela de cobranzas y envíos.

Los ciberdelincuentes (Empleados y Exempleados) aprovechaban sus conocimientos sobre la empresa, las fallas de seguridad del sistema de

administración de envíos basado en una versión vieja y fácil de hackear, debido a que estaba en un sistema operativo cuyos parches de seguridad dejaron de producirse y de tener soporte desde el año 2014.

Esto que se comenta es una situación poco común, pero aún en pleno 2021, existen muchas empresas con miles de computadoras y servidores con sistemas operativos viejos, no actualizados y para uso doméstico, queriendo ahorrar los costos, derivados de la adquisición de licencias nuevas, recientes y seguras de sistemas operativos empresariales.

Estas afectaciones económicas, financieras y reputacionales, luego de cuantificados los daños por ataques informáticos y ciberataques, por las fallas en el sistema, por paquetes extraviados o como en este caso por redes criminales amparadas al tamaño de la organización, es cuando realmente se dan cuenta de la magnitud y de los daños que representa todo esto para la empresa y organización.

Ataques Informáticos, cibernéticos o ciberataques internos no intencionados:

Este tipo de amenazas, clasificadas como ataques Informáticos, cibernéticos o ciberataques internos no intencionados, es un verdadero dolor de cabeza para los expertos en seguridad informática. En este caso el usuario no pretende hacer daño alguno, simplemente por falta de conocimiento comete un error que muchas veces, lleva consigo graves consecuencias para la operación, las finanzas y la reputación de la empresa u organización.

Cada vez que, en una empresa, están creando una cuenta o asignándole credenciales de acceso a un nuevo empleado, o se les da acceso privilegiado a ciertas áreas de los sistemas internos de la empresa; realmente se está abriendo la puerta a alguien que, en cualquier momento por error humano, podría poner toda tu red y los activos de la empresa en peligro.

Este problema para las empresas, en realidad se basa en que están, tan preocupados en protegerse de ataque informáticos o ciberataques externos, que no invierten o ignoran que las amenazas más peligrosas se encuentran dentro de las empresas y organizaciones, teniendo en cuenta que estos ataques internos, realmente son las que más daños causan.

Estos ataques internos se pueden apreciar y se presentan en todos los tipos de empresas, pero en los últimos años, el número de ataques e intrusiones informáticas internas en las principales compañías financieras se ha visto incrementado respecto a los ataques producidos externamente en lo que va de año. Esta es la principal conclusión del informe de Seguridad Global 2020 que ha realizado Deloitte (Deloitte 2020).

Anexo G: Etapa de Ciberataques Externos:

Como se había establecido anteriormente en esta metodología, al hablar de ataques informáticos, ataques cibernéticos, podemos agrupar estos ciberataques en tres (3) categorías, por un lado, tenemos los ataques externos, ataques internos y estos últimos por su impacto y frecuencia de ocurrencia requieren que sean clasificados a su vez como ataques intencionados o no intencionados).

Es por ello que al hablar de ataques informáticos, cibernéticos o ciberataques externos, debemos contemplarlos como los que se ejecutan por ciberdelincuentes, hackers o ciberorganizaciones de forma remota, en la gran mayoría de los casos, sin tener conocimientos algunos del funcionamiento de la red que están atacando; para ello estos cibercriminales ejecutan, utilizan y aplican una serie de herramientas, conocimientos, plataformas, protocolos y equipos con la única finalidad de vulnerar los activos de la empresa víctima.

Generalmente y dependiendo del nivel de experticia, tecnologías aplicadas y cantidad de ciberterroristas involucrados, estos ataques tomarán horas, días, semanas o meses; acá este tiempo de igual manera es proporcional y depende del tipo de seguridad, políticas, controles, protecciones o salvaguardas, con las que cuente la red empresarial, por así decirlo.

La presencia online o en el ciberespacio de las empresas es ya una necesidad incuestionable en todos los sectores. Del mismo modo que ha crecido la presencia en internet de las empresas lo ha hecho la amenaza de sufrir un ciberataque. Para estar protegido es imprescindible conocer los riesgos y adoptar al menos una serie de medidas básicas. La presencia de empresas de todos los sectores en la red sigue creciendo. Hoy en día, prácticamente cualquier producto o servicio es susceptible de venderse o promocionarse online, y las compañías son cada vez más conscientes de la capacidad de difusión que puede ofrecerles y, de hecho, en 2021 el 95% de las empresas a nivel mundial cuentan con página web propia (FEM 2021).

Vender, realizar transacciones en línea, ejecutar procesos educativos online a través del eCommerce, E-Banking, E-Learning o disponer de una web corporativa donde mostrar las líneas principales de actuación de una empresa o contar con una presencia constante en redes sociales para comunicarse con sus clientes son algunas de las diferentes incursiones en la red que tienen la mayoría de proyectos empresariales.

La última década ha sido fiel testigo del cambio en los paradigmas en los que los hackers o ciberterroristas, buscan explotar vulnerabilidades dentro de las organizaciones y las infraestructuras criticas nacionales a lo largo de todos los países del mundo.

Si desde la sociedad se desea contrarrestar todo ello, se debe tener en cuenta la necesidad de cambiar la perspectiva hacia la forma en que se percibe la seguridad digital y la ciberseguridad, conocer cientos ataques y cómo se puede aprender de los mismos para estar lo mejor preparados posibles, ya que no es posible decir en seguridad “preparados” o “100% Protegidos” a secas.

En términos generales cuando se desea conocer el listado de posibles ataques informáticos o ciberataques externos, que se pueden y se están realizando en contra de los activos de las empresas u organizaciones, mínimamente se deben tener en cuenta la siguiente clasificación de estos ataques informático:

A. Ataques de denegación de servicio (DoS).
B. Ataques distribuidos de denegación de servicio (DoS)
C. Ping Flood.
D. Ping de la muerte.
E. Escaneos de puertos.
F. ARP Spoofing.
G. ACK Flood.
H. Ataques FTP Bounce.
I. TCP Session Hijacking.
J. Ataques Man-In-The-Middle.
K. Ataques de Ingeniero Social.
L. OS Finger Printing.
M. Reconocimientos de puertos expuestos.
N. KeyLoggers.
O. ICMP Tunneling.
P. Ataque LOKI.
Q. Ataque de secuencia TCP.
R. CAM Table Overflow.
S. Ataques a Aplicaciones Web.
T. Virus Informáticos.
U. Gusanos.
V. Malware.
W. Adware.
X. Spyware.
Y. Troyanos.
Z. Root kit.
AA. Entre otros muchos más.

Anexo H: Etapa de Ciberataques a la Información:

Se define un anexo a este tipo de ataques informáticos o ciberataque, pues es uno de los que mayor crecimiento viene presentando y de una manera exponencial a nivel de Colombia y a nivel mundial. Se debe entender y tener presente que hoy día la información es su activo más valioso para todas las empresas, organizaciones e instituciones.

Ataques como el sufrido este año 2021, por la empresa de Oleoductos “Colonial” en EEUU, donde a través de una Malware de nivel Ransoware le secuestraron toda la información y se tuvo que parar la información en gran parte del país, habla del nivel de exposición que tienen todas las empresas, lo sofisticado que vienen desarrollando este tipo de ataques a la información y a los sistemas de información.

Básicamente los ataques informáticos o ciberataques a la información y a los sistemas de información están afectando la privacidad, confidencialidad, integridad y disponibilidad de la información en las empresas y en las organizaciones, esto visto realmente como un secuestro a los datos e información de la empresa y unos bloqueos a los sistemas de información empresariales por los cuales se mueve dicha información.

Como ya se había expresado, recientemente se ha producido un aumento exponencial en los ataques de ransomware a nivel global. El ransomware es un tipo de malware con el que se logra acceder a información personal de los usuarios y, para que las víctimas logren acceder a esta, los ciberatacantes exigen que se depositen pagos, la mayoría de las veces en cifras supremamente altas y en criptomonedas por la dificulta que representa rastrear este tipo de monedas digitales.

Muchas empresas y países a nivel mundial han sido víctimas de este tipo de ataques informáticos, como los casos de Telefónica en España (Ransoware) y casos en empresas de estados unidos, donde el gobierno de Estados Unidos ha sido susceptible a esta serie de ataques cibernéticos y ha emprendido campañas para contrarrestar su amenaza. Por ejemplo: el Departamento de Policía de Washington DC, fue blanco de un ataque cibernético hacia fines de abril de 2021 y se conoció que las bases de datos del departamento se habían visto comprometidas.

De igual manera el 7 de mayo de 2021, el ataque al Oleoducto Colonial, conocido como uno de los oleoductos más grandes de Estados Unidos, causó que este dejara de prestar su servicio, provocando gran impacto en todo Estados Unidos y tendiendo que pagar una suma cercana a los 75 bitcoins o su equivalente de 4,4 Millones de dólares para poder recuperar su información. Como informó

Segurilatam, Joseph Blount, presidente y CEO de Colonial Pipeline, admitió haber pagado el rescate al considerar que “era lo mejor para el país”.

Según informes de agencias como la Oficina Federal de Investigaciones (FBI 2021) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA 2021), el ataque a Colonial Pipeline, fue llevado a cabo por un hacker profesional externo, utilizando una variante de ransomware altamente sofisticada.

La complejidad y variedad de los ataques cibernéticos es cada vez mayor, con un tipo de ataque diferente para cada propósito nefasto. Aunque las medidas de prevención de la ciberseguridad difieren para cada tipo de ataque, las buenas prácticas de seguridad y la higiene básica de TI son generalmente buenas para mitigar estos ataques.

Según una investigación tras el ataque a Colonial Pipeline (EEUU), se determinó que los operadores de ransomware llamados DarkSide llevaron a cabo el ataque y se señaló que Rusia podría estar relacionada con el suceso.

El segundo gran ataque en Estados Unidos relacionado con ransomware se produjo contra CNA Financial, una de las compañías de seguros más grandes de EEUU. Donde los funcionarios de la compañía declararon en un comunicado que fueron víctimas de un ataque de ransomware llevado a cabo por el grupo Evil Corp, vinculado a Rusia.

Esto a generando grandes problemas diplomáticos entre dos (2) grandes potenciales mundiales, como lo es EEU y Rusia, a tal punto que este tema fue uno de los temas tratados en la reciente reunión entre Bladimir Putin (Rusia) y Joe Biden (EEUU) en la reunión llevada a cabo en junio de 2021 en Davos (Suiza).

Tras los ataques a empresas e instituciones públicas de EEUU, países de Europa y Asia también fueron blanco de diversas variantes de ransomware. Por ejemplo, en el último mes, la sede europea de Toshiba; la compañía Bose en Alemania; la compañía de seguros AXA en Francia; HSE, la agencia oficial de servicios de salud de Irlanda; y la compañía aérea Air India anunciaron que fueron atacados con sistemas de ransomware. Después de los informes y declaraciones oficiales, el mundo entró en estado de alarma, dado el Increíble aumento de los ataques de ransomware (Malware) contra de la información y los sistemas de información de empresas y tecnologías críticas de las naciones.

Cabe destacar que los daños a gran escala causados por los ataques de ransomware a nivel internacional han aumentado aún más en el último año. Por ejemplo, según informes de varias agencias gubernamentales y empresas profesionales de ciberseguridad, los ataques globales de ransomware en 2020 aumentaron en un 150% en comparación con el año anterior. Además, se determinó

que hubo un aumento de hasta un 300% en los pagos de rescate realizados por las víctimas para que lograran acceder a su información personal.

Además, los ataques globales de ransomware a infraestructuras críticas, empresas e instituciones públicas han aumentado drásticamente en el primer trimestre de 2021. Con la intensificación de los ataques, hubo un gran aumento en la cantidad de dinero de rescate exigido por los atacantes a las víctimas. Especialmente debido al aumento en el valor de la moneda virtual bitcoin, los rescates pagados por las empresas gigantes a los atacantes alcanzaron decenas de millones de dólares.

Todos estos ataques de ransomware que tuvieron lugar en 2021, tienen un patrón en común y es que se les observan algunos cambios en términos cualitativos y de método en comparación con períodos anteriores. Por ejemplo, ha habido ataques de "phishing" a través de correos electrónicos. Otros ataques se destinaron a las vulnerabilidades de infraestructura cibernética de algunas empresas.

En otra modalidad, los datos de la víctima son encriptados y los atacantes exigen una cierta cantidad de dinero para entregar las claves de encriptación. Se ha visto recientemente que los datos se filtran a varias plataformas, a veces de forma parcial o total, junto con el cifrado, y se comparten en el entorno de la "web oscura – Dark Web", donde los ciberdelincuentes operan intensamente.

Además, la lucha se vuelve más difícil a medida que las variantes de ransomware se vuelven cada vez más sofisticadas y los atacantes utilizan varios métodos de operación. Últimamente se ha observado que grupos de hackers, patrocinados por un Estado, pueden realizar una operación de ciberespionaje con el único propósito de recopilar información y enviar los datos que obtiene a un gobierno interesado. Sin embargo, al hacerlo, puede presentarse como un grupo de piratas informáticos ordinario/independiente al exigir un monto de rescate a sus víctimas, enmascarando así su propósito original y su relación con un Gobierno.

Un ejemplo de esto puede ser la operación de Irán contra objetivos israelíes en noviembre y diciembre del año pasado (2020). El grupo iraní Pay2Key exigió un rescate de más de USD 1 millón de dólares, en total por los datos que obtuvieron al lograr hackear una serie de importantes empresas israelíes. Al parecer, el grupo en cuestión apuntó a la industria de defensa y empresas de tecnología cibernética y compartió los datos que obtuvo de ellos con los servicios de inteligencia iraníes.

Hay que tener en cuenta que incluso si los atacantes cibernéticos no están afiliados al Estado, es posible que estos cooperen y vendan sus datos debido a motivaciones financieras. Por lo tanto, es posible que los actores de las amenazas cibernéticas le den más peso a este “mercado oscuro”. Si bien la protección de los datos personales es responsabilidad de cada empresa, los gobiernos también tienen

deberes importantes ya que el Estado, se puede ver afectado debido a esta clase de ataques.

La administración del presidente estadounidense, Joe Biden, tomó una serie de medidas luego del devastador ataque del Oleoducto Colonial, para actualizar los protocolos de seguridad y mejorar la colaboración con la industria. Del mismo modo, las empresas israelíes objetivo de los grupos de amenazas cibernéticas iraníes han tomado medidas para tomar precauciones en la cooperación Estado-empresa como resultado de las advertencias de las instituciones pertinentes del Estado.

Aunque muchas empresas o instituciones conocen los pasos que se pueden tomar para protegerse de las amenazas de ransomware, a menudo estas no se llevan a cabo. Se debe adoptar un enfoque proactivo en este sentido, se deben evaluar las posibles vulnerabilidades de seguridad de las compañías y gobiernos y se deben tomar las precauciones necesarias en cooperación con las instituciones locales e internacionales, si no se quiere que información sensible caiga en manos equivocadas. (AA News 2021).

Por ejemplo, Ersin Cahmutoglu, se desempeña en el área de inteligencia y actividades cibernéticas patrocinadas por el Estado y trabaja para el Departamento de Estudios de Seguridad del Centro de Estudios Iraníes (İRAM).

Esto ha llevado a que las guerras físicas, tipo guerra fría y del golfo por poner solo ejemplos, se estén llevando o trasladando al mundo digital y del ciberespacio, donde los países y las empresas que no sean fuertes no estén preparadas y entrenadas, no cuenten realmente con recursos de todo tipo, van a terminar colapsados y siendo las víctimas de toda esta nueva tendencia.

Además de implementar buenas prácticas de ciberseguridad, su organización debe ejercer prácticas de codificación segura, mantener actualizados los sistemas y el software de seguridad, aprovechar los cortafuegos y las herramientas y soluciones de gestión de amenazas, instalar software antivirus en todos los sistemas, controlar el acceso y los privilegios de los usuarios, realizar copias de seguridad con frecuencia y buscar proactivamente amenazas desconocidas (riesgos, vulnerabilidades, etcétera)

En resumen, se puede decir que Los ataques de ‘ransomware’, al alza, los casos de Colonial Pipeline y, posteriormente, la empresa cárnica JBS han generado preocupación en la Casa Blanca. Al respecto, Gina Raimondo, secretaria de Comercio de EEUU, ha asegurado que “los ataques de ransomware han llegado para quedarse y es lógico pensar que se intensificarán”. Por otra parte, un reciente estudio de ciberseguridad realizado por los investigadores de Check Point pone de manifiesto que los ataques de ransomware han aumentado un 56% a nivel mundial desde principios de año (SecuritiLatam 2021).

Figura 22- Secuestro de Datos 2020 (SafetyDetectives 2021).

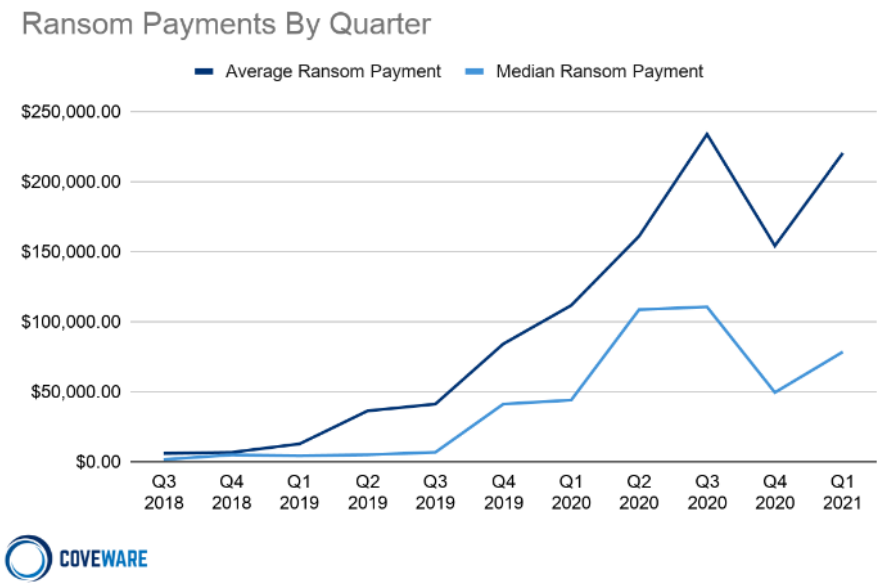


Figura 23- Promedio de pagos realizados por ataques de Ransomware en las empresas en los últimos cuatro (4) años. (Coveware 2021).

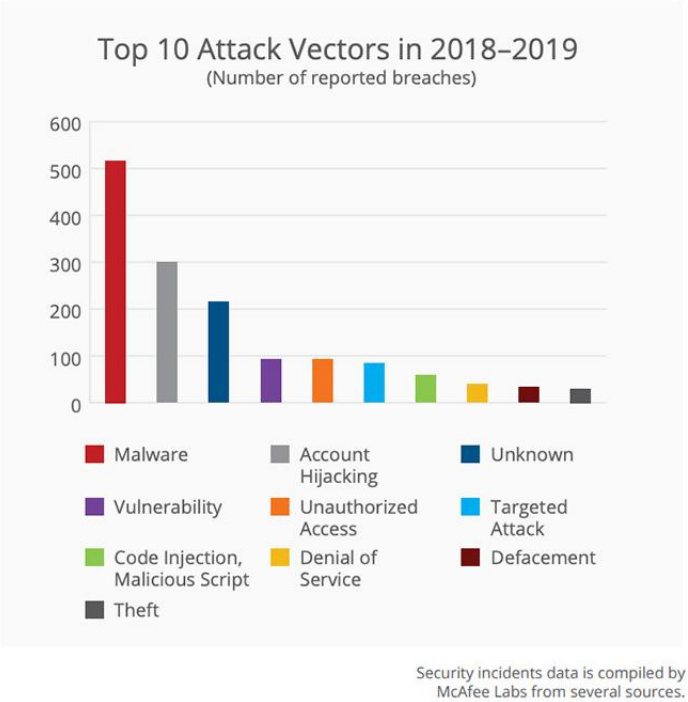


Figura 24- Top 10 de ataques en años 2018 y 2019. (McAfee Labs 2020).

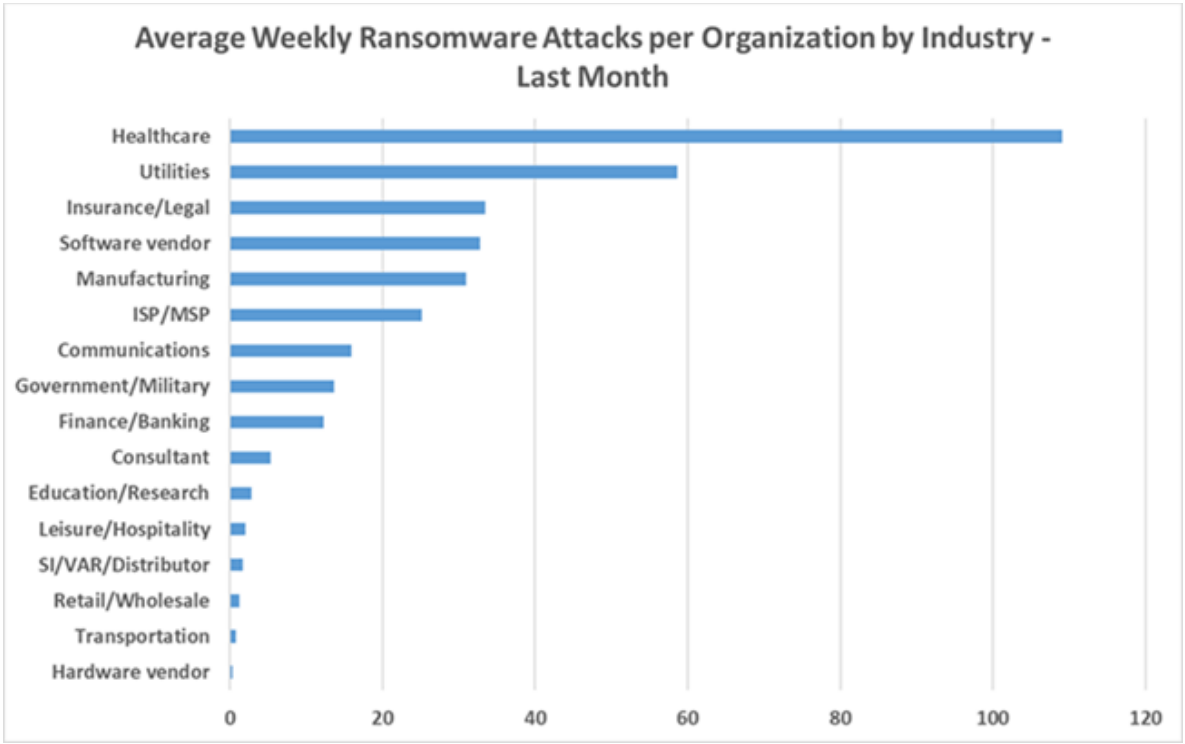


Figura 25- Tipos de empresas afectadas por ataques Ransomware en 2020. (Coveware 2021).

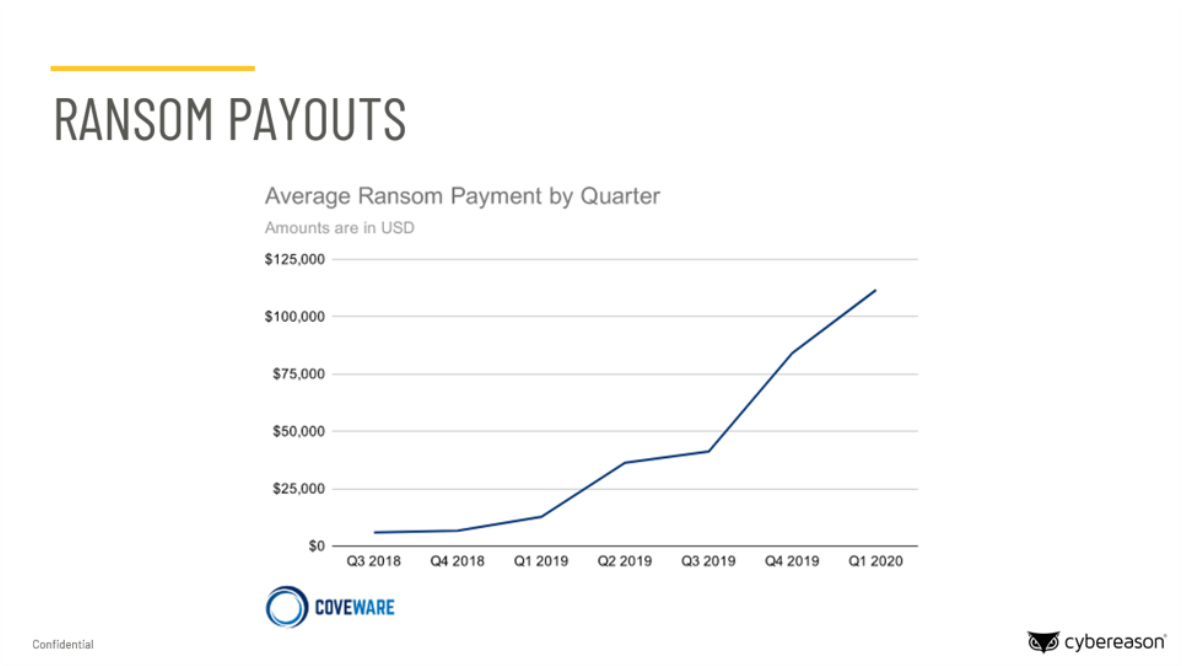


Figura 26- Promedio de pagos en empresas americanas en los últimos cuatro (4) años por ataques Ransomware en 2020. (Coveware 2021).

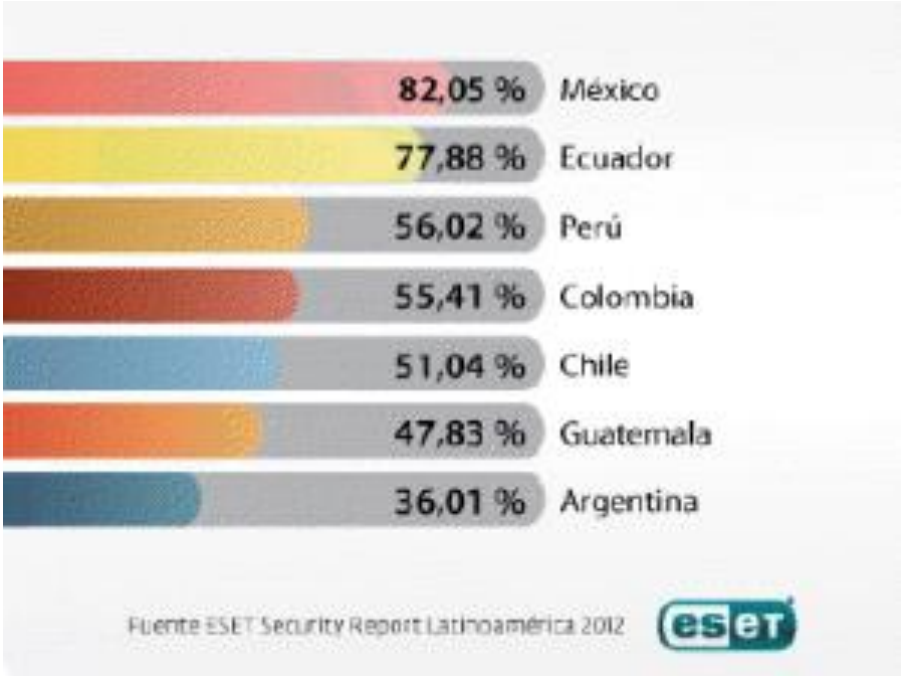


Figura 27- Porcentajes de Ataques por Ransomware en Latinoamérica 2012. (eset 2013).

Según un informe de Hiscox en 2021, apunta que las empresas españolas se recuperan más rápido de estos ataques informáticos contra la información y los sistemas de información por que El 58% de las compañías afectadas por 'ransomware' pagan el rescate (Hiscox 2021).

Muy a pesar de que hacen grandes inversiones en ciberseguridad, como se puede apreciar en la siguiente figura, donde se observa el nivel de resiliencia de las empresas españolas desde el punto de vista de seguridad de la información y ciberseguridad.

Figura 28- Resiliencia de las empresas españolas en materia de ciberseguridad a 2020. (Hiscox 2021).

Si se observa al detalle este país de Europa, como antecedentes a tener en cuenta para países de Latinoamérica se puede decir:

- El 58% de las compañías que recibe un ataque de ransomware, es decir, de secuestro de datos, paga un rescate por los mismos, según el informe de Ciberpreparación 2021 elaborado por la compañía de seguros especializados Hiscox y presentado en el mes de abril de 2021.

- Estos ataques son los más habituales y suponen un costo promedio anual de 29.535 euros para las empresas españolas y de 46.136 euros para las del resto de los países, mientras que los ataques generales representan una media de 10.080 euros en España y 11.150 euros en el resto del mundo. Sin embargo, el colaborador de Hiscox Fernando Conde insistió en no confiarse por unas cifras relativamente

moderadas, ya que existe una gran desviación en los datos: el caso más grave en España llegó a alcanzar los 504.000 de euros.

- Además, el 42% de los ataques se repite hasta en cuatro (4) ocasiones, por lo que el experto expuso que carece de sentido pagar un rescate si no se va a mejorar la ciberseguridad de las empresas, pues “solo se contribuirá a que los cibercriminales se lucren aún más”.

- El Covid (Pandemia), ha puesto esta tendencia al descubierto y en la mira, ya que el 45% de las empresas reconoce que son más vulnerables a los ataques desde el comienzo de la pandemia, lo que el 58% de ellas vincula con el teletrabajo. Como consecuencia, el 58% ha incrementado la ciberseguridad de sus sistemas. “La buena noticia es que estas inversiones en ciberseguridad han dejado de ser vista como un gasto y se reconoce como una inversión estratégica”, reconoció Conde.

- Las empresas españolas, especialmente las de mayor tamaño, son más ciberresilientes, es decir, se recuperan mucho más rápido tras un ataque informático que el resto de países. Un hecho que contrasta con el menor número de compañías consideradas ciberexpertas en el país: solo un 9% de ellas lo son, frente al 25% de Estados Unidos y el 23% de Reino Unido.

- En España se observan dos (2) velocidades: mientras que en el caso de las grandes compañías el porcentaje de ciberexpertas llega al 14% y el de novatas, al 21; en las pymes estos porcentajes son del 8% y el 36%, respectivamente, y en las microempresas, del 3% y el 58%.

Mirando al detalle a Colombia, se puede definir que el impacto que sufren las empresas colombianas luego de un ciberataque trasciende el costo económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y data sensible.

Al tener en cuenta los Ataques BEC son una de las principales amenazas a la cadena de suministros, componente fundamental en la actividad diaria de una empresa. Las comunicaciones con proveedores externos y socios de confianza requieren de entornos seguros, que garanticen la integridad de correos electrónicos y servicios de mensajería instantánea utilizados.

Según el FBI, los ataques BEC durante el 2018 generaron pérdidas en organizaciones globales por valor de 12.000 millones de dólares, mientras que, en Colombia, el monto promedio de las cifras de pérdidas por ataque puede oscilar entre 300 millones y 5.000 millones de pesos, según el tamaño de la empresa afectada.

Al mirar el tema de los ataques Ransomware, Colombia recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año (2020), seguido de Perú (16%), México (14%), Brasil (11%) y Argentina (9%). Las PYMES fueron el blanco preferido por los ciberatacantes, pues conocen que los niveles de seguridad suelen ser más bajos en este tipo de compañías. (Policía Nacional e Interpol -2021).

Las cifras de cobro de rescate por los ataques a empresas colombianas, utilizando ransomware, oscilan entre 0,5 y 5 BITCOINS, y el monto que perciben los atacantes depende de la cotización de las criptomonedas. La dificultad en la trazabilidad de las transacciones de las criptomonedas, se ha convertido en un aliciente para las redes de cibercriminales que, en el modelo de ecuación criminal, entienden que siempre las ganancias percibidas serán mayores a las probabilidades de ser arrestados o condenados.

En los últimos meses el Ransomware “SAMSAM” cobró relevancia en Colombia, porque permite al atacante el robo de contraseñas para el acceso remoto a los dispositivos a través del acceso a credenciales RDP (Remote Desktop Protocol) y de ese modo secuestrar la información de las compañías víctimas.

Estos ataques estuvieron dirigidos a entidades o individuos con efectos altamente severos por la complejidad del ataque. SamSam elevó el monto de los rescates al situarlo entre 32 millones de pesos (COP) hasta más 160 millones de pesos (COP) por ataque. El Ransomware GandCrab mucho más común que SAM SAM exigió rescates a partir de 3 millones de pesos (COP) (Policía Nacional e Interpol -2021).

Como resumen general a este anexo se puede decir que los ciberataques golpean a las empresas cada día. John Chambers, CEO de la multinacional Cisco dijo: «Existen dos (2) tipos de empresas: Aquellas que han sido hackeadas y Aquellas que han sido hackeadas, pero no lo saben». Para combatir un mundo donde la seguridad informática se ha convertido en uno de los pilares de las organizaciones se requiere tener la conciencia de ello y conocer las implicaciones o los daños que los delitos informáticos o ciberataques pueden ocasionar en las empresas u organizaciones.

Un ciberataque a la información se puede definir como un conjunto de acciones ofensivas contra sistemas de información. Estos pueden ser bases de datos, sistemas de información, portales de transacciones en línea de las empresas, sistemas de intercambios de información entre dependencias de una empresa o

entre empresas de un grupo económico en general. El objetivo es dañar, alterar o destruir organizaciones o personas. Además, pueden anular los servicios que prestan, robar datos o usarlos para espiar.

Hoy día vivimos en una era digital. Hoy en día la mayoría de las personas utilizan un ordenador con Internet. Por eso, debido a la dependencia de las herramientas digitales, la actividad informática ilegal crece sin parar y busca nuevas y más efectivas formas de delinquir. Podemos clasificar los tipos de ataques de ciberseguridad a la información en tres (3) categorías:

- Phishing attacks
- Malware attacks
- Web attacks

Phishing:

El phising es un tipo de ingeniería social que se emplea, por lo general, para robar datos de usuario. Pueden ser números de tarjetas de crédito o contraseñas, por ejemplo. Ocurre cuando un delincuente se hace pasar por una persona de confianza. Entonces, engaña a la víctima para que abra un mensaje de texto, correo electrónico o SMS mediante un enlace malicioso. Este enlace puede causar la congelación de un sistema ransomware, revelar información confidencial o instalar malware.

Se trata de una técnica sencilla y muy fácil de utilizar, por eso es una de las más peligrosas. Puede tener resultados desastrosos. Para un individuo, puede suponer el robo de identidad, de fondos o la realización de compras no autorizadas. (IEBS 2020)

SPEAR PHISHING

Por otro lado, los spear phishing son ataques informáticos que tienen como objetivo una persona o empleado específico de una compañía en concreto. Para llevar a cabo este tipo de ataques los criminales recopilan meticulosamente información sobre la víctima para ganarse su confianza. Caer en estos ataques suele ser muy usual, ya que un correo bien elaborado, ya sea con enlace o documento adjunto malicioso, es muy difícil de distinguir de uno legítimo. Esta técnica se utiliza mucho para atacar empresas, bancos o personas influyentes.

WHALING

En el tercer lugar de la lista de tipos de ataques en ciberseguridad nos encontramos los ataques whaling. Estos ataques se centran en un perfil de alto directivo, como CEOs o CFOs. El objetivo, igual que los anteriores, es robar información vital, ya que aquellos que ocupan puestos altos en una empresa suelen tener acceso ilimitado a información confidencial. En la

mayoría de estas estafas llamadas «caza de ballenas» el delincuente manipula a la víctima para permitir transferencias electrónicas de alto valor.

La frase «caza de ballenas» hace referencia al tamaño del ataque, ya que las ballenas son atacadas dependiendo de su posición dentro de la organización. Este tipo de ataques son más fáciles de detectar en comparación con los phishing estándar. Los responsables de seguridad informática de una empresa pueden disminuir la efectividad de este pirateo. (IEBS 2020).

Malware o software malicioso:

En segundo lugar, entre los tipos de ataques en ciberseguridad se encuentran los malware. Un malware es un código creado para corromper sigilosamente un sistema informático. Es un término amplio que describe cualquier programa o código malicioso perjudicial para los sistemas. Un malware intrusivo invade, daña o deshabilita ordenadores, sistemas informáticos, móviles, etcétera, asumiendo el control de las operaciones.

El objetivo del malware suele ser sacarle dinero al usuario de forma ilícita. Aunque este por lo general no puede dañar el hardware de los sistemas, sí puede robar, cifrar, borrar datos, o secuestrar funciones básicas de un ordenador, así como espiar su actividad sin que nadie lo note. Los malware incluyen muchos tipos de softwares maliciosos, como spyware, ransomware, troyanos, etcétera (IEBS 2020).

RANSOMWARE O SECUESTRO DE DATOS

El ransomware es un software malicioso que al penetrar en nuestro equipo le otorga al hacker la capacidad de bloquear un dispositivo desde una ubicación remota. También a encriptar los archivos quitándole al usuario el control de toda la información y datos almacenados.

En cuanto a su método de propagación, los ransomware normalmente se transmiten como un troyano. Es decir, infectando el sistema operativo. Por ejemplo, descargando un archivo o explotando una vulnerabilidad del software. El ciberdelincuente, que ha cifrado los archivos del sistema operativo inutilizando el dispositivo, suele pedir un rescate a cambio de quitar la restricción a los documentos.

DESCARGAS AUTOMÁTICAS

Las descargas automáticas para propagar malware son uno de los métodos más comunes entre los tipos de ataques en ciberseguridad. Los ciberdelincuentes buscan páginas web inseguras y plantan un script malicioso en el código HTTP o PHP en una de ellas. Este script puede instalar malware directamente en el dispositivo del usuario que visite el sitio. También

puede coger la forma en un iframe que redirige a la víctima a un sitio controlado por los atacadores. Estos ataques se llaman «descargas automáticas» porque no requieren ninguna acción por parte de la víctima. Solo tiene que visitar dicha web.

TROYANO

Un troyano es un programa de software malicioso que intenta camuflarse como herramienta útil. Se propagan al parecer un software y persuadir a una víctima para que lo instale. Los troyanos se consideran entre los tipos de ataques en ciberseguridad más peligrosos, a menudo diseñados para robar información financiera.

Los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, estos permiten a los cibercriminales espiarte o robar tu información confidencial. A diferencia de virus y gusanos, los troyanos no pueden autorreplicarse. Para que un malware sea un troyano solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, bajo una apariencia inocua. (IEBS 2020).

Ataques a una web:

INYECCIÓN SQL

Entre los tipos de ataques en ciberseguridad más conocidos se encuentra la Inyección SQL. Se trata de un método de infiltración de un código intruso que se aprovecha de una vulnerabilidad informática presente en una aplicación. Es decir, se aprovechan de errores de diseño habituales en las páginas web. La amenaza de las inyecciones SQL supone un grave problema de seguridad relacionado con las bases de datos. Se emplean para manipular, robar o destruir datos.

Los ciberdelincuentes son capaces de inyectar consultas SQL maliciosas en el campo de entrada de una web, engañar a la aplicación para que haga uso de los comandos que deseen y acceder a la base de datos que quieran. Un ataque de inyección SQL puede ralentizar el funcionamiento de una web, el robo, la pérdida o la corrupción de datos, la denegación de acceso de cualquier compañía o incluso la toma del control absoluto del servidor. (IEBS 2020).

XSS O CROSS SITE SCRIPTING

Los ataques XSS utilizan recursos web de terceros para ejecutar secuencias de comandos en el navegador web de la víctima o en la aplicación programable.

Son una especie de inyección en la que el atacante envía secuencias de comandos maliciosos al contenido de páginas web para desacreditarlas. Esto ocurre cuando una fuente dudosa puede adjuntar su propio código en las aplicaciones web. Este se envía en formas de fragmentos de código JavaScript ejecutados por el navegador de la víctima.

Los exploits pueden incluir scripts ejecutables maliciosos en muchos idiomas, incluidos Flash, HTML, Java y Ajax. Los ataques XSS pueden ser muy devastadores. Sin embargo, aliviar las vulnerabilidades que permiten estos ataques es relativamente simple.

Anexo I: Etapa de Ciberataques contra Los Recursos, La Infraestructura, Funcionamiento y Operación de las empresas:

Al tener en cuenta y analizar para esta metodología, los ataques informáticos o Ciberataques contra los Recursos, la Infraestructura, funcionamiento y operación de las empresas, debemos si o si hablar sobre los ataques que van dirigidos y llevan la finalidad de afectar directamente el principio de la seguridad que tiene que ver con la disponibilidad de los servicios, infraestructuras, equipos, plataformas, etc.

Donde los ciberatacantes solo les interesa afectar la disponibilidad de estos recursos, servicios e infraestructura de las empresas y de las nacionales, a través de su destrucción total, parcial o por un largo periodo de tiempo.

En este orden de idea, estos son de los ataques informáticos o ciberataques que se deben tener en cuenta en el BIA (ISO 22301:2018) de la organización y en todo el plan de recuperación del desastre de la compañía, es decir, de la continuidad del negocio.

Las motivaciones de los ciberterroristas para ejecutar este tipo de ataques son variadas, algunas son como actos terroristas, otros por motivaciones religiosas, políticas, comerciales a través de prestarle servicios a terceros que son los que les quieren hacer realmente daño consentido a las organizaciones, etc.

Estos ataques en sí, se han facilitado o vienen creciendo exponencialmente, debido a que estamos en una sociedad digital, que cada día, necesita estar más interconectada, que cada día se vienen conectando más equipos y dispositivos al ciberespacio, muchos de estos con altos estándares de seguridad, pero en contravía a esto también equipos con cero o nulas protecciones en cuanto a ciberseguridad.

El IoT (Internet de la Cosas), el IIOT (Internet Industrial de las cosas), las virtualizaciones de soluciones, la migración a entornos de cloud computing, los sistemas de data analítica, orquestaciones de soluciones, automatización de procesos y servicios, en general todos estos avances tecnológicos y la llegada de tecnologías como 5G y todo lo que significa industrias 4.0; hacen que todo esté más interconectado y que exista mayor interoperabilidad de soluciones y servicios.

Esto en cierto sentido hace que los procesos sean las inteligentes, agiles, automatizados; pero de igual manera aumenta el número de vulnerabilidad, amenazas y los riesgos en contra del correcto funcionamiento y operación de las empresas, al exponer cada vez más todo en lo que se apoya la operación, el funcionamiento y el agregar valor a las organizaciones.

A nivel de los países y naciones, esto toma mayor relevancia e importancia si se incluyen en este anexo las infraestructuras críticas de las naciones.

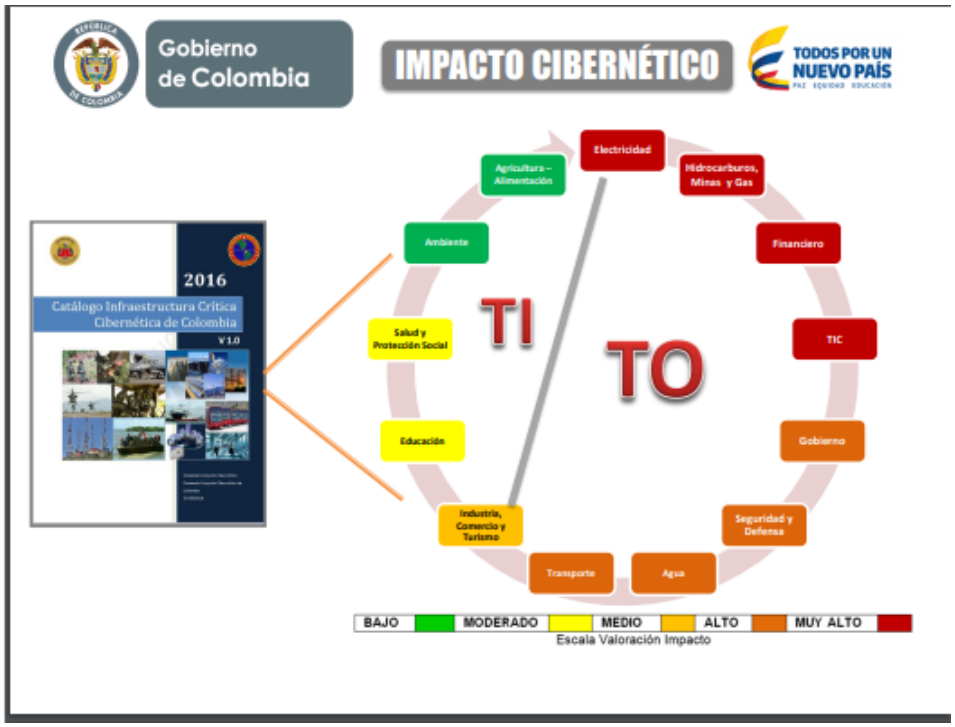


Figura 29- Análisis de Impacto en las Infraestructuras Criticas de Colombia. (CCOC 2016).

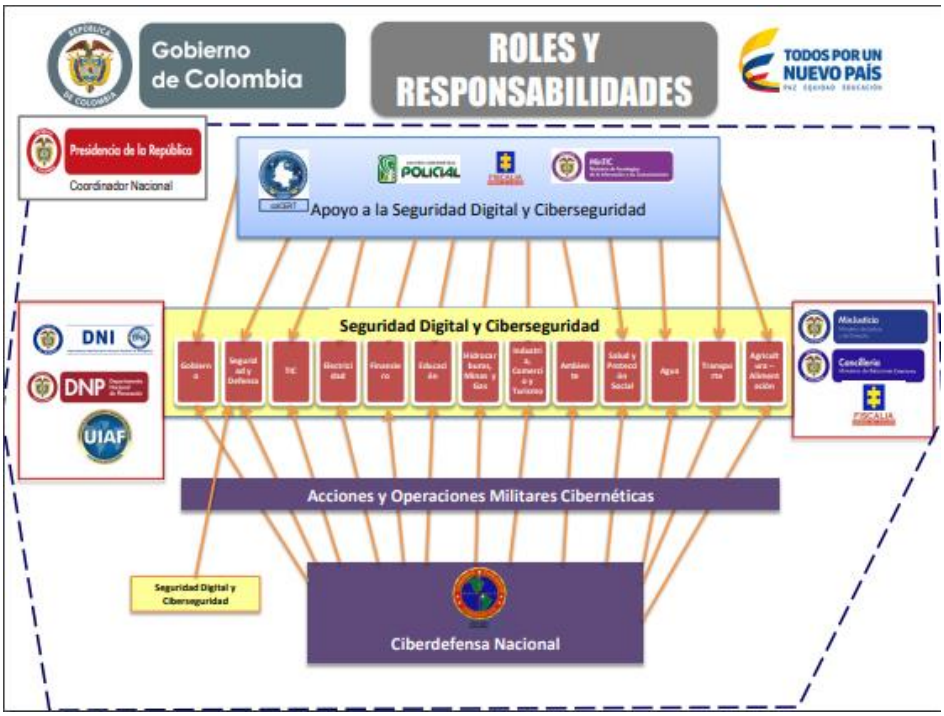


Figura 30- Roles y responsables de las Infraestructuras Criticas de Colombia. (CCOC 2016).

Las Infraestructuras Críticas de todos los países estás expuestas a multitud de riesgos y amenazas fruto de sus vulnerabilidades. Las Infraestructuras Críticas son el objetivo más deseado de los atentados terroristas, los ataques cibernéticos de particulares e incluso ataques híbridos por parte de gobiernos y servicios de inteligencia, de ahí que necesiten una protección más avanzada. Ejemplos como los ataques terroristas del 11S en EEUU, las acciones cibernéticas de Anonymous o malwares diseñados por Servicios de Inteligencia como fue el caso de Stuxnet contra las Centrales Nucleares de Irán han provocado que la mayoría de los gobiernos establezcan líneas de acción estratégicas para garantizar la protección de sus Infraestructuras Críticas.

Como ciudadanos, pero especialmente como profesionales, conviene reconocer y saber qué es una Infraestructura Crítica de la que depende nuestra calidad de vida. Conocer cómo y con qué criterios se protegen, nos permitirá proteger nuestros propios sistemas u organización con la misma eficacia. A diario utilizas la electricidad, bebes agua, utilizas el transporte público, realizas pagos con tarjetas bancarias, buscas a través de Google Maps, llamas por teléfono, te conectas a Internet o realizas trámites con la Administración.

Todas esas actividades esenciales dependen de las Infraestructuras Críticas: centrales eléctricas o nucleares, sistema de aguas, transporte ferroviario, sistema bancario, tecnología de satélite, sistemas de telecomunicaciones o de la Administración. (Lisa Institute 2019).

La Directiva europea 2008/114/CE del 8 de diciembre de 2008 establece por infraestructura crítica como:

“El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones”.

En el caso de España, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), protege a ese país, en el caso de Colombia las actividades para la identificación de la infraestructura crítica cibernética del País, en el marco del manejo de riesgo operacional, Ciberseguridad y Ciberdefensa está liderada por el Comando Conjunto Cibernético del Ministerio de Defensa Nacional.

La define guías y lineamientos que aplican a todas las entidades, públicas, privadas o de economía mixta, que cuenten con infraestructura de Tecnologías de Información y Comunicaciones o Tecnologías de Operación, es decir, el Comando Conjunto Cibernético (CCOC), en coordinación con el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) del Ministerio de Defensa

Nacional. Se encargan de proteger a Colombia ante este tipo de ataques informáticos o ciberataques en contra de las infraestructuras críticas del país.

Todos los países tienen un sistema de clasificación de estas infraestructuras, servicios esenciales e infraestructuras estratégicas, para el caso de Colombia, de definen de la siguiente manera:

- Servicio esencial: "Es el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas."

- Infraestructura Crítica: "Son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales."

- Infraestructura Estratégica: "Infraestructura Estratégica: Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales."

En otras palabras, las infraestructuras críticas son todos aquellos sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económicos, medioambiental y político. Una alteración o interrupción en su funcionamiento debido a causas naturales (por ejemplo: una inundación que afecta al suministro eléctrico) o provocada por el hombre (por ejemplo: un atentado terrorista o un ataque cibernético a una central nuclear o a una entidad financiera) podría conllevar graves consecuencias.

Las amenazas a las infraestructuras críticas podrían afectar a cualquier Estado al no poder continuar y desarrollar con normalidad las actividades básicas de la sociedad. Sin embargo, el problema empeora cuando una infraestructura crítica es dependiente de otra. La caída de una infraestructura crítica supondría la paralización o menoscabo de los servicios de ambas, por lo que la protección de estas adquiere mayor importancia. A pesar de que las infraestructuras críticas son similares en todos los países, su práctica puede variar en función de las necesidades, recursos y nivel de desarrollo de cada país en particular.

Muy similarmente como los países y naciones definen, analizan, estudian los riesgos, vulnerabilidades y amenazas a sus tecnologías críticas, se debe tener en cuenta y aplicar a todas las empresas y organizaciones, máximo si parte de sus

servicios, recursos, infraestructura está asociada o interconectada al ciberespacio, guardando claro está, las proporciones de los casos.

La mayoría de los ataques informáticos o ciberataques que pueden afectar las tecnologías críticas de un país, pero de igual manera a los servicios, operación, funcionamiento y misión de las empresas y las organizaciones son:

Malware: El término Malware se refiere de forma genérica a cualquier software malicioso que tiene por objetivo infiltrarse en un sistema para dañarlo. Aunque se parece a lo que comúnmente se le conoce como virus, este último es un tipo de malware y existe en la misma categoría junto con los gusanos, troyanos, etc.

Virus: El virus es un código que infecta los archivos del sistema mediante un código maligno, pero para que esto ocurra necesita que un usuario lo ejecute. Una vez que este entre en funcionamiento, se disemina por todo el sistema y todo elemento al que nuestra cuenta tenga acceso, desde dispositivos de hardware hasta unidades virtuales o ubicaciones remotas en una red.

Gusanos: Un gusano es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por la red. A diferencia del virus, no necesita nuestra intervención, ni de un medio de respaldo, ya que pueden transmitirse utilizando las redes o el correo electrónico. Son difíciles de detectar, pues al tener como objetivo el difundir e infectar a otros equipos, no afectan al funcionamiento normal del sistema. Su uso principal es el de la creación de botnets, que son granjas de equipos zombies utilizados para ejecutar acciones de forma remota como por ejemplo un ataque DDoS a otro sistema.

Troyanos: Son similares a los virus, pero persiguiendo objetivos diferentes. Mientras que el virus es destructivo por sí mismo, el troyano lo que busca es abrir una puerta trasera para favorecer la entrada de otros programas maliciosos. Su nombre es alusivo al “Caballo de Troya” porque su misión es precisamente, pasar desapercibido e ingresar a los sistemas sin que sea detectado como una amenaza potencial. No se propagan a sí mismos y suelen estar integrados en archivos ejecutables aparentemente inofensivos.

Ataque de Denegación de Servicio (DOS): Los ataques DOS funcionan inundando sistemas, servidores y/o redes con tráfico para sobrecargar recursos y ancho de banda. Este resultado hace que el sistema sea incapaz de procesar y satisfacer las solicitudes legítimas. Además de los ataques de denegación de servicio (DoS), también hay ataques de denegación de servicio distribuidos (DDoS).

Los ataques DoS saturan los recursos del sistema con el objetivo de impedir la respuesta a las solicitudes de servicio. Por otro lado, se lanza un ataque DDoS desde varios equipos host infectados con el objetivo de lograr la denegación de

servicio y desconectar un sistema, allanando así el camino para que otro ataque entre en la red o en el entorno. Los tipos más comunes de ataques DoS y DDoS son el ataque de inundación TCP SYN, el ataque de lágrimas, el ataque de pitufo, el ataque de ping-of-death y las botnets.

Denegación de servicio distribuido (DDoS): Los ataques de DDoS consisten en realizar tantas peticiones a un servidor, como para lograr que este colapse o se bloquee. Existen diversas técnicas, entre ellas la más común es el uso de botnets, equipos infectados con troyanos y gusanos en los cuales los usuarios no saben que están formando parte del ataque. De todos los tipos de ataques informáticos este es uno de los más conocidos y temidos, ya que es muy económica su ejecución y muy difícil de rastrear al atacante.

De esta forma, la eficacia de los ataques DDoS se debe a que no tienen que superar las medidas de seguridad que protegen un servidor, pues no intentan penetrar en su interior, solo bloquearlo generando severas pérdidas económicas al negocio objetivo.

Rootkits: Los rootkits se instalan dentro de un software legítimo, donde pueden obtener control remoto y acceso a nivel de administración a través de un sistema. El atacante utiliza el rootkit para robar contraseñas, claves, credenciales y recuperar datos críticos.

Dado que los rootkits se esconden en software legítimo, una vez que permite que el programa realice cambios en su sistema operativo, el rootkit se instala en el sistema (host, ordenador, servidor, etc.) y permanece inactivo hasta que el atacante lo activa o se activa a través de un mecanismo de persistencia. Los rootkits se propagan normalmente a través de archivos adjuntos de correo electrónico y descargas de sitios web inseguros.

Ataques a dispositivos y soluciones de IoT e IIoT: Mientras que la conectividad a Internet a través de casi todos los dispositivos imaginables crea comodidad y facilidad para los individuos, también presenta un número creciente -casi ilimitado- de puntos de acceso para que los atacantes los exploten y causen estragos. La interconexión de las cosas hace posible que los atacantes rompan un punto de entrada y lo utilicen como puerta para explotar otros dispositivos de la red.

Los ataques de IoT e IIoT son cada vez más populares debido al rápido crecimiento de los dispositivos de IoT e IIoT y (en general) a la baja prioridad que se da a la seguridad integrada en estos dispositivos y en sus sistemas operativos. En un caso de ataque a la IoT e IIoT, un casino de Las Vegas fue atacado y el hacker logró entrar a través de un termómetro conectado a Internet dentro de uno de los bancos de peces del casino.

Las mejores prácticas para ayudar a prevenir un ataque IoT incluyen la actualización del sistema operativo y el mantenimiento de una contraseña segura para todos los dispositivos IoT de la red, así como el cambio frecuente de contraseñas.

APT o Ataques Cibernéticos de Amenaza Persistente Avanzada: Una APT se define como un ataque centralizado en un objetivo específico con el fin de comprometer el sistema y robar información; utiliza diferentes herramientas para obtener acceso a su objetivo y ampliar el ataque.

Características de los ataques APT

1. Troyanos de puerta trasera generalizados

Los ataques APT dependen de troyanos de puerta trasera, porque los atacantes necesitan volver a los sistemas en los que han establecido una entrada principal para filtrarse en dicho software.

2. Flujos de información.

Se establece el uso de VPNs por parte de los atacantes, mediante el uso del HTTPS, por lo que un buen punto de partida para identificar dicho malware, es saber cómo se ve normalmente tu flujo de información.

3. Paquetes de datos inesperados

Estos paquetes de datos pueden ser tu información que se filtra a los atacantes. Debes estar atento a grandes cantidades de información que está donde no debería estar, especialmente si está comprimida.

4. Campañas enfocadas de spear phishing

Se emplean correos electrónicos que comúnmente tienen un archivo de documento infectado generado por enlaces URL maliciosos o código ejecutable malicioso, por lo que rastrear el sistema infectado podría llevarte al punto cero del ataque APT.

Fases de una APT

1. Conocer el objetivo; la información recopilada puede ayudar a promover el ataque.

2. Encontrar una entrada y enviar malware personalizado; se puede lograr mediante phishing o usando otros medios.

3. Obtener el punto de apoyo; engañar a un usuario para que ejecute el malware en su sistema, dentro de la red objetivo.

4. Ampliando el alcance del ataque.

5. Encontrar y robar información; esto puede implicar la elevación de privilegios.

6. Mover y cubrir pistas; puede ser necesario mover o expandir los puntos de entrada para avanzar en el ataque.

Tres (3) ejemplos reales de APT

GhostNet

Este grupo de ciberataques APT, con sede en China, utilizó spear Phishing, así como archivos adjuntos maliciosos para obtener acceso a los sistemas en más de 100 países a partir de 2009. Entre las muchas técnicas de ataque que GhostNet utilizó fueron el audio y la captura de pantalla para obtener información sobre los objetivos.

Sykipot APT

El grupo de ataque Sykipot es conocido en parte por crear la familia de malware Sykipot APT. Este malware personalizado aprovechó vulnerabilidades en productos de Adobe y usó ataques de spear phishing para efectuar exploits de día cero sobre sus víctimas.

Mettel

Este grupo de ataque, junto con otros incluidos Carbanak y GCMAN, se dirigió a instituciones financieras. Mettel usó malware personalizado para infectar cajeros automáticos. Cuando los cajeros automáticos se liquidaron al final del día, el malware hizo transacciones de los cajeros automáticos. Esto demuestra que los ataques APT pueden robar dinero e información.

A partir de dicha información podremos catalogar a las APT como una especie de “suite” de Malware ya que combina una amplia variedad del mismo, desde un malware preexistente hasta un malware personalizado, así como algunos métodos de trabajo adecuados para lanzar ataques dirigidos que pueden continuar durante un período de tiempo prolongado ya que tienden a persistir después de los intentos iniciales de detección y mitigación, convirtiéndolos en grandes riesgos de malware junto al ransomware.

Ejemplo de esto es la caída que sufre la red de redes internet, generalizada a nivel mundial durante una hora, en el mes de junio de 2021. Donde en torno a un mediodía, varias webs como Amazon.com, The Guardian, The NY Times y la propia eitb.eus; han dejado de estar accesibles. El problema se ha debido a un ataque que ocasionó la caída del proveedor de contenidos Fastly.

Anexo J: Etapa de Ciberataques Causantes de Pérdidas Económicas y Financieras Directas:

Se suele pensar y percibir, de manera errada o equivocada, que los ataques cibernéticos representan un riesgo mayormente para entidades individuales. No obstante, los ciberataques masivos y de significativo impacto apuestan por hackear información albergada en redes de gran escala: infraestructuras estratégicas, empresas multinacionales, instituciones gubernamentales y un sinfín de PYMES que, o bien no reportan el caso por miedo o vergüenza, o porque no están plenamente conscientes de lo sucedido.

El principal objetivo de los ataques cibernéticos es el dinero, o por lo menos es el más común. Así como los recientes virus ransomware #Wannacry y #Petya aplican la extorsión, hay otros que van directo a los datos personales para acceder a datos bancarios o información financiera. Se estimaba que las pérdidas por ataques cibernéticos a 2017, sumarian más de USD $445 mil millones a nivel mundial, pero esta cifra se duplicó al terminar el 2017, es decir, estas cifras proyectadas quedaron muy por debajo de la realidad. Esta cifra es alarmante y no muestra indicios de mermar o reducirse, sobre todo cuando se consideramos las cifras y proyecciones a nivel mundial nos informan:

- Según el último informe de ciberseguridad anual publicado por el IC3 (Crime Complaint Center del FBI), las pérdidas económicas por ciberataques en 2020 han superado los 4.000 millones de dólares. Sin duda, una cifra que revela la magnitud de las consecuencias que provocan estos incidentes y la necesidad urgente que tienen empresas y administraciones públicas de estar bien preparados en materia de ciberseguridad.

- El informe también señala que el número de denuncias presentadas por víctimas de diferentes tipos de delitos cibernéticos aumentó un 69% respecto al año 2019. Y los tres (3) principales delitos denunciados estaban relacionados con la interacción humana, lo que pone de manifiesto, una vez más, la importancia de la concienciación y formación en ciberseguridad de las plantillas de las organizaciones para poder hacer frente a los lucrativos ataques de ingeniería social del cibercrimen.

- Los ciberdelincuentes aprovecharon la vulnerabilidad general tras la irrupción de la COVID-19 para multiplicar sus ataques, cada vez más elaborados y con objetivos económicos. Aparte de que para las empresas o administraciones que sufren un ciberataque, las consecuencias van mucho más allá ocasionando también graves crisis reputacionales.

- Los ataques de Business Email Compromise (BEC) o estafas por correo electrónico siguen siendo las más costosas para las empresas, según el informe del IC3 más de 1,8 mil millones de pérdidas anuales reportadas, y teniendo en cuenta que muchos ataques no se reportan.

- Las estafas por correo electrónico han sido especialmente importantes con la situación generalizada de teletrabajo, con los empleados de las organizaciones fuera de las redes corporativas y más expuestos a este tipo de ataques. De nuevo, es preciso recordar que la formación en ciberseguridad es crítica para evitar los más del 90% de incidentes de ciberseguridad que se producen por errores humanos.

- Por otro lado, también es cada vez más frecuente el fraude de soporte técnico que genera pérdidas superiores a los 146 millones de dólares. El IC3 recibió 15.421 quejas de víctimas en 60 países relacionadas con este tipo de fraude.

- El rescate medio pagado por las organizaciones en 2020, como consecuencia de ataques ransomware, fue de 312.493 dólares, lo que supone un incremento interanual del 171% respecto a 2019. Así lo refleja el informe anual de la firma norteamericana de ciberseguridad Palo Alto Networks.

- Además, desde el año pasado ha crecido lo que se conoce como la “doble extorsión” en los ataques ransomware, que consiste no solo en cifrar los archivos si no en robarlos. De esta manera, los ciberdelincuentes amenazan a las compañías o administraciones afectadas con publicar los datos sensibles que hayan capturado en el ataque si se niegan a pagar el rescate.

- Todos estos datos son preocupantes si tenemos en cuenta, además, que los ataques ransomware han aumentado un 62% a nivel mundial según el nuevo ‘Informe de Ciberamenazas 2021’ de SonicWall. La misma investigación expone también que las técnicas que utilizan los ciberdelincuentes para cometer estos delitos son más sofisticadas y con variantes más peligrosas, como el ya famoso Ryuk, y que se han identificado más variantes de malware desconocidas hasta el momento.

- Está demostrado que los ataques cibernéticos se producen en los momentos de mayor vulnerabilidad de las compañías y administraciones, cuando más desprotegidas pueden estar. Por eso, la ciberseguridad en la pandemia ha sido clave ya que la llegada de la COVID-19 fue el escenario perfecto para que el cibercrimen lanzase sus numerosos y agresivos ataques.

- En el entorno laboral han ido evolucionando a la par los entornos de trabajo en remoto y las técnicas utilizadas por los ciberdelincuentes para encontrar las brechas de seguridad para atacar. Según la investigación de SonicWall la transición de empleados del entorno presencial al teletrabajo, puede estar directamente relacionada con el aumento del 67% en los archivos de Office maliciosos en 2020.

- Por otro lado, el comercio minorista, el sector sanitario y la administración pública han sido grandes víctimas de los ataques ransomware y se siguen enfrentando a diario a un volumen creciente de amenazas. Especialmente el sector de la salud ha sido el más afectado por el ransomware en 2020. Sin duda, los primeros meses de la pandemia fueron críticos y se registró un incremento del 95,17% de incidentes de ransomware con respecto al mismo periodo del año anterior.

- Los sectores más afectados por estos ciberataques son "la administración pública, el sector empresarial industrial y el sector sanitario". Los ataques a los hospitales "ponen en juego la vida de las personas". Estos ataques son "masivos y secuestran la información y piden un rescate". Detrás de estos ataques se encuentran "organizaciones profesionalizadas dedicadas a estafar".

- Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19.

- En solo un cuatrimestre (entre enero y abril de 2021), uno de los socios de INTERPOL del sector privado detectó 907.000 correos basura, 737 incidentes de tipo malware, y 48.000 URL maliciosas, todos ellos relacionados con la COVID-19.

- Más de 45.000 ciberdelitos reportados en el país en 2020, un 89 % más que el año anterior, un incremento del 303 % en los casos de suplantación de sitios web para la captura de datos personales y más de 5.440 denuncias por ataques o dispersiones de archivos maliciosos en redes corporativas, dan cuenta de la importancia que ha adquirido en este tiempo la ciberseguridad y la protección de la información para las organizaciones.

- Las cifras, presentadas por la Cámara Colombiana de Informática y Telecomunicaciones –CCIT– y el Tanque de Análisis y Creatividad de las TIC

–TicTac–, al cierre del año anterior, reflejan un panorama que califican como preocupante ante el incremento de los ataques cibernéticos.

- Además, según FortiGuards, organización de investigación e inteligencia de amenazas de Fortinet, en 2020 hubo 7 billones de intentos de ciberataques en Colombia y 41 billones en América Latina.

- En ese contexto, los delincuentes han aprovechado que muchas empresas, debido a la pandemia, han debido acelerar sus procesos de transformación digital y en esa transición han expuesto sus vulnerabilidades informáticas.

- La ANDI, en cabeza de su vicepresidente de Transformación Digital, Santiago Pinzón, ha indicado que si hace cuatro años solo una de cada cuatro empresas en el país había adoptado un proceso de este tipo, en 2021 ya son seis de cada diez las que lo vienen haciendo.

- La CCIT y TicTac aseguran que el phishing (suplantación de sitios web), el Spoofing (suplantación de identidad) o el pharming (redirigir a sitios web maliciosos) hacen parte de las modalidades más frecuentadas por los ciberdelincuentes.

- De hecho, ni las entidades gubernamentales, como la DIAN, la Registraduría Nacional o la Fiscalía General de la Nación–de acuerdo con sus propios reportes– se han salvado de estos ataques.

Por otro lado, el Reporte Global de Riesgo en 2020, nos mostraba las preocupaciones a nivel mundial a causa de Ataques informáticos o ciberataques, como se puede apreciar en las dos (2) siguientes figuras:

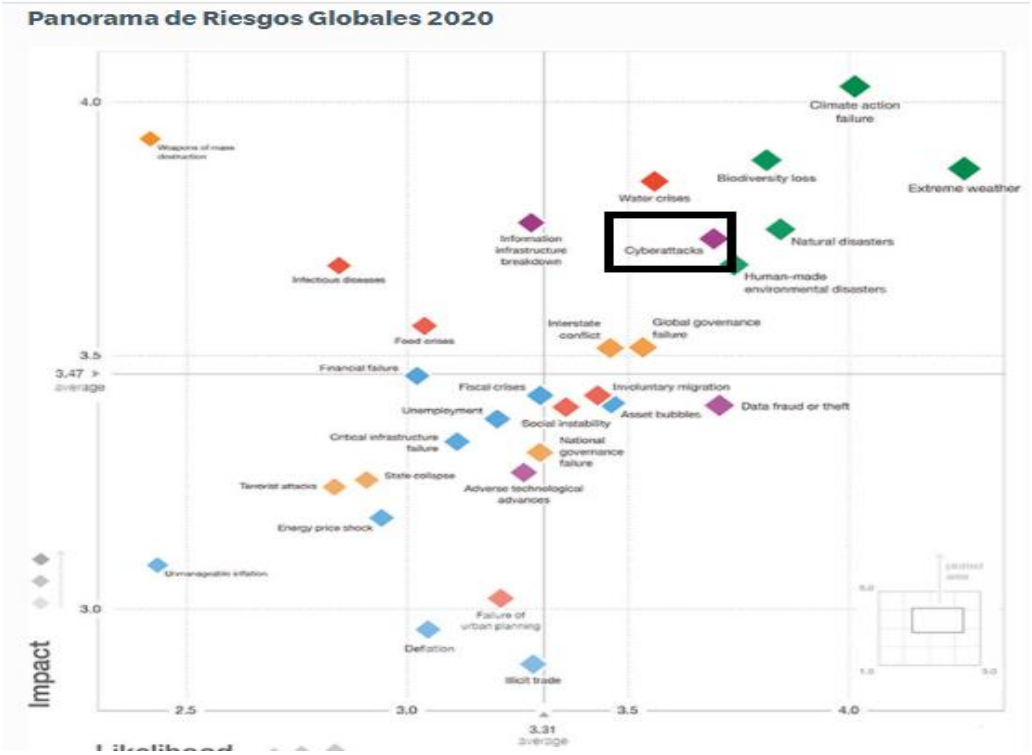


Figura 31- Panorama de Riesgos Globales 2020. (Informe Global de Riesgos 2020)

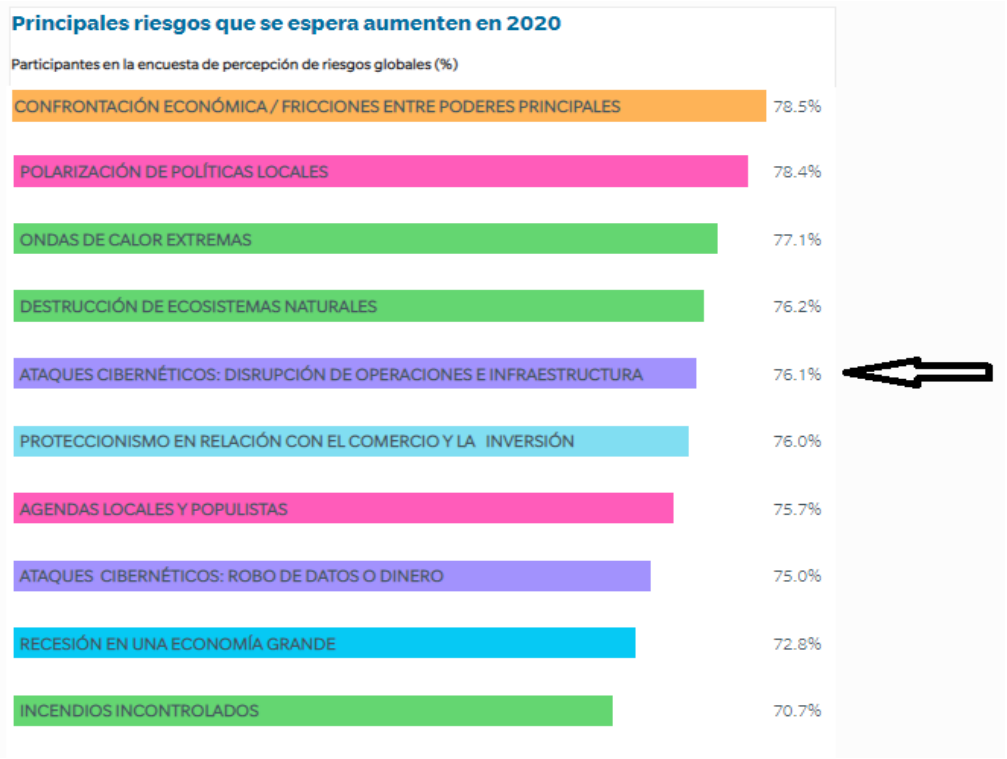


Figura 32- Principales Riesgos Globales 2020. (Informe Global de Riesgos 2020)

Como se puede apreciar las repercusiones y afectaciones negativas económicas, financieras, comerciales y reputacionales contra las empresas víctimas de delitos informáticos o ciberataques continua en crecimiento.

Y uno de estos ataques más costosos para las empresas y organizaciones afectadas es el ransomware, dado que cada vez son más comunes los ataques cibernéticos y el denominador común de estos virus informáticos es que secuestran los datos de la computadora infectada, y sucesivamente imposibilitan el uso del dispositivo. Pero la trampa no termina allí: una ventana emergente le indicará al usuario que debe pagar una determinada cantidad de dinero para recuperar la funcionalidad del dispositivo. En pocas palabras, estamos hablando de un secuestro digital o ransomware.

En el caso de #Wannacry, por ejemplo, se ha documentado que Asia y Europa recibieron el mayor impacto. No obstante, tal y como reitera Kaspersky Labs, México también ha sufrido las repercusiones del ataque cibernético. No podemos cometer el error de bajar la guardia en Latinoamérica.

Se puede definir que las cinco (5) repercusiones por riesgos y ataques cibernéticos, como lo evidencian numerosos casos, los riesgos cibernéticos pueden generar consecuencias de gran alcance, tales como:

1. Interrupciones operativas: La empresa se ve incapacitada para continuar desarrollando sus actividades con normalidad, con las consecuencias en pérdidas en ventas o incluso la parálisis completa de la actividad.

2. Pérdida de información: Esta puede originar extra-costes para protegerse del uso fraudulento de la misma. Cuando esta información incorpora datos personales de clientes, nos encontramos además con potenciales sanciones por falta de diligencia en la custodia de estos datos personales.

3. Riesgos reputacionales: Pueden deteriorar la imagen de la marca.

4. Acciones legales: Pueden ser contra los directores y gerentes, iniciadas por clientes o accionistas por los perjuicios causados por la disrupción o por la filtración de datos.

5. Pérdidas económicas directas: Estas ocurren cuando la motivación del ciberataque es económica y se produce un "secuestro" con finalidad lucrativa.

Algunas cifras que conviene tomar en cuenta:

- México es el noveno país más afectado por el crimen cibernético, con 605 casos reportados. En América Latina solo es superado por Brasil.
- Más de $6,000 millones de dólares se perderán globalmente derivado de la actividad cibercriminal en 2021.
- 467,351 incidentes de ciberseguridad fueron reportados globalmente en 2019.
- 71% de los robos de información tuvieron como motivo obtener dinero; 25% fueron con fines de espionaje. (https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/)).
- El método elegido en el 52% de los casos de robo de información fue el hackeo directo, en el 33% de los casos se recurrió a phishing o ingeniería social y el 28% correspondió a malware.

- 43% de los ciberataques afectan a pequeños negocios. Los ataques entre un año y otro a estas organizaciones crecieron 424%.

- El tiempo promedio para identificar un robo de información es de 206 días. Desde que sucede hasta su contención puede pasar 314 días.

- El fraude por pagos en línea costará al eCommerce por lo menos $25,000 millones de dólares al año para 2024.

- El 34% de las 11,000 vulnerabilidades cibernéticas no tiene un parche conocido.

- En el 63% de las compañías los datos estuvieron potencialmente comprometidos en los últimos 12 meses por culpa de una vulnerabilidad de hardware. En 28% de los casos, las empresas no están contentas con el manejo de seguridad de sus proveedores.

- 65% de los grupos cibercriminales utilizan spear-phishing como su principal vector de infección.

- El 100% de las grandes compañías (Fortune 500) tendrá un CISO o posición equivalente para 2021.

Este anexo aplica para cuando la empresa ha sido víctima de ataques informáticos o ciberataques, donde se deben respetar los requerimientos de manejo de la información desde el punto de vista de computación o informática forense.

Es decir, La computación forense, también llamado informática forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir elementos informáticos, examinar datos residuales, autenticar datos y explicar las características técnicas del uso de datos y bienes informáticos.

Esta disciplina no sólo hace uso de tecnologías de punta para mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar qué ha sucedido dentro de cualquier dispositivo electrónico. La formación del informático forense abarca no sólo el conocimiento del software sino también de hardware, redes, seguridad, piratería, craqueo y recuperación de información. La informática forense ayuda a detectar pistas sobre ataques

informáticos, robo de información, conversaciones o evidencias en correos electrónicos y chats.

La evidencia digital o electrónica es sumamente frágil, de ahí la importancia de mantener su integridad. El simple hecho de pulsar dos veces en un archivo modificaría la última fecha de acceso al mismo. Dentro del proceso del cómputo forense, un examinador forense digital puede llegar a recuperar información que haya sido borrada desde el sistema operativo. El informático forense debe tener muy presente el principio de intercambio de Locard por su importancia en el análisis criminalístico, así como el estándar de Daubert para hacer admisibles las pruebas presentadas por el perito forense en un juicio.

Es muy importante mencionar que la informática o cómputo forense no tiene como objetivo prevenir delitos, por lo que resulta imprescindible tener claros los distintos marcos de actuación de la informática forense, la seguridad informática y la auditoría informática.

Una vez respetados y tenidos en cuenta los lineamientos de la computación forense procedemos a valorar o cuantificar la afectación por delitos informáticos en las organizaciones.

Para ello debemos tener en cuenta lo siguiente:

1. Valoración de los activos: ¿Por qué interesa un activo? Por lo que vale.
   No se está hablando de lo que cuestan las cosas, sino de lo que valen.

   Si algo no vale para nada, prescíndase de ello.

   Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que valorar. La valoración se puede ver desde la perspectiva de la ‘necesidad de proteger’ pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

   El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos.

   El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la empresa u organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio.

Al entrar en los detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Sobre esto se especifica a manera de ejemplo o guía, el siguiente caso:

> Caso o ejemplo: Si en una empresa se adquirió hace muchos años un gestor de bases de datos y en un ataque este sufre pérdida parcial o total de la información contenida.
>
> Debemos recurrir a los principios técnicos de valoración, esto quiere decir, aplicar o tener en cuenta:
>
> a. Que no se debe valorar solo por lo que costo del gestor de bases de datos como tal, sino por lo que este contenía, aportaba a la empresa, lo imprescindible de ese activo para la empresa y por el valor aculado que hasta el momento de la afectación tenía. Es decir, se debe sumar en la valoración de este activo lo siguiente:
> b. Valor propio del activo: Costo del instalador y la licencia. Acá no es el valor que tiene en facturas o en la contabilidad, luego de las depreciaciones, sino que se debe tener en cuenta el valor comercial actual, es decir, lo que vale hoy comprar el activo en el mercado productivo. (Valor presente)
>
> c. Valor pagado por instalación y afinamiento del gestor de bases de datos. Este valor es doble, es decir, lo que ya se había invertido al inicio para poner en funcionamiento el activo + el valor de la nueva instalación y afinamiento posterior al ataque. (Reinicio de la continuidad del negocio) – (Valor presente).
>
>   Si el daño no fue total, sino parcial y se debió invertir tiempos en horas hombre o pago de servicio de mantenimiento correctivo, este debe estar incluido como mano de obra para reestablecer el funcionamiento del bien afectado, en reemplazo del valor total si la afectación fuera al 100%.

d. Valor actual y acumulado de los registros que tenían las bases de datos del Gestor de BD. (Valor Presente).

e. Valor de lo imprescindible para la empresa: En esta parte va muy relacionado por las pérdidas ocasionadas a la empresa por el tiempo que el Gestor de bases de Datos estuvo no operativo y las pérdidas operacionales en la empresa por esta para o detención. (Lucro Cesante) (Valor presente). ***(MTPD/MAO = Tiempo de reanudación total de los niveles normales de operación del Activo (Iso 22301:2018))***

f. En el caso de que sean Bases de Datos de procesos comerciales, mercadeo o ventas, se debe revisar el histórico de las ventas anteriores en el mismo volumen de tiempo sin operar. Es decir, cuanta utilidad de la operación real hubiera agregado al valor de la empresa si el gestor no hubiera sido atacado o afectado, este valor se debe sumar a la valoración. (Valor presente y Utilidad Neta). ***(MTPD/MAO = Tiempo de reanudación total de los niveles normales de operación del Activo (Iso 22301:2018))***

g. Si la afectación o para del servicio ocasionó de igual manera multas, sanciones o pago de pólizas; por cláusulas contractuales o por incumplimientos de ley, estas deben ser tenidas en cuenta y sumar estos valores a la valoración total del activo afectado. (Valor presente y valor futuro).

h. Si este activo tiene dependencia relacionada con otro u otros activos requerido o requeridos para otro servicio u otros servicios en la organización, este valor o valores de pérdida por la detención en el funcionamiento del activo o servicio dependiente; se debe tener en cuenta, sumar y considerar acá en esta valoración total. Es decir, lo que dejo de recibir como utilidad neta la empresa por el tiempo que el servicio o los servicios dependientes dejaron de generarles utilidad o valor a la empresa. Se deben tener en cuenta los históricos de la organización en cuanto al tiempo y utilidades netas en ese tiempo de para y traer esos costos a valor presente. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

(MTPD/MAO = Tiempo de reanudación total de los niveles normales de operación del Activo (Iso 22301:2018))

Esta afectación cuantitativa total en formula, en las empresas que no coticen en bolsas de valores, seria:

Afectación Cuantitativa por Ataques Informáticos o Ciberataques en las empresas no cotizantes en Bolsa de Valores = CP+COI+COA+CRA+TINPMTPD+VRA+MSPPILC+COAADAM.

Si la empresa cotiza en bolas de valores se le debe adicionar la parte de VTPAMTPDPLDS (Valor Total de Pérdidas en Acciones por Tiempo de Afectación y Proyección de afectación futura Línea Directa Semestre siguiente), quedando la fórmula de la cuantificación cuantitativa de la afectación en empresas cotizantes en bolsas de valores así:

Afectación Cuantitativa por Ataques Informáticos o Ciberataques en las empresas cotizantes en Bolsa de Valores = CP+COI+COA+CRA+TINPMTPD+VRA+MSPPILC+COAADAM+ VTPAMTPDPLDS.

Nota 01: En las fórmulas anteriores estas siglas significan lo siguiente:

CP = Capex (Valor Presente)

COI = Costo Opex Inicial – Valor pasado traído a valor presente.

COA = Costo Opex Actual – Valor de nuevo Setup requerido.

CRA = Costo de Reparación del Activo – Incluye todas las reparaciones o mantenimiento correctivos requeridos.

TINPMTPD = Costo Total Imprescindible no percibido en para – Lucro cesante no recibido.

VRA = Valor de los registros informáticos o información afectada.

MSPPILC = Costos totales por multas, sanciones, pago de pólizas; incurridos por la empresa afectada o atacada, considerando los aspectos legales, administrativos, financieros y/o contractuales por incumplimientos a raíz de la afectación.

COAADAM = Costos derivados y asociados a las afectaciones de otros activos afectados que dependan del activo principal o de mayor afectación.

VTPAMTPDPLDS = Valor Total de Pérdidas en Acciones por el tiempo de las afectaciones y afectaciones proyectadas futuras lineales directas semestre siguiente.

El sumatorio total de estos valores, es lo que da o define el valor total final del activo afectado y es lo que se precede a recuperar o que resarzan económicamente hablando, ante las autoridades o el juez competente o ante la aseguradora previo acuerdo de los valores a asegurar.

Nota 02: Se debe ser muy detallado y precavido al momento de asegurar estos activos, pues las aseguradoras solo pagan o reconocen los valores propios del bien de acuerdo con las facturas en valores pasados, es decir, sin tener en cuenta el valor acumulado, sin tener en cuenta las variaciones o incrementos del IPC año a año, y el valor presente del activo afectado.

El cual se complica si es un activo que se debe importar, donde entra a jugar el valor pasado de la TRM al momento de la importación o compra anterior (Valor pasado) o anterior vs el valor presente de la TRM a considerar en la nueva compra (Valor presente).

Nota 03: Al momento de asegurar o adquirir pólizas de seguros para los activos físicos y digitales de la empresa, se recomienda tener en cuenta estos valores definidos anteriormente, esto permitirá la recuperación y el lucro cesante de mejor manera en la empresa u organización.

Como, además, hacer una correcta valoración del bien o el activo, antes de asegurarlo.

En términos generales y a manera de un resumen de toda la parte anterior, se hace necesario tener en cuenta la salud o el nivel de salud y funcionamiento del activo.

¿Cuánto vale la “salud” de los activos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que valorarlo. La valoración es la determinación del costo que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

• Costo de reposición: adquisición e instalación.

• Costo de mano de obra (especializada) invertida en recuperar (el valor) del activo.

• Lucro cesante: pérdida de ingresos

• Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.

• Sanciones por incumplimiento de la ley u obligaciones contractuales.

• Daño a otros activos, propios o ajenos.

• Daño a personas.

• Daños medioambientales.

Todos estos valores o costos se deben tener en cuenta al calcular o establecer el valor del activo afectado. Adicional a ello, se deben tener en cuenta dos (2) aspectos o criterios de los activos.

La homogeneidad: Es importante poder comparar valores, aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.

• La relatividad: Es importante poder relativizar el valor de un activo en comparación con otros activos (Magerit 2012).

Ambos criterios se satisfacen con valoraciones económicas (costo en dinero requerido para “curar”, “recuperar” o “reemplazar” el activo) y es frecuente la tentación de ponerle precio a todo. Una vez tenidos en cuenta todos esos costos, valores y asignado el valor total real del activo es excelente.

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente “natural”. La interpretación de las sumas no es nunca motivo de controversia. Si la valoración es en dinero, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución.

El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias. Para esta valoración se recomienda conocer y aplicar los criterios

de ISO 22301:2018, donde se pueden ver, entender y aplicar las relaciones entre los principales parámetros de la gestión de continuidad de negocio: RTO, MTPD/MAO y MBCO.

RTO: Tiempo para reanudar la actividad del negocio, así no sea al 100% de la capacidad. (Reiniciar cuanto antes la continuidad del negocio).

MTPD/MAO: Tiempo para la reanudación de los Niveles normales de operación. (100% o Normalidad).

MBCO: Objetivo o métrica para retomar la operación del negocio o la continuidad del negocio, aunque sea a un nivel inferior (ISO 22301:2018).

Anexo K: Etapa de Ciberataques Causantes de Pérdidas o Afectaciones Reputacionales (Pérdidas Económicas y Financieras Indirectas y/o Colaterales):

En la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, se incluye este anexo debido a que es unos de los campos y temas más álgidos y de mayor discusión a nivel internacional.

Esto debido a que una marca, el buen nombre, Good Will, un activo lógico, un activo computacional pueden y son considerados la mayor parte del tiempo como activos o bienes intangibles, y les resulta en muchos casos, realmente difícil para las personas entender el valor que aportan estos activos, bienes y la empresa como tal.

Es importante que, al sentarse para determinar una valoración o cuantificación cualitativa de estos bienes, activos y de la marca como tal, se determinen qué incluyen estos, que aportan estos, porque son generadores de valor de acuerdo con la misión y los servicios de la empresa, etcétera. En términos generales se habla de marcas registradas, logotipos, empaques, estrategias de marketing, activos digitales, colores de marca, etcétera.

Es resumen se debe tener en cuenta todo lo que realmente, los consumidores asocian con la imagen, la reputación y el buen nombre de las empresas y organizaciones. Toda esa marca, buen nombre, bienes y activos intangibles son fuentes y generadores de valor en las empresas y en detalle y en conjunto poseen grandes y fuertes valores, como, por ejemplo: Al tener en cuenta las cinco (5) marcas más valiosas del mundo reconocidas por la revista Forbes, a partir del 2018:

Apple: $ 182.8 mil millones

Google: $ 132.1 mil millones

Microsoft: $ 104.9 mil millones

Facebook: $ 94.8 mil millones

Amazon: $ 70.9 mil millones.

Para poder entender mejor todo esto se debe tener en cuenta y conocer que es el riesgo reputacional. Es decir, el riesgo reputacional se debe comprender como la posibilidad de una opinión o comentarios, que pueden ser positivos o negativos, frente a las actividades, prácticas, servicios, procesos o situaciones desarrolladas por una empresa u organización y que pueden generar un o varios impactos negativos, viéndose reflejado en la reducción de clientes, reducción de inversionistas, reducción de ventas, reducción de EVA, reducción de Ebitda y utilidades netas, aumento de costos por pagos de pólizas, pago de sanciones en las

organizaciones por caída, pérdidas o interrupciones en los servicios o caída de ingresos en general.

El análisis y control de este tipo de riesgo se lleva a cabo comúnmente en instituciones del sector financiero, aseguradoras, pero hoy día ante las posibilidades de que todas las empresas pueden ser víctimas de ataques informáticos o ciberataques, resulta obligatorio que todo tipo de empresa haga este tipo de evaluaciones y considere los daños que pueden sufrir en su reputación.

Estas afectaciones reputacionales van a impactar directa e indirectamente en los resultados económicos, administrativos y financieros de las empresas y en muchos casos van a ser objeto de estudios y análisis por autoridades competentes en el caso de demandas, litigios legales etcétera. Es decir, dado que una afectación de la imagen o reputación puede verse reflejada directamente en el valor de las acciones o en la desconfianza de inversionistas, quienes podrían no encontrar en la organización la sensación de seguridad suficiente, lo que llevaría a afectaciones en las decisiones de no inversión, entre otras afectaciones más. Las Facenews, las calumnias, las falsas noticias, pueden ocasionar de igual manera estas afectaciones reputacionales en las empresas.

Es posible analizar este tipo de riesgo también como un riesgo consecuencia de otros. El riesgo reputacional aparece usualmente como consecuencia de una explotación de vulnerabilidades o fallos que evidencian riesgos en seguridad de la información y por ende generan de inmediato desconfianza en usuarios y clientes, entre otros. Para contextualizar mejor esta idea, es necesario presentar varios ejemplos de empresas que se han enfrentado al riesgo reputacional asociado a la materialización de riesgos de seguridad de la información o de base tecnológica.

Como primer ejemplo, se sugiere tener en cuenta y mirar unos años atrás, para recordar la ola de ataques que enfrentó la firma Sony y sus filiales a lo largo del mundo durante el año 2011. En dichos ataques, que fueron logrados debido a las relaciones de confianza e infraestructuras similares establecidas entre las filiales de la compañía, se identificó fuga de información relacionada con cuentas de acceso, correos electrónicos y tarjetas de crédito de más de 30 millones de usuarios en todo el mundo. De acuerdo con análisis realizados por matemáticos de la revista Forbes, las pérdidas o el costo de los ataques significó a la empresa Sony aproximadamente 24 billones de dólares. Además de todos los costos en favor de mantener a sus clientes y evitar que optaran por cancelar sus cuentas y dejar de usar productos de la compañía, todo esto a partir de numerosos regalos a través de la misma red a sus usuarios, disculpas públicas y múltiples estrategias de mercadeo que hicieron del 2011 un año menos tormentoso de lo que ya era para la firma de videojuegos. (Forbes 2018).

Como segundo ejemplo se propone tener en cuenta casos de Entidades Certificadoras (CA) mundialmente reconocidas, donde dos (2) compañías que se presentan en este ejemplo. Ambas compañías pertenecen al mercado de seguridad de la información, ofreciendo servicios de firmado de certificados digitales y cumpliendo un rol como entidades certificadoras dentro de los esquemas de Infraestructura de Llave Pública (PKI).

DigiNotar sufrió un ataque en julio de 2011, en el cual un atacante logró comprometer la infraestructura de la Entidad Certificadora (CA) para generar cientos de certificados digitales falsos de diferentes dominios de alto perfil, tales como Google, Yahoo, Mozilla y Wordpress, entre muchos otros. En este proceso, luego de varias investigaciones realizadas por parte del gobierno alemán y, de haber tomado control de la compañía en el mes de septiembre del mismo año, se determinó que toda la infraestructura había sido comprometida en el ataque. Esto dio lugar a la materialización del riesgo reputacional en torno a la responsabilidad de la compañía en este fallo de seguridad y a la desconfianza de todos sus clientes, lo que llevó a DigiNotar a declararse en bancarrota y cerrar sus puertas (Forbes 2018).

Un segundo caso similar, pero con un final diferente, se registró con la empresa Comodo, la cual logró identificar a tiempo el acceso no autorizado por parte de un reseller a su plataforma para la realización del firmado de nueve (9) certificados digitales de Siete (7) dominios diferentes. En el mismo ataque lograron comprometer la Autoridad de Registro (RA), parte de la Infraestructura de Llave Pública (PKI) de la compañía. Comodo logró identificar el fallo y solucionarlo en solo nueve (9) días posteriores a la intrusión, registrada el 15 de marzo de 2011. En la actualidad, la compañía aún funciona normalmente. Sin embargo, por más que fue controlada la situación, en el mercado de seguridad de la información (luego del fallo) ha perdido mucho terreno. (Forbes 2018).

Los incidentes de seguridad se han convertido en una de las principales fuentes de riesgo para la reputación de las empresas, por detrás solamente de los escándalos éticos, de acuerdo con “Reputation@Risk”, un informe de Deloitte Touche Tohmatsu Limited (DTTL). El tema de seguridad corporativa incluso ha superado, aunque por un pequeño margen, a las cuestiones de seguridad del producto y servicio de atención al cliente como la principal causa de riesgo de reputación. Debido a este delicado panorama crecen las preocupaciones entre los presidentes ejecutivos, directores y ejecutivos en las áreas de riesgo sobre el impacto de los incidentes de seguridad en la reputación de sus compañías.

En la encuesta se entrevistaron a más de 300 altos ejecutivos, directores, y ejecutivos de riesgo de todo el mundo para conocer sus puntos de vista en relación con el riesgo reputacional: qué lo motiva, quién es responsable, la capacidad de la

organización para hacer frente al mismo, y su impacto. Dada la preponderancia de los ataques cibernéticos y el enorme potencial de dañar las marcas de las compañías, las preocupaciones por el tema de seguridad, tanto física como cibernética, fueron un tema central en la encuesta.

Casi el 20% de los encuestados señaló que experimentó un incidente de seguridad en los últimos tres años que terminó dañando la reputación de su empresa. Entre los encuestados que experimentaron un incidente que produjo un daño reputacional (relacionado a la seguridad, la ética, el medio ambiente, o algo más), señalaron que el tema de seguridad es el incidente más citado. De cara al futuro, el 38% de los encuestados prevé que un problema de seguridad (en concreto, la pérdida de datos de clientes) tendrá un impacto significativo en sus empresas en los próximos tres años, y el 65% de los encuestados se siente preparado para hacer frente a tal evento.

El impacto de los eventos que crean un riesgo reputacional es palpable, un 41% de los encuestados cuyas empresas experimentaron un incidente que terminó dañando su reputación dijo que la pérdida de ingresos fue la consecuencia más importante. El mismo número de encuestados citó a la pérdida de valor de la marca como el mayor impacto del incidente, mientras que el 37% puso la investigación por parte de los reguladores al tope de la lista de ramificaciones.

Teniendo en cuenta que el riesgo reputacional se encuentra entre los principales riesgos estratégicos de las empresas, y que la seguridad es uno de los principales impulsores de riesgo reputacional, los CIO, o directores de tecnología, y CISO, responsables centrales de seguridad informática, seguramente serán vigilados mucho más de cerca por los presidentes ejecutivos y los directores en el tema de seguridad cibernética», señaló Henry Ristuccia, líder de Gobierno, Riesgo y Cumplimiento para Deloitte. «Los CIO y CISO deben estar preparados para explicar en forma concisa el perfil de riesgo cibernético de la empresa y las medidas que están tomando para reducir el riesgo.». (Deloitte 2020).

Ristuccia señala que la reputación de una empresa se ve afectada por su desempeño y las decisiones de negocio que toman sus líderes en una amplia gama de áreas, incluyendo la seguridad. Cómo elige una empresa abordar el tema de seguridad cibernética, desde el nivel de inversión en la preparación hasta la búsqueda de un enfoque holístico, puede tener una enorme influencia en la reputación de una empresa. Los encuestados parecen reconocer esta situación si se toma en cuenta que el 40% dice que en la actualidad están enfocados en administración de los riesgos de seguridad y el 43% que estima que la seguridad seguirá siendo el segundo mayor motor de riesgo de reputación durante los próximos tres años.

«Incluso si una empresa experimenta un incidente de seguridad altamente publicitado, una respuesta eficaz durante la crisis puede reducir el daño reputación», señala Ristuccia. «Cada decisión durante una grave crisis puede afectar el valor. Los ejecutivos deben ser conscientes de que los riesgos reputacionales destruyen valor más rápidamente que los riesgos operacionales».

Según Kaspersky Lab y B2B International, los ataques cibernéticos han costado una media de 1,3 millones de dólares por empresa en 2017 en Norteamérica, el 11 por ciento más que en 2016. Para las PYME, el coste medio de la recuperación asciende a 117.000 dólares. Estas estimaciones incluyen tanto el coste de negocio perdido, las mejoras de software y sistemas y los gastos extra en personal interno y en asesoramiento experto.

Sin embargo, el activo que más está en riesgo es la reputación corporativa. Aquellas empresas que no saben gestionar correctamente un ataque y – en especial – su comunicación a clientes y accionistas, están en peligro de sufrir una caída de reputación. Un informe de Forbes Insights indica que el 46 por ciento de las organizaciones habían sufrido daños en la reputación y en el valor de su marca como resultado de un ataque.

Además, la combinación de las consecuencias económicas y del daño reputacional, es a menudo fatal: Según datos de la National Cyber Security Alliance de EE.UU. el 60% de las PYME desaparece dentro de los seis meses siguientes a sufrir un ciberataque.

Es por ello que para calcular y cuantificar estos ataques informáticos esta metodología propone y sugiere el siguiente método, procedimiento y formulas:

1. Tener en cuenta y a la mano las cifras de las utilidades netas de los últimos veinticuatro (24) meses.

2. Sumar estos valores de Utilidad Neta de los últimos veinticuatro (24) meses.

3. Este valor total de la sumatoria de las utilidades netas, dividirlo entre Setecientos veinte (720) días que corresponden a los 24 Meses y de allí resulta el Valor Ponderado de la Utilidad Neta diaria que ha tenido la empresa o compañía **(PDUNeta).**

4. Traer a valor presente el Valor Ponderado de la Utilidad Neta diaria que ha tenido la empresa o compañía. (PDUNeta), para ello se debe revisar que el valor resultante no esté por debajo del valor reciente (mes anterior al ataque), en caso de estarlo se procede a trabajar con el valor actual **(IPCUNeta).**

5. A estos valores sumarle el valor del o los activos físicos afectados, dañados o destruidos en el ataque informático recibido. Para ello se puede tomar el valor que reposa en factura del bien o el activo y traer ese valor pasado a valor presente. (**VPAA** = Valor Presente del o de los equipos, bienes y activos afectados por el ataque informático). (Capex). Si el Activo no fue destruido o afectado en su totalidad de recomienda tener en cuenta el **CRA** = Costo de Reparación del Activo – Incluye todas las reparaciones o mantenimiento correctivos requeridos.

6. Sumar el valor total o gasto acumulado pagado por la empresa para constituir su marca, buena imagen, good Will o reputación (Lo que ha permitido generar valor a la empresa), en este caso los valores al detalle que se deben tener en cuenta y sumar son:

    A. Costo Acumulado pagado por Publicidad en la empresa en toda su historia **(CAPP).**

    B. Gastos acumulados pagado por Promoción y divulgación de la Marca y de la empresa, en toda su existencia **(GAPPD).**

    C. Costos totales pagado para la creación de la empresa **(CTPC).** Traído este valor a valor presente.

    D. Costos Totales pagados por el Registro y los registros históricos acumulados de la empresa. Estos valores pagados anualmente **(CTPR).**

    E. Si la operación de la empresa está sujeta a licencias de cualquier tipo, se debe considerar y sumar el valor total de las licencias pagadas por la organización, desde su constitución hasta la fecha **(VTLP).**

7. Sumar el valor correspondiente al **MSPPILC** = Costos totales por multas, sanciones, pago de pólizas; incurridos por la empresa afectada o atacada, considerando los aspectos legales, administrativos, financieros y/o contractuales por incumplimientos a raíz de la afectación.

8. Sumar el valor correspondiente al **COAADAM** = Costos derivados y asociados a las afectaciones de otros activos afectados que dependan del activo principal o de mayor afectación.

9. Si la empresa comprometida, atacada o afectada cotiza en bolsas de valores se debe sumar la afectación negativa que sufran sus acciones, en este caso el **VTPAMTPDPLDS** = Valor Total de Pérdidas en Acciones por el tiempo de las afectaciones y afectaciones proyectadas futuras lineales directas semestre siguiente.

Al sumar todos los anteriores valores implicados, es lo que da o define el valor total final del activo afectado y es lo que se debe proceder, a recuperar o que resarzan económicamente hablando, ante las autoridades o el juez competente o ante la aseguradora previo acuerdo de los valores a asegurar.

Estos cálculos de las afectaciones reputacionales a tener en cuenta se definen en las siguientes formulas:

Afectación Reputacional Cuantificada por Ataques Informáticos o Ciberataques en las empresas no cotizantes en Bolsa de Valores = (((PDUNeta + IPCUNeta) * Números_de_Días_Afectados (No operados "MTPD") + VPAA + CRA + CAPP + GAPPD + CTPC + CTPR + VTLP + MSPPILC + COAADAM.

Si la empresa cotiza en bolas de valores se le debe adicionar la parte de VTPAMTPDPLDS (Valor Total de Pérdidas en Acciones por Tiempo de Afectación y Proyección de afectación futura Línea Directa Semestre siguiente), quedando la fórmula de la cuantificación reputacional cuantitativa de la afectación en empresas cotizantes en bolsas de valores así:

Afectación Reputacional Cuantificada por Ataques informáticos o Ciberataques en las empresas no cotizantes en Bolsa de Valores = (((PDUNeta + IPCUNeta) * Números_de_Días_Afectados (No operados "MTPD") + VPAA + CRA + CAPP + GAPPD + CTPC + CTPR + VTLP + MSPPILC + COAADAM + VTPAMTPDPLDS.

Anexo L: Etapa de Ciberataques a las Personas:

Se debe tener en cuenta que un ciberataque es un conjunto de acciones ofensivas contra sistemas de información. Estos pueden ser bases de datos, redes informáticas, etcétera. El objetivo es dañar, alterar o destruir organizaciones, pero en muchos casos estas afectaciones también se presentan con personas. A estas personas les pueden:

- Anular los servicios que prestan.
- Denegar servicios.
- Suplantarlos con diferentes finalidades.
- Robarles datos e información personal o privilegiada.
- Sustraerles sin autorización dinero de sus cuentas.
- Utilizar para compras o pagos de servicios en líneas las tarjetas débitos y créditos de la persona víctima.
- Ser utilizados para espiar.
- Obligarlos a hacer actos en contra de su voluntad.
- Extorsionarlos.
- Violar su integridad.
- Engañados.
- Ser utilizados para atacar, dañar o robar a otras personas.
- Entre muchas afectaciones más.

Hay diferentes tipo o clases de ataques a personas, que se caracterizan por sus objetivos (personas naturales, CEO, grupos empresariales) y los medios que usan para ser ejecutados (correos electrónicos, mensajes de texto, llamadas telefónicas, entre otras). Estas son los tres categorías de ciberataques y las acciones que se las componen:

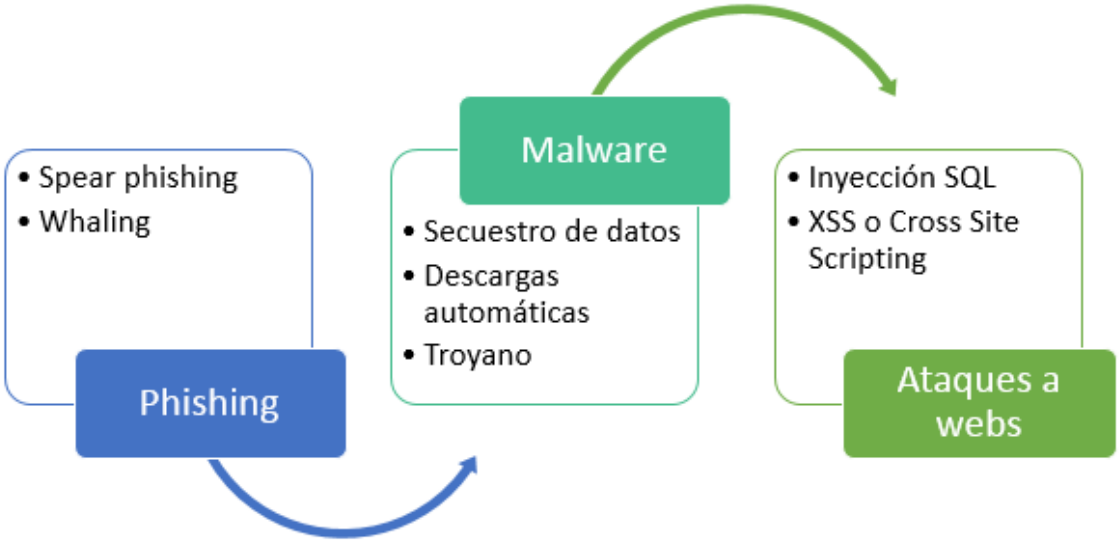


Figura 33- Categorías de Ciberataques a personas (INCP 2019).

Vivimos en una era digital. Hoy en día la mayoría de las personas utilizan un ordenador con Internet. Por eso, debido a la dependencia de las herramientas digitales, la actividad informática ilegal crece sin parar y busca nuevas y más efectivas formas de delinquir.

Podemos clasificar los tipos de ataques de ciberseguridad en tres categorías:

- Phishing attacks
- Malware attacks
- Web attacks

Nota: Detalles de estos ataques informáticos o ciberataques fueron tratados anteriormente en esta metodología y en este caso se definen como aplicables para atacar a personas.

Anexo M: Etapa de pérdidas por Leyes y Normas Nacionales e Internacionales:

En la gran mayoría de los países las empresas que no implementen controles y salvaguardas para sus activos empresariales y resulten ser víctimas de ataques informáticos o ciberataques se deben enfrentar a riesgos, impactos y consecuencias legales de acuerdo con la normatividad y leyes en cada uno de esos países.

Se vienen cada vez presentando mayores sanciones, demandas en contra de las empresas por mal manejo de los datos personales de clientes, empleados y en general de las personas involucradas con estas organizaciones.

Un ataque cibernético, o ciberataque, consiste en una seria de acciones cuyos objetivos son destruir o comprometer los sistemas informáticos de una organización. También puede tener como objetivo el acceso ilegal o robo masivo de datos personales, en este caso se denomina "cibervigilancia", por la cual muchas organizaciones o empresas a nivel nacional e internacional, pueden resultar juzgadas por la falta de controles para evitar la exposición, robo o incorrecta manipulación de los datos de las personas que confiaron en ellas y entregaron sus datos personales. Estas acciones delictivas se han vuelto cada día más frecuentes debido a la mayor presencia que tienen las empresas los gobiernos y los ciudadanos en Internet y con el mayor uso de sistemas y dispositivos conectados a la Red.

En todo caso, la respuesta de las empresas, frente a un ataque informático o ciberataque, tiene que articularse a lo largo de tres (3) niveles:

Técnico: Para restablecer el servicio desde el punto de vista operativo,

Legal: ***Para evaluar las posibles implicaciones legales frente a clientes, proveedores o las necesidades de notificación a las autoridades públicas.***

Gestión de crisis: Para llevar a cabo una comunicación eficaz de lo ocurrido frente a clientes y medios de comunicación y reducir el impacto sobre la reputación de la empresa.

Son empresas expuestas a ataques informáticos o cibernéticos aquellas empresas que tengan en sus ordenadores fijos y sistemas: datos de clientes y proveedores, almacene, manipule o transmita datos, se encuentra expuesta a un ataque cibernético. Las empresas con un mayor riesgo de ataque cibernético son:

- Empresas de Comunicación
- Consultoras Tecnológicas
- Empresas de Telecomunicaciones

- Comercios
- Empresas de Servicios
- Asesorías y Gestorías
- Clínicas, Hospitales y Consultas Médicas.
- Entidades Financieras
- Intermediarios financieros y de seguros
- Hoteles y Ocio
- Comercio electrónico
- Otros.

¿Cómo afectan los ataques cibernéticos en las empresas?

Las empresas expuestas a ataques informáticos o cibernéticos son conscientes de que no pueden evitar todos los ciber ataques, pero pueden limitar sus consecuencias con una actuación rápida y coordinada. No se puede improvisar cuando se produce un ataque cibernético. Debemos tener un plan de contingencia y actuación. Debemos tener en cuenta que estos ataques cibernéticos afectan a las empresas de forma muy importante en diversas áreas clave:

Informática. Desinfectar Archivos, Restaurar información. Copias de Seguridad

Legal. LOPD información a afectados y Responsabilidad.

Financiera. Perdida de horas de trabajo. Horas Extraordinarias. Pérdida de Ventas. Pérdida de Beneficios.

Marketing**.** Daños a su Imagen y Reputación.

Muchas de las grandes empresas ya tienen contratados los nuevos seguros que cubren las consecuencias de estos ataques cibernéticos, evitando el grave perjuicio económico que les puede generar.

El seguro de Riesgos Cibernéticos tiene coberturas que no tenían hasta ahora otros seguros contratados por las empresas. Por ello es recomendable que se revise y se contrate un seguro adecuado y proporcional al tamaño de cada empresa que cubra las consecuencias económicas que se deriva de estos ataques. Algunas compañías aseguradoras junto con la contratación de las pólizas de seguro de riesgos cibernéticos prestan servicio de asesoramiento previo a sus clientes para reducir los riesgos y tratar de evitarlos.

Como lo evidencian numerosos casos, los riesgos cibernéticos pueden generar consecuencias de gran alcance, tales como:

1. Interrupciones operativas. La empresa se ve incapacitada para continuar desarrollando sus actividades con normalidad, con las consecuencias en pérdidas en ventas o incluso la parálisis completa de la actividad.

2. Pérdida de información. Esta puede originar costos extras para protegerse del uso fraudulento de la misma. Cuando esta información incorpora datos personales de clientes, nos encontramos además con potenciales sanciones por falta de diligencia en la custodia de estos datos personales.

3. Riesgos reputacionales. Pueden deteriorar la imagen de la marca.

4. Acciones legales***. Pueden ser contra los directores y gerentes, iniciadas por clientes o accionistas por los perjuicios causados por la disrupción o por la filtración de datos.***

5. Pérdidas económicas directas. Estas ocurren cuando la motivación del ciberataque es económica y se produce un "secuestro" con finalidad lucrativa.

Según las cifras que se manejan actualmente, el coste aproximado de los ataques cibernéticos en todo el mundo asciende a 600 mil millones de dólares. Además, todo apunta a que este coste seguirá aumentando en los próximos años, alcanzando los 6 billones de dólares en 2021. De forma paralela al coste de los ciberataques aumenta la inversión en el campo de la seguridad cibernética, que crece a un ritmo del 10% anual. (BID 2021).

Muchas de estas afectaciones deben ser resarcidas o pueden ocasionar que las empresas deben tener repercusiones o enfrentar procesos penales y ante autoridades judiciales, por las fallas que permitieron esos ataques informáticos o ciberataques en sus organizaciones, allí responden directamente los Representantes Legales de las empresas, compañías, organizaciones o instituciones; por ello deben ser estas personas y roles los primeros en exigir mayor nivel de ciberseguridad en sus empresas a cargo.

Es por ello que las autoridades legales y jurídicas en Colombia recomiendan tener en cuenta los siguientes aspectos si las empresas son víctimas de ciberataques:

La mayoría de los riesgos informáticos están relacionados con estafa tecnológica, y muy pocos son llevados en procedimientos judiciales por falta de pruebas e imposibilidad para identificar al cibercriminal. Es por esto mismo que las autoridades recomiendan siempre acudir a los tribunales llevando las evidencias que puedan aportar en el desarrollo de la investigación. Estos son cinco aspectos que deben tenerse en cuenta:

Figura 34- Recomendaciones de las autoridades y en derecho penal a empresas víctimas de ataques Informáticos (INCP 2021).

Cinco riesgos legales a tener en cuenta en un ciberataque

Las estadísticas de la Fiscalía General de la Nación demuestran que ocho de cada diez delitos informáticos en España están relacionados con estafas a través de la tecnología, tanto a empresas como a particulares. Y de éstos, apenas el 10% de las investigaciones termina en un procedimiento judicial.

El problema es que casi todas las denuncias terminan archivadas por falta de pruebas y por la imposibilidad de identificar al cibercriminal. Aun así, los expertos recomiendan acudir a los tribunales, ya sea por la vía civil o por la penal, pero siempre teniendo en cuenta las evidencias que se pueden aportar y la dimensión o cuantía del pleito, ya que el coste no siempre compensa.

Tiempo de prescripción. En casos graves, cuando una estafa supere, por ejemplo, los 50.000 euros, el plazo para acudir a los tribunales es de diez años y el acusado se enfrenta a penas de entre uno y seis años de prisión. Para cantidades inferiores,

el delito prescribe a los cinco años y la condena puede saldarse con penas de entre seis meses a tres años.

Ciberestafas internacionales. Muchos ciberdelincuentes actúan desde el extranjero. Estas situaciones son todavía más complejas. Asegurar las pruebas y documentar todo es clave para poder acceder a los tribunales internacionales.

El objetivo de una ciberestafa es lucrativo; pero el modus operandi puede variar mucho y no siempre se logra sustrayendo dinero. La información que posee una empresa tiene un valor, en muchos casos, incalculable, y los ciberdelincuentes lo saben. El Código Penal recoge como delito el apoderamiento por medios ilícitos de secretos de empresa y su distribución no consentida. En estos casos, la acción judicial es clave, pero es necesario aportar pruebas. Ante la tentación de ceder al chantaje y no denunciar por miedo a que esa información confidencial y secreta se haga pública durante el proceso, los expertos recuerdan que un cibercriminal no es precisamente una persona de confianza y nada garantiza que no difunda los documentos en el futuro.

Perder datos confidenciales. Cuando se produce un robo de datos, hay que tener en cuenta que, más allá del perjuicio económico que pueda ocasionar, también puede tener consecuencias legales para la propia compañía afectada, ya que ella es responsable de custodiar cualquier dato personal de sus clientes o proveedores. Por ejemplo, si se produce una brecha de seguridad grave, hay que comunicárselo en un plazo máximo de 72 horas a la Agencia Española de Protección de Datos (AEPD).

Continuidad del negocio. Ocasionar daños informáticos, como borrar, alterar o secuestrar sistemas es un delito que está tipificado en el Código Penal, por lo que es fácilmente identificable y defendible ante un tribunal. Sin embargo, más allá de las herramientas legales, es recomendable contar con copias de seguridad para asegurar la continuidad del negocio. En caso contrario, y en función de la actividad, los clientes podrían presentar reclamaciones a la empresa y ésta tener que compensarlos, aunque haya sufrido un ciberataque (Deloitte 2020).

Para Adriana Ceballos, directora de desarrollo de programas del Tanque de Análisis y Creatividad de las Tic (TicTac) “la ciberseguridad es el área que mayor atención deberá tener en el 2021, pues un gran número de colaboradores seguirán operando desde sus hogares” además agregó que “el nuevo documento construido por el programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), llamado ciberseguridad en entornos cotidianos, en el que participó Claro, es precisamente, el análisis de diferentes contextos como, trabajo remoto, ciberseguridad en dispositivos móviles, ciberataques a correos electrónicos, entre otros, donde hoy en día es más necesario implementar políticas robustas de ciberseguridad”

A nivel internacional también se conocen aspectos legales que ameritan tenerlas en cuenta y que son antecedentes para futuras aplicaciones en Colombia, cuando las empresas no puedan garantizar su seguridad, tales como:

- ✓ Medidas preventivas legales (España y UE): Medidas relativas a la adecuación y cumplimiento de la legislación aplicable (LOPD y RLOPD) que incluyen, fundamentalmente, (i) el establecimiento de una circular sobre los principios generales a observar en el tratamiento de datos de carácter personal por parte de los empleados que tengan acceso a datos de carácter personal en el desempeño de sus funciones, (ii) contar con un sistema adecuado de investigación de incidencias y violaciones de seguridad de los datos.

  Solicitud de aceptación de la política de seguridad por parte de los empleados.

  Cláusulas contractuales con empleados en relación con la custodia, conservación y utilización de la información.

  Cláusulas contractuales con terceros en materia de confidencialidad.

  El establecimiento de una política de uso de medios tecnológicos, que determine el alcance del uso de los dispositivos y medios puestos a disposición del empleado por parte de la empresa y las facultades del empresario en relación con el control de la actividad de los empleados, así como las consecuencias derivadas del incumplimiento de la misma.

- ✓ Un ciberataque y la fuga de información, hoy por hoy, son uno de los más frecuentes dolores de cabeza de los empresarios en todo el mundo. Este tipo de acciones al margen de la ley, no solo generan significativos perjuicios económicos a las empresas, sino, que, a su vez, afectan negativamente su reputación, y generan cierto grado de desconfianza entre los clientes y la sociedad que a diario consume este tipo de nuevas tecnologías que mueven el comercio y la economía digital a nivel mundial.

  En España, la responsabilidad legal se define como “la obligación de toda persona de pagar por los daños y perjuicios que cause en la persona o el patrimonio de otra”, y está determinada y regulada desde el punto de vista civil (regida por el código civil) y penal (regida por el código penal).

TIPOS DE RESPONSABILIDADES FRENTE A UN CIBERATAQUE

Cuando ocurre un ciberataque en una empresa, se ponen de relieve varios escenarios, desde el punto de vista de la Responsabilidad Legal, estos, a grandes rasgos, son:

Responsabilidad penal del atacante o ciberdelincuente (particular o empresa); que será examinada en primer lugar desde el punto de vista penal y de nuestro código penal, según haya sido la conducta delictiva o delito (s) cometidos por él, o, los autores materiales e intelectual(es) para la consecución de su objetivo. Este tipo de responsabilidad está regulada en el código penal con el fin de juzgar y condenar el tipo de pena (s) o sanción (es) que deberá cumplir o pagar el ciberdelincuente.

Responsabilidad civil derivada del delito Una vez determinada la responsabilidad penal del ciberdelincuente, se procede a determinar la responsabilidad civil derivada del delito; la cual está dirigida a la materialización y cálculo de la indemnización económica que deberá pagar el ciberdelincuente a la (s) víctima (s) que ha(n) sido afectada (s) o perjudicada (s), con el fin de reparar el daño o perjuicio causado con su conducta penal.

Responsabilidad civil del empresario: El empresario, o empresa, pese a ser la victima directa de un ataque cibernético, es a su vez responsable de aquellos daños o perjuicios que dicho ataque haya podido haber causado a sus clientes; con quienes, en la mayoría de los casos existe una relación contractual (responsabilidad civil contractual) derivada de la prestación de un servicio o el manejo de información y sus datos. A su vez el empresario es responsable de dicho ciberataque frente aquellos terceros con quienes, a pesar de no tener una relación contractual, se han visto afectados por el ciberataque (responsabilidad civil extracontractual).

Responsabilidad penal de los empresarios: Los empresarios son responsables penalmente por su propia actuación u omisión, o la de un tercero del que sean responsables por la comisión un delito o ante la falta grave del deber objetivo de cuidado o incumplimiento injustificado de la normativa vigente para la protección de datos e información de sus clientes.

Responsabilidad laboral del empresario: El empresario es responsable también frente a sus propios trabajadores que hayan sido afectados con el ciberataque y está obligado a la reparación de este tipo de perjuicios.

Responsabilidad administrativa: Frente a un ciberataque, el empresario también está llamado a responder ante a las autoridades administrativas, de ser el caso, por el incumplimiento injustificado de sus deberes y obligaciones

administrativas y legales. Lo que conlleva a sanciones administrativas de tipo económico o sancionatorio, según cada caso.

Una vez detallada de forma muy general algunas de las diferentes responsabilidades en las que pueden incurrir los empresarios ante un ciberataque, es muy importante recomendar mantener las medias de seguridad y protección en materia de ciberseguridad, así como cumplir estrictamente la normativa legal y administrativa actual en materia de protección de datos y riesgos cibernéticos de las empresas, para evitar así problemas legales que nos pueden acarrear muchos dolores de cabeza. Por último, es recomendable y de vital importancia contratar una adecuada póliza de ciberriesgos que contemplé este tipo de riesgos y sus coberturas. (Deloitte 2020).

Anexo N: Etapa de Recomendaciones:

Dada la orientación y finalidad de esta metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, se procede a realizar las siguientes recomendaciones:

1. Esta metodología se puede aplicar en cualquier orden de acuerdo con lo que se establezca en el plan de actividades del grupo de trabajo que vaya a aplicar la metodología en la organización o empresa afectada por delitos informáticos o ciberataques.

2. Pueden aplicarla en el orden que tiene la metodología, la cual lleva al grupo de trabajo paso a paso y desde lo más básico hasta lo más detallado los temas tratados, esto para mejor comprensión, aplicación y efectividad en la aplicación en la empresa afectada por delitos informáticos o ciberataques.

3. Como ya se ha expresado anteriormente esta metodología se puede aplicar en dos (2) momentos:

    A. El primero cuando la empresa ya es víctima de un Ataque informáticos o ciberataques y se necesita valorar o cuantificar la afectación económica, financiera, administrativa, comercial o reputacional de la afectación.

    B. EL segundo si se requiere hacer una valoración real de los riesgos en cuanto a ataques informáticos o ciberataques que pueda sufrir la empresa de acuerdo con las vulnerabilidades y amenazas que tenga contra sus activos.

        En este segundo momento se puede tomar el resultado para:

        - Cuantificar las afectaciones que se puedan sufrir en la empresa y con base en ese estudio poder implementar planes de salvaguarda o mitigación de esos posibles ataques.

        - Para poder adquirir una póliza de seguro contra este tipo de ataques, que realmente cubra todo lo requerido en la organización y sean consecuente con el valor de la

empresa y lo que esos activos tangibles e intangibles agregan valor a la empresa.

- Para revisar, analizar la relación Costo-Beneficio entre los riesgos que se tienen en la empresa y el valor que se debe invertir para proteger y salvaguardar los activos, es decir, si vale o no la pena la inversión en pro de la protección y la ciberseguridad de la empresa u organización.

4. Si lo que desea es ir a cuantificar daños por delitos informáticos en la empresa en activos físicos y tangibles, por favor tenga en cuenta todo el "Anexo J: Etapa de Ciberataques Causantes de Pérdidas Económicas y Financieras Directas" y las fórmulas que allí se recomiendan y explican.

5. Si lo que desea es ir a cuantificar daños por delitos informáticos en la empresa en activos no físicos o intangibles, por favor tenga en cuenta todo el Anexo K: Etapa de Ciberataques Causantes de Pérdidas o Afectaciones Reputacionales (Pérdidas Económicas y Financieras Indirectas y/o Colaterales).

6. Si va a aplicar el Anexo J o en Anexo K, se sugiere que, de igual manera, tenga en cuenta el Anexo M: "Etapa de pérdidas por Leyes y Normas Nacionales e Internacionales", donde se despejan las implicaciones jurídicas o sanciones a lugar.

7. Se sugiere que todas las empresas tengan implementado un Sistema Integrado de Gestión y que entre los sistemas de gestión tenidos en cuenta este el Sistema de Gestión de la Seguridad de la Información (SGSI).

8. En lo posible toda empresa en Colombia y a nivel internacional, debe tener implementado y certificado al menos dos (2) Estándares de Seguridad, se recomiendan mínimo la Certificación en ISO 27001:2013 (SGSI) y en ISO 22301:2018 (SGCN).

9. Todos los representantes legales, gerentes generales, CEO, Miembros de Juntas directivas y las altas gerencias en todas las empresas, organizaciones, compañías o instituciones públicas y privadas, deben tener muy presente todo este tema de ciberseguridad y los riesgos a los cuales se enfrentan todos los días sus organizaciones a cargo, este es un tema que como lo manifiestan entidades, autoridades y organizaciones nacionales e internacionales es uno de los riesgos más grandes, presentes y con mayor crecimiento que se tiene en las empresas y en los países. Donde todos los

países han trasladado la guerra al ciberespacio a una guerra digital y cuando se atacan los países se va contra la infraestructura críticas de esos países, pero de igual manera contra empresas públicas y privadas de los países atacados o afectados.

10. Todas las empresas deben tener mecanismos de detección y/o contención contra estos ataques informáticos, pues estos crecen cada día, donde Según la consultora PwC (2021), el costo de no identificar al agresor de los ciberataques será de US$ 6000 M en 2021.

11. Las empresas y sus directorios deben ser conscientes de que las amenazas a la seguridad informática no solo se mantienen, sino que van en aumento en cuanto a tamaño, sofisticación y costos. Debido a ello, la necesidad de una estructura de administración y supervisión efectivas se hace cada vez más crítica y requiere de un enfoque integrador, resaltó Alejandro Rosa, socio de PwC Argentina de la práctica de Gobierno Corporativo.

12. Algunas áreas de foco que los directores, gerentes, administradores, deben incorporar a su agenda son:

    a) Considerar como clave para el negocio los riesgos de ciberseguridad.

    b) Tener un enfoque de supervisión que incluya la asistencia directa de expertos en seguridad informática y digitalización.

    c) Discutir si la estrategia y los planes de defensa contra ataques informáticos son adecuados, incluyendo la definición del riesgo tolerable.

    d) Establecer cuál es la información periódica o por excepción que necesitarán para monitorear la gestión del riesgo.

    e) Monitorear la resiliencia de la organización ante los ataques, es decir, sus capacidades para resistir y recuperarse de los eventos.

13. Las empresas y sus directorios deben ser conscientes de que las amenazas a la seguridad informática no solo se mantienen, sino que van en aumento en cuanto a tamaño, sofisticación y costos. Debido a ello, la necesidad de una estructura de administración y supervisión efectivas se hace cada vez más crítica y requiere de un enfoque integrador. Establecer un programa

efectivo y eficiente de gestión de riesgos es un camino que debe ser recorrido por la empresa, con el objetivo de mitigar los riesgos clave y lograr una organización resiliente a los ataques informáticos.

14. Se recomienda la Concientización y educación a los usuarios de todas las empresas y a todo nivel en las empresas, capacitándolos y a través de la producción de políticas de seguridad, el uso de sus sistemas de modo seguro y prácticas que incluyan mantener conciencia de los riesgos cibernéticos.

15. En todas las empresas como medida de prevención al acceso no autorizado a los sistemas y aplicaciones, se deben establecer políticas de control de acceso físico y lógico.

16. Es importante establecer un plan para estar preparados ante cualquier eventualidad. Se deben establecer responsabilidades y procedimientos.

17. Contratar ciberseguros o seguros contra delitos informáticos (Transferir el riesgo de la empresa) cuya finalidad es proteger a las entidades frente a los incidentes derivados de los riesgos cibernéticos, el uso inadecuado de las infraestructuras tecnológicas y las actividades que se desarrollan en dicho entorno. Así, las principales garantías ofrecidas por el mercado asegurador son las siguientes:
    - ✓ Responsabilidad civil frente a terceros perjudicados.
    - ✓ Cobertura de los gastos materiales derivados de la gestión de los incidentes.
    - ✓ Cobertura de las pérdidas pecuniarias ante la interrupción de la actividad derivada de un fallo de seguridad y/o sistemas.
    - ✓ Cobertura de los gastos de asesoramiento legal en los que se debe incurrir para hacer frente a los procedimientos administrativos.
    - ✓ Cobertura ante la denegación de acceso a otros sistemas.
    - ✓ Acompañamiento en la gestión de la crisis.

    Estos seguros suelen venir acompañados de servicios adicionales tales como son:
    - La desaparición de huellas e historial.
    - La reparación de sistemas y equipos.
    - La recuperación de datos.
    - La descontaminación de virus.

Nota: *Se recomienda cuantificar bien los activos de las empresas antes de asegurarlos, de esta manera se traslada el riesgo de la empresa a la aseguradora y en los montos correctos.*

18. Una vez detallada de forma muy general algunas de las diferentes responsabilidades en las que pueden incurrir los empresarios ante un ciberataque, es muy importante recomendar mantener las medias de seguridad y protección en materia de ciberseguridad, así como cumplir estrictamente la normativa legal y administrativa actual en materia de protección de datos y riesgos cibernéticos de las empresas, para evitar así problemas legales que nos pueden acarrear muchos dolores de cabeza. Por último, es recomendable y de vital importancia contratar una adecuada póliza de ciberriesgos que contemplé este tipo de riesgos y sus coberturas.

19. Dado a la impredecibilidad y a la constante evolución de los ataques cibernéticos, es imperativo la continua evaluación y gestión de riesgo. Ahora, más que nunca, es el momento de:

    ● Analizar las áreas de negocio y los procesos de la empresa potencialmente expuestos.

    ● Identificar los riesgos y proponer los mecanismos de control y mitigación necesarios.

    ● Discutir las opciones disponibles con un ejercicio de costo-beneficio para transferir o asumir los riesgos identificados, según el apetito de riesgo y la capacidad de absorción disponible.

    ● Preparar la necesaria información para la transferencia, en los mercados nacionales e internacionales y por vías tradicionales o alternativas, si fuese necesario.

Ante este tipo de ciberataques, ya no sólo corresponde hablar de prevención o de aseguramiento. Éstos últimos son imprescindibles, pero no suficientes. Toca hablar de resiliencia, dando por hecho que el riesgo se va a manifestar y disponiendo de todas las estrategias a nuestro alcance para mitigarlo, gestionarlo y superarlo.

Anexo O: Etapa de Conclusiones:

Como conclusiones a toda esta metodología se puede expresar lo siguiente:

- ✓ Esta versión inicial de la metodología para cuantificar las pérdidas económicas y financieras de una empresa tanto a nivel nacional o internacional, cuando es afectada por Ciberataques o Ataques Informáticos, se ofrecerá y se aplicará en varias empresas en Colombia y a nivel internacional, con la finalidad de ir ajustándola cada día y se puede llegar a una versión plenamente reconocida en Colombia y a nivel Internacional. Los aportes y recomendaciones de las personas, empresas y autoridades que la pongan en práctica, enriquecerán esta metodología en favor de la sociedad y las empresas.

- ✓ Esta metodología se puede utilizar para valorar o cuantificar las afectaciones en cuanto a temas económicos, financieros, administrativos, comerciales y reputaciones en las empresas víctimas de ataques informáticos o Ciberataques a nivel internacional. Teniendo en cuenta los activos físicos, no físicos, tangibles e intangibles de las organizaciones y que le generan valor a estas empresas e instituciones públicas, privadas nacionales e internacionales.

- ✓ La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida (BID 2021).

- ✓ Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y el suministro de agua y energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales (BID 2021).

- ✓ Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel

agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB (BID 2021).

- ✓ En un sentido más general, en la última década, los ataques cibernéticos han aumentado en frecuencia e ingenio. El bajo costo y el riesgo mínimo que conllevan estos delitos han sido factores clave en su crecimiento. Con el simple uso de una computadora y el acceso a Internet, los ciberdelincuentes pueden causar daños enormes mientras permanecen relativamente anónimos. (OEA 2021).

- ✓ Tanto las personas como las instituciones están expuestas a la incertidumbre y la impredecible naturaleza del delito cibernético. Por lo tanto, es imprescindible abordar estas amenazas. Los esfuerzos para hacerlo deben ser de naturaleza multidimensional, porque se requiere una variedad de factores para construir una cibersociedad resistente. Las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad civil, así como los sectores público y privado, deben trabajar para crear una cultura de ciberconciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad; por lo tanto, es un esfuerzo continuo y complejo (OEA 2021).

- ✓ Dado el aumento de los ciberataques, la OEA y el BID han visto necesario implementar nuevamente el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés) a fin de poder medir el crecimiento y el desarrollo de las capacidades de nuestros Estados Miembros para defenderse de las crecientes amenazas del espacio cibernético.

- ✓ Los analistas apuntan que cerca del 90 % de los ciberataques que sufren las empresas en Colombia se deben a la ingeniería social, que obedece a técnicas de engaño para conseguir información confidencial, con la que luego suplantan identidades, falsifican correos, entre otras actividades maliciosas.

- ✓ En Colombia, el monto promedio de las cifras de pérdidas por ataque a empresas varía entre los 300 millones y 5.000 millones de pesos (Csirt Ponal y Csirt Financiero (2020).

- ✓ De acuerdo con Flabio Rodríguez Correa, coordinador de Riesgos y Arquitectura de Claro, y quién participó en el estudio, “en el CSOC -Centro de Operaciones de Ciberseguridad de Claro, por sus siglas en español- ubicado en el Data Center Triara de Claro, se han gestionado en lo que va del año 2020, en promedio, más de cuatro millones de eventos de seguridad al mes, protegiendo servicios propios y de otras compañías, además de la confidencialidad de la información y datos personales de todos los clientes y usuarios”.

- ✓ En Colombia, el delito que mayores denuncias presentó fue la suplantación de sitios web para capturar datos personales con un crecimiento del 372% comparado con el 2019. Este delito tiene una relación directa con modalidades conocidas, tales como el Phishing, Spoofing y Pharming que sufrieron las empresas. Adicionalmente, hubo 3.800 casos denunciados donde este tipo de ataques fueron utilizados por los cibercriminales para capturar datos personales o dispersar malware en las redes corporativas.

- ✓ Estos ciberataques afectaron por igual diferentes sectores productivos del país, los métodos de propagación continúan siendo las campañas de phishing que contienen archivos adjuntos maliciosos. Las entidades de gobierno con mayor presencia de trámites en línea también se vieron afectadas, entre ellos, la Administración de Impuestos y Aduanas, la Registraduria Nacional del Estado Civil, la Fiscalía General de la Nación y las autoridades de tránsito que en su orden han sido las instituciones mayormente suplantadas.

- ✓ Evitar el cibercrimen es un trabajo que implica esfuerzos desde la empresa, las entidades de control, y por supuesto la Policía Nacional, que cuenta con el Centro de Capacidades para la Ciberseguridad de Colombia “C4” y hacen un constante seguimiento a este tipo de casos.

- ✓ Actualmente, resulta imposible crear un entorno informático inaccesible a delincuentes informáticos, aunque si se puede constituir un entorno preventivo que dificulte el acceso a los hackers.

- ✓ El momento en el que se detecta un incidente de fuga de información es un momento crítico en cualquier entidad. Una buena gestión de la fase de detección del ataque informático puede suponer una reducción significativa del impacto del ataque. Esta fase es muy importante, ya que muchas veces se tiene conocimiento de la irrupción una vez la información sustraída se revela al público o a la red, o el ciberdelincuente se pone en contacto con el

despacho de abogados correspondiente, para revenderles la información, extorsionarles o amenazarles.

- ✓ A las empresas se les recomienda, apoyarse en terceros expertos independientes que puedan ayudarnos tanto en el desarrollo de todo el proceso, desde el desarrollo de políticas internas, como en la custodia de información, como a la hora de actuar ante alguno de los incidentes expuestos.

- ✓ Un ciberataque y la fuga de información, hoy por hoy, son uno de los más frecuentes dolores de cabeza de los empresarios en todo el mundo. Este tipo de acciones al margen de la ley, no solo generan significativos perjuicios económicos a las empresas, sino, que, a su vez, afectan negativamente su reputación, y generan cierto grado de desconfianza entre los clientes y la sociedad que a diario consume este tipo de nuevas tecnologías que mueven el comercio y la economía digital a nivel mundial.

- ✓ Se espera que el costo global de los ataques informáticos pase de US$ 3 mil millones en 2015 a US$ 6 mil millones en 2021, según un estudio realizado en 2017 por el grupo CyberSecurity Ventures and Herjavec.

- ✓ No suele haber un inventario de los activos digitales de las empresas: sólo el 37% de los directores considera que la empresa identificó sus activos digitales más valiosos y sensibles.

- ✓ Las empresas tienen políticas de “higiene informática endebles: el 93% de los ataques podrían ser prevenidos con mejores políticas (actualizaciones de software, bloqueo de mails sospechosos, capacitación digital sobre phishing, etc.). Las amenazas a la seguridad informática están en todos lados y los ataques producen titulares cada vez más a menudo. También son muy costosos, tanto en dinero como en pérdida de reputación.

- ✓ Los costos de la “ciberdelincuencia incluyen daños y destrucción de datos, robo de dinero y propiedad intelectual, pérdida de productividad, malversación, fraude, daño a la reputación e interrupción del curso normal de los negocios. Su restablecimiento demanda normalmente de una investigación detallada (“forense”), restauración de datos y de sistemas atacados, y de una reorganización general de todas las áreas de la empresa.

- ✓ Además, la combinación de las consecuencias económicas y del daño reputacional, es a menudo fatal: Según datos de la National Cyber Security

Alliance de EE.UU. el 60% de las PYME desaparece dentro de los seis meses siguientes a sufrir un ciberataque.

Anexo P: Documentación y Referencias Adicionales:

Existe mucha documentación y referencias adicionales al respecto de este tema y ya cada persona va de acuerdo con su necesidad, empresas e intereses, mirando cual le parece más pertinente y adecuada.

Acá se presenta un listado de documentos que se consideran pertinentes para este tema:

1. Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Documento de la OEA y el BID a 2021. Ciberseguridad (observatoriociberseguridad.org)

2. Informe Global de Amenazas de CrowdStrike® 2021. Informe Global de Amenazas de CrowdStrike 2021

3. Tendencias del Cibercrimen en Colombia 2019-2020. Tendencias del Cibercrimen en Colombia 2019-2020 - CCIT - Cámara Colombiana de Informática y Telecomunicaciones

4. Reporte de Delitos Informáticos. Policía Nacional de Colombia. Ciberseguridad | Policía Nacional de Colombia (policia.gov.co)

5. Análisis jurídico de la Ley 1273 de 2009 en Colombia. 2020_analisis_delitos_informaticos.pdf (ucc.edu.co)

6. Informe Tendencias Cibercrimen Colombia 2019 -2020. ::Evaluamos - Periodismo de Código Abierto::

7. Entre la Actualidad y las Buenas Prácticas Digitales. Mayo de 2020. Interlat Digital Enterprise Intelligence. (E-Book). EBOOK MAYO 7 INTERLAT 2020 (yumpu.com)

8. Ciberdefensa y ciberseguridad en el Sector Defensa de Colombia. Universidad Piloto. 2015. http://polux.unipiloto.edu.co:8080/00002590.pdf.

9. COLOMBIA: ¿Es un Estado efectivo en términos de seguridad digital con énfasis en el sector privado? Universidad Javeriana. 2019. https://repository.javeriana.edu.co/bitstream/handle/10554/46540/TRABAJO%20DE%20GRADO.pdf?sequence=1&isAllowed=y

10. Análisis de vulnerabilidades. https://ciberseguridad.com/servicios/analisis-vulnerabilidades/

11. Guía Metodológica de Pruebas de Efectividad. MinTic Colombia. https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

12. Guía de gestión de riesgos. MinTic Colombia. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

13. Ciberataques a tu empresa, ¿Qué puedes hacer para evitarlos? https://ticnegocios.camaravalencia.com/servicios/tendencias/ciberataques-a-empresa-que-hacer-para-evitarlos/

14. CYBER RISK APPETITE: Defining and Understanding Risk in the Modern Enterprise. https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf

15. CYBERTHREAT REAL-TIME MAP. Kaspersky. https://cybermap.kaspersky.com/

16. ¿Miedo a los ataques internos? Así puedes defender tu empresa. Panda a WatchGuard Branch. https://www.pandasecurity.com/es/mediacenter/seguridad/ataques-internos/

17. Tipos de ataques informáticos y previsiones para el 2021. Fortinet 2021. https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2021/

18. 6 ataques informáticos a objetivos gubernamentales y empresariales en EE.UU. CNN 2021. https://cnnespanol.cnn.com/2021/05/31/6-ataques-informaticos-ee-uu-orix/

19. La información es su activo más valioso. Claro 2021. https://www.claro.com.co/negocios/todo-claro/noticias-interes/seguridad-informatica/

Apéndice A.

Organismos nacionales e internacionales de apoyo en ciberseguridad, Roles y perfiles Interno y Externos a las empresas, para ciberseguridad:

Organismos y organizaciones nacionales de apoyo en ciberseguridad:

- ✓ *Csirt Financiero:* Es el equipo de apoyo para la respuesta a incidentes cibernéticos sectorial, comunidad de intercambio y centro de excelencia en investigación y colaboración gremial para anticipar y mitigar riesgos derivados de amenazas cibernéticas, así como, apoyar la respuesta de los incidentes bajo una visión global. https://csirtasobancaria.com/

- ✓ *Csirt Ponal:* Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones. https://cc-csirt.policia.gov.co/

- ✓ *ColCERT:* Actualmente, el colCERT es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa y tiene como misión la protección de la infraestructura crítica del Estado Colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. http://www.colcert.gov.co/

- ✓ *CAI Virtual Policía Nacional – Centro Cibernético Policía Nacional*: Primera iniciativa en Iberoamérica en atención en línea policial. https://caivirtual.policia.gov.co/#servicios

- ✓ *Comando Conjunto Cibernético de las Fuerzas Armadas de Colombia*: El Comando Conjunto Cibernético de las Fuerzas Armadas de Colombia planea y conduce operaciones militares en el ciberespacio, para contrarrestar amenazas y ataques en Internet. https://www.ccoc.mil.co

- ✓ *Ministerio de Tecnologías de la Información y Comunicaciones*: El Ministerio de Tecnologías de la Información y las Comunicaciones es un ministerio

de Colombia encargado de las tecnologías de la información y la comunicación. El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones y a sus beneficios. https://www.mintic.gov.co/portal/inicio/

- ✓ *Ministerio de Defensa:* El Ministerio de Defensa Nacional, es la máxima autoridad en materia de defensa, seguridad y asuntos militares de la República de Colombia; formula, diseña, desarrolla y ejecuta las políticas de defensa y seguridad nacionales; conduce la Fuerza Pública, conformada por las Fuerzas Militares, y la Policía Nacional. Funciones del Ministerio. https://www.mindefensa.gov.co/irj/portal/Mindefensa

Organismos y organizaciones Internacionales de apoyo en ciberseguridad:

- ✓ *Centro de Ciberseguridad Industrial:* El CCI ha conformado el mayor ecosistema de organizaciones industriales (usuarios finales), proveedores de servicios y soluciones de ciberseguridad industrial, ingenierías, integradores, organizaciones públicas; pero, sobre todo, a sus profesionales. https://www.cci-es.org/

- ✓ *OEA – Programa de Ciberseguridad***:** El programa de Ciberseguridad del CICTE está consolidado como líder regional en la provisión de iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de ciberseguridad en las Américas. El programa se centra en 3 pilares: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), e investigación y divulgación. http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

- ✓ *ICTE es el Comité Interamericano contra el Terrorismo – Programa Ciberseguridad***:** CICTE es el Comité Interamericano contra el Terrorismo. Es la única entidad regional que tiene como propósito prevenir y combatir el terrorismo en las Américas. CICTE fomenta la cooperación y el diálogo entre los Estados Miembros para contrarrestar el terrorismo, de acuerdo con los principios de la Carta de la OEA, con la Convención

Interamericana contra el Terrorismo, y con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional. http://www.oas.org/es/sms/cicte/default.asp

- ✓ *Instituto Nacional de Ciberseguridad (INCIBE):* INCIBE trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España. El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional. https://www.incibe.es/

- ✓ *Agencia Europea de Seguridad de las Redes y de la Información (ENISA, en sus siglas en inglés) (Europa):* Es un centro que ayuda a la Unión Europea y a sus Estados miembros a estar mejor preparados para prevenir, detectar y dar respuesta a incidentes de seguridad de la información mediante la sinergia y la cooperación entre Estados. https://www.enisa.europa.eu/

- ✓ *Centro de Excelencia de la OTAN para la Ciberdefensa (NATO CCD COE, por sus siglas en inglés):* Con sede en Tallin, Estonia. Es una organización militar internacional cuya misión es aumentar la capacidad, cooperación y transmisión de información entre los Estados miembros de la OTAN y sus aliados en el ámbito de la ciberdefensa a través de la educación, la investigación, las lecciones aprendidas y el diálogo. https://ccdcoe.org/

- ✓ *Naciones Unidas: Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC):* Con sede en Viena, Austria, y a través de la creación en 2014 de un Grupo de Expertos sobre Ciberseguridad. La mayor organización internacional es consciente del papel relevante que tiene en la importancia de mantener la seguridad en la red y la protección de la información. https://ccdcoe.org/

Roles, perfiles y áreas Internas en las empresas, para ciberseguridad**:**

- ✓ *NOC:* Un NOC (Network Operations Center) es un centro de operaciones de Red, también conocido por otro nombre dentro de los administradores de sistemas de nuestro país como Centro de Control de Red (CCR). Como su propio nombre indica es un sitio especializado en el control de las redes de comunicación, ya sean de Internet, televisión o satélites, y en general cualquier otro tipo de red local o nacional. Evidentemente no hay solo un CCR o NOC, sino muchos repartidos estratégicamente por el ancho y largo de cada país. Algunos son propiedad del estado, otros son privados (la mayoría) y en casi todos los ámbitos están gestionados por los ISP de dicho país (menos inteligencia y sistemas de investigación).

- ✓ *SOC***:** Las siglas en ingles SOC (Security operation Center) se refieren a los Centros de Operaciones de Seguridad. Su función principal es el monitoreo, seguimiento y análisis de las actividades de las redes de datos, servidores, bases de datos, aplicaciones, sitios web entre otros, con el fin de identificar actividades anómalas que puedan indicar incidentes o compromisos de seguridad informática.

- ✓ *CISO***:** La persona responsable de velar por la ciberseguridad de una empresa es el CISO (Chief Information Security Officer). También podemos conocerlo como director de seguridad de la información. Esta persona es la que se encarga de proteger la información ante posibles ciberataques y fugas de datos. De esta manera, garantiza la seguridad dentro de las posibilidades tanto humanas, técnicas como económicas que tenga cada empresa. Podemos decir que el CISO es un ejecutivo de alto nivel responsable de alinear las iniciativas de seguridad de un negocio. Con el avance tecnológico, la transformación digital y el uso de la nube, el CISO ha dejado de ser un profesional técnico al margen de la estrategia empresarial, y ha tenido que incorporarse en los procesos de negocio de las empresas.

- ✓ *CIO***:** Son muchos los puestos que se han convertido en fundamentales dentro del organigrama actual de las empresas, pero no hay duda que uno de los principales es el del CIO (Chief Information Officer). Este profesional ha llegado a tener una importancia extrema en cualquier tipo de empresa que quiera estar preparada para exprimir la manera

en la que la tecnología de la información se aprovecha dentro de la unidad de negocio. Las responsabilidades del CIO están directamente relacionadas con el trabajo codo con codo con el CEO, al cual reportan de sus acciones y de los progresos realizados dentro de la empresa.

- ✓ *Administrador de sistemas*: El administrador de sistemas es en realidad una de las profesiones más importantes en el camino hacia una carrera en ciberseguridad. CyberSeek, un sitio que proporciona una variedad de información acerca de la planificación de carrera en ciberseguridad, ubica el rol del Sysadmin en el área de profesionales que se dedican a las redes informáticas y como una posición que funciona como la puerta de entrada para ocupar posiciones más específicas en el campo de la seguridad. Esto significa que los administradores de sistemas no se describen estrictamente como profesionales de la ciberseguridad. Sin embargo, necesitan tener importantes conocimientos en seguridad para realizar su trabajo correctamente, tal como lo explican los mandamientos de seguridad que debe tener presente en su trabajo un Sysadmin.

  Los administradores de sistemas son indispensables para la mayoría de las empresas, ya que son responsables de la configuración, mantenimiento, operación y seguridad de los sistemas informáticos y servidores, así como de solucionar problemas y brindar apoyo a otros empleados. Si estás buscando convertirte en administrador de sistemas, algunos de los principales requisitos son el conocimiento de Linux y de los principales hardware de red, ingeniería de redes y soporte técnico. Para poder realizar una transición exitosa a la ciberseguridad, recomendamos que agregues sistemas y seguridad de la información, seguridad de redes y operaciones de seguridad a tu arsenal de habilidades.

- ✓ *Incident responder o Analistas de Seguridad*: Quienes ocupan la posición de respuesta ante incidentes de seguridad —que como ocurre muchas veces en el campo de la seguridad suele hacerse referencia a estas posiciones bajo el título en inglés: Incident responder— son responsables de investigar, analizar y responder a los ciberataques o incidentes cibernéticos. Sin embargo, su posición no solo es reactiva, sino que también deben monitorear activamente los sistemas y redes para detectar intrusiones, realizar auditorías de seguridad y desarrollar planes de respuesta, así como conocer los planes de continuidad del negocio de la empresa si se produce un ataque exitoso.

Una vez finalizado un ataque, quien ocupe esta posición también debe ser capaz de redactar un reporte acerca del incidente en el que se explique con cierto detalle cómo ocurrió el ataque y qué medidas se pueden adoptar para evitarlo en el futuro. Para convertirse en un Incident responder no es necesario un título; sin embargo, contar con una titulación de grado en seguridad o en informática probablemente sea un beneficio.

Entre las principales habilidades y conocimientos que los empleadores suelen solicitar para ocupar esta posición aparece conocimiento de Linux, Unix, seguridad de redes, sistemas de información, y gestión de proyectos. El puesto está clasificado como de nivel de entrada y, según CyberSeek, en la descripción de las ofertas de trabajo los títulos más comunes pueden ser analista senior en seguridad, técnico especialista en redes, entre otros.

- ✓ *Analista forense digital*: Los especialistas en informática forense pueden describirse como los detectives del ciberespacio. Son responsables de investigar diversas violaciones de datos e incidentes de seguridad, recuperar y examinar datos almacenados en dispositivos electrónicos y reconstruir sistemas dañados para recuperar datos perdidos. También se espera que los especialistas forenses ayuden a las autoridades a evaluar la credibilidad de los datos y proporcionen asesoramiento experto a los profesionales del derecho cuando se utilicen pruebas electrónicas en un caso legal.

  Para convertirse en un especialista forense digital es imprescindible una licenciatura en ciberseguridad o informática, e incluso es muy valorado contar con una maestría en informática forense. Algunas de las habilidades solicitadas por los empleadores incluyen el dominio de la informática forense, conocimientos en el campo de la seguridad de la información y la capacidad de analizar la electrónica de consumo y los discos duros.

- ✓ *Pentester*: Los pentester son la antítesis de los hackers de sombrero negro. La labor principal de quienes se dedican a realizar pruebas de penetración es analizar sistemas y encontrar vulnerabilidades que puedan explotarse para obtener acceso a los sistemas informáticos. Sin embargo, lo que los distingue de un criminal es que lo hacen legalmente (a instancias de sus empleadores) para identificar las debilidades que deben solucionarse y las fortalezas que deben

mantenerse. Esto permite a las empresas ajustar sus entornos en consecuencia.

El pentester es un rol de nivel medio y requiere que el posible candidato tenga sólidos conocimientos en seguridad de la información y sea capaz de manejar una variedad de lenguajes de programación, como Java o Python. Vale la pena mencionar que los pentester pueden complementar sus ingresos a través de los programas de bug bounty; algunos incluso pueden optar por seguir este camino como carrera a tiempo completo.

- ✓ *Ingeniero en ciberseguridad*: La razón por la que el puesto de ingeniero en ciberseguridad aparece al final de esta lista es que es el más avanzado del grupo. Esta función requiere al menos una licenciatura en informática o en seguridad y el posible candidato debe tener un alto nivel de competencia en detección, análisis y protección de amenazas.

  Los ingenieros en ciberseguridad deben ser creativos y técnicos, ya que algunas de sus responsabilidades incluyen la creación de procesos que resuelvan problemas de seguridad en la producción, la realización de pruebas de vulnerabilidad e incluso el desarrollo de scripts de automatización que ayudarán a manejar y rastrear incidentes. También son responsables de configurar, instalar y mantener los sistemas de seguridad y de detección de intrusiones. Para gestionar todas las obligaciones que conlleva el puesto, los ingenieros en ciberseguridad deben ser competentes en seguridad de la información y la red, así como tener sólidos conocimientos en criptografía.

Apéndice B.

Leyes, Normas y referentes legales nacionales e Internacionales en Ciberseguridad y Seguridad de la Información:

- Nacionales:

  - ✓ *CONPES 3701*.

  - ✓ *Ley 1273 de 5 de enero de 2009*, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Diario Oficial nº 47.223).

  - ✓ *Ley 1341 de 30 de julio de 2009*, sobre principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones (Diario Oficial nº 47426 de 30 de julio de 2009). (Deroga el Artículo 51 de la Ley 1978 de 25 de julio de 2019 el Artículo 66 de la Ley 1341 de 2009). (Declarada exequible por la Sentencia C-127 de 2020 de la Corte Constitucional).

  - ✓ *Ley 1621 de 2013* (Marco jurídico que para desempeño de funciones de los organismos de inteligencia y contrainteligencia & Protección a las bases de datos).

  - ✓ *Decreto 0032 de 2013* (Creación de la Comisión Nacional Digital y de Información Estatal).

  - ✓ *Decreto 045 de 15 de enero de 2021*. "Por el cual se derogan el Decreto 704 de 2018 y el artículo 1.1.2.3. del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

  - ✓ *Directiva Presidencial nº 03 de 15 de marzo de 2021*. Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.

  - ✓ *Proyecto de Ley Estatutaria nº de 2018*, por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del Hábeas Data con relación a la información financiera,

crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- ✓ *Ley 1928 de 24 de julio de 2018*, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

- ✓ *Decreto 1078 de 26 de mayo de 2015*, "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". (Artículo 1.1.2.3 derogado por el Artículo 1 del Decreto 045 de 15 de enero de 2021).

- ✓ *Ley 1712 de 6 de marzo de 2014*, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones. (Diario Oficial nº 49.084 de 6 de marzo de 2014).

- ✓ *Resolución 146 de 8 de mayo de 2014* del Grupo de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

- ✓ *Decreto 886 de 13 de mayo de 2014*. Reglamenta el Registro Nacional de Bases de Datos, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.

- ✓ *Proyecto de Ley de abril de 2011* por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet.

Internacionales:

- ✓ *Naciones Unidas "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos -2019*" - El presente informe se ha preparado en cumplimiento de la resolución 73/187 de la Asamblea General, titulada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos". En esa resolución, la Asamblea General solicitó al secretario general que recabara las opiniones de los Estados Miembros sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y que presentara un informe basado en esas opiniones para examinarlo en su septuagésimo cuarto período de sesiones.

- ✓ *Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest)*: El Convenio de Budapest es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos, cuyo objetivo es establecer una legislación penal y procedimientos comunes entre sus Estados Parte. Está considerado como un referente obligado en los esfuerzos de la Comunidad Internacional para fortalecer el Estado de Derecho en el ciberespacio.

  I. Antecedentes Generales
  a. Origen
  El Convenio sobre Ciberdelincuencia es un acuerdo internacional destinado a combatir los ciberdelitos, o los delitos cometidos por medio de Internet. Busca establecer una legislación penal y procedimientos comunes entre los países miembros del Consejo de Europa y los invitados a participar en el mismo.

  b. Objetivos
  Su principal objetivo es llegar a establecer una política penal común para proteger a la comunidad internacional frente a la cibercriminalidad. Junto al propósito de lograr una legislación específica, también busca la creación de nuevos mecanismos de cooperación transnacional frente a los delitos cibernéticos.

  c. Contenido
  En consideración a la emergencia de amenazas cibernéticas y la especificidad de nuevos delitos, este instrumento internacional entrega una clasificación propia, organizada en cuatro vectores principales:
    - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos;
    - Delitos informáticos;
    - Delitos relacionados con el contenido (como, por ejemplo, delitos relacionados con la pornografía infantil); y
    - Delitos relacionados con infracciones a la propiedad intelectual.

- ✓ *OEA*: En el marco regional, la Organización de los Estados Americanos (OEA) realizó una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, en el que el

organismo reconoce la necesidad de desarrollar una cultura cibernética en las Américas; idear medidas de prevención eficaces para prever, tratar y responder ataques cibernéticos, entre otros métodos contra el cibercrimen. Igualmente se siguen los lineamientos de las recomendaciones para instaurar una red hemisférica de CSIRT y el intercambio eficaz de información entre estados miembros. Los distintos estados de la región han introducido distintas regulaciones para contrarrestar la ciberdelincuencia y hacer más seguros sus espacios cibernéticos, sin embargo, siempre está
presente el peligro de que sus legisladores propongan iniciativas que atenten a los derechos humanos.

Anexo 02: Encuesta aplicada a las empresas.

Ciberseguridad en las empresas publicas y privadas, en colombia y a nivel internacional.(Valoración del Daño Informático).

Encuesta para mirar la percepción, cultura, inversión, afectaciones en las empresas publicas y privadas; en colombia y a nivel internacional.

De igual manera identificar las afectaciones sufridas por delitos informáticos o ciberataques en estas empresas, organizaciones e instituciones y la forma como cuantifican o valoran estas afectaciones desde el punto de vista económico, financiero y reputacional.

Esta información será un insumo, para un proyecto de grado del MBA en Administración en la Universidad Eafit (Medellin - Colombia).

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES:
En cumplimiento de las disposiciones de la Ley 1581 de 2012 y del Decreto reglamentario 1377 de 2013 que desarrollan el derecho de habeas data, solicitamos su autorización para que el autor de este proyecto de grado del MBA en Administración de la Universidad EAFIT (Medellín) y la Universidad EAFIT de Medellin, en calidad de Responsables del Tratamiento pueda recopilar, almacenar, archivar, copiar, analizar, usar y consultar los datos que se señalan a continuación. Estos datos serán recolectados por el autor del proyecto de grado y la Universidad con las siguiente finalidad, relacionada con las actividades de la universidad y el ejercicio de su objeto y sus actividades:

1) Utilizar la información adquirida como insumo para un proceso pedagógico, demás objetivos educativos y académicos establecidos por la Universidad, específicamente dentro del MBA en Administración en la sede de Medellín (Colombia).

Muchas gracias por su tiempo y por aportarnos esta información, esencial para nuestro ejercicio académico y su posterior aplicación al servicio de la sociedad.

*Obligatorio

1. Correo *

2. Por favor especificar su edad, en cual de los siguientes rangos se ubica. *

   Marca solo un óvalo.

   - ◯ 18 a 30 años.
   - ◯ 31 a 45 años.
   - ◯ 45 a 60 años.
   - ◯ Mas de 60 años.

3. Ciudad de residencia: *

4. Pais de residencia: *

5. Profesión: *

6. Labora actualmente o ha laborado en los últimos tres (3) años. *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

7. La empresa, organización o institución en la cual labora o laboró, es de tipo: *

Marca solo un óvalo.

- ◯ Publica
- ◯ Privada
- ◯ Mixta

8. Que clasificación posee la empresa, organización o institución en la cual labora o laboró: *

Marca solo un óvalo.

- ◯ Microempresa
- ◯ Pymes
- ◯ Empresa Grande
- ◯ Multinacional
- ◯ Otro: _____

9. A que sector se dedica la empresa: *

Marca solo un óvalo.

- ◯ Manufactura
- ◯ Comercio al por mayor
- ◯ Comercio al detal
- ◯ Educación
- ◯ Servicios
- ◯ Gobierno
- ◯ Salud
- ◯ Bancario y/o Financiero
- ◯ Fuerza Publica o Fuerzas Armadas
- ◯ Seguros y/o Aseguradoras
- ◯ Derecho y/o Jurídica.
- ◯ Otro: _____

10. Cargo que desempeña o desempeño en su ultima empresa: *

_____

11. Su cargo en la empresa, es de tipo: *

Marca solo un óvalo.

- ◯ Gerencial
- ◯ Directivo
- ◯ Mandos medios
- ◯ Ejecutivo
- ◯ Asesor
- ◯ Consultor
- ◯ Operativo - Trabajador
- ◯ Otro: _____

12. Sabe si la empresa tiene, ofrece o utiliza servicios en linea:

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

13. Conoce usted los riesgos a los cuales se exponen las empresas y personas, al interactuar o utilizar servicios en linea en el ciberespacio o Internet. *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

14. Conoce usted, si empresas para las cuales usted ha trabajado o trabaja han sido victimas de ataques informáticos o ciberataques. *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

15. Si su respuesta a la anterior pregunta fue "Si" o "Tal Vez", por favor podría definir que tipo de afectación sufrió la empresa afectada o atacada. *

Marca solo un óvalo.

- En la operación de la empresa
- En los servicios ofrecidos por la empresa
- Robo de información
- Perdida de confidencialidad o privacidad de la información
- Perdida en la Integridad o calidad de la información de la empresa
- Perdida de la Disponibilidad de la información o los servicios de la empresa
- Reputacionales por noticias falsas (Fake News)
- Contra personas de la empresa
- Contra equipos, elementos o activos de la empresa
- Suplantaciones
- Secuestro de información o sistemas de la empresa
- Otro tipo de afectación
- No conozco o conocí el detalle del Ataque Informático o Ciberataque.

16. Conoce usted, algún caso donde una empresas ha sido victimas de ataques informáticos o ciberataques. *

Marca solo un óvalo.

- Sí
- No
- Tal vez

17. Si su respuesta a la anterior pregunta fue "Si" o "Tal Vez", por favor podría definir que tipo de afectación sufrió la empresa afectada o atacada. *

Marca solo un óvalo.

- En la operación de la empresa
- En los servicios ofrecidos por la empresa
- Robo de información
- Perdida de confidencialidad o privacidad de la información
- Perdida en la Integridad o calidad de la información de la empresa
- Perdida de la Disponibilidad de la información o los servicios de la empresa
- Reputacionales por noticias falsas (Fake News)
- Contra personas de la empresa
- Contra equipos, elementos o activos de la empresa
- Suplantaciones
- Secuestro de información o sistemas de la empresa
- Otro tipo de afectación
- No conozco o conocí el detalle del Ataque Informático o Ciberataque.

18. Por favor podría usted, indicarnos el nombre de la empresa que fue afectada y que usted hace referencia como caso conocido de ataques por delitos informáticos o ciberataques. *

_____

19. Para usted, es importante que las empresas estén protegidas contra ataques informáticos o ciber ataques. *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

20. Es una escala de uno (1) a cinco (5), donde 1 es "No tan Importante" y 5 "Demasiado Importante" . Que valor asignaría usted a las protecciones e inversiones en protección en ciberseguridad en su empresa. *

Selecciona todos los que correspondan.

- ☐ 1 - No tan importante
- ☐ 2- ligeramente importante
- ☐ 3 - Importante
- ☐ 4 - Muy importante
- ☐ 5 - Demasiado Importante

21. En su profesión o cargo en la empresa, tiene alguna relación con seguridad informática o ciberseguridad *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

22. Usted en su empresa es consciente y conoce las vulnerabilidades, amenazas y riesgos en cuanto a ataques informáticos o ciberataques , que pueden presentarse y/o afectarlos. *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

23. Sabe si su empresa tiene implementado algún Sistemas de Gestión de Seguridad de la Información (SGSI). *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

24. Sabe usted si su empresa está en proceso de certificación o fue certificada en alguna norma o estándar nacional o internacional de seguridad de la información o ciberseguridad.

Marca solo un óvalo.

- Sí
- No
- Tal vez

25. Sabe usted como medir, valorar o cuantificar el impacto económico, financiero, comercial y reputacional que pueden afectar a su empresa si llegan a ser victimas de un ataque informático o ciberataque. *

Marca solo un óvalo.

- Sí
- No
- Tal vez

26. Sabe usted si en su empresa o familia poseen o tienen contratados seguros o pólizas de seguros, que los amparen si llegan a ser victima de ataques informáticos o ciberataques *

Marca solo un óvalo.

- Sí
- No
- Tal vez

27. Conoce usted que existen seguros o pólizas de seguros que lo protegen a usted, su familia y a su empresa ante caso de delitos informáticos o ciberataques. *

Marca solo un óvalo.

- Sí
- No
- Tal vez

28. Conoce usted en su pais y de acuerdo a las leyes en su pais, cuando le corresponde pagar o resarcir por el daño causado, a un ciberdelincuente que lo afecta a usted o a su empresa a través de un delito informático o ciberdelito. *

Marca solo un óvalo.

- Sí
- No
- Tal vez

29. Le gustaría conocer y contar con una Metodología que le permita a usted, a su empresa, a los jueces, a las autoridades del pais, a sus asesores jurídicos, como además a las empresas auguradoras; poder cuantificar, valorar científicamente, de manera exacta y real; las afectaciones sufridas por ataques por delitos informáticos o ciberataques. *

Marca solo un óvalo.

- Sí
- No
- Tal vez

Anexo 03: Ponderación y resultados de la encuesta aplicada a las empresas.

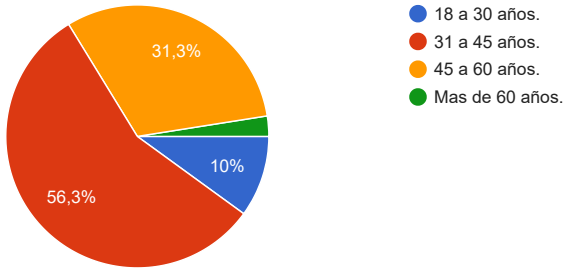
Ciberseguridad en las empresas publicas y privadas, en colombia y a nivel internacional.(Valoración del Daño Informático).

80 respuestas

Publicar datos de análisis

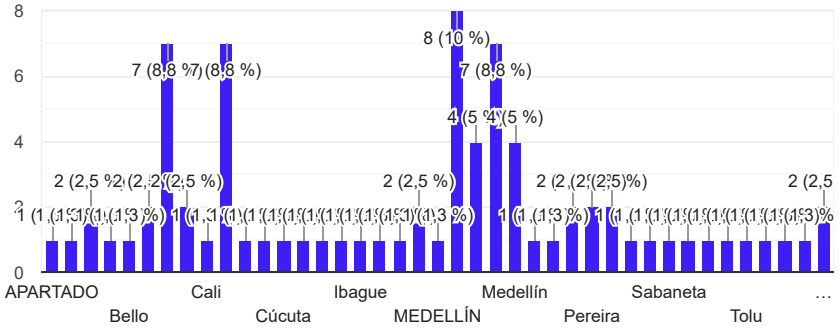
Por favor especificar su edad, en cual de los siguientes rangos se ubica.

80 respuestas



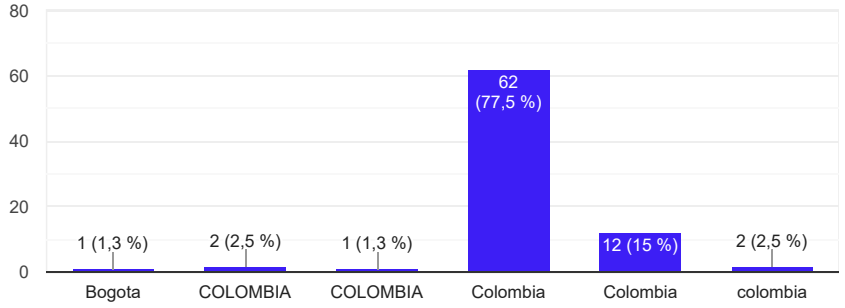
Ciudad de residencia:

80 respuestas



Pais de residencia:

80 respuestas



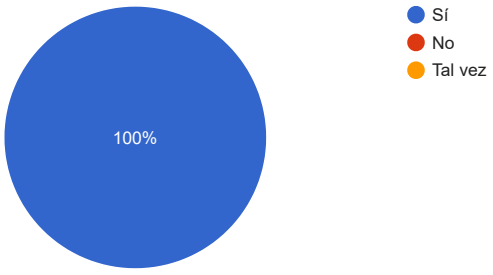
Profesión:

80 respuestas

- Ingeniero de sistemas
- Ingeniero de Sistemas
- Ingeniero electrónico
- Ing de sistemas
- Ingeniero Electrónico
- Ingeniera de sistemas
- Economista
- Economista
- Ventas

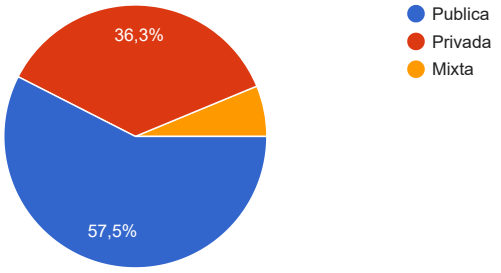
Labora actualmente o ha laborado en los últimos tres (3) años.

80 respuestas



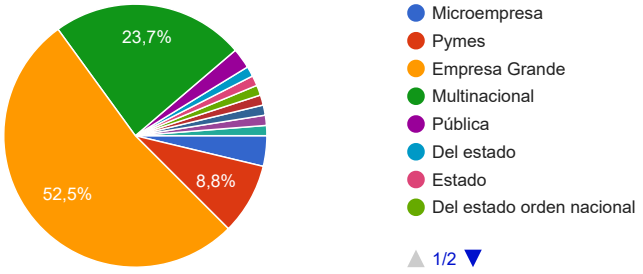
La empresa, organización o institución en la cual labora o laboró, es de tipo:

80 respuestas



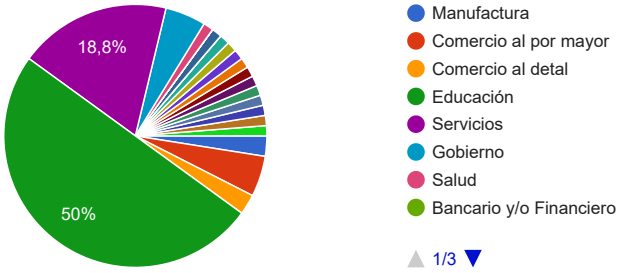
Que clasificación posee la empresa, organización o institución en la cual labora o laboró:

80 respuestas



A que sector se dedica la empresa:

80 respuestas



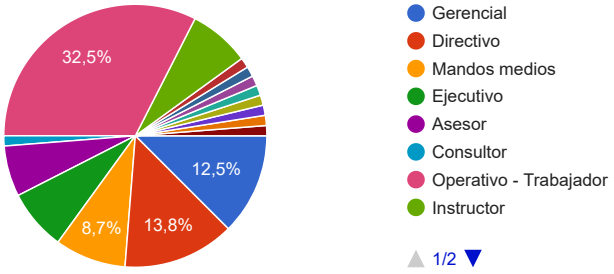
Cargo que desempeña o desempeño en su ultima empresa:

80 respuestas

- Instructor
- Instructor
- Docente
- Instructora
- Gerente
- Gerente Mercadeo
- Director comercial
- Asesor
- Administrador de Datacenter - Instructor

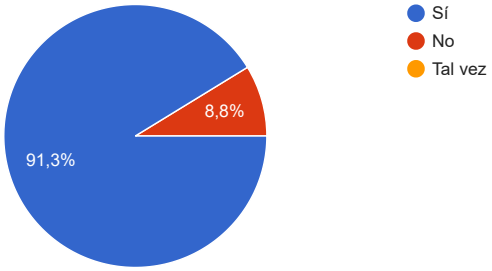
Su cargo en la empresa, es de tipo:

80 respuestas



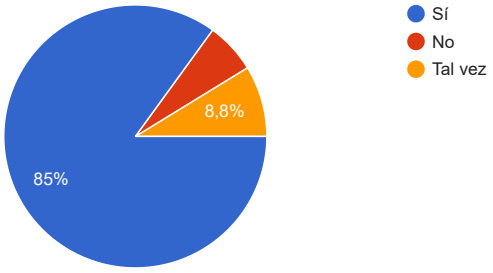
Sabe si la empresa tiene, ofrece o utiliza servicios en linea:

80 respuestas



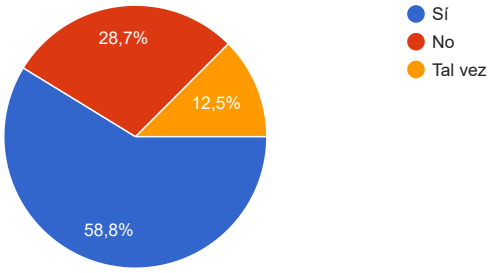
Conoce usted los riesgos a los cuales se exponen las empresas y personas, al interactuar o utilizar servicios en linea en el ciberespacio o Internet.

80 respuestas



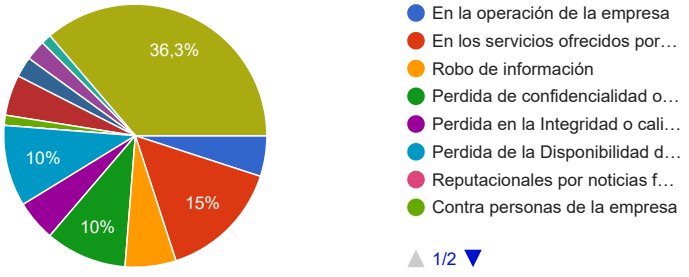
Conoce usted, si empresas para las cuales usted ha trabajado o trabaja han sido victimas de ataques informáticos o ciberataques.

80 respuestas



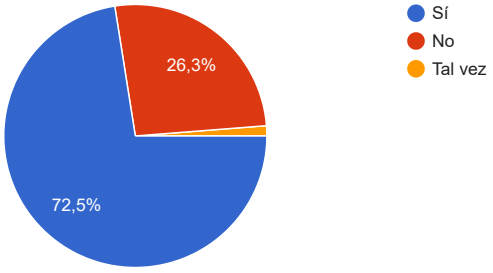
Si su respuesta a la anterior pregunta fue "Si" o "Tal Vez", por favor podría definir que tipo de afectación sufrió la empresa afectada o atacada.

80 respuestas



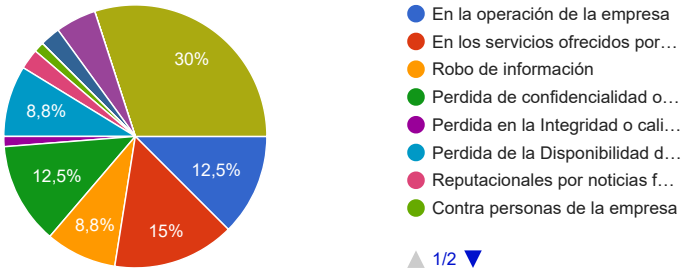
Conoce usted, algún caso donde una empresas ha sido victimas de ataques informáticos o ciberataques.

80 respuestas



Si su respuesta a la anterior pregunta fue "Si" o "Tal Vez", por favor podría definir que tipo de afectación sufrió la empresa afectada o atacada.

80 respuestas



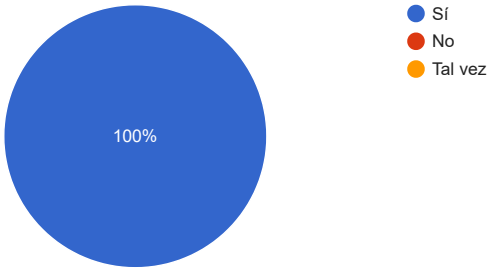
Por favor podría usted, indicarnos el nombre de la empresa que fue afectada y que usted hace referencia como caso conocido de ataques por delitos informáticos o ciberataques.

80 respuestas

- Bancolombia
- N/A
- Confidencial
- Sena
- Ninguna
- NA
- Fecon SAS
- No conozco
- No

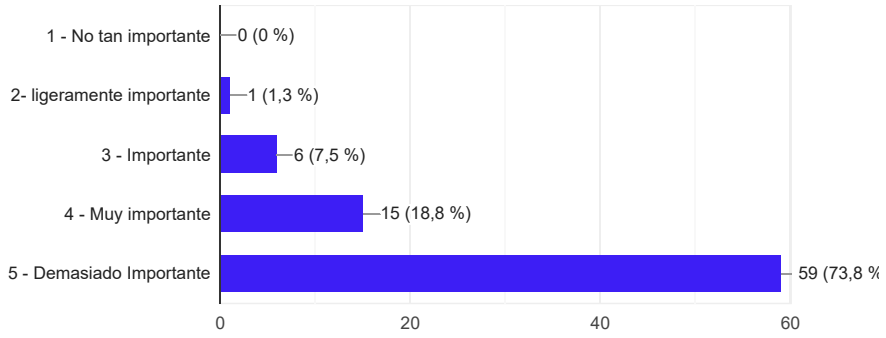
Para usted, es importante que las empresas estén protegidas contra ataques informáticos o ciber ataques.

80 respuestas



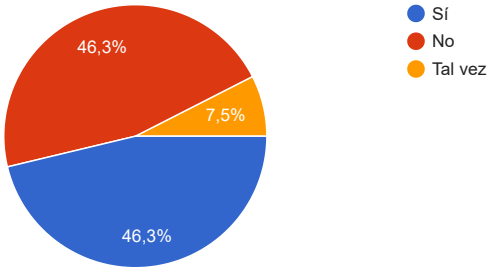
Es una escala de uno (1) a cinco (5), donde 1 es "No tan Importante" y 5 "Demasiado Importante" . Que valor asignaría usted a las protecciones e inversiones en protección en ciberseguridad en su empresa.

80 respuestas



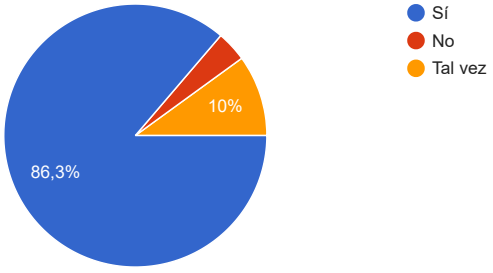
En su profesión o cargo en la empresa, tiene alguna relación con seguridad informática o ciberseguridad

80 respuestas



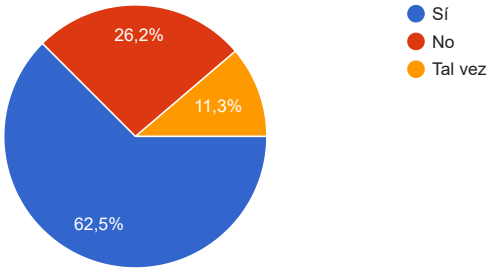
Usted en su empresa es consciente y conoce las vulnerabilidades, amenazas y riesgos en cuanto a ataques informáticos o ciberataques , que pueden presentarse y/o afectarlos.

80 respuestas



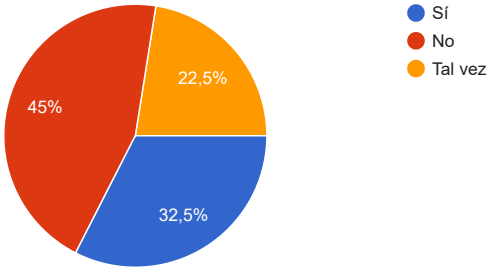
Sabe si su empresa tiene implementado algún Sistemas de Gestión de Seguridad de la Información (SGSI).

80 respuestas



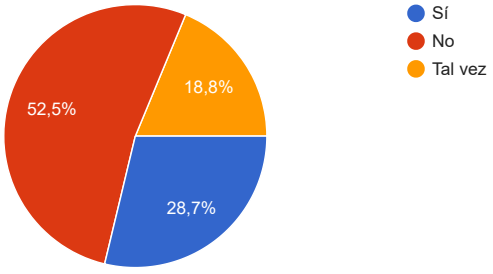
Sabe usted si su empresa está en proceso de certificación o fue certificada en alguna norma o estándar nacional o internacional de seguridad de la información o ciberseguridad.

80 respuestas



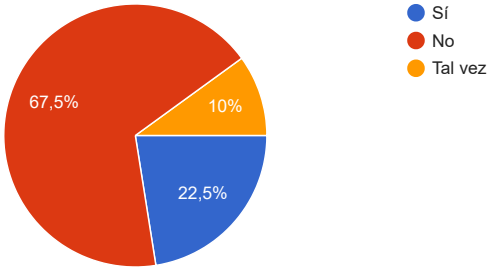
Sabe usted como medir, valorar o cuantificar el impacto económico, financiero, comercial y reputacional que pueden afectar a su empresa si llegan a ser victimas de un ataque informático o ciberataque.

80 respuestas



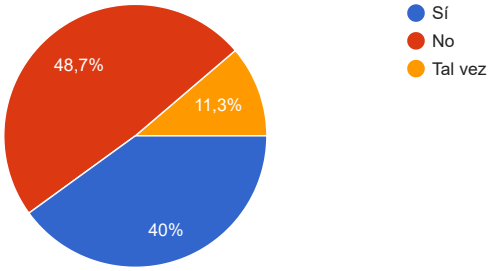
Sabe usted si en su empresa o familia poseen o tienen contratados seguros o pólizas de seguros, que los amparen si llegan a ser victima de ataques informáticos o ciberataques

80 respuestas



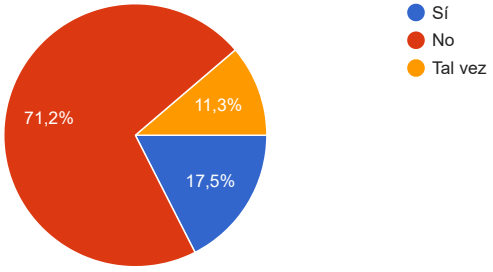
Conoce usted que existen seguros o pólizas de seguros que lo protegen a usted, su familia y a su empresa ante caso de delitos informáticos o ciberataques.

80 respuestas



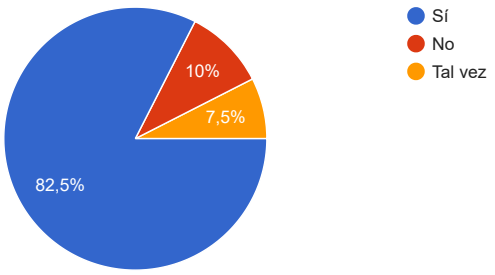
Conoce usted en su pais y de acuerdo a las leyes en su pais, cuando le corresponde pagar o resarcir por el daño causado, a un ciberdelincuente que lo afecta a usted o a su empresa a través de un delito informático o ciberdelito.

80 respuestas



Le gustaría conocer y contar con una Metodología que le permita a usted, a su empresa, a los jueces, a las autoridades del pais, a sus asesores jurídicos, como además a las empresas auguradoras; poder cuantificar, valorar científicamente, de manera exacta y real; las afectaciones sufridas por ataques por delitos informáticos o ciberataques.

80 respuestas



Anexo 04: Casos reportados de Ciberataques a empresas en Colombia y a nivel mundial.

Los hermanos adolescentes acusados de cometer una de las mayores estafas con bitcoins de la historia

Redacción
BBC News Mundo

6 horas

Cuentas de clientes vacías y hasta U$$3.600 millones desvanecidos, miles de clientes afectados y dos adolescentes en el punto de mira.

Ameer y Raees Cajee, de 18 y 20 años respectivamente, fundaron la **plataforma de criptomonedas Africrypt**, que comenzó a operar desde Sudáfrica en 2019.

Según una denuncia presentada en abril por un despacho de abogados en nombre de un grupo de inversores ante la policía, clientes de usuarios dejaron de tener acceso a sus cuentas, coincidiendo con las semanas en las que el bitcoin alcanzó su máximo histórico.

La criptodivisa más famosa **llegó a cotizar a U$$63.226 por unidad**, el precio más alto de su historia.

Figura 7. Caso 1 - Reporte de Ciberataque (BBC, 2021)

"Colosal" ciberataque golpea a cientos de empresas en EE.UU.

Redacción
BBC News Mundo

3 julio 2021

GETTY IMAGES

Unas 200 empresas en Estados Unidos fueron golpeadas por un "colosal" ataque cibernético tipo "ransomware" o cibersecuestro, en el que los sistemas quedan intervenidos por hackers hasta que los individuos o compañías afectadas paguen por desbloquearlos.

La empresa de ciberseguridad Huntress Labs afirmó que el objetivo del ataque fue la compañía de tecnología informática **Kaseya**, basada en Florida, y luego se extendió por las redes corporativas que usan su software.

Kaseya publicó un comunicado en su sitio web señalando que estaba investigando el "potencial ataque".

Huntress Labs afirmó que cree que **el grupo criminal de hackers conocido como REvil** –que realiza este tipo de ataques por dinero y tiene vínculos con Rusia– fue el responsable.

Figura 8. Caso 2 - Reporte de Ciberataque (BBC, 2021)

El "impactante" atraco del Grupo Lázaro, el equipo de élite de Corea del Norte que casi roba US$1.000 millones en un solo asalto

Geoff White y Jean H. Lee
BBC News

24 junio 2021

En 2016, piratas informáticos de Corea del Norte planearon un ataque al Banco de Bangladesh para obtener US$1.000 millones. Y estuvieron a punto de conseguirlo.

Solo la suerte evitó que todas las transferencias, excepto una por US$81 millones, siguieran adelante.

Pero, ¿cómo acabó uno de los países más pobres y aislados del mundo formando a un equipo de ciberdelincuentes de élite?

Todo comenzó con una impresora que funcionaba mal, algo a lo que ya estamos habituados en la vida moderna, por lo que cuando le sucedió al personal del Banco de Bangladesh pensaron lo mismo que la mayoría de nosotros: un día más con otro dolor de cabeza por problemas tecnológicos.

Figura 9. Caso 3 - Reporte de Ciberataque (BBC, 2021)

Colonial: por qué es de vital importancia para EE.UU. el oleoducto que fue objeto de un ciberataque a gran escala

Redacción
BBC News Mundo

10 mayo 2021

El oleoducto Colonial pertenece a una empresa privada que no cotiza en los mercados bursátiles.

Con una orden de emergencia emitida este fin de semana, el gobierno de Estados Unidos flexibilizó temporalmente las normas que regulan el transporte de combustible en ese país.

Con esta decisión extraordinaria, que permitirá que quienes transportan por vía terrestre productos derivados del petróleo en 18 estados puedan trabajar horas extras o con horarios más flexibles, las autoridades intentan hacer frente a las consecuencias del ciberataque que sufrió el viernes pasado **la mayor red de oleoductos del país**, propiedad de la empresa Colonial Pipeline.

El ataque, ejecutado por un grupo de hackers denominados DarkSide, **obligó al cierre preventivo e indefinido de este gigantesco sistema de tuberías**, poniendo en peligro el suministro de combustible para gran parte de Estados Unidos.

La dimensión y las posibles consecuencias de esta acción criminal obligaron a que más allá del FBI, tuvieran que tomar cartas en el asunto la Casa Blanca, el Departamento de Energía y el Departamento de Transporte, entre otras agencias del gobierno.

Figura 10. Caso 4 - Reporte de Ciberataque (BBC, 2021)

EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país

Redacción
BBC News Mundo

10 mayo 2021
Actualizado 10 mayo 2021

El ciberataque afectó a una de las mayores redes de oleoductos de EE.UU.

El gobierno de EE.UU. declaró este domingo un estado de emergencia regional tras un ciberataque a la mayor red de oleoducto del país, que la dejó inactiva desde la noche del viernes.

Un grupo de piratas informáticos desconectó por completo y robó más de 100 GB de información del Oleoducto Colonial, que transporta más de **2,5 millones de barriles por día**, el 45% del suministro de diésel, gasolina y combustible que consumen los aviones de la costa este.

Analistas del mercado petrolero indican que, como consecuencia, es probable que los precios del combustible aumenten entre un 2% y un 3% el lunes, pero el impacto será peor si el "apagón" del oleoducto se prolonga por mucho más tiempo.

EE.UU. trabajaba en **restablecer el servicio**, pero ante las continuas fallas de las líneas principales, el gobierno decidió decretar el estado de emergencia para facilitar el transporte del combustible por otros medios, principalmente carretera.

Figura 11. Caso 5 - Reporte de Ciberataque (BBC, 2021)

El "inusualmente agresivo" ciberataque del que Microsoft acusa a China (y por qué no es simplemente una nueva crisis de ciberseguridad)

Redacción
BBC News Mundo

9 marzo 2021

Decenas de miles de usuarios de Microsoft Exchange podrían estar afectados.

Un potente hackeo al servicio de correos electrónicos de Microsoft tiene en riesgo a decenas de miles de organizaciones.

Y la escala de la filtración apenas se está comenzando a **dimensionar**, según los especialistas.

Microsoft asegura tener un "alto nivel de confianza" en que detrás hay un grupo de atacantes patrocinados por **China, algo que Pekín niega.**

La semana pasada, cuando se dio a conocer el ataque, se pensó que había sido limitado, pero luego se ha reportado un **aumento en el uso de estas tácticas**, quizás debido a que otros *hackers* están aprovechando las debilidades del sistema que se hicieron públicas, según informa Gordon Corera, corresponsal de seguridad de la BBC.

Figura 12. Caso 6 - Reporte de Ciberataque (BBC, 2021)

SolarWinds: 5 ataques informáticos de Rusia que transformaron la ciberseguridad en Estados Unidos

El último ciberataque atribuido a Rusia es una especie de recopilatorio de los hitos en el adversario más antiguo de Estados Unidos en el ciberespacio.

Figura 13. Caso 7 - Reporte de Ciberataque (BBC, 2021)

Andrey Turchin, el hacker llamado "el dios invisible" al que acusan de robar información de 300 empresas en 44 países

Figura 14. Caso 8 - Reporte de Ciberataque (BBC, 2021)

COLOMBIA

En el 2021 aumentaron en un 30% los ciberataques en Colombia

De acuerdo con datos de la Fiscalía General de la Nación, la violación de datos personales y la suplantación de sitios web fueron las modalidades más usadas por los ciberdelincuentes durante el primer semestre del año.

2 de julio de 2021

PUBLICIDAD

Imagen de referencia. En los primeros seis meses de 2021, los ataques cibernéticos se incrementaron en un 30%. Foto: EFE/SASCHA STEINBACH/Archivo.

Figura 15. Caso 9 - Reporte de Ciberataque (Infobase, 2021)

Figura 16. Caso 10 - Reporte de Ciberataque (El País, 2021)

COLOMBIA

Escuchar este artículo

Universidad El Bosque fue víctima de ataque informático a sus plataformas académicas

Este lunes la Universidad El Bosque fue víctima de un ataque cibernético a sus plataformas virtuales y redes sociales. La denuncia la realizaron varios estudiantes, quienes alertaron no tener acceso a sus correos institucionales.

A través de redes sociales los estudiantes y egresados de la institución informaron que no hacer uso de varias de las plataformas virtuales de la Universidad, entre ellas el Campus Virtual y el Sistema Sales.

Además, compartieron los correos electrónicos que les llegaban desde la cuenta oficial de la rectoría, en los que les aseguraban que toda la información académica y financiera de la Universidad había sido eliminada.

Figura 17. Caso 11 - Reporte de Ciberataque (El país, 2021)

Figura 18. Caso 12 - Reporte de Ciberataque (El Colombiano, 2021)