Universidad Zaragoza
1542

Trabajo Fin de Grado

Seguridad de la información y aplicación de la Ley Orgánica de Protección de Datos en la empresa

Autor/es

Laura Jaime Gomara

Director/es

María Jesús Lapeña Marcos

Facultad de Economía y Empresa / 2014 – 2015

Información

Título del trabajo: Seguridad de la información y aplicación de la Ley Orgánica de Protección de Datos en la empresa.

Autor: Laura Jaime Gomara

Director del trabajo: María Jesús LaPeña Marcos

Titulación: Grado en Administración y Dirección de Empresas

Resumen

Este trabajo se centra en el tema de la seguridad informática y la seguridad de la información en la empresa, profundizando en la aplicación y evaluación de cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal; ésta es una ley de obligado cumplimiento que afecta al entorno profesional de la empresa y exige una serie de medidas organizativas y técnicas para garantizar la seguridad de los datos de carácter personal.

Para ello, comenzamos introduciendo los conceptos de seguridad informática y seguridad de la información, ya que es fundamental tener claramente definidos estos conceptos.

A continuación hacemos un análisis de los riesgos a los que se está expuesta una organización, así como la forma de evitarlos y gestionarlos para evitar las posibles consecuencias de su impacto.

Por otro lado, se analiza el marco normativo al que deben de ajustarse las empresas para cumplir el nivel de seguridad exigido legalmente. Se analiza también la normativa en materia de protección de datos en el resto del mundo.

Como aplicación de todo el tema de estudio, se han realizado dos casos prácticos: un estudio sobre las medidas de seguridad de la información que se aplican en la entidad financiera “La Caixa”, y la evaluación de cumplimiento de la LOPD en una Pyme; observamos que en una Pyme el grado de sensibilización sobre la necesidad de garantizar la protección de datos personales es muy inferior al de las grandes organizaciones.

También, a modo de conclusión, se desarrolla una guía dirigida a las empresas para cumplir con la normativa de la LOPD. Además, se indica cómo realizar una auditoría de cumplimiento y se adjunta un cuestionario para analizar el grado de adaptación a la ley.

Abstract

This paper is focused on the Information Technology and Data Protection Security within a company, emphasizing on the application and evaluation of the Organic Law on Protection of Personal Data compliance; this is a mandatory law that affects the professional environment of a company and requires a series of organizational and technical measures in order to guarantee the Personal Data Security.

That is why we begin with an introduction of the basic concepts of information technology and data protection security, because is essential to know and be clear about these concepts.

Next, we carry on an analysis of the risks which an organization is exposed to and we indicate how to avoid and manage these to prevent possible consequences of their impact.

On the other hand, it is analyzed the regulatory framework which every company has to adapt to, so as to accomplish with the level of security legally required. In addition, it is analyzed also the regulations on data protection in the rest of the world.

As an application of the whole study topic, there have been two case studies: a study about information security measures currently applied by “La Caixa” bank, and the compliance evaluation of the Organic Law on Protection of Personal Data in an SME; we observe that in an SME the degree of sensitivity regarding the need to ensure the personal data protection is far lower than in a big organizations.

Moreover, as a conclusion, it is developed a handbook for companies in order to comply with the Organic Law on Protection of Personal Data regulations. Furthermore, it is indicated how to perform a compliance audit and encloses a questionnaire to analyze the degree of adaptation to the law.

INDICE

GRÁFICOS

FIGURAS

TABLAS

1. INTRODUCCIÓN

1.1 MOTIVACIÓN Y JUSTIFICACIÓN DEL TEMA

La motivación para realizar mi trabajo fin de grado en la línea de la seguridad informática y seguridad de la información tiene su origen al cursar la asignatura de tecnologías de la información y la comunicación; con esta asignatura he podido conocer aspectos realmente importantes en materia de seguridad y, puesto que en un futuro mi objetivo es tener mi propio negocio, considero relevante conocer aquello que me ayude a garantizar dicha seguridad.

Otra de las razones que me han llevado a elegir esta línea es la importancia y actualidad del tema de la protección de datos personales. Es un tema de gran relevancia sobre el que todavía hay un gran desconocimiento. En muchas ocasiones se encuentran por la calle documentos con datos de carácter personal o en muchas entidades tienen papeles encima de la mesa en los que se pueden ver datos de personas que han realizado algún tipo de actividad con ellos; con estas acciones más frecuentes de lo que sería deseable se está violando el derecho de intimidad de las personas, por lo tanto, creo que una formación en este punto es de gran importancia para el correcto desarrollo de las actividades de la empresa (que continuamente trabaja con datos de estas características).

Para mentalizarnos de la importancia de la seguridad, basta pensar en los casos de empresas en todo el mundo que sufren grandes pérdidas de dinero o de información debido a diferentes ataques informáticos. Por tanto, es necesario conocer todos los tipos de medidas y mecanismos que debemos aplicar para garantizar la seguridad, así como ser conscientes de las distintas normas, estándares y legislación vigente relativa a esta materia.

En mi opinión creo que tener conocimientos sobre seguridad informática y seguridad de la información es fundamental tanto para el trabajo profesional como para el trabajo personal; pensemos que, en nuestra casa, simplemente entrando en nuestro navegador ya estamos expuestos a una gran cantidad de amenazas

A nivel personal, en mi caso, con las perspectivas de futuro que tengo, es importante que conozca todos los riesgos que conlleva una mala gestión de la información y una

mala utilización de los sistemas informáticos, ya que puede ocasionar grandes problemas e incluso llevar a la quiebra.

Por todo lo expuesto considero imprescindible una concienciación general en lo relativo a seguridad de la información y la necesidad de garantizar la protección de datos personales, preservando la intimidad y privacidad de las personas. Debemos de tener una información mínima en estos aspectos y, en el caso de las empresas, es necesario que todo el personal este concienciado, mentalizado e informado de todas las medidas de seguridad que deben de aplicar.

1.2 PLANTEAMIENTO Y OBJETIVOS DEL TRABAJO

A lo largo del trabajo se desarrolla el tema de la seguridad de la informática y de la información en las organizaciones, la cual, en los últimos años está alcanzando la relevancia e importancia que merece.

Hasta hace algunos años, cuando no era habitual el uso de sistemas informáticos en el desarrollo de las actividades empresariales, todo se realizaba en formato papel y lo único de lo que se tenían que preocupar era de tener bien custodiados dichos papeles, pero hoy en día todo esto ha sufrido un importante cambio y es imprescindible utilizar todas las medidas necesarias para proteger la información en cualquier tipo de formato. Otro factor importante a tener en cuenta es el uso de Internet; Internet es un medio clave en el desarrollo de las actividades de las empresas, por lo que es necesario extremar las buenas prácticas en su uso, ya que Internet es una fuente de amenazas que pueden atacar nuestros equipos y sistemas; además, hay que tener un especial cuidado en lo que se refiere a la transmisión de información, ya que las empresas realizan gran cantidad de operaciones de forma telemática y en estos procesos se pueden producir robos de información, por lo que tener un buen sistema de seguridad de la información es fundamental.

El uso de las nuevas tecnologías de la Información y la Comunicación hacen que aumente la productividad, haciendo generar a las empresas unos mayores beneficios, pero también, como contrapartida, aumenta las amenazas e incrementa el riesgo.

Por todas estas razones, con este trabajo pretendemos alcanzar una serie de objetivos, que son los siguientes:

- Conocer la importancia que tiene la seguridad informática y la seguridad de la información en el desarrollo diario de las actividades de una empresa.
- Hacer una revisión documental de leyes y normas relativas a la seguridad de la información.
- Analizar el grado de cumplimiento de la LOPD en España, revisando estudios de investigación
- Diseñar y desarrollar una guía de adaptación para el cumplimiento de la LOPD dirigido a PYMES.
- Evaluar en entornos reales el cumplimiento de la Ley Orgánica de Protección de Datos.

1.3 ESTRUCTURA

El trabajo, que hemos iniciado con esta introducción, se estructura en 4 partes principales, de las cuales, las dos primeras corresponden más al marco teórico y las otras dos corresponden a una aplicación práctica, al estudio de casos reales…

El capítulo siguiente, **capítulo 2**, está centrado en definir los conceptos fundamentales de seguridad informática y de la información; se justifica él por qué de su importancia, se muestran los distintos tipos de seguridad a considerar… También, explicamos el proceso análisis y gestión de riesgos, y cómo llevarlo a cabo. Además, se define el concepto de Auditoría Informática, enfocado hacia la Auditoría de Seguridad cuyo fin es evaluar el sistema informático para saber si estamos aplicando las medidas correctas para garantizar la seguridad.

En el **capítulo 3** se hace una revisión de la normativa a aplicar para garantizar la seguridad de la información, concretamente se analiza la ISO 27001, que es una norma internacional, el Esquema Nacional de seguridad y la Ley Orgánica de Protección de Datos Personales. En esta última centraremos nuestro estudio; analizaremos la protección de datos en España y en el resto del mundo, y será objeto de estudio en el capítulo siguiente.

En efecto, en el **capítulo 4** abordamos un análisis sobre el cumplimiento (aplicación en casos prácticos) de la LOPD en una empresa de grandes dimensiones, concretamente, la entidad financiera La Caixa, y el análisis de cumplimiento en una PYME. Tras el análisis, también se incluyen una serie de recomendaciones para alcanzar el

cumplimiento en la PYME, ya que se observa una gran falta de cumplimiento, extensible en general a la pequeña y mediana empresa, que no tiene en consideración la aplicación de la norma.

Por último, se desarrolla una **guía práctica para PYMES**, en la que se indican las medidas que tienen que llevar a cabo para el cumplimiento de la Ley Orgánica de Protección de Datos, indicando, en particular, todo lo que se debe de incluir en el documento de seguridad, requisito fundamental para cumplir con la legislación.

Para finalizar el trabajo he incluido un apartado de conclusiones y la bibliografía utilizada para el desarrollo del trabajo.

2. SEGURIDAD INFORMÁTICA EN LA EMPRESA

En este apartado vamos a desarrollar el tema de la seguridad informática, destacando los aspectos que debemos de considerar en una empresa, tanto para proteger nuestro equipo como nuestra información. Además, también nos adentramos en el análisis de riesgos, que nos permitirá decidir qué medidas aplicar. Para acabar el apartado dedicamos un punto a la auditoría informática, indicando qué es, para qué sirve y los beneficios que puede reportar.

2.1 SEGURIDAD INFORMÁTICA

Hasta hace unas décadas, toda la información que había en una empresa se conservaba en papel, lo cual era un problema para su acceso, transporte y almacenaje. Al aparecer los sistemas informáticos nos facilitan todas estas tareas permitiendo digitalizar gran volumen de información, reduciendo el espacio que ocupa, y facilitando su acceso y procesamiento.

Aquí es donde entra el concepto de seguridad informática, puesto que es el área de la informática que tiene como objetivo proteger tanto la información como los sistemas de información, para asegurar que no se produce acceso, uso, interrupción, divulgación o destrucción no autorizada de la misma.

Podemos definir la **seguridad informática** como el conjunto de medidas de protección de las infraestructuras computacionales así como todo lo que esté relacionado con ella, principalmente la información que contiene.

Para garantizar dicha seguridad existen un conjunto de protocolos, herramientas, métodos, estándares y leyes que velan por minimizar los posibles riesgos que puedan sufrir tanto las estructuras como la información.

Dentro de los tipos de seguridad, distinguimos dos tipos claramente diferenciados: seguridad lógica y seguridad física. Es de gran importancia considerar los dos tipos de seguridad, ya que sin seguridad física no podemos garantizar la seguridad lógica.

Seguridad lógica

Con seguridad lógica nos referimos a la seguridad ante el uso del software y los sistemas, programas y procesos y el acceso por parte de los usuarios a la información. Con este tipo de seguridad se controla el acceso lógico, mediante el cual se previene que las personas que no están autorizadas no puedan tener acceso a los sistemas. En lo que se refiere al control de acceso, el National Institute for Standars and Technology establece unos controles de seguridad mínimos que hay que cumplir; son los que se explican a continuación.

• **Identificación y autentificación:** Es la primera barrera de defensa que se establece en los sistemas, ya que con ello se previene que puedan acceder personas que no están autorizadas; además, permite informar sobre las actividades que realizan los distintos usuarios y mantener un control de los accesos.

Con la identificación nos referimos a que el usuario se da a conocer en el sistema y con la autenticación nos referimos a la verificación de la identificación por parte del sistema. A continuación mostramos las diferentes técnicas que podemos emplear para la autenticación:

- Utilización de elementos que solamente un individuo conoce como, por ejemplo, un código PIN, una contraseña, clave criptográfica…
- Utilización de algún elemento que tiene el usuario como, por ejemplo, una tarjeta magnética.
- Utilización de controles biométricos, es decir, como forma de autenticación se utilizan factores que identifican solamente a un usuario y que son personales como, por ejemplo, la huella dactilar o el iris del ojo.
- Utilización de algo que el usuario es capaz de hacer como, por ejemplo, un patrón de escritura.

Estas técnicas las podemos utilizar tanto de forma individual como de forma combinada, lo cual aportara una mayor seguridad a nuestra información. Puesto que es recomendable que el usuario solo tenga que identificarse y autenticarse una vez para poder acceder a toda la información y a las aplicaciones que tiene autorizadas, se puede utilizar un servidor de autenticaciones, en el cual, los diferentes usuarios se identifican y el servidor se encarga de realizar la autenticación en los demás sistemas y aplicaciones para las que se tiene el acceso autorizado.

- **Transacciones:** Es necesario implementar un control para las transacciones como, por ejemplo, solicitar una clave para realizar una transacción en concreto.
- **Roles:** Cuando hablamos de roles hacemos referencia a que el acceso a la información sea mediante un rol de usuario, es decir, que tan solo esa persona, con ese perfil, es la que tiene acceso como, por ejemplo, un programador, el administrador del sistema…etc.
- **Limitaciones a los servicios:** Este tipo de limitaciones se refiere a la restricción de una aplicación por el administrador del sistema. Un ejemplo sería la licencia de uso de un software en una empresa para ser usado tan solo en un equipo; para ello existe un control que hace que solo pueda ser usado en un equipo y no en varios.
- **Modalidad de acceso:** Define la forma en la que el usuario puede acceder tanto a los recursos como a la información de la organización. Las posibles modalidades son de escritura, lectura, ejecución, borrado o una combinación de las tres.

Aparte de estas modalidades también nos encontramos con la modalidad de creación, en la que el usuario puede crear nuevos archivos, y la modalidad de búsqueda en la que el usuario puede listar los archivos de un directorio en concreto.

- **Ubicación y horarios:** En lo que se refiere a la ubicación, hace referencia a que el acceso a los recursos del sistema puede ser de forma física o lógica. Por otro lado, también puede establecer un control de las horas en las que pueden acceder los usuarios; de esta forma, el acceso está más controlado y restringido.
- **Control de acceso interno:** Como su nombre indica, consiste en controlar el acceso desde el interior de la organización; para ello se utilizan las técnicas que se indican a continuación.
  - *Palabras clave (Password):* Estas son las contraseñas y se utilizan para la autenticación del usuario. Lo recomendable es disponer de una sincronización de

contraseñas, y no una distinta para tener acceso a cada sistema; eso sí, esta contraseña debe de tener un alto nivel de seguridad.

Es necesario realizar un control sobre el cambio de contraseñas para aumentar el grado de seguridad; para ello, se debe definir un periodo mínimo, durante el cual no se puede cambiar la contraseña y un periodo máximo para que caduque.

Para establecer una contraseña segura (robusta) es necesario tener un cuenta unos requisitos mínimos:

- Longitud mínima: 8 caracteres pero es aconsejable que esté formada por 14 o más, ya que con cada carácter adicional aumenta el grado de protección.
- Los caracteres deben de combinarse, conteniendo mayúsculas, minúsculas y símbolos intercalados.

Además de estos requisitos mínimos también es necesario que los usuarios tengan en cuenta las siguientes acciones:

- Cambiar la contraseña regularmente.
- No utilizar la misma contraseña para distintos entornos, por ejemplo, no utilizar la contraseña utilizada en el trabajo como contraseña del correo electrónico personal.
- No proporcionar la contraseña a nadie y no introducirla en sistemas que no son controlados por uno mismo.
- No utilizar el mismo nombre que utilizamos para iniciar sesión
- No usar secuencias ni caracteres repetidos.

- *Encriptación:* La información está encriptada; solo puede ser desencriptada por aquella persona que tiene la clave para ello.
- *Listas de control de acceso:* Contienen una relación de los usuarios que tienen acceso a un determinado recurso del sistema, así como la modalidad de acceso que tienen.
- *Limites sobre la interfaz del usuario:* Estos límites restringen la realización de ciertas funciones en el sistema por parte del usuario
- *Etiquetas de seguridad:* Se utilizan para designar ciertos recursos que puedan servir para realizar diferentes funciones como el control de acceso, medidas de seguridad…etc.

- **Control de acceso externo:** En este caso se controla el acceso desde fuera de la organización; para ello se utilizan las técnicas que a continuación se relacionan.

- *Firewalls:* Permiten filtrar o bloquear el acceso entre dos redes, normalmente una publica y una privada. Con esta técnica, los usuarios de la organización pueden conectarse a una red externa sin sufrir el riesgo de un ataque externo.
- *Dispositivos para controlar los puertos:* Estos dispositivos tienen como función autorizar el acceso a un determinado puerto como, por ejemplo, un modem.
- *Acceso del personal contratado:* Cuando tenemos en nuestra organización personal que nos presta un servicio de forma temporal, debemos de tener un mayor cuidado a la hora de administrar sus perfiles de acceso.
- *Accesos públicos:* Hay que prestar gran atención en los que se refiere a los sistemas de información que pueden ser consultados de forma pública.

• **Administración de la seguridad:** Es necesario administrar de una forma correcta todas las medidas de seguridad lógica. En primer lugar, es necesario determinar los permisos de acceso; para ello, primero tenemos que clasificar la información por niveles en función de las medidas de seguridad que le debemos de aplicar. También es necesario concienciar a los empleados de lo importante que es la información para la organización y las grandes pérdidas que podría acarrear su destrucción, modificación, robo, fuga…etc.

Seguridad física:

La seguridad física tiene como objetivo proteger físicamente los distintos recursos e información de la empresa. Consiste en establecer una serie de medidas y barreras físicas que impidan que las amenazas puedan materializarse. La seguridad física la podemos clasificar en las cuatro categorías que se muestran a continuación:

- Obstrucciones físicas: Medidas que impiden el acceso a aquellos bienes o información que están protegidas. Estas obstrucciones físicas son las puertas blindadas, candados, llaves de acceso, claves de seguridad para el acceso…etc.
- Técnicas de vigilancia: Están orientadas a detectar cualquier tipo de movimiento que pueda afectar a la seguridad; para ello las medidas que podemos adoptar son, por ejemplo, instalar alarmas de seguridad, videocámaras,etc.
- Sistemas de inteligencia: Son utilizados para analizar la información recogida mediante las técnicas de vigilancia.

- Personal de seguridad: En esta categoría se incluyen las personas que están encargadas de la seguridad; son las que deciden cómo actuar y qué realizar en el caso de que se encienda una alarma o se produzca algún tipo de error.

En este campo, las amenazas que hemos de considerar son: las derivadas de acciones del propio hombre (como, por ejemplo, los robos), los desastres naturales y los cambios producidos en el entorno de la organización. Dichas amenazas las podemos ver desarrolladas en el Anexo I.

Además, el Ministerio de Educación, Cultura y Deporte proporciona en su página web una serie de mecanismos básicos para garantizar una correcta seguridad física, que los podemos ver explicados detalladamente en el Anexo II.

2.2 ANÁLISIS DE RIESGOS

Cuando realizamos un estudio sobre la seguridad informática y de la información en una organización, es de gran importancia llevar a cabo un "análisis y gestión del riesgo", ya que con ello podemos determinar, analizar y realizar una valoración de los distintos riesgos que nos podemos encontrar y aplicar una serie de medidas que nos permitan controlarlo. Para llevar a cabo este proceso es necesario conocer qué entendemos por vulnerabilidad, amenaza, riesgo e impacto.

Vulnerabilidades

Las vulnerabilidades son las debilidades del sistema; es todo aquello que no hemos tenido en cuenta a la hora de proteger los activos y que les puede afectar de forma negativa; podríamos decir que son, en efecto, los puntos débiles. Estas vulnerabilidades hacen que las amenazas se materialicen y afecten a los activos. Estas pueden ser de distinta

- *Físicas:* Estas hacen referencia al acceso al lugar donde se encuentra los distintos equipos que contienen información. Este tipo de vulnerabilidad se puede dar por una falta de control de acceso del personal a los sistemas y a la utilización de dispositivos de almacenamiento con los que poder extraer datos de forma no autorizada.
- *Naturales:* Este tipo de vulnerabilidades se refiere a la falta de protección ante aquellos daños que puede sufrir un sistema por fenómenos naturales. Estas se pueden producir por no tener instaladas distintas medidas para evitarlos como, por

ejemplo, no tener un sistema de ventilación para evitar temperaturas extremas que calienten y estropeen los sistemas.

- *De hardware:* Aquí podríamos citar, a modo de ejemplo, la falta de protección del sistema para evitar un mal uso del hardware, que puede llevar a un deterioro causante de futuros problemas.
- *De software:* Estas vulnerabilidades pueden ser debidas a errores de programación o a deficiencias por no tener en consideración ciertos aspectos como, por ejemplo, el control de acceso o de registro.
- *De factor humano:* Éstas son muy habituales y son las derivadas por la falta de concienciación sobre las distintas medidas de seguridad que se deben de aplicar y el uso de los distintos equipos.
- *De red:* Las redes están compuestas por un conjunto de ordenadores conectados entre sí en los que, de forma habitual, se transmite información entre ellos, por lo que las vulnerabilidades que encontramos en este campo son las relacionadas con la pérdida de información en esas transmisiones entre equipos.

Amenazas

Entendemos como amenaza informática todo aquello que puede ocasionar un daño en los activos del sistema. Éstas aprovechan las vulnerabilidades del sistema para tener acceso a los equipos y manipularlos sin necesidad de obtener el permiso del administrador de éstos.

Las amenazas las podemos clasificar en tres tipos en función de su origen. Estas pueden ser asociadas a personas, a las condiciones físico – ambientales o al software. En el Anexo III podemos ver desarrolladas los diferentes tipos de amenazas con los que podemos encontrarnos.

Impacto

El impacto lo podemos definir como las consecuencias debidas a la materialización de una amenaza; por supuesto, estos impactos son negativos en la empresa, siendo algunos de éstos la perdida de dinero, de confianza, de imagen, de información, etc.

Riesgos

De forma general podemos definir el riesgo como la posibilidad de que ocurra un problema de forma imprevista, que impida el cumplimiento de los objetivos que

tenemos determinados. Centrándonos en el riesgo informático, según la Organización Internacional de Estandarización (ISO) lo define como "la probabilidad de que una amenaza se materialice utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándoles pérdidas o daños".

Una vez que tenemos claro estos conceptos, podemos adentrarnos en el análisis y gestión de riesgos. Este proceso lo podemos dividir en cuatro fases principales:

Análisis: En esta fase se establecen las distintas partes del sistema que tienen la necesidad protección, las amenazas que les pueden afectar y las vulnerabilidades del sistema. Según el BS ISO/ IEC 27001:2005, para realizar un análisis adecuado sobre los riesgos es necesario llevar a cabo las acciones que se indican:

- Identificar los distintos activos de la empresa.
- Identificación de los requisitos legales y de negocios que son relevantes para la identificación de los activos.
- Realizar una valoración de los activos identificados, teniendo en cuenta los requisitos legales identificados de negocio y el impacto que supondría una perdida tanto de confidencialidad, integridad y disponibilidad..
- Identificar las amenazas y vulnerabilidades que son relevantes para los activos que hemos identificado.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades que pueden ocurrir.
- Calcular el riesgo producido. Este lo podemos calcular mediante la siguiente ecuación:

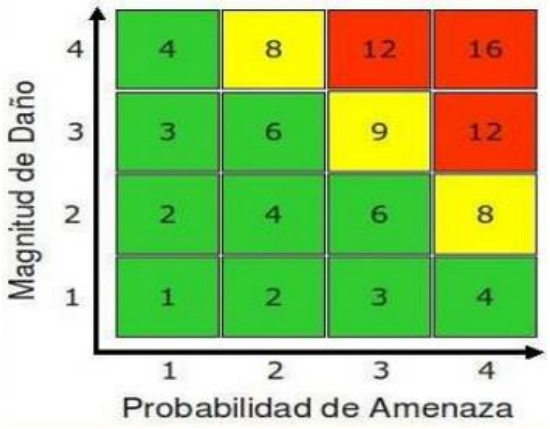
RT (Riesgo Total) = Probabilidad x Impacto Promedio

A partir de este riesgo total también podemos conocer el riesgo residual, el cual, es el riesgo que tenemos una vez establecidas las distintas contramedidas.

- Evaluar los distintos riesgos (total y residual).
- Evaluación de los riesgos ante una escala de riesgos preestablecidos.

En este proceso de análisis de los riesgos se genera la matriz de riesgos; éste es un documento que recoge todos los elementos identificados, la forma en que éstos se relacionan y los distintos cálculos realizados. En la siguiente imagen mostramos un ejemplo de matriz de riesgo en la que se valora con "bajo riesgo" del 1 – 6 (verde), como "medio riesgo" del 8 – 9 (amarillo) y "alto riesgo" del 12 – 16 (rojo).

Figura 1. Matriz de riesgo



Fuente: **http://es.slideshare.net**

A continuación se realiza una clasificación de los distintos riesgos con los que nos encontramos en función de cómo nos pueden afectar.

El objetivo consiste en reducir los riesgos mediante la implantación de medidas de protección. Las medidas que podemos utilizar pueden ser tanto para reducir el riesgo como para eliminarlo. Dichas medidas las podemos encontrar en el Anexo IV.

2.3 AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

De forma general, podemos decir que la auditoria es un proceso mediante el cual una empresa o un profesional externo a la organización auditada, realiza una recopilación de información para posteriormente realizar una evaluación y elaborar un informe.

En el caso de la auditoria informática, lo que se analiza y evalúa son las evidencias que determinan si el sistema de información de la organización protege el activo más importante de la empresa, la información, si garantiza la integridad de los datos y si está al corriente con la normativa. A lo largo de este proceso se estudian los distintos mecanismos de control que la organización tiene implantados, si éstos son adecuados o no y, en el caso de que no lo sean, qué tipo de medidas serían necesaria adoptar.

Con la auditoria informática se persiguen principalmente 3 objetivos:

1. Analizar la eficacia que tienen los sistemas informáticos de la empresa.
2. Comprobar que están cumpliendo la normativa referente a este campo.
3. Revisar que los recursos informáticos se están gestionando eficazmente.

Dentro de la auditoría informática podemos encontrar otros tipos de auditorías, que se centran en partes más específicas de la informática, los cuales, los podemos encontrar en el Anexo V.

Centrándonos en la auditoria de cumplimiento de la normativa en materia de protección de datos, podemos decir que pretende verificar que se están cumpliendo las distintas medidas de seguridad establecidas en la Ley Orgánica de Protección de Datos referentes a ficheros automatizados y no automatizados que contengas datos de carácter personal. Ésta, según establece la ley para determinados niveles de datos, deberá realizarse cada dos años excepto si se realizan importantes cambios en los sistemas de información que puedan perjudicar a la seguridad de dicha información; en este caso deberá de realizarse la auditoria para comprobar la seguridad.

El proceso de auditoria consta de cuatro fases principales:

Planificación

Esta fase consiste en identificar dónde se encuentran los datos personales, qué fuentes de información utilizaremos, dónde podemos encontrar los ficheros o las instalaciones a auditar. En base a ello, hacemos un programa para el desarrollo de la auditoría.

Recogida de información

Una vez que hemos realizado la planificación es necesario recabar todos los datos necesarios, pudiendo ser éstos la relación de ficheros, así como su estructura y su contenido, el documento de seguridad, las auditorías realizadas años anteriores, la política de seguridad, la relación de los usuarios, cuáles son sus funciones y que accesos tienen autorizados, un inventario de soportes, así como su entrada y salida, inspección visual… etc. Una forma muy útil de recabar información es la realización de un cuestionario en el que se recojan los aspectos relevantes a considerar en la auditoría.

Evaluación

Una vez que tenemos toda la información se lleva a cabo una evaluación de la misma.

Se determina los tipos de medidas que deben de tomar y si tienen algún tipo de deficiencia.

Redacción del informe de auditoría

El siguiente paso es la realización del informe de auditoría, en el cual, será necesario incluir lo siguiente: las medidas y controles que se establecen en el reglamento, las deficiencias encontradas y las medidas qué se podrían utilizar para corregirlas.

El informe deberá de incluir además todas aquellas pruebas, datos… que nos han llevado a determinar que se ha producido una deficiencia, son las evidencias.

Una vez realizado el informe, el responsable de seguridad deberá de analizarlo y sacar unas conclusiones, las cuales, se las tendrá que hacer saber al responsable del fichero para que lleve a cabo las medidas necesarias. Dicho informe deberá de estar a disposición de la Agencia Española de Protección de Datos para su revisión.

2.4 SEGURIDAD DE LA INFORMACIÓN: La protección de la intimidad

La seguridad informática, refiere, en último término, a la **seguridad de la información.** La información es considerada el activo más importante de la empresa y hay que evitar que ésta sea modificada por terceras personas no autorizadas, así como evitar su pérdida, puesto que la información para las empresas es valiosa, crítica y sensitiva.

- **Valiosa**: es el activo más importante de la empresa.
- **Critica:** Es un elemento imprescindible para las operaciones de la empresa.
- **Sensitiva:** Solo debe ser considerada y manejada por personas autorizadas y de confianza para la empresa

La seguridad de la información consiste fundamentalmente en preservar estas tres dimensiones: confidencialidad, disponibilidad e integridad; adicionalmente se han de contemplar otra serie de requisitos como son la autenticidad, el no repudio, la confiabilidad y la trazabilidad.

- **Confidencialidad:** Refiere a que la información solo sea conocida por personal autorizado. Cuando se produce una falta de confidencialidad puede provocar grandes daños al propietario.
- **Integridad:** Refiere a que el contenido no se altere por personal no autorizado y que se mantenga la exactitud y completitud de la información. Los distintos fallos que pueden estar relacionados con la integridad son las anomalías en el hardware, virus informáticos, software malicioso o modificaciones realizadas por personas que se infiltran en los sistemas.

- **Disponibilidad:** Es la capacidad o característica de la información que la hace siempre disponible para el manejo por parte del personal autorizado. Si preservamos la disponibilidad, conseguiremos controlar y evitar cortes en el servicio producidos, por ejemplo, por fallos en el hardware o en las actualizaciones del sistema.

Aparte de estas características, que son las fundamentales, la seguridad de la información también requiere preservar lo que se indica a continuación.

- **Autenticidad:** Asegura la identidad del origen de la información, además de determinar que la información es válida y se puede utilizar en forma, tiempo y distribución.
- **No repudio:** Es la propiedad que garantiza demostrar quién envió o recibió un mensaje
- **Confiabilidad:** Refiere a que la información debe de obtenerse de aquellas fuentes que sean fiables.
- **Trazabilidad:** Nos permite conocer la trayectoria e historia de la información.

3. MARCO LEGAL Y ESTÁNDARES NACIONALES E INTERNACIONALES

En materia de seguridad informática existen una serie de normas, estándares, protocolos, reglas, métodos y herramientas que se han desarrollado para ayudar a minimizar los posibles riesgos que se puedan presentar en el sistema informático. En este apartado vamos hacer en primer lugar, una severa revisión de algunos de ellos; la norma ISO 27001, ya que es la norma principal de la serie 27000 y es la que contiene los requisitos para un óptimo sistema de gestión de la seguridad de la información; el esquema nacional de seguridad en el cual podemos encontrar las medidas a implantar, para poder garantizar la seguridad en las operaciones electrónicas realizadas con la administración pública; y finalmente nos centraremos en la legislación en materia de protección de datos (qué será objeto de nuestro estudio en el capítulo siguiente).

3.1 NORMA ISO 27001

Cuando hablamos de ISO nos estamos refiriendo a la Organización Internacional de Normalización nacida tras la segunda guerra mundial, concretamente el 23 de febrero de 1947. Está formada por un conjunto de Institutos de normas nacionales correspondientes a 163 países, teniendo cada país un miembro en esta organización. Para una buena coordinación del sistema posee una sede central en Ginebra (Suiza).

Las normas elaboradas por dicha organización son de carácter voluntario para su adopción en los distintos países, ya que es una organización no gubernamental y además no depende de ningún organismo internacional.

Su objetivo principal es desarrollar estándares en diferentes campos: en procesos de producción, en materia medio – ambiental…o en seguridad de la información.

Dentro de todas las normas activas que posee, nos centramos en la norma ISO 27001, certificable y de gran relevancia en lo que se refiere a la seguridad informática y de la información. Ésta fue publicada en octubre de 2005 para gestionar la información de las empresas. Con este estándar se facilita un modelo para poder implementar, establecer, monitorizar, utilizar, revisar, mantener y mejorar lo que denominamos sistema de gestión de la seguridad de la información (SGSI).

Este estándar es certificable, por lo que cualquier organización que haya llevado a cabo la implantación del SGSI, puede solicitar que se le realice una auditoría externa por una

entidad acreditada. Si la organización supera dicha auditoria esta podrá recibir el certificado de ISO 27001. En el Anexo VI podemos ver la estructura de esta norma.

Sistema de seguridad de la información (SGSI)

El SGSI, también conocido por sus siglas en inglés ISMS (Information Security Management System) se desarrolla en la norma ISO 27001. Es un proceso documentado, estructurado, eficiente y sistemático que tiene que ser conocido por todo el personal de la empresa y que se pueda adaptar a los cambios del entorno. Según establece ISO, el SGSI debe disponer de una serie de documentos, los cuales, se desarrollan en el Anexo VII.

Modelo PDCA

Para poder implantar y gestionar el SGSI es necesario seguir el ciclo continuo PDCA, también denominado Edward Deming, basado en la mejora continua. Se utiliza este ciclo, ya que para garantizar la seguridad de la información no es suficiente la implantación de un sistema de gestión de la información (SGSI) sino que también es necesario realizar una revisión periódica y una continua actualización y mejora de dicho sistema. Por tanto, el modelo PDCA ayuda a la implementación y seguimiento del SGSI.

Sus siglas "PDCA" significan Plan (planificar) – Do (hacer) - Check (verificar) y Act(actuar). Estas son las cuatro etapas que hay que realizar para conseguir la mejora continua; además, una vez que llegamos a la última etapa hay que volver al principio para seguir mejorando (mejora continua).

Plan (planificar)

Consiste en establecer el SGSI; para ello es necesario:

1. Tener claro cuál es el alcance del SGSI
2. Definir la política de seguridad de la organización, en la cual es necesario incluir los objetivos que tiene la empresa respecto a la seguridad de la información; debe de estar enlazada con la gestión de riesgos, y debe de establecer los criterios que se van a utilizar para evaluar los riesgos
3. Establecer el método que se va a utilizar para evaluar los riesgos, así como los criterios necesarios que tiene que tener un riesgo para poder aceptarlo.

4. Identificar todos aquellos activos del SGSI y los responsables de los mismos. Conocer las vulnerabilidades que tienen, amenazas que se puedan aprovechar de ellas y los impactos posibles.
5. Evaluar el impacto que se puede producir en el caso de un error en la seguridad de la información, la probabilidad de que ocurra el error y determinar si un riesgo se acepta o no en función de los criterios que se han establecido.
6. Identificar y evaluar las distintas opciones que tenemos para tratar los riesgos, para de esta forma poder establecer controles, evitar el riesgo, transferirlo o asumirlo.
7. El SGSI debe de ser aprobado por la dirección de la empresa el uso y implantación del mismo, además de los riesgos residuales.

Do (hacer)

Consiste en implementar y utilizar el SGSI. Se define un plan para tratar los riesgos a los que nos enfrentemos, en el cual se debe de identificar las acciones realizadas, los recursos utilizados y las responsabilidades en la gestión de los riesgos. Este plan debe ser implantado para poder conseguir los objetivos de control que se han identificado. También se deben de implantar controles que se han utilizado anteriormente y un sistema de medida para obtener resultados comparables y reproducibles para poder medir si los controles utilizados son eficaces. Además, se gestionarán los recursos necesarios para el mantenimiento de la seguridad, así como el establecimiento de controles que permitan detectar de una forma rápida los incidentes surgidos y responder ante ellos. Por último, es necesario formar y concienciar al personal sobre la seguridad de la información

Check (verificar)

Consiste en realizar un control para verificar que todos aquellos procedimientos que se han implantado en el SGSI son los adecuados. Para ello, es necesario realizar periódicamente exámenes para asegurarnos de que el SGSI que se ha implantado es eficaz. También hay que revisar los niveles de riesgo que son aceptados por la organización y realizar de forma periódica una auditoria del SGSI.

Act (actuar)

Es la última etapa del ciclo, y en ella se desarrollan las mejoras a los problemas que hemos identificado en el SGSI. Se valoran las propuestas y se llevan a cabo una serie de medidas correctivas o preventivas; es necesario mantener cierta comunicación con el personal de la empresa para que esté informado de las nuevas medidas que se incorporan.

Una vez que hemos llegado a la última etapa del ciclo es necesario regresar a la primera, para estar continuamente introduciendo nuevas mejoras en el SGSI.

Certificación del SGSI

Según ISO (Organización Internacional de Normalización) la definición de certificación es la siguiente: "procedimiento mediante el cual un organismo da una garantía, por escrito, de que un producto, proceso o servicio está conforme a los requisitos especificados". Estos certificados deben de ser emitidos por entidades que tienen potestad para ello, es decir, las entidades de certificación. Según el ENAC (Entidad Nacional de Acreditación), existen 18 entidades de certificación, de las cuales cuatro de ellas son las que hacen referencia a la certificación de sistemas de seguridad de la información, siendo éstas las siguientes:

- AENOR, Asociación Española de Normalización y Certificación
- LGAI TECHNOLOGICAL CENTER S.A (Applus +)
- BUREAU VERITAS IBERIA S.L
- OCA Instituto de certificación, S.L (Unipersonal)

La encuesta ISO Survey, recoge la cantidad de certificados realizados de cada una de las normas, así como su evolución a lo largo de los años. Respecto a la Norma ISO 27001 del año 2013 al 2014 ha aumentado el número de certificados en un 7% como podemos ver en la siguiente tabla.

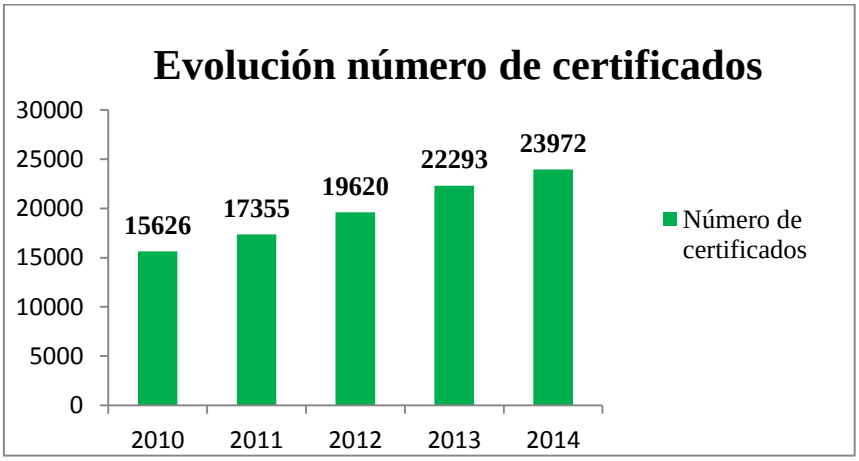
Tabla 1. Número de Certificaciones

Standard	number of certificates in 2014	number of certificates in 2013	evolution	evolution in %
ISO 9001	1 138 155	1 126 460	11 695	1 %
ISO 14001	324 148	301 622	22 526	7 %
ISO 50001	6 778	4 826	1 952	40 %
ISO/IEC 27001	23 972	22 349	1 623	7 %
ISO 22000	30 500	26 847	3 653	14 %
ISO/TS 16949	57 950	53 723	4 227	8 %
ISO 13485	27 791	25 655	2 136	8 %
ISO 22301	1 757			
TOTAL	**1 609 294**	**1 561 482**	**47 812**	**3 %**

Fuente: **http://www.iso.org**

Con los datos obtenidos mediante esta encuesta también podemos observar que se ha producido un aumento en este tipo de certificaciones en el periodo 2010 – 2014 de forma general, englobando a todos los países. A continuación mostramos una gráfica de elaboración propia de dicha evolución en función de los datos obtenidos mediante dicha encuesta.

Gráfico 1. Evolución número de Certificados



Fuente: **http://www.sbqconsultores.es**

En lo que respecta a España, ésta se encuentra en el puesto número 8 del ranking, con 799 certificados. En el Anexo VIII podemos encontrar la tabla del ranking de países en certificaciones.

En España, las dos entidades certificadoras que consideramos más importantes, son AENOR y Bureau Veritas Iberia S.L

AENOR es la Asociación Española de Normalización y Certificación creada en 1986 como consecuencia de la unión de España a la Unidad Económica Europea, ya que se hizo necesario disponer de una entidad similar a la que poseían otros países en este tipo de materia, como IRANOR, con el fin de divulgar que la calidad es un aspecto importante en las organizaciones para mejorar la competitividad de las mismas.

Ésta es una entidad privada y sin ánimo de lucro que es de alto reconocimiento en el ámbito nacional, comunitario e internacional. El objetivo es mejorar la calidad y competitividad tanto de las empresas como de sus productos y servicios mediante normas técnicas y certificaciones, que proporcionen garantía y confianza.

En materia de seguridad de la información, AENOR tiene como objetivo principal garantizar la seguridad del sistema de información de las empresas, así como la seguridad de los distintos procesos informáticos que se utilizan, ya que cualquier fallo en este sentido puede generar grandes pérdidas en la organización, así como en la calidad del propio servicio que se ofrece.

La certificación expedida por AENOR garantiza que la empresa que la posee tiene identificadas y controladas las amenazas y que, tras analizar los riesgos a los que está expuesta, ha establecido una serie de controles (o contramedidas o salvaguardas) que le permiten prevenir, reducir o eliminar dichos riesgos, garantizando la seguridad y la eficiencia en la gestión y en los servicios que ofrece.

Para poder obtener la certificación es necesario que se lleve a cabo una auditoria. Ésta solamente se podrá llevar a cabo una vez que han pasado tres meses desde que entró en funcionamiento el Sistema de Seguridad de la Información (SGSI).

Una vez realizada la auditoria, si ésta se pasa satisfactoriamente, se certifica que la organización tiene un SGSI conforme a la correspondiente norma. Los certificados y normas que se pueden obtener son los siguientes:

- Certificado AENOR de sistemas de gestión de seguridad de la información.
- Licencia para usar la marca de AENOR de seguridad de la información.
- Certificado IQNet, el cual permite que el certificado AENOR se reconozca internacionalmente.
- Licencia para usar la marca IQNet.

Las marcas que utiliza para indicar la certificación son las siguientes:

Figura 3. Marca de Certificación de Aenor

Figura 2. Marca Certificado IQNet

Fuente: www.aenor.es

La otra entidad certificadora es **LGAI TECHNOLOGICAL CENTER S.A.** Esta entidad pertenece al grupo Applus, que, entre otras actividades, se dedica a la certificación. Esta entidad tiene sus orígenes en el año 1907 en Barcelona, cuando se decidió crear el laboratorio de investigaciones y ensayos.

Es una empresa dedicada a la inspección, ensayos y certificaciones para garantizar que los productos y activos de las organizaciones cumplen las normas y los reglamentos establecidos.

Sus orígenes se remontan al año 1996 con la denominación de Nace Agbar Automotive. En el año 2000 entra en el mercado de EE.UU cuando decidió comprar una empresa dedicada a controlar las emisiones de los vehículos y dos años más tarde se lanza la marca Applus + de forma global. En 2003 consigue expandirse tecnológica e internacionalmente mediante la gestión de LGAI, empresa dedicada a los ensayos e investigaciones en laboratorios. En 2004 pasa a ser la mayor compañía en lo que se refiere a asistencia técnica en España e inspección industrial y medioambiente.

En lo que se refiere a las certificaciones, Applus + puede proporcionar distintos tipos de certificaciones ya que tiene experiencia en varios sectores. En lo que refiere a seguridad de la información Applus + certifica el cumplimiento de las normas ISO 27001, certificando que el sistema de seguridad de la información que tiene implantado es el adecuado. La marca de Applus + para reconocer dicha certificación es la siguiente:

Figura 4. Certificado Applus +

Fuente: www.applus.com

3.2 ESQUEMA NACIONAL DE SEGURIDAD

El Esquema Nacional de Seguridad también denominado ENS, es un documento regulado por el real decreto 3/2010, de 8 de enero, BOE 29 enero, en el cual, se determinan las distintas medidas de seguridad de la información que deben de tomar las administraciones públicas en el uso de los distintos medios electrónicos. Con dicha ley se obliga a tener que definir una serie de medidas para tener una adecuada protección de la información.

Si se aplica este esquema de la forma correcta estamos asegurando la integridad, confidencialidad, disponibilidad, acceso, autenticidad, trazabilidad, conservación de datos y de información, así como los servicios utilizados en medios electrónicos.

Según lo dispuesto en dicha ley estarán obligados a su aplicación los siguientes grupos:

- Administraciones públicas. Dentro de éstas encontramos la administración general del estado, de las comunidades autónomas, las entidades que integran la administración local y las entidades de derecho público que son dependientes o vinculadas de éstas.
- Ciudadanos que mantengan relaciones con las administraciones públicas.
- Relaciones entre las diferentes administraciones.

Es importante tener en cuenta que dicha ley no se aplicara a las administraciones públicas en las actividades que éstas desarrollen en régimen de derecho privado.

Respecto a su estructura, el ENS se encuentra dividido en tres partes fundamentales: los requisitos mínimos, los principios básicos y las medidas de seguridad. En el Anexo IX podemos ver la estructura con más detalle.

3.3 NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS.

En el siguiente apartado nos centramos en la protección de datos de carácter personal; analizamos el marco legal en España y en el resto del mundo.

3.3.1 La protección de datos en España: La LOPD (Ley Orgánica de Protección de Datos)

En España la ley que regula la protección de datos personales es la Ley Orgánica de Protección de Datos Personales, denominada LOPD. Ésta fue desarrollada para dar cumplimiento al artículo 18 de la Constitución Española, en el cual, se trata el tema de la intimidad y el honor de las personas. Dicha ley fue aprobada en las Cortes Españolas el 13 de diciembre de 1999. Esta ley es de aplicación en el entorno laboral ya que en él se manejan datos de carácter personal; por tanto, esta ley obliga a las empresas a realizar una serie de acciones para mantener la seguridad de este tipo de datos. En el caso de no cumplir la normativa, las empresas tendrán que hacer frente a las sanciones establecidas por la Agencia Española de Protección de Datos (AEPD).

La LOPD establece como derecho fundamental de las personas físicas el derecho de protección de los datos personales. Por tanto, obliga a la protección de dichos datos, tanto si están en ficheros informatizados como en papel, en todos los entornos, tanto empresas como administraciones públicas, y para distintos usos (ya sean datos de clientes, empleados,…)

Como primera medida, para dar cumplimiento a la LOPD todos los ficheros con datos personales deben de ser notificados a la AEPD para ser inscritos; una vez inscritos, si es necesario, estos podrán ser modificados o suprimidos.

En la LOPD los datos de carácter personal se clasifican en tres niveles: básico, medio y alto; cada nivel requiere unas medidas a aplicar para garantizar la seguridad. A continuación mostramos un cuadro en el que mostramos distintos tipos de datos personales (de diferentes niveles) y las medidas que les corresponde aplicar.

Tabla 2. Niveles y medidas de seguridad

Nivel básico	Nivel Medio	Nivel Alto
Nombre Apellidos Domicilio Teléfono Correo electrónico	servicios financieros Hacienda infracciones administrativas infracciones penales	Religión Ideología Salud Origen racial
Medidas de seguridad		
Control de acceso Gestión de soportes Copias de recuperación y respaldo Identificación y autenticación de usuarios Documento de seguridad Actividades y obligaciones del personal	Responsable de seguridad Auditoria bianual Controlar el acceso físico	Seguridad sobre la distribución de los soportes Registro de los accesos Mayor número de medidas para las copias de respaldo

Conforme subimos de nivel, además de aplicar las normas del nuevo nivel también hay que aplicar las de niveles anteriores.

Como la aplicación de la ley es de carácter obligatorio, la Agencia Española de Protección de Datos, proporciona distintas herramientas y utilidades para facilitar el cumplimiento de la Ley. Dichas utilidades están disponibles en el sitio web de la AEPD (Agencia Española de Protección de Datos).

- **Evalua:** Esta herramienta es gratuita para los responsables de los ficheros. Con ella se permite que las empresas y administradores puedan realizar una evaluación sobre el grado de cumplimiento de la LOPD. Con esta autoevaluación se consigue conocer el nivel de cumplimiento que se alcanza y verificar si se están cumpliendo las medidas de seguridad que son necesarias.
- **Dispone:** Esta herramienta está enfocada a aquellas organizaciones que deben de notificar ficheros que son de titularidad pública. Esta herramienta es de gran

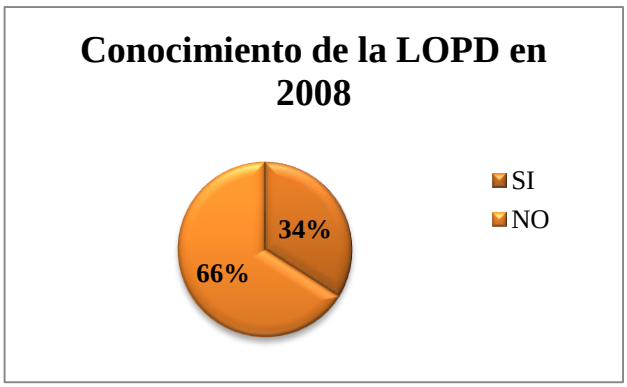
ayuda a los responsables para elaborar la disposición general, el acuerdo de creación, modificación o supresión de los ficheros.

- **Guía documento de seguridad**
- **Guía de video - vigilancia**
- **Guía de uso de cookies**
- **Guía de seguridad y privacidad de las tecnologías RIDF (identificación por frecuencia)**
- **Guía para realizar una evaluación del impacto en la protección de datos**
- **Guía para clientes que contraten servicios de Cloud Computing**
- **Guía para el responsable de seguridad**

Con estas herramientas la Agencia Española de Protección de Datos Personales, está favoreciendo el cumplimiento de la ley por parte de las organizaciones, ya que les orientan en cómo adaptarse a la ley y como evaluar el grado de cumplimento de la misma.

Para analizar el grado de cumplimiento de dicha ley he tomado como referencia un estudio realizado por el Instituto Nacional de tecnologías de la comunicación (INTECO), denominado actualmente INCIBE (Instituto Nacional de Ciberseguridad). En este informe se indica que en 2012 el 86,4% de las empresas conocían dicha normativa frente a un 36% en 2008. En el siguiente gráfico mostramos lo gráficos correspondientes a 2008 y 2012.

Gráfico 2. Conocimiento de la LOPD en 2008



Fuente: https://www.incibe.es

Gráfico 3. Conocimiento de la LOPD en 2012

Fuente: https://www.incibe.es

Por otro lado, la mayoría de empresas afirman estar aplicando la normativa, un 80,4%, frente a un 10,4% que no están aplicándola y un 9,2% que no sabe o no contesta.

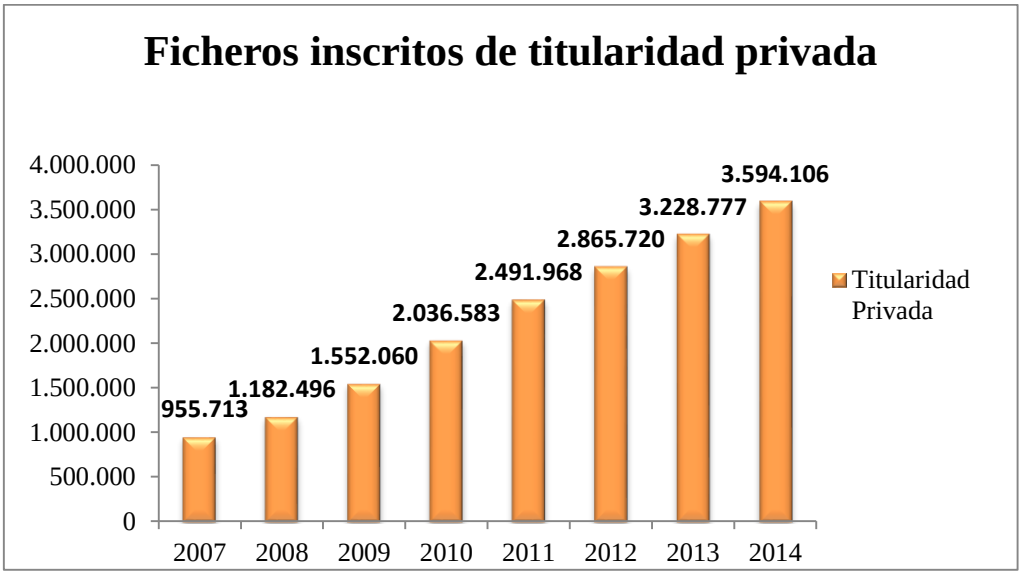
Todos estos datos son generales, englobando a todas las empresa, pero si nos centramos en las pymes, estos porcentajes bajan notablemente. Con esto llegamos a la conclusión de que cuanto mayores son las dimensiones de la empresa mayor es el grado de aplicación de la normativa de protección de datos personales.

Otra indicador para medir el grado de cumplimento de la LOPD es atendiendo al número de ficheros que han sido inscritos en el Registro General de Protección de Datos. De forma general, según la Memoria 2014 de la Agencia General de Protección de Datos personales, el número de ficheros inscritos a finales de 2014 fue de 3.746.930 ficheros, de los cuales, el 95,92% corresponden a titularidad privada y el 4,07% a titularidad pública. Haciendo una comparación respecto 2013, año en el que se inscribieron 3.375.059 ficheros, se ha producido un incremento de 11%.

A continuación, vamos a realizar un análisis de los ficheros inscritos en función de si éstos son de titularidad privada o pública.

En el caso de los ficheros de titularidad privada, si realizamos una comparación entre 2013 y 2014, podemos decir que el número de inscripciones ha aumentado un 11,31%; además, se ha producido un incremento de las entidades pertenecientes al sector privado que tienen ficheros inscritos, pasando de un 11% a un 12%. En el gráfico que mostramos a continuación podemos observar una evolución del aumento de ficheros inscritos desde 2007.

Gráfico 4. Evolución Ficheros Inscritos Titularidad Privada

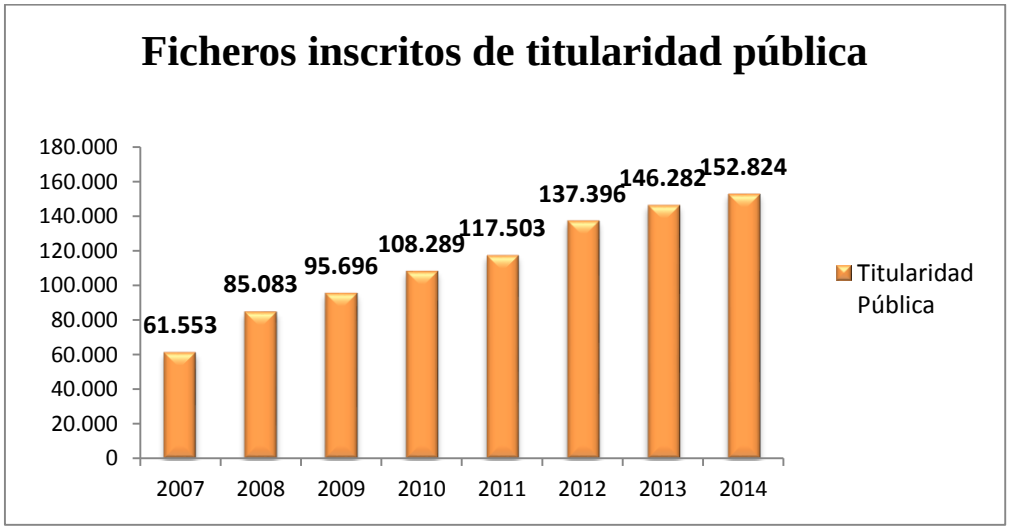


Fuente: http://www.agpd.es/

Con estos datos, podemos deducir que está aumentado el grado de sensibilización para el cumplimiento de la LOPD por parte de las organizaciones, principalmente las privadas.

El número de ficheros de titularidad pública inscritos también se ha visto incrementado en un 4,8% respecto 2013; también significativo tener en cuenta que se produjo un incremento del 6,5 % entre 2012 y 2013. En el siguiente gráfico podemos observar la evolución de ficheros inscritos desde 2007 a 2014.

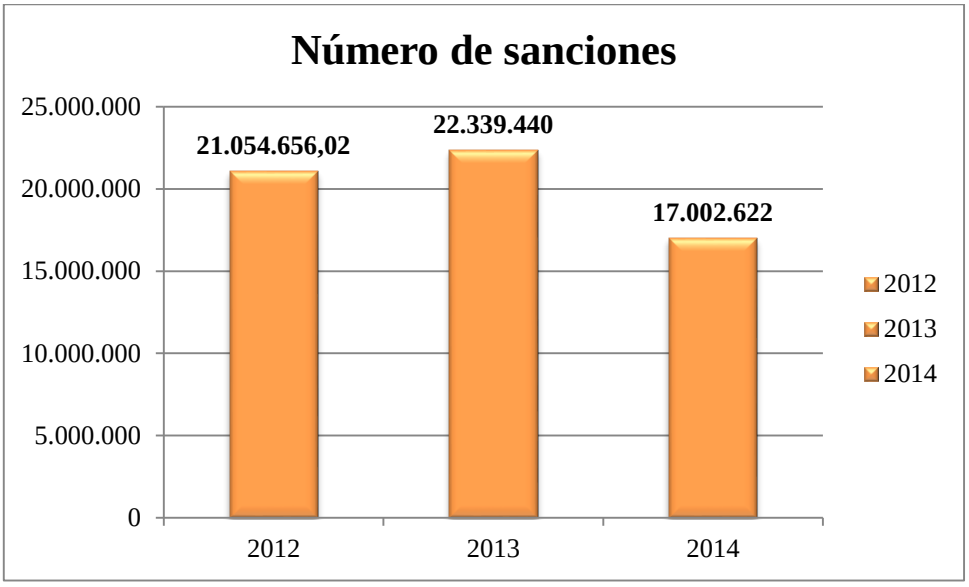
Gráfico 5. Evolución Ficheros Inscritos Titularidad Pública



Fuente: http://www.agpd.es/

Otra indicador para medir el grado de cumplimiento de esta ley es observando el número de sanciones que se han producido. Para ello hemos realizado una comparación entre 2012 y 2014.

Gráfico 6. Evolución Número de Sanciones por Incumplimiento LOPD

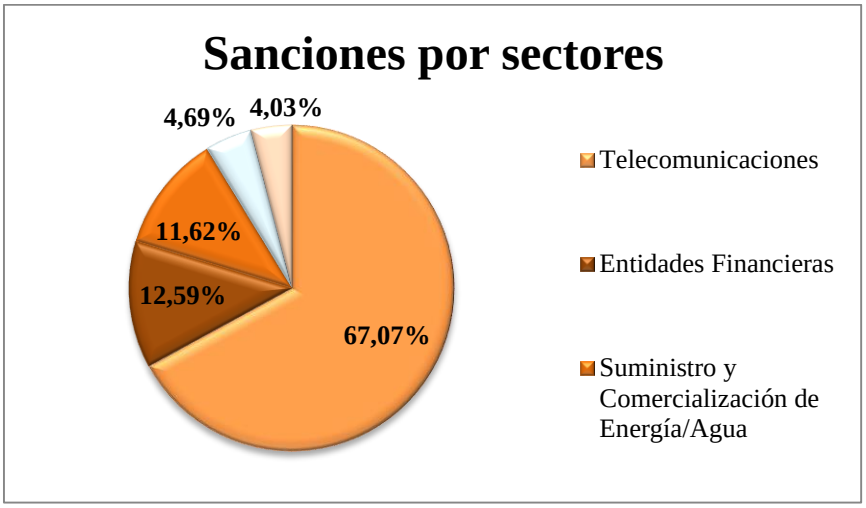


Fuente: https://www.incibe.es

Como podemos observar, en 2014 se ha producido una disminución del número de sanciones aplicadas, aunque de 2012 a 2013 hubo un incremento.

Por otro lado, si realizamos la comparación por sectores, como podemos ver en el siguiente gráfico, el sector más sancionado es el sector de las telecomunicaciones. En mi opinión, esto es debido a que cada vez es más frecuente el uso de las tecnologías y sobre todo de Internet, y en muchas ocasiones no se informa claramente al usuario de la recopilación y tratamiento de datos personales. En segundo lugar en este ranking, se encuentran las entidades financieras, lo cual hace desconfiar a los clientes de éstas, ya que en este sector es de gran relevancia la protección de datos personas. En menor medida encontramos sanciones en el sector de los suministros y comercialización de energía y agua, publicidad y comunicaciones electrónicas comerciales, mayoritariamente debido al Spam.

Gráfico 7. Número de Sanciones por Sectores



Fuente: https://www.incibe.es

Por último, otro indicador para medir el grado de cumplimiento es la existencia de documento de seguridad. Es obligatorio para dar cumplimiento a la LOPD y en él, en particular, todas las medidas técnicas y organizativas para la seguridad de la información. Según los datos obtenidos del Instituto Nacional de tecnologías de la comunicación (INTECO) sobre cumplimiento de la LOPD durante 2012, ya que no hemos obtenido datos más recientes, todavía hay un 43% de empresas que no lo tienen.

3.3.2 Protección de datos en el mundo

En la actualidad, son habituales las relaciones con empresas de diferentes países, por lo que son frecuentes las transferencias internacionales de datos de carácter personal. Por tanto, es necesario conocer la normativa que se aplica para el tratamiento de este tipo de datos en el resto de países.

Todos los países pertenecientes a la Unión Europea se rigen por una normativa en común, la Directiva 95/46/CE, que entró en vigor en 1995 y que trata lo relativo a la protección de datos de carácter personal y su libre circulación entre los distintos países de la Unión Europea; además, prohíbe la transferencia de datos a países que no regulan un nivel adecuado para protección de este tipo de datos. En 2012 se propuso realizan una reforma en la legislación, ya que cada día es más habitual realizar operaciones de forma online, en las que nuestros datos personales pueden quedar desprotegidos. Tras tres años de debate, en junio de este mismo año se aprobó la nueva legislación, en la que se pretende proteger datos en este tipo de operaciones, es decir, proteger los derechos

online del usuario. Con esta nueva ley se pretende que todos los usuarios tengan que dar consentimiento para el procesamiento de sus datos y que las empresas tengan que ser más claras a la hora de explicarles a los usuarios por qué se recogen los datos y cuál será su uso; también permite que se realice una portabilidad de datos a los usuarios que piensen que sus datos no se encuentran seguros en la red; establece que las empresas tendrán un periodo de 72 horas para comunicar a los clientes si han sufrido algún tipo de ataque externo que pueda afectar a los datos que tienen almacenados, así como la obligatoriedad de contratar oficiales de protección de datos a las grandes empresas; las compañías de internet solo podrán procesar información personal en el caso de que se dé el consentimiento del afectado. Es importante destacar la incorporación del derecho al olvido, por el cual, el usuario puede reclamar que se borre su información personal si ésta le puede perjudicar o no es oportuna. Por último, respecto a las sanciones aplicadas en el caso de incumplimiento de la protección de datos serán de un 2% de la facturación global de la empresa y, en el caso de tener que extender una queja, se realizará ante la Agencia de Protección de Datos Nacionales.

Además de esta norma, cada país dispone de una ley de protección de datos particular que se adapta a las diferentes condiciones económicas, culturales y políticas de cada país. Como éstas no son igual de restrictivas en todos los países, la Unión Europea obliga revisar la legislación a los países que por debajo del nivel requerido y que quieran realizar transferencia de datos.

Para la transferencia de datos a terceros, según establece la Directiva, es necesario un cierto nivel de seguridad. Según establece la Agencia Española de Protección de Datos, los países que alcanzan este nivel son los siguientes:

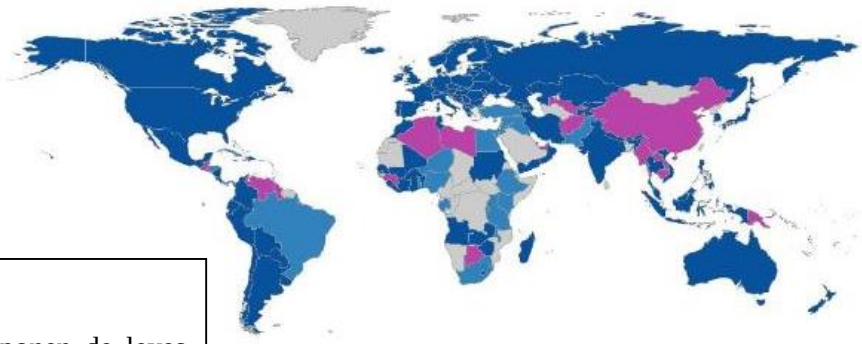
Suiza	Canadá	Argentina
Guernsey	Isla de Man	Jersey
Islas Feroe	Andorra	Israel
Uruguay	Nueva Zelanda	

Son los países considerados seguros para transferir datos con ellos, ya que estos tienen elaboradas sus propias normas específicas para la protección de datos personales, en las que se cumplen los principales principios establecidos por la Unión Europea. En el caso de tener que realizar transferencias de datos con países que, en principio no tienen

garantizado un nivel adecuado de seguridad, es necesario, la autorización de la Agencia de Protección de Datos respectiva de cada país.

En el siguiente mapa, podemos ver qué países disponen de legislación en materia de protección de datos, cuáles no la tienen, si tienen proyectos de ley o simplemente no se disponen de datos suficientes para poder clasificarlo en uno de los tres grupos anteriores.

Figura 5. Mapa de legislación en protección de datos



Leyenda:

Azul oscuro: disponen de leyes en vigor

Azul claro: proyectos de ley

Violeta: sin legislación

Gris: no se disponen de datos

Fuente: www.unctad.com

Observando el mapa, vemos que hay muchos países que disponen de leyes para la protección de datos o, por lo menos, tienen proyectos de ley, lo cual, favorece la transferencia de datos en entre países.

A continuación, mostramos la normativa que regula la protección de datos en otros países, fuera de la Unión Europea.

Australia:

Ley Federal Australiana de Protección de Datos, The Privacy and Protection Bill 1994 (NSW)

Rusia:

Ley de Protección de Datos, 2006. El 1 de septiembre de 2015 se aprobaron las enmiendas de esta ley, en las que desarrolla que cualquier compañía, sea nacional o extranjera, que trabaje con usuarios de internet que sean rusos, deberán de recoger,

manipular y almacenar los datos en servidores o bases de datos que se encuentren dentro del propio país.

Norte América

Si comparamos las leyes sobre protección de datos personales que se aplican en Norte América no son muy restrictivas en comparación con las establecidas en la países miembros de la Unión Europea. En los distintos países se establecen diferentes normas de protección de datos.

- Canadá: PIPEDA (Ley de Protección de Información Personal y de Documentos Electrónicos). Esta ley está dirigida a la protección de la información personal por parte del sector privado.
- Estados Unidos: En este país no existe ninguna ley general para la protección de datos personales, sino que dispone de tres normas específicas referentes a los datos de salud, datos de crédito y protección de los menores.

HIPPA (Ley de Transferibilidad y Responsabilidad del Seguro Sanitario)

Promulgada en 1996 con el objeto de proteger la información de salud individual. En el desarrollo de esta ley se indica quiénes pueden tener acceso a este tipo de información, siendo generalmente los médicos.

FACTA (Ley Federal de Transacciones Crediticias Justas y Exactas)

Esta ley fue aprobada en el año 2003 con el objeto de proteger la información sobre créditos.

COPPA (Ley de Protección de la Privacidad de los Menores en Estados Unidos)

Esta ley se elaboró en 1998 para proteger la privacidad de los menores de 13 años. Principalmente está dirigida a las páginas web dirigidas a niños, en las que deben de indicar las políticas de privacidad que utilizan e informan sobre la información personal se almacena y que se realiza con ella.

Estados Unidos es un país potencial con el que muchos países de la comunidad realizan continuamente transferencia de datos personales. Esto es posible debido a que Estados Unidos está adherido a los acuerdos de cooperación "Safe Harbour" (Puerto Seguro), en los que se desarrollan una serie de principios que se tienen que tener en cuenta para proteger este tipo de datos. Al encontrase adherido a estos

acuerdos, tiene la obligación de cumplir la legislación en esta materia establecida por la Unión Europea. Dichos principios son 7 y son los siguientes:

- Información: Aquellos a los que se les recojan datos, será necesario que se les informe de su recogida y de que solo se tratarán para la finalidad para la que se han recogido
- Elección: Tendrán derecho a cancelar u oponerse a que su datos se recojan una vez que se han recabado y oponerse a que se cedan o transfieran a terceras personas.
- Transferencia progresiva: Cuando se cedan datos a terceros se realizará con organizaciones que garantizan un correcto nivel de cumplimiento de protección de datos
- Seguridad: es necesario determinar y cumplir todas las medidas de seguridad que son necesarias para que no se pierda la información y no se realicen accesos que no están autorizados.
- Integridad de los datos: Los datos no deben de sufrir modificaciones.
- Acceso: aquellos a los que se les haya recabado información podrán acceder en cualquier momento a ella y corregirla o eliminarla.
- Ejecución: Se deben de utilizar los medios y recursos que garanticen el cumplimiento de todos estos principios.

Iberoamérica

Las mayorías de leyes aplicadas a la protección de datos personales son semejantes a las de la Unión Europea. De forma general, para proteger los datos utilizan un mecanismo denominado "Habeas Data", el cual, se utiliza para detener el abuso de datos personales. Este mecanismo no exige a las entidades públicas y privadas que protejan este tipo de datos, sino que favorece que la persona afectada, después de presentar una denuncia ante la justicia, pueda acceder y tenga la capacidad para poder rectificar los datos personales que puedan atentar a la privacidad del individuo.

Todos los países que iberoamericanos tienen normas que hacen referencia a los datos de carácter personal. Algunas de ellas se nombran a continuación.

- México: Ley Federal de Protección de Datos en Posesión de Particulares, julio de 2010, por la que se regula el tratamiento de datos personales por parte del sector

privado y no es de aplicación a datos que han sido procesados por organismos estatales.

- Argentina: Este país fue el primero en introducir una ley que afectará a la protección de datos personales; esta es la Ley nº 25.326, Ley de Protección de los Datos Personales.
- Chile: Ley nº 19.628, de 1999.
- Colombia: Ley 1.581 del 17 de octubre de 2012, Ley Estatutaria de Protección de Datos Personales. Aparte de esta ley, también disponen de la Ley 1.266 de 2008, que es una ley especial que protege los datos personales de carácter financiero.
- Perú: Ley 29.733 del 2 de julio de 2011, Ley de Protección de Datos Personales.

África

En este continente, la mayoría de países no disponen de legislación o no se tiene datos de su existencia, por lo que no es segura la transmisión de datos dentro del propio continente. Para supervisar y controlar que se cumple la normativa de protección de datos de la Unión Europea, en cada país miembro existe una autoridad para realizar esta tarea y para intervenir en las decisiones de la elaboración de la propia ley.

4. CASOS PRÁCTICOS: Auditoria de cumplimiento de la LOPD

En este apartado nos centramos en los casos prácticos: dos auditorías de cumplimiento de la LOPD en dos entornos reales. En primer lugar, hemos realizado un auditoria sobre el cumplimiento de la LOPD en la entidad financiera La Caixa; en este tipo de entidades se trabaja con una gran cantidad de datos de carácter personal y cada vez es más usual el realizar las operaciones bancarias de forma online, en las que se transmite información a través de la red y en las que estamos expuestos a una gran cantidad de riesgos. Por otro lado, en segundo lugar, realizamos la evaluación de cumplimiento en una pequeña empresa de muebles; estos dos entornos tan diferentes nos servirán para comparar el grado de cumplimiento de la ley en una pyme frente a una empresa de grandes dimensiones.

4.1 AUDITORÍA DE CUMPLIMIENTO EN LA CAIXA

Para proteger la información y cumplir con la LOPD, es necesaria la aplicación tanto de medidas físicas como lógicas. Para ello, existe la Orden INT/317/2011, de 1 de Febrero, sobre las Medidas de Seguridad Privada, en la que se regulan las distintas medidas de seguridad obligatorias para Cajas de Ahorro, Bancos y Entidades de Crédito. Dicha orden la podemos encontrar en el Anexo X.

Aparte de las medidas de obligado cumplimiento que se desarrollan en la Orden Ministerial que hemos nombrado anteriormente, La Caixa también aplica otra serie de medidas seguridad. A la hora de aplicar dichas medidas, un aspecto muy importante que tiene en cuenta es el cumplimiento de los principios de confidencialidad e integridad de la información, ya que sobre éstos se basa la entidad. A continuación mostramos las distintas medidas que aplica.

Seguridad en las instalaciones

Es muy importante proteger las instalaciones, ya que si éstas no están protegidas tampoco lo están los equipos informáticos y la información. Para la seguridad de éstas, principalmente hay que aplicar las medidas exigidas por la ley que hemos visto anteriormente. También aplica otra serie de medidas como, por ejemplo, todas las sucursales que pertenecen al grupo la Caixa se encuentran localizadas en zonas céntricas, concretamente en las esquinas, para de esta forma evitar los robos durante el horario de apertura al público.

En esta entidad se echa en falta un control de acceso a las instalaciones por los clientes durante el horario de apertura, es decir, disponer de un sistema que controle la apertura de la puerta principal de entrada para garantizar una mayor seguridad.

Seguridad de los sistemas informáticos

Todos los sistemas informáticos de las sucursales del grupo la Caixa se encuentran protegidos de las amenazas exteriores mediante firewalls y programas antivirus, para que de esta forma no puedan interrumpir la actividad de los sistemas, dañarlos o producirse robo de información.

Diariamente se realiza un control (monitorización) sobre las diferentes acciones que se realizan en los equipos, se controla todo lo que realiza cada uno de los empleados de la entidad en ellos.

Otra medida de seguridad empleada para proteger los equipos informáticos es la prohibición de utilización de otros tipos de dispositivos ajenos a la entidad, para de esta forma evitar el poder copiar información o introducir algún tipo de amenaza que pueda dañar el sistema.

Seguridad de la información

Como hemos dicho al comienzo del apartado, la confidencialidad e integridad de la información son dos principios a tener en cuenta en todas las actividades de la entidad, por lo que se desarrollan en el código ético de la misma; dichos principios los podemos encontrar desarrollados en el Anexo XI.

Para garantizar esta confidencialidad e integridad de la información aplica las siguientes medidas:

- En una sucursal cualquiera del grupo, no todos los empleados pueden acceder al mismo tipo de información, sino que se encuentran divididos por niveles en función del tipo de información que manejan.

  Concretamente, en la sucursal que he visitado para obtener información, se encuentran trabajando 5 personas; 2 de ellas pueden acceder a la información de nivel alto, otras dos a la de nivel medio y una última a la de nivel bajo. De esta forma se está garantizando una mayor seguridad.

- Además de estar divididos por nivel, dependiendo del tipo de información que se requiere para llevar algunas gestiones será necesario solicitarla al departamento jurídico del grupo, para cumplir la Ley Orgánica de Protección de Datos.
- Todos los equipos tienen instalados sistemas biométricos en sus equipos para controlar el acceso a los mismos; concretamente utilizan la huella dactilar pero en un futuro pretenden utilizar como forma de acceso el iris del ojo.
- Las copias de seguridad y de recuperación se encuentran localizadas en instalaciones distintas de la entidad, para aumentar el grado de seguridad de la información, dando cumplimiento a la LOPD.

Además de proteger la información dentro de la propia sucursal, también es necesario aplicar una serie de medidas en las operaciones bancarias que se realizan de forma online, ya que se transmite información relevante y estamos expuestos a una gran cantidad de riesgos.

Seguridad de la información en Línea Abierta

Línea Abierta es la herramienta de banca online que utiliza la Caixa. Ésta es una herramienta proporcionada por los bancos para agilizar las operaciones de los clientes y no tener que desplazarse hasta las instalaciones, ahorrando de esta forma tiempo. Cuando se lanzó por primera vez, los clientes eran reacios a su uso puesto que lo veían muy peligroso, pero poco a poco va aumentando su utilización, ya que las entidades ponen las medidas necesarias para que la actividad se desarrolle sin incidencias.

Lo primero que realiza la Caixa es informar a los usuarios "clientes" de las medidas que deben de tomar en la utilización de internet y la banca online. Estas medidas las podemos encontrar en la página web de la entidad y en el Anexo XII.

Por otro lado, la entidad cumple con todos los requisitos legales que son necesarios para prestar este tipo de servicio garantizando la máxima seguridad de la información. Los aspectos legales que tiene en cuenta son los siguientes:

Secreto Bancario y Ley Orgánica de Protección de Datos

Cuando realizamos operaciones de forma online con la Caixa podemos encontrarnos seguros, porque ésta cumple con todos los requisitos establecidos en la Ley de Protección de Datos, ya que los datos bancarios son de carácter personal (de nivel medio) y se debe garantizar la confidencialidad, seguridad de almacenamiento y el tratamiento de dichos datos.

Identificación y control de acceso

Para poder acceder el servicio de Línea Abierta es necesario identificarse mediante un usuario y una clave formada por un PIN de cuatro caracteres, que son proporcionados por la entidad.

De forma adicional, también se puede utilizar un certificado digital para identificarse como el DNI electrónico y el IdCar (CarCert), con objeto de aumentar el grado de seguridad. Para ello es necesario que los clientes dispongan de DNI electrónico, de un dispositivo con lector de tarjetas chip que sea compatible con el certificado, los drivers del lector de tarjetas y tener instalados los software proporcionados por la entidad que nos ha emitido el certificado.

Para garantizar una mayor seguridad, en las operaciones que se realicen movimientos de fondos, será necesario utilizar un segundo PIN o la tarjeta Línea Abierta. Ésta es una tarjeta de coordenadas, es decir, en el dorso tiene inscritas 60 claves diferentes, lo cual, aumenta el grado de dificultad para descifrarla ya que siempre no se utiliza la misma. Al solicitarse una clave de esta tarjeta, aunque algún "desconocido" conozca tu PIN secreto, no podrá realizar ningún tipo de operación.

En el caso de que designes a alguien para que realice las operaciones, para que los datos sigan siendo confidenciales, la propia entidad la Caixa le proporcionará unos datos para poder conectarse.

Garantías técnicas

Cuando intercambiamos información entre nuestro ordenador personal y los sistemas informáticos que posee la entidad financiera, tememos que durante el proceso en el que realizamos las operaciones podamos sufrir robo de información o incluso de fondos si nos roban el número de cuenta. Para garantizar que esto no va a ocurrir, en este tipo de operaciones, la Caixa utiliza un tipo de cifrado de los caracteres para impedir que las personas que no están autorizadas para ello puedan acceder a la información del cliente.

Con esto nos referimos a que todos los datos que mandamos mediante la red se encuentran cifrados mediante un algoritmo, además de que cada vez que se realiza una conexión se cambia de clave. Con ello se garantiza una mayor seguridad de la información.

Los diferentes sistemas de la entidad que se encuentran conectados a Línea Abierta están en continua monitorización, revisión y actualización.

Cookies

Los Cookies son pequeños ficheros de texto y que suelen encontrarse encriptados. Se encuentran localizados en los navegadores que poseemos. Estos los utilizan los propietarios de las páginas web para que sus usuarios puedan navegar de una forma más fácil en la Web y poder realizar determinadas funciones. Además, tienen un papel fundamental para permitir realizar según qué procesos en las web. Los Cookies funcionan de la siguiente forma:

En primer lugar, es necesario saber que éstos se crean cuando un usuario está cargando una página web. Esta página web en la que estamos navegando envía cierta información al navegador y, en ese momento, se crea el archivo de texto, es decir, los cookies.

Los cookies son utilizados, por ejemplo, para facilitar la identificación de un usuario para entrar en una zona segura de la web; cuando nosotros nos identificamos, esos datos de identificación son los que se almacenan en los cookies, de manera que cuando el usuario quiera volver a entrar en esa página web no tenga que volver a introducir todos los datos de identificación; también almacena los datos sobre preferencias de navegación, es decir, los sitios web que solemos visitar de forma habitual.

La Caixa permite desactivarlos, eliminar permanentemente los Cookies que se tienen en el ordenador personal o el móvil.

Línea Abierta en Facebook

Línea Abierta también se encuentra en Facebook, pero por esta vía no puede acceder a nuestros datos ya que esta aplicación es de la Caixa y se encuentra en los servidores de dicha entidad. Además, también en este caso, es necesaria la utilización de un PIN.

Cuando estamos navegando en internet (utilizando la banca online), nos podemos encontrar con distintos ataques. La Caixa le da gran relevancia a un tipo de estafa que es muy común hoy en día como es el Phishing; esta estafa consiste en la suplantación de identidad de la propia entidad. Este tipo de estafa consiste en crear páginas web que aparentemente parecen la página web de la propia entidad, pero que en realidad no es así y lo utilizan para robar datos de identificación y poder entrar en las cuentas de los clientes. Para protegerse de este tipo de amenaza la Caixa informa en su página web de las distintas formas en las que nos podemos encontrar el Phishing.

- Generalmente los ataques se realizan mediante correos electrónicos, mensajes en los teléfonos móviles o llamadas. Mediante estas tres vías se intenta suplantar la identidad de la propia entidad.
- Con las formas de ataque anteriores, lo que se hace es redirigir al cliente a una página web que aparentemente parece la de la entidad pero que en realidad no es la original. En esta página se solicitan datos personales y las claves para acceder a la banca online o a las tarjetas.
- Para identificar que no es la página original debemos de fijarnos en la cabecera del mensaje, ya que para asegurarnos de que es la página correcta deberá aparecer en esta el nombre y los apellidos junto con las últimas cifras del DNI.

Para que los clientes de Caixa no sufran este tipo de ataques, la entidad lleva a cabo las siguientes acciones:

- Nunca pide a los clientes contraseñas, datos personales o claves utilizando la vía telefónica, los mensajes o los correos electrónicos.
- Cuando se envía un correo de la propia entidad, siempre lleva alguna dirección adjunta que se redirige a una página web en la que no te solicitan ningún tipo de información que sea de carácter personal.
- Los correos que recibimos de la entidad nunca te enlazan de forma directa con el servicio de banca online.
- Cuando recibimos un correo electrónico de la Caixa podemos comprobar que éste realmente proviene de esta entidad porque en la cabecera del mensaje aparecen el nombre y los apellidos junto con las últimas cifras del DNI.

Figura 5. Cabecera de correo electrónico seguro

Fuente: https://portal.lacaixa.es

Empleados

Aparte de las medidas de seguridad que aplica la propia entidad, los empleados también deben de cumplir todas las medidas necesarias establecidas para cumplir con la ley.

Para garantizar la seguridad, en primer lugar, cuando se abre una sucursal no puede hacerlo un solo empleado, sino que por lo menos tiene que haber dos; ésta es una norma impuesta por la entidad, tanto para garantizar la seguridad física de los empleados (en el caso de que se produjera un robo) como para impedir el robo de información parte de algún empleado. Para poder realizar el acceso es necesario que los empleados utilicen su huella dactilar; de esta forma se conoce quién es el que ha realizado dicho acceso.

La entidad dispone de una "Intranet", que permite a los empleados realizar las distintas actividades y comunicarse con el resto de empleados, tanto a nivel de la propia sucursal como de otras sucursales. Además, se puede acceder a la Intranet desde cualquier sucursal del grupo siempre que sea en horario de atención al público

En la utilización de la Intranet hay que tener en cuenta una serie de medidas: Solo se pude utilizar en horario de apertura al público, ya que fuera de este horario la aplicación esta inutilizable.

- Continuamente está controlado, para ver qué es lo que realiza cada uno de los empleados.
- Para acceder cada uno de los empleados dispone de un nombre de usuario y contraseña.
- De forma general solo se puede acceder a la Intranet desde un ordenador que se encuentre en alguna de las sucursales del grupo, pero en algunos casos está permitido el uso de esta aplicación fuera de las instalaciones.

Formación de los trabajadores

Otra forma de garantizar la seguridad es proporcionando formación a los empleados de manera que conozcan qué medidas tienen que aplicar y qué deben de realizar. Para ello la entidad proporciona diferentes cursos sobre seguridad a los empleados, tanto seguridad frente a atracos como seguridad en la realización de las diferentes actividades para dar cumplimiento a las distintas normativas referentes a seguridad informática y de la información.

Concretamente durante el ejercicio 2014 todos los empleados que forman la Caixa debieron de someterse a un curso en formato e – learning de una hora de duración en el que se daban los conocimientos necesarios sobre las distintas medidas y criterios de protección de la información que deben de aplicar en el desarrollo de sus actividades.

También realizaron otro curso dirigido a conocer las formas de detección y comunicación de operaciones sospechosas tanto en abuso de mercado como en los deberes que tienen los empleados en relación a la información privilegiada.

La garantía del certificado ISO 27001

La Caixa fue la primera entidad financiera Europea que obtuvo el certificado ISO 27001: 2005 por el que se garantiza la protección y seguridad de sus servicios web. Dicha entidad obtuvo este tipo de certificación de la mano de British Standard Institute, mediante la superación de la auditoría realizada por dicha entidad en la que se revisaron todos los procedimientos de seguridad implantados. A continuación mostramos el certificado de que la Caixa cumple con las normas ISO 27001.

Figura 6. Certificado 27001 La Caixa

Fuente: https://portal.lacaixa.es

Durante el año 2014 según el informe de auditoría realizado por Deloitte sobre la entidad la Caixa renovó dicho certificado por la entidad certificadora Applus +, ya que posee un sistema de gestión de la seguridad de la información compuesto por las mejores prácticas internacionales. Con esta renovación se está garantizando el correcto funcionamiento del sistema de gestión de seguridad de la información

A modo de ejemplo, he realizado un cuestionario de auditoria de cumplimiento de la ISO 27001. Dicho cuestionario lo podemos encontrar en el Anexo XIII.

Certificación de continuidad del negocio ISO 22301:2012

Aparte de la certificación ISO 27001, la Caixa también cuenta con la certificación ISO 22301:2012, la cual garantiza que la entidad implementa todas las medidas prácticas necesarias para que el negocio pueda seguir adelante en el caso de que se produzca

algún tipo de contingencia que pueda afectar al desarrollo normal de las actividades de la entidad.

Según el informe de auditoría 2014, la Caixa tiene un plan de contingencias tecnologías con el que puede hacer frente a diferentes situaciones de gran dificultad para que los servicios informáticos puedan funcionar correctamente. El último certificado que obtuvo en lo referente a continuidad operativa y de negocio fue en 2012, mediante la entidad acreditadora British Standard Institute por el que se certifica que:

- La alta dirección de la entidad tiene un alto compromiso con la continuidad del negocio.
- Que se llevan a cabo las mejores prácticas para la continuidad del negocio.
- Que la entidad dispone de un sistema de gestión de continuidad del negocio que tiene implantado y que cumple las distintas normas internacionales.

Disponer este tipo de certificado aporta a la entidad una serie de ventajas:

- Se genera confianza en todas aquellas partes que operan con la Caixa, ya que este tipo de certificado garantiza que la entidad puede responder ante incidentes de gran calibre que puedan afectar a la continuidad del negocio.
- Genera beneficio en la imagen de la empresa y su reputación
- Garantiza que las distintas auditorías que se han realizado en la entidad, tanto internas como externas, certifican que se dispone de un sistema de gestión continuamente actualizado.

4.2 AUDITORÍA DE CUMPLIMIENTO EN UNA PYME

En este aparado vamos a realizar un análisis del cumplimiento de la LOPD en una PYME; observamos que no existe el mismo grado de cumplimiento de la ley en una PYME que en una empresa de grandes dimensiones. He elegido una pequeña empresa de muebles, ya que me han facilitado información para poder realizar el estudio.

La Ley Oficial de Protección de Datos de Carácter Personal es de obligado cumplimiento para todas las empresas independientemente de su tamaño, ya que todas manejan datos de carácter personal, bien sean de clientes, proveedores, empleados… Aun siendo obligatorio, todavía muchas de las pequeñas empresas no cumplen con la normativa, ya que hay un gran desconocimiento de la normativa Otras, aun conociendo

la ley, no la aplican porque no son conscientes de su importancia; no han sufrido ningún tipo de sanción y no están sensibilizadas al respecto.

Al comenzar la evaluación de esta empresa, lo primero que hice fue preguntarles si conocían la Ley Orgánica de Protección de Datos. Su respuesta fue "que habían escuchado hablar de ella pero nada más". Por ello, desde un primer momento, ya deduje que no cumplirían las medidas de seguridad en lo que respecta a la protección de datos personales.

A continuación expongo los resultados del análisis destacando algunas anomalías encontradas.

Respecto a la **seguridad de las instalaciones**, que es de gran importancia para la protección de la información, hay que decir que, en este caso, se encuentran desprovistas de medidas de seguridad para impedir el fácil acceso a personas no autorizadas. La puerta principal de acceso tan solo tiene como sistema de cierre una simple cerradura, al igual que la puerta de entrada a la zona donde se encuentran los sistemas informáticos y toda la información de la empresa. Únicamente tienen como medida adicional un sistema de alarma para evitar los robos en horario que no es de atención al público.

En lo que se refiere a la **seguridad de los sistemas informáticos**, observamos que disponen de algunos medios de seguridad para frenar posibles ataques externos. Por ejemplo, disponen de un sistema de antivirus que se actualiza periódicamente para evitar daños en el equipo, y también disponen de firewalls.

En el caso de la **seguridad de la información**, hay que recordar que, es necesario que todas las empresas dispongan de un documento de seguridad, en el que se indique quién es el responsable de seguridad, las distintas medidas de seguridad de obligatorio cumplimiento, así como las obligaciones y funciones que tiene el personal respecto a la protección de datos personales. En el caso de esta pequeña empresa, según la información recabada, no disponen de dicho documento; no tienen designado un responsable de seguridad y nadie les ha informado a los empleados de las distintas medidas de seguridad que tienen que tener en cuenta para la protección de la información. Por ello, se llevan a cabo prácticas que son de un elevado riesgo; por ejemplo, los empleados pueden introducir un dispositivo externo, como es una memoria USB, sin tener ninguna repercusión su acción, ya que nada ni nadie lo impide. También

observamos otro error de seguridad en el hecho de que todos los empleados tienen acceso a todo tipo de información disponible tanto en ficheros automatizados como en los ficheros de papel. Además, en los diferentes ordenadores, no existe medio para proteger el acceso al mismo, como podría ser un simple código de identificación de usuario, por lo que una vez que entras en el sistema puedes acceder a toda la información que este contenga. Disponen de copia de seguridad, que se realiza de forma diaria, pero se encuentra en las propias instalaciones, lo cual es un riesgo; por tanto, también ahí tienen una deficiencia importante Es importante recordar que, cuando se recoge información de carácter personal, es obligatorio informar a la persona afectada, obtener su consentimiento e informarle de qué uso y utilidad tendrá; esto no se realiza en esta empresa y supone un grave incumplimiento de la LOPD.

Por otro lado, atendiendo a los **empleados,** descubrimos que cuando un empleado comienza a trabajar en dicha empresa no se le informa de las distintas medidas de seguridad que debe de aplicar durante su permanencia en la empresa. Tampoco reciben ningún tipo de formación sobre las diferentes medidas de seguridad para proteger la información y como cumplir con Ley Orgánica de Protección Datos. Éste es un tema que nunca ha sido tratado entre los distintos empleados de la empresa, hay un total desconocimiento.

Sí que están en orden con la normativa en lo que respecta a la inscripción de fichero en la Agencia Española de Protección de Datos; este proceso se realiza a través de la Asesoría que les realiza las diferentes gestiones.

Evidentemente, esta PYME está muy lejos de cumplir con la legislación en materia de protección de datos personales y mucho más lejos de poder obtener un certificado en seguridad informática.

Sería necesario que la empresa decidiera tomar este tema de una forma seria, ya que aunque hasta ahora no han sufrido ningún tipo de sanción, en el futuro podrían producirse; los perjuicios que pueden sufrir podrían ser, además de económicos, de pérdida de imagen y confianza. Por ello, he propuesto una serie de recomendaciones que deberían considerar para mejorar la seguridad de la información y dar cumplimiento a la LOPD.

Recomendaciones

- Ponerse al corriente de la normativa vigente en protección de datos personales, y concienciarse de que es de obligado cumplimiento para todo tipo de empresas; conocer las sanciones que se les podrían aplicar por incumplimiento de la ley.
- Realizar una monitorización de los sistemas, para saber lo que hacen los empleados en los diferentes sistemas de la organización; de est forma, pueden controlar dónde acceden y qué actividades realizan.
- Prohibir la utilización de soportes externos a la organización, para minimizar riesgos.
- Elaborar el documento de seguridad y designar un responsable de dicha seguridad. En este documento, debe de reflejarse quién es el responsable de seguridad, así como sus funciones y obligaciones. También deben de indicarse las medidas de seguridad que deben ser de obligada aplicación en la organización por parte de todos los empleados de la misma.
- Dividir la información con la que trabajan en niveles, en función del grado de seguridad que se le debe de aplicar.
- Es recomendable que no todo el personal pueda acceder a la totalidad de la información, por lo que deberán de designar distintas personas para la utilización de la información, en función del nivel en el que se encuentra.
- Implantación de un sistema de identificación y autentificación en los diferentes sistemas que poseen, para impedir el acceso no autorizado.
- Las copias de seguridad deberían almacenarse en un lugar diferente a la ubicación de la propia organización; de esta forma aumentará el grado de seguridad.
- Cuando se recaban datos personales, han de tener en cuenta que es necesario que informen de ello a los afectados, así como indicarles cuál es el uso que se les dará a los datos recopilados.
- Cuando se contrate personal, deberán de informarle de las diferentes medidas de seguridad que deben de aplicar para garantizar la seguridad.
- Deberán de realizar cursos de formación en esta materia cada cierto tiempo, puesto que las tecnologías avanzan continuamente, y por tanto, nos podemos encontrar con nuevos riesgos que requieren nuevos medios para su control.

5. GUÍA PRÁCTICA DE ADAPTACIÓN PARA EL CUMPLIMIENTO DE LA LOPD DIRIGIDA A PYMES

En el siguiente apartado elaboramos una guía práctica dirigida a PYMES para el cumplimiento de la LOPD, en la que se indican los pasos a seguir para cumplir con la ley; en particular, detallamos la estructura y contenido que ha de tener el documento de seguridad.

5.1 PASOS A SEGUIR PARA CUMPLIR LA LOPD

A continuación indicamos los pasos a seguir para dar cumplimiento a la ley.

1. **Inscripción/registro de los ficheros de datos personales en la AEPD..**
2. **Nombrar un responsable de seguridad.**
3. **Elaboración del documento de seguridad**

En este documento se recogen todas las medidas, procedimientos y estándares que se deben de seguir para garantizar la seguridad de la información, lo cual, es de obligado conocimiento por todo el personal que tenga acceso a los sistemas de la organización.

4. **Determinar las obligaciones y funciones del personal**

Todo el personal de la organización deberá de conocer claramente todas las funciones y medidas establecidas para garantizar la correcta seguridad de la información; se darán a conocer como establezca el responsable de seguridad. Todas estas funciones deberán de verse reflejadas en el documento de seguridad indicando qué función tiene cada uno de los empleados en función de su perfil. También, si se cree que es oportuno, se mandarán circulares o recordatorios para asegurarse de que todo el personal conoce todas las funciones y medidas, informando además si se lleva a cabo algún tipo de cambio.

Cada miembro del personal deberá de tener determinado un perfil de usuario; tendrán la obligación de mantener sus perfiles y contraseñas de forma confidencial para evitar que el personal ajeno a la organización pueda acceder a dicha información. También es obligatorio que todo el personal que trabaje con información de carácter personal guarde secreto sobre la información de carácter personal que maneje en el desarrollo de su actividad.

Mientras realizan sus funciones, tendrán la obligación de notificar al responsable de seguridad si se ha producido algún tipo de incidencia, siempre utilizando el procedimiento que se haya establecido para ello.

En el caso de que el personal no cumpla sus obligaciones y las medidas que se establecen en el documento de seguridad, podrá haber sanciones por parte de la AEPD. Dichas sanciones variarán en función del grado de incumplimiento; se clasifican en leves, graves y muy graves.

- **Infracción leve:** Dentro de este tipo de infracción podemos considerar acciones como recopilar datos de carácter personal sin el consentimiento de los afectados. La sanción correspondiente a este tipo de infracción correspondería entre 601,01 € y 60.101,21 €.
- **Infracción grave:** Un ejemplo de estas infracciones puede ser utilizar los ficheros para finalidades distintas de las que realmente se crearon o no seguir los principios establecidos en la LOPD. Para este tipo de infracciones la sanción corresponde a una cuantía entre 60.101,21 € y 300.506,25 €.
- **Infracción muy grave:** Este tipo de infracciones son las más relevantes y dentro de ellas algunas de las acciones que podemos encontrar son la comunicación de datos de carácter personal a terceros cuando no está permitido, recoger datos de forma engañosa, recabar datos que tienen una alta protección sin solicitar autorización… etc. La sanción correspondiente a este tipo de infracción esta entre los 300.506,25€ y los 601.012,1 €.

5. Notificar, gestionar y solucionar incidencias

En primer lugar definimos incidencia en seguridad como cualquier incumplimiento de las normas establecidas en el documento de seguridad. También será considerada como incidencia cualquier tipo de anomalía que se pueda dar en la información de carácter personal.

Todas aquellas incidencias que afecten a datos de carácter personal deberán de ser notificadas y gestionadas; además, se deberá de formar un registro en el que se anoten todas ellas.

Una vez que la incidencia ha sido detectada, ésta debe de ser notificada al director de la organización a través del responsable de seguridad del fichero en el que se ha producido la incidencia. Para llevar a cabo dicha notificación el responsable del fichero tendrá que crear un registro en el cual se deberá de indicar el tipo de incidencia de que se trata, qué efectos se han derivado de dicha incidencia y qué tipo de medidas o procedimientos se

han utilizado para corregirlas; además se indicará dónde se han producido las incidencias y en qué fecha y hora. También será necesario indicar quién ha realizado el proceso, qué datos se han restaurado y qué datos se han tenido que grabar manualmente durante el proceso de recuperación.

6. **Revisión del documento de seguridad**

El documento de seguridad deberá de encontrarse en todo momento actualizado y revisado. Se considerara como cambio relevante todo aquello que pueda influir en el correcto cumplimiento de las medidas adoptadas en el documento. También será necesario que el documento se adapte a los cambios normativos que se puedan producir en la LOPD.

5.2 EL DOCUMENTO DE SEGURIDAD

Mantener la seguridad de los datos de carácter personal es una obligación legal, por lo que es necesario disponer de una serie de medidas, normas y procedimientos una manipulación de dicha información garantizando la seguridad. Todas estas medidas deben de estar incluidas en el documento de seguridad. A continuación indicamos la estructura de dicho documento y el contenido que debe tener; para ello hemos tomado como referencia la guía de seguridad de datos de la Agencia Española de Protección de Datos.

1. **Ámbito de aplicación**

Es necesario delimitar el ámbito de aplicación. En dicho ámbito, las medidas, normativa y procedimientos deberán de aplicar a todos aquellos ficheros que contengan información de carácter personal; también deberán de aplicarse a los sistemas de información, equipos y soportes utilizados para el tratamiento de dicha información.

A continuación desarrollamos las distintas medias a seguir para garantizar la seguridad:

2. **Determinar el responsable de seguridad y sus funciones**

Designar un responsable de seguridad es fundamental, ya que sobre esta persona es sobre la que recae la responsabilidad sobre los ficheros y el tratamientos de los mismos; además, éste también se encargará de decidir sobre la finalidad, contenido y tratamiento del mismo. En el caso de que hubiera varios responsables, deberá de indicarse quién es el responsable o responsables de los distintos ficheros. También será necesario indicar cuáles son las funciones que tiene que realizar cada uno de los responsables para

garantizar el cumplimiento de la Ley. Dichos responsables tendrán las siguientes obligaciones

- Notificación al Registro General de protección de datos los distintos ficheros que posean para poder llevar a cabo su inscripción
- Deberán de garantizar que los datos con los que se trabaja son ciertos y adecuados, que se han obtenido de forma licita y legítimamente y que son utilizados para los fines que fueron recabados.
- Tendrán la obligación de informar a aquellas personas afectadas por los datos de carácter personal recogidos.
- Deben garantizar que están cumpliendo con los deberes tanto de secreto como de seguridad.
- Deben garantizar que cuando se realizan prestaciones de servicios a terceros en las que se comparten datos personales se está cumpliendo con la normativa de la LOPD.

Además de llevar a cabo todas estas funciones, los responsables de seguridad también serán los encargados de adoptar una serie de medidas para hacer que todo el personal de la organización conozca las medidas de seguridad de la información que tienen que adoptar, así como las repercusiones habrá en el caso de incumplimiento de éstas.

3. Aplicación de medidas de identificación y autenticación:

Es necesario aplicar todas las medidas y normas relacionadas con la identificación y autentificación del personal que se encuentra autorizado para el tratamiento de datos personales.

Para llevar a cabo la identificación se utilizará el nombre de usuario que será el correspondiente al DNI de cada uno de los empleados. Por otro lado, la autenticación se llevará a cabo mediante un sistema de contraseñas. Estas contraseñas se asignarán de forma aleatoria mediante algún tipo de programa como, por ejemplo, el Norton Identity Safe, el cual, le asignara una contraseña a cada uno de los usuarios.

Estas contraseñas estarán formadas por letras minúsculas, mayúsculas, números y caracteres especiales, todos ellos intercalados para incrementar la seguridad. Lo aconsejable es utilizar una contraseña durante 3 meses y luego cambiarla.

4. **Control de acceso:**

Los trabajadores solo podrán tener acceso a aquellos datos que sean necesarios para poder desarrollar de forma correcta sus funciones y actividades.

El responsable de los ficheros deberá de establecer una serie de medidas y mecanismos para que solamente pueda tener acceso a los ficheros el personal que está autorizado para ello. Dentro de sus funciones el responsable de seguridad también deberá de mantener una lista actualizada de los usuarios y sus perfiles; además, dentro de sus funciones, también deberá de mantener actualizada la lista donde figuran los accesos autorizados para cada uno de los usuarios.

5. **Registro de accesos:**

Se deberá de llevar a cabo un registro de todos los accesos realizados, por lo que cada vez que se intente acceder a un fichero determinado se deberá de almacenar la identificación del usuario, así como la hora y la fecha en la que se ha realizado el acceso y si este ha sido autorizado o denegado. Todos estos datos almacenados deberán de ser guardados durante un periodo mínimo de 2 años para poder comprobarlos en el caso de que se produjese algún tipo de incidencia.

Cuando se produzca un acceso autorizado también deberá de guardarse la información, ya que con esta se puede identificar el registro accedido.

El personal encargado de la seguridad también tendrá como función el revisar como mínimo una vez al mes la información sobre el control que se ha registrado; con dichas revisiones deberá de realizar un informe en el que se plasmen las distintas revisiones que se han realizado y los problemas que se hayan detectado.

6. **Gestión de soportes y documentos:**

Aquellos soportes y documentos que posean información de carácter personal deberán facilitar la identificación de la información que contienen; además, también deberán de ser inventariados. A éstos solo podrán tener acceso aquellas personas que se encuentren autorizadas en el documento de seguridad.

En el caso de tener la necesidad de sacar los soportes o documentos fuera del local donde se encuentra el control de éstos, se deberá de solicitar autorización al personal responsable de seguridad del fichero (si dicha autorización no está expresamente reflejada en el documento de seguridad). El responsable de seguridad se deberá asegurar

de que se anote la hora de salida del soporte y quién realiza esa salida, para tenerlo registrado en caso de incidencias.

Será necesario aplicar una serie de medidas para que durante su traslado no se produzcan pérdidas, sustracción o un acceso prohibido a la información. Dichas medidas será las siguientes:

- Generación de códigos QR: son códigos de barras bidimensionales que almacenan información. Estos se generarán mediante la aplicación X- Ren QRcode, estando en dichos códigos almacenada la información de carácter personal.
- El traslado deberá de ser realizado por personal autorizado para ello; además, el traslado se deberá realizar en los vehículos de la empresa, lo cuales, estarán en todo momento localizados por GPS.
- Los documentos deberán de trasladarse en carpetas que tengan como sistema de cierre gomas, para que de esta forma no se pueda extraviar ningún papel por los laterales de dichas carpetas.

En el caso de que sea necesario eliminar algún tipo de soporte y documento que contenga datos de carácter personal, éstos deberán de ser destruidos o borrados para evitar su acceso. Para ello, en el caso de documentos no automatizados, se deberá de proceder a la trituración de los documentos y su incineración. Por otro lado, los ficheros informatizados deberán de ser eliminados de raíz, así como las copias de seguridad que puedan existir.

Los soportes que posean información personal deberán ser identificados por etiquetas de colores para facilitar al personal autorizado su identificación. Así, a la información de nivel básico le corresponderá una etiqueta de color amarillo, a la de nivel medio le corresponde una etiqueta verde y a la de nivel alto de color rojo.

7. Control de acceso físico

Solamente el personal autorizado podrá acceder a aquellas instalaciones donde se encuentren los equipos físicos que dan soporte a los sistemas de información.

Estos equipos se encontraran localizados en habitaciones que se encontrarán cerradas con llave (para aumentar la seguridad) y a las que sólo tendrá acceso el personal autorizado para ello. En el caso de que sea necesario el acceso de otra persona, ésta deberá solicitar la autorización al responsable de seguridad. Este último deberá

garantizar el registro de la fecha, hora de entrada y de salida del acceso, por si fuera necesario en caso de incidencia.

8. Acceso de datos a través de redes de comunicación

Para acceder a ficheros y datos mediante redes de comunicación también será necesario tener desarrolladas una serie de medidas, al igual que para el acceso local. Cuando los datos de carácter personal corresponden al nivel alto y se han de transmitir mediante redes inalámbricas o públicas, se deberá de llevar a cabo un cifrado de los datos para que sea más difícil su visualización

9. Utilización de ficheros fuera de su localización habitual

En el caso de que sea necesaria la utilización de ficheros fuera de su localización habitual (organización) deberá de indicarse en el documento de seguridad quién tiene la autorización para ello. También deberá de indicarse para qué periodo se tiene dicha autorización.

El responsable de seguridad de los ficheros será el encargado de dar la autorización para poder llevar a cabo el almacenamiento de datos en dispositivos portátiles o que estos se traten fuera de las instalaciones en las que se encuentran los ficheros.

En el caso de que algún miembro solicite esta autorización y no se encuentre reflejado en el presente documento, el responsable de seguridad deberá de realizar un registro sobre la persona que solicitó la autorización, el tipo de dispositivo, y fecha y hora del acceso con el fin de garantizar que se hace un buen uso de los distintos datos.

10. Traslado de documentación

Cuando se lleve a cabo el traslado de documentación de un lugar a otro, ya sea información de nivel alto o no, deberán de establecerse una serie de medidas para evitar la manipulación y robo de dicha información. Para ello, algunas de las medidas básicas para el traslado son: toda la información se debe recoger en carpetas que impidan la visibilidad de la información a través de sus tapas y además estarán cerradas mediante un sistema de gomas, para evitar el extravío de algún documento; cuando se trate de información de nivel alto, se deberá de llevar a cabo otra serie de medidas adicionales, como que el traslado se realice mediante personas o vehículos pertenecientes a la propia organización, que han de ser vehículos dotados de un sistema de GPS para poder tener localizada la información en cualquier momento.

11. Realización de copias de respaldo y recuperación

Se deberá disponer de una copia de respaldo de todos los datos, así como de los procedimientos que se utilicen en la recuperación. Estas copias deberán de encontrarse en un lugar distinto de donde se encuentren los equipos informáticos.

En el documento de seguridad se deberá de indicar quién es el responsable de seguridad que estará encargado de dar la autorización para la generación de dichas copias.

12. Realización de copias de trabajo de documentos o ficheros temporales

Con este tipo de copias o ficheros nos referimos a aquellos documentos que se crearon con un fin concreto, para una actividad concreta. Aunque sean para su utilización en un periodo determinado, también será necesario aplicar las medidas de seguridad que establece la LOPD. Una vez que haya terminado la actividad para la que eran necesario dichos datos, éstos deberán de ser eliminados y destruidos sin dejar rastro de ellos.

13. Realización de copia o reproducción de documentos

La copia o reproducción de documentos que contienen información de carácter personal sólo podrán realizarse bajo el control y la supervisión del personal que está autorizado para ello. En el documento de seguridad deberá de indicarse quiénes son los usuarios que pueden llevar a cabo esta actividad.

Aquellas copias que ya no vayan a ser utilizadas para ningún fin deberán de ser destruidas para que posteriormente no se pueda acceder a ellas. En este documento de seguridad deberá de indicarse a su vez cuáles son los medios que deberán de utilizar para destruirlos**.**

Para comprobar que se cumple con la normativa de protección de datos, y, por tanto, que se cumplen las medidas y procedimientos indicados anteriormente, he elaborado un cuestionario de auditoria de cumplimiento en el que se evalúan los distintos aspectos estudiados hasta ahora. Dicho cuestionario lo podemos ver en el Anexo XIII.

6. CONCLUSIONES

- El activo más importante de una organización es la información que ésta posee, por lo que es necesario invertir en seguridad informática para evitar la destrucción, pérdida o fuga de dicha información.
- Garantizar la seguridad informática y de la información, también es un aspecto importante que debemos de tener en cuenta en nuestro vida personal, ya que cada vez realizamos más operaciones de forma online, como las operaciones bancarias, por lo que estamos expuestos a una gran cantidad de riesgos.
- Toda empresa que maneje datos de carácter personal, (todas) deben de aplicar la normativa de protección de datos personales, ya que de no ser así se le impondrá una sanción.
- Para garantizar la seguridad de la información, es necesario implantar en la organización un sistema de seguridad de la información y gestionarlo de una forma adecuada.
- Si tenemos implantado el SGSI adecuado, la organización podrá pasar el control de auditoria y con ello obtener el certificado 27001, el cual, garantiza la seguridad de la información ofreciendo un carácter diferenciador frente a la competencia.
- Es necesario realizar una auditoría de cumplimiento si se realiza cualquier tipo de cambio el Sistema de Gestión de la Información.
- Es necesario, que en todas las organizaciones dispongan de un documento de seguridad, en el que se detallen las distintas medidas de seguridad que se deben aplicar a los diferentes niveles de datos (para cumplir la ley de protección de datos), así como las funciones y obligaciones que tiene los empleados en esta materia.
- Todos los países que pertenecen a la comunidad europea se rigen por una misma normativa para garantizar la seguridad de datos personales en la transferencia de estos.
- Los países que no pertenecen a la Comunidad Europea deben de adherirse a una serie de acuerdos que contienen unos principios mínimos, para poder garantizar la seguridad en transferencia de datos.
- Muchas empresas no cumplen la Ley Orgánica de Protección de Datos, sobre todo las Pymes. Todavía hay mucho desconocimiento al respecto.

- Al evaluar el cumplimiento de la LOPD en una gran empresa, la Caixa, observamos un óptimo nivel de cumplimiento, en este caso, mediante la aplicación de normativas propias perfectamente alineadas con la LOPD.
- En la evaluación de la PYME encontramos graves deficiencias en el cumplimiento de la LOPD, algo que entendemos que es extensible a muchas de las pequeñas y medianas empresas.
- A modo de conclusión, hemos elaborado el siguiente cuadro resumen con los distintos pasos que hay que seguir para cumplir con la LOPD.

GUIA RESUMEN: PASOS PARA CUMPLIR CON LA LOPD
1. Inscripción/ registro de los ficheros de datos personales en la AEPD
2. Nombrar un responsable de seguridad
3. Elaboración del documento de seguridad • Determinar el ámbito de aplicación • Determinar el responsable de seguridad y sus funciones • Aplicación de medidas de identificación y autenticación • Controlar los accesos • Registrar los accesos • Gestión de soportes y documentos • Control de acceso físico • Acceso de datos a través de redes de comunicaciones • Utilización de ficheros fuera de su localización habitual • Traslado de documentación • Realización de copias de respaldo y recuperación • Realización de copias de trabajo de documentos o ficheros temporales • Realización de copia o reproducción de documentos
4. Determinar las obligaciones y funciones del personal
5. Notificar, gestionar y solucionar incidencias
6. Revisión del documento de seguridad

7. BIBLIOGRAFÍA

ABOGACIA ESPAÑOLA, CONSEJO GENERAL. El cumplimiento de la normativa de protección de datos en Iberoamérica. http://www.abogacia.es/ , 11 de Noviembre de 2013. [Fecha de consulta: 10 de Noviembre de 2015]. Disponible en: http://www.abogacia.es/2013/11/11/el-cumplimiento-de-la-normativa-de-proteccion-de-datos-en-iberoamerica/

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Memoria AEPD 2014. http://www.agpd.es. [Fecha de consulta: 4 de Noviembre de 2015]. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del responsable de ficheros. http://www.agpd.es. [Fecha de consulta: 30 de septiembre de 2015]. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Guía de Seguridad de Datos. https://www.agpd.es, [Fecha de consulta: 30 de Septiembre de 2015]. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. El acuerdo de Puerto Seguro con Estados Unidos de América. https://www.agpd.es. [Fecha de consulta: 16 de Noviembre de 2015]. Disponible en: https://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf

AGENCIA ESPAÑOLA DE RPTECCIÓN DE DATOS. Protección de datos en el mundo. http://www.agpd.es. [Fecha de consulta: 18 de Noviembre de 2015]. Disponible en: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

ARCHIVOS Y GESTION DOCUMENTAL S.L. Medidas de seguridad aplicadas en los centros de custodia. http://archivosygestion.com/ [Fecha de consulta: 30 de Septiembre de 2015]. Disponible en: http://archivosygestion.com/garantias/garantias-seguridad/

COMPUTING. Caixa Bank implanta una solución completa de Big Data de Oracle. http://www.computing.es/, 29 de Octubre de 2015. [Fecha de consulta: 11 de Noviembre de 2015]. Disponible en: http://www.computing.es/bases-datos/noticias/1084885012201/caixa-bank-implanta-solucion-completa.1.html

BÉCARES, B. Lo que necesitas saber sobre la nueva ley de protección de datos europea. http://www.channelbiz.es , 17 de junio de 2015. [Fecha de consulta: 18 de Noviembre de 2015]. Disponible en: http://www.channelbiz.es/2015/06/17/lo-que-necesitas-saber-sobre-la-nueva-ley-de-proteccion-de-datos-europea/

CONSEJO PERMANENTE DE LA ORGANICACION DE LOS ESTADOS AMERICANOS. Principios y recomendaciones preliminares sobre la protección de datos. http://www.oas.org/ [Fecha de consulta: 16 de Noviembre de 2015]. Disponible en: http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf

COSTAS SANTOS, J. (2006). *Seguridad y alta disponibilidad.* Ra-Ma. Madrid

CRISTALINO, G. Seguridad Informática. http://seguridadinformatica4b.blogspot.com, 12 de Abril de 2013.[Fecha de consulta: 6 de Octubre de 2015]. Disponible en: http://seguridadinformatica4b.blogspot.com.es/2013/04/tipos-de-seguridad-informatica.html

ERB, M. Gestión de Riesgo en la Seguridad Informática. https://protejete.wordpress.com . [Fecha de consulta: 20 de octubre de 2015]. Disponible en: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

INCIBE. Estudio sobre la protección de datos en las empresas españolas. https://www.incibe.es, 9 de octubre de 2012. [Fecha de consulta: 15 de Noviembre 2015]. Disponible en: http://www.teclopd.com/el-cumplimiento-de-la-lopd-en-las-empresas-espanolas/

INCIBE. Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD). https://www.incibe.es, 1 de agosto de 2008. [Fecha de consulta: 15 de Noviembre de 2015]. Disponible en: https://www.incibe.es/CERT/guias_estudios/Estudios//estudio_lopd_pymes

ISO 27000. El portal de ISO 27000. http://www.iso27000.es/ . [Fecha de consulta: 1 de Octubre de 2015]. Disponible en: http://www.iso27000.es/sgsi.html

LA CAIXA**.** Seguridad y la "Caixa". https://portal.lacaixa.es. [Fecha de consulta: 26 de Octubre de 2015], Disponible en:

https://portal.lacaixa.es/seguridad/seguridadlacaixa_es.html

LA CAIXA. CaixaBank liderará la próxima gran alianza europea por la ciberseguridad. http://www.cronicaglobal.com/ , 29 de Mayo de 2015. [Fecha de consulta: 11 de Noviembre de 2015]. Disponible en: http://www.cronicaglobal.com/es/notices/2015/05/caixabank-liderara-la-primera-gran-alianza-europea-por-la-ciberseguridad-20507.php

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. https://www.boe.es, 5 de Marzo de 2015. [Fecha de consulta: 1 de Octubre de 2015]. Disponible en: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. http://www.boe.es, 10 de Mayo de 2014. [Fecha de consulta: 5 de Noviembre de 2015]. Disponible en: https://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

MIFSUD, E. Monográfico: Introducción a la Seguridad Informática – Seguridad de la Información / Seguridad Informática. http://recursostic.educacion.es/, 26 de Marzo de 2012. [Fecha de consulta: 2 de Septiembre de 2015]. Disponible en: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

MINISTERIO DE EDUCACION, CULTURA Y DEPORTE. Introducción a la seguridad informática – Mecanismos básicos de seguridad. http://recursostic.educacion.es, [Fecha de consulta: 2 de Septiembre de 2015]. Disponible en: http://recursostic.educacion.es/observatorio/web/eu/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=2

MINISTERIO DEL INTERIOR. Medidas de seguridad específicas para bancos, cajas de ahorro y entidades de crédito. http://www.interior.gob.es/ [Fecha de consulta: 19 de octubre de 2015]. Disponible en: http://www.interior.gob.es/web/servicios-al-ciudadano/seguridad/medidas-de-seguridad-en-entidades-y-establecimien/medidas-de-seguridad-especificas

ORDEN INT/317/2011, de, 1 de febrero, sobre medidas de seguridad privada. http://www.boe.es/ [Fecha de consulta: 26 de Octubre de2015]. Disponible en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-3171

PARLAMENTO EUROPEO Y CONSEJO. Directiva 95/46/CE, de 24 de Octubre de 1995. http://eur-lex.europa.eu/ . [Fecha de consulta: 10 de Noviembre de 2015]. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=es

PLAZA, É. Comparativa de la protección de datos en Europa y Estados Unidos. http://www.eljurista.eu/. [Fecha de consulta: 16 de Noviembre de 2015]. Disponible en: http://www.eljurista.eu/2015/04/26/comparativa-de-la-proteccion-de-datos-en-europa-y-en-estados-unidos/

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. http://www.boe.es/. [Fecha de consulta: 14 de Octubre de 2015]. Disponible en: http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

SANCHEZ PEREZ, G; ROJAS GONZALES, ISAI. (2012). "Leyes de protección de datos en el mundo y la protección de datos biométricos". *Revista seguridad, defensa digital*. Nº 13.

SIGMA DATA SECURITY CONSULTING S.L. Estudio sobre el cumplimiento de la lopd por la pyme española 2010. (2010). http://www.sigmadata.es/. [Fecha de consulta: 16 de Noviembre de 2015].Disponible en: http://www.sigmadata.es/downloadf/ESTUDIO%20EMPRESAS%20ESPA%C3%91OLAS%20Y%20LOPD.pdf

TABOR, E. Leyes de protección de datos en Estados Unidos. http://www.ehowenespanol.com/. [Fecha de consulta: 17 de Noviembre de 2015]. Disponible en: http://www.ehowenespanol.com/leyes-proteccion-datos-estados-unidos-lista_475258/

UNTAC. Los mapas mundiales de la ciberlegislación desvelan notables carencias, pese a los avance. http://unctad.org/ , 24 de Marzo de 2015. [Fecha de consulta:18 de Noviembre de 2015]. Disponible en: http://unctad.org/es/Paginas/PressRelease.aspx?OriginalVersionID=238

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Ciclo PDCA. http://datateca.unad.edu.co/. [Fecha de consulta: 6 de Octubre de 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

ANEXO I

AMENAZAZ FISICAS

Las amenazas físicas con las que nos podemos encontrar son las producidas por el hombre, los desastres naturales, y los cambios producidos en el entorno. A continuación se explican de forma detallada.

Las amenazas **derivadas por el hombre** están ligadas al acceso físico en dónde se encuentran los sistemas. Este punto es muy importante y hay que tenerlo en cuenta ya que aunque tengamos una gran cantidad de medidas para proteger los sistemas si no se puede saltar el acceso físico el resto de medidas ya no son útiles. Algunas medidas de prevención y detección problemas para garantizar la seguridad de acceso s limitar el acceso, utilizar cámaras de seguridad, guardas seguridad…etc. También es muy importante detectar los problemas una vez que ha aparecido por lo que las medidas que podemos tomar para ello son por ejemplo el controlar los accesos tanto los autorizados como los que no que se producen en el sistema, utilización de alarmas, cámaras…etc.

Los **desastres naturales** también son una amenaza importante, ya que pueden generar unos daños mayores que los que pueden producir las propias personas. Los desastres naturales con los que nos podemos encontrar son varios como los incendios, inundaciones, tormentas eléctricas, terremotos…etc. Aunque este tipo de amenazas no suelen producirse de forma muy habitual es necesario establecer las medidas de seguridad oportunas para estar protegidos en el caso de que se dieran.

Las tormentas eléctricas son un fenómeno que sí que se producen de una forma más habitual y que producen cambios en la tensión eléctrica, los cual, puede afectar a los equipos de la empresa. Para ello es necesario tomar una serie de medidas como tener instalado un pararrayos o apagar los equipos cuando se produzca una tormenta.

En el caso de producirse una inundación si algún equipo entra en contacto con el agua este se queda inutilizable y por tanto perdemos todo lo que el contiene por lo que es necesario aplicar una serie de medidas como por ejemplo tener algún sistema instalado que apague el resto cuando este detecte agua a la vez que corte el suministro eléctrico a los sistemas.

Aunque en España no es habitual que se dé un terremoto también es necesario que nos encontremos protegidos por si se diera el caso. Para ello, algunas de las medidas de

prevención que podríamos aplicar seria no situar los equipos en zonas altas ya que se podrían caer al suelo y romperse, los equipos deben de estar situados en unas plataformas de Gomara para que estas absorban las vibraciones y de esta forma no se dañe el equipo, los equipos deben de estar alejados de las ventanas para que estos no pudieran caer por las mismas, dependiendo del tipo de equipo debería de encontrarse anclado para impedir su movimiento…etc.

Los **cambios producidos en el entorno** pueden afectar a los diferentes sistemas que tenemos en la empresa. Estos cambios pueden afectar al desarrollo diario de las actividades de la organización, siendo estos los producidos por la red eléctrica, la temperatura y el ruido eléctrico.

La mayoría de los problemas con los que podemos encontrarnos son los producidos por la red eléctrica ya que se pueden producir picos de tensión, cortacircuitos…etc. Para solucionar este tipo de problemas es recomendable tener instalada toma tierra o un filtro que regule la tensión, también se puede utilizar sistemas de alimentación interrumpida que hacen que el flujo de corrientes se mantenga constante sin que se produzca ningún tipo de corte que pueda estropear los equipos y sistemas, mediante la incorporación a los equipos de una especie de batería para que pueda aguantar un tiempo determinado haciendo que las diferentes partes del equipos se vayan apagando de la forma adecuada y no de golpe.

La temperatura a la que nos encontramos también hay que tenerla en cuenta, ya que tener una temperatura extrema, es decir, muy alta o muy baja puede afectar al funcionamiento y rendimiento de los equipos, siendo aconsejable mantenerles a una temperatura entre los 10 y los 32 grados. Como medidas a utilizar para ello es aconsejable tener instalados aparatos acondicionados para regular la temperatura.

Los ruidos eléctricos son los generados por los distintos ordenadores, aparatos eléctricos y maquinaria que tiene la empresa en funcionamiento. Una medida que podemos tomar para ello es la instalación de los hardware alejados de aquellos elementos que generan ruido.

ANEXO II

MECANISMOS BÁSICOS DE SEGURIDAD

Los mecanismos básicos de seguridad que proporciona el Ministerio de Educación, Cultura y Deporte en su página web son los siguientes:

Autenticación

Es un proceso con el cual se intenta verificar la identidad del usuario cuando accede a una base de datos o entra en el sistema o la red. De forma general, para poder entrar en un sistema informático se requiere un nombre de usuario y una contraseña, pero actualmente, se utilizan otra serie de técnicas. Para poder autenticarse encontramos tres formas:

- Sistemas basados en algo que conocemos: Un claro ejemplo es la utilización de contraseñas.
- Sistemas basados en algo que poseemos: Algunos medios con los que podemos realizar la autenticación es mediante una tarjeta magnética (tarjeta de identidad)
- Sistemas basados en las características físicas de los usuarios: Estos últimos sistemas son los menos utilizados ya que son de uso más reciente como la utilización de la huella digitales o con el iris del ojo.

Si utilizamos más de un método para llevar a cabo la autenticación aumentan las probabilidades de que esta sea correcta, pero por otro lado, en las empresas el utilizar más de un método de autenticación debe estar ligado al valor que tiene la información que quiere proteger.

La técnica que se utiliza de forma más habitual es la utilización de contraseñas aunque no siempre se utiliza de forma correcta. Esta técnica se considerará mejor o peor dependiendo de las características que posee la contraseña. Para que esta sea más difícil de adivinar debe estar compuesta por amplio conjunto de caracteres y variados (números, mayúsculas y minúsculas) ya que así será más difícil saltársela. Esta debe de ser confidencial, solo la debe de conocer el usuario.

Autorización

Consiste en un proceso mediante el cual se determina qué, cómo y cuándo un usuario que se ha autenticado puede utilizar los distintos recursos de la organización.

Dependiendo de qué es lo que se pretende proteger el grado de la autorización puede oscilar, ya que toda la información que se posea en la organización no es igual de crítica.

La autorización siempre debe de ser registrada para más tarde poder ser controlada, da igual que sea una autorización por medio de una firma en un formulario o mediante la utilización de una contraseña.

Administración

La administración es la encargada en establecer, mantener y eliminar las autorizaciones de los usuarios de los recursos del sistema, del propio sistema y de las relaciones entre estos dos. Esta es la encargada de transformar las políticas de la organización y las autorizaciones que han sido otorgadas en un formato adecuado para poder ser usado por el sistema.

Dentro de una organización administrar la seguridad informática es una tarea que se encuentra en un cambio continuo y evolución, ya que las tecnologías sufren cambios continuamente y por tanto también lo hacen los riesgos a los que nos exponemos.

Auditoria y registro

La auditoría consiste en vigilar continuamente los servicios en producción, para ello es necesario recabar información y analizarla. Con este proceso se permite que los administradores puedan verificar las distintas técnicas de autenticación y autorización que se han utilizado y si se han utilizado de la forma correcta cumpliendo los objetivos que la organización había fijada.

Por otro lado, el registro, es un mecanismo mediante el cual si se intenta saltar las reglas de seguridad queda guardado en una base de eventos para luego poder analizarlo.

Para que estos dos conceptos tengan sentido es necesario que se realice posteriormente un estudio para analizar la información que se ha recabado.

Para estudiar la información registrada o auditada podemos utilizar tanto medios manuales como automáticos, y con una periodicidad dependiendo de lo critica que sea la información que queremos proteger o el nivel de riesgo.

Mantenimiento de la integridad

Consiste en un conjunto de procedimientos que se han establecido para controlar o evitar que los archivos sufran cambios que no han sido autorizados y que además la información enviada desde un determinado punto llegue de forma correcta y sin ninguna alteración a su destino.

Algunas de las técnicas más utilizadas para controlar o mantener la integridad de los datos son la utilización de antivirus, encriptación, sistemas de detección de intrusos, sistema de prevención de intrusos, firewalls, las cuales, explicamos a continuación.

Antivirus

Los antivirus son programas informáticos que utilizamos tanto para detectar como para eliminar virus u otras amenazas que puedan perjudicar nuestro sistema informático tanto antes como después de entrar en el sistema.

Encriptación

Consiste en la codificación de un documento o un archivo, para que de esta manera no se pueda conocer su información

Sistema de prevención de intrusos

Son software que tienen como función detectar y bloquear cualquier tipo de intrusión, amenazas de la rede, la transferencia de códigos malignos…etc.

Sistema de detección de intrusos

Estos sistemas detectan todos los accesos no autorizados a una red o un equipo informático

ANEXO III

CLASIFICACIÓN DE LAS AMENAZAS INFORMÁTICAS

Amenazas producidas por personas

Este tipo de amenazas a su vez pueden ser clasificadas en dos tipos:

- Intencionadamente: Son aquellas que tienen un fin maligno como el robo de información o la introducción de un virus. Estas son producidas por piratas informáticos o hackers.
- No intencionadamente: Son acciones que son permitidas debido a la existencia de una vulnerabilidad, pero el fin último de estas acciones no es hacer ningún tipo de daño pero que sin darnos cuenta ponemos en peligro la seguridad informática de los equipos y de la información.

Estas personas las clasificamos en dos grupos en función del tipo de acción que realizan:

- Agentes pasivos, estos lo que hacen es fisgonear por el sistema pero no lo modifican ni lo destruyen.
- Agentes activos, estos hacen daño y lo manipulan a su antojo.

Este tipo de amenazas producidas por personas también podemos clasificarlas en función de si se realizan de forma interna o externa.

- Amenaza interna: Esta amenaza puede es realizada por el personal de la propia organización y la puede realizar tanto de forma intencionada como no intencionada. De forma intencionada lo puede realizar ya que conocen el sistema de la organización así como las vulnerabilidades que puedan tener. Por otro lado, también las pueden realizar de forma no intencionada como por ejemplo abriendo un correo electrónico que no sabemos su procedencia.
- Amenazas externas: Estas son producidas mayoritariamente por Hackers que son personas que les gusta conocer e aprender cosas nuevas sobre la informática asi como entender su funcionamiento. Estos a su vez se dividen en función de si con sus acciones solo pretenden informase y aprender o por otro lado pretenden llevar a cabo una acción intrusiva o destructiva.

Amenazas físico – ambientales

Este tipo de amenaza son las que afectan a las instalaciones y a los hardwars que hay en ellas. Algunas amenazas de este tipo son las subidas de la corriente eléctrica que pueden producir que un equipo se vea afectado por ello, temperaturas excesivas o por el contrario temperaturas muy frías, catástrofes naturales como una inundación, terremoto…etc.

Amenazas lógicas

Estas son un código que se crean de forma intencionada para hacer daño en un sistema o también se pueden crear por error. Algunas de estas amenazas son las siguientes

- *Virus:* Es una serie de código que se introduce en un fichero que es ejecutable, de manera que cuando se abre el fichero el virus también se ejecuta.
- *Gusanos:* Son una serie de programas dañinos que una vez que se han penetrado en comienzan a realizar copias para expandirse mediante la red, mensajería instantánea, correo electrónico…etc.
- *Backdoor (puerta trasera):* Estos programas son diseñas para crear una "puerta trasera" por la que la persona que la ha creado puede acceder a todo el sistema y realizar con él lo que quiera.
- *Spyware:* Es un programa que actúa como espía, el recopila información y la envía a una unidad externa sin la autorización del propietario.
- *Rogueware:* Es una aplicación intenta parecerse a otra en nombre o apariencia, para de esta forma despistar al usuario y engañarlo y timarlo
- *Troyanos:* Son un tipo de virus, estos los que hacen es engañar al usuario, ya que disfrazan programas haciéndoles creer al usuario que son buenos.Al abrir este tipo de archivos se crea una "puerta trasera", por la cual se puede acceder al sistema.
- *Programas conejo o bacteria:* Son unos programas que no tienen ningún utilidad, lo único que hacen es realizar copias hasta que se agotan los recursos del sistema y este deja de navegar correctamente.
- *Canales cubiertos:* Son canales de comunicación por los cuales se transfiere información sin tener una autorización previa para ello.

Por otro lado, también podemos hacer una clasificación de las amenazas en función de cómo se realiza el ataque, este tipo de amenazas las clasificamos en los siguientes grupos:

Spam

Son correos no solicitados y que no conocemos su remitente. Estos son enviados de forma masiva. Por tanto, cuando recibimos un correo de estas características lo idóneo es que no lo abramos y directamente lo eliminemos, ya que en muchas ocasiones pueden poseer elementos dañinos para nuestro sistema.

Scam

Se trata de una estafa electrónica mediante la utilización de un correo engañoso. Con este tipo de correos se intenta engañar a las personas mediante donaciones que se suponen que vas a recibir, transferencias de dinero por el cobro de un premio de lotería por ejemplo o la compra de productos que son fraudulentos.

Phishing

Esta técnica cosiste en enviar un correo electrónico en el que lleva adjunto una enlace en el cual el usuario debe de pinchar para validar sus claves como en el caso de las claves de acceso en una entidad financiera. En el momento en el que pinchas el enlace y metes las claves estas ya te han sido robadas.

Algunas de las formas para averiguar si el enlace que nos indica es seguro o no es comprobar que la dirección comienza por https://, también podemos fijarnos en la parte inferior de la ventana de nuestro navegador, si nos encontramos en una página segura entonces aparecerá un candado

Pharming

Dicha técnica consiste en redirigirnos a una página web falsa sin que el usuario tenga que pinchar en ningún tipo de enlace.

Spoofing

Esta forma de ataque consiste en la falsificación o la suplantación de identidad de una persona en la red.

Malware

Son software malintencionados que se infiltran en un sistema teniendo como objetivo controlarlo, reenviar spam o dejar el sistema inutilizable. Dentro de este grupo podemos encontrar los troyanos, virus y gusanos entre otros.

Ingeniería social

Este tipo de ataque tiene como objetivo obtener información sobre credenciales usando la persuasión, abusando de la confianza y la ingenuidad del usuario. El conseguir este tipo de información tiene como fin último obtener beneficios económicos.

Un ejemplo que podemos encontrar es el recibir un correo electrónico que supuestamente es del banco con el que operamos, este nos indica que se están produciendo una serie de problemas en el servicio de internet y que para corregirlos es necesario que ejecute la aplicación que se adjunta. Al instalar esta aplicación se es solicitado los credenciales, al introducirlos estos ya pueden acceder a tus cuentas bancarias en dicha entidad.

Sniffing

Consiste en dispositivos que son capaces de "escuchar" todo aquello que circula entre ordenadores mediante la red sin necesidad de una autorización.

Botnet

Son un conjunto de robots informáticos que tienen la capacidad de poder controlar muchos ordenadores a la vez de forma remota, para de esta forma poder propagar virus, spam o realizar otra serie de actos delictivos.

Password cracking

Consiste en descifrar las contraseñas, estas pueden ser descifradas mediante distintos métodos como el sniffing, también se pueden descifrar observando la introducción de estas, probando distintas combinaciones o mediante la fuerza bruta.

Denegación de servicio

Trata de que el usuario no pueda acceder a un determinado servicio o recurso.

ANEXO IV

MEDIDAS PARA LA REDUCCIÓN DE RIESGOS

A continuación mostramos las distintas medidas que se pueden utilizar para conseguir la reducción de los riesgos. Estas las podemos clasificar en dos grupos, medidas activas y medidas pasivas, en función de si se pretende reducir la posibilidad de ocurrencia de un riesgo o minimizar el impacto producido por este.

Medidas de seguridad activas

Están destinadas a minimizar la posibilidad de que se produzca un riesgo. Esta medida, a su vez se puede dividir dos tipologías:

- **Preventivas:** Estas se toman antes de que se produzca el incidente. Alguna de ellas son las siguientes:
  - Autenticación de usuarios mediante el uso de contraseñas.
  - Llevar un control severo del acceso a los distintos datos.
  - Encriptar datos sensibles o confidenciales.
  - Instalación de antivirus y que este ese continuamente actualizado.
  - Que los usuarios estén socializados con las normas y las políticas de seguridad informática.
  - Actualización de los distintos software

  Es importante la instalación de hardware redundantes en los servidores como por ejemplo discos espejo, tarjetas de red, fuentes de energía.

  Implementación de sistemas de acceso al CPD.

- **Detectivas:** Estas medidas se aplican durante el incidente y pueden ser las siguientes:
  - *Antivirus:* Son programas informáticos que se crean para detectar y eliminar virus o programas que son perjudiciales para el sistema, tanto antes como después de que estos entran en él.
  - *Antispyware:* Es un software que se encarga de detectar y eliminar los spyware que se encuentran en el sistema, siendo este un programa que tiene como función recopilar información de un ordenador sin que el usuario lo sepa durante la actividad de este.

- *Firewalls o cortafuegos:* Este tipo de medida es una barrera de defensa entre las líneas de red corporativa o privada y las públicas. Estas tienen como finalidad bloquear las conexiones que no están autorizadas.
- *Sistema de detección de intrusos:* Intenta detectar los eventos que ocurren en un sistema para evitar los intentos de intrusión que puedan poner en la integridad, disponibilidad y confidencialidad de una red o un ordenador.

Medidas de seguridad pasiva

Éstas se utilizan para minimizar el impacto una vez que se ha producido el incidente. Algunas de estas medidas son la recuperación de datos mediante una copia de seguridad o ejecutando un plan de contingencias.

Control del riesgo: Una vez que se han implantado las medidas necesarias hay que realizar un control sobre su funcionamiento de éstas, para garantizar que la probabilidad de que las amenazas se conviertan en hechos sean mínimas. Si las medidas aplicadas son las correctas y funciona todo de forma adecuada no es necesario realizar nada más, pero en el caso contrario será necesario ajustar las medidas existentes o aplicar nuevas.

Por otro lado, si las medidas no son las adecuadas entonces nos encontramos con el riesgo, con el cual, podemos llevar a cabo los siguientes procedimientos:

- *Eliminación del riesgo:* para ello eliminamos el activo relacionado.
- *Transferir el riesgo:* podemos realizar acuerdos contractuales para traspasar el riesgo a terceros.
- *Asumir el riesgo:* Si decidimos aceptar el riesgo, entonces estamos determinando que el nivel de exposición es adecuado.

ANEXO V

TIPOS DE AUDITORÍA INFORMÁTICA

Auditoría de explotación: Cuando hablamos de explotación informática nos estamos refiriendo a resultados informáticos, es decir, listados, archivos magnéticos, ordenes automatizadas…etc. En el proceso de explotación informática los datos se transforman mediante un proceso informático que está dirigido por otros programas, además pasan controles de integridad y calidad. Pues bien, este tipo de auditoria consiste en analizar las distintas partes que intervienen en este proceso.

- Control de entrada de datos:
- Planificación y recepción de aplicaciones
- Centro de control y seguimiento de trabajos
- Operadores de centros de cómputo
- Centro de control de red y de diagnosis

Auditoría de sistemas: Como bien dice su nombre en este tipo de auditoria lo que se analizan son los distintos sistemas que tiene la organización, dejando aparte las comunicaciones, redes y líneas de las instalaciones informáticas que se auditan de forma separada. En los sistemas que nos centramos en este tipo de auditoría son los siguientes:

- **Sistemas operativos:** Es necesario verificar que estos se encuentran actualizados con las últimas versiones lanzadas por el fabricante. Analizando las diferentes versiones podemos detectar problemas de incompatibilidad con algún tipo de software.
- **Software básico:** Este es el conjunto de productos que configuran completamente el sistema informático sin pertenecer al sistema operativo. Es necesario analizar que este tipo de software no perjudica al funcionamiento del sistema.
- **Tunning:** Lo podemos definir como un conjunto de medidas y técnicas que tienen como objetivo evaluar cómo se comportan los subsistemas y el sistema de forma global.
- **Optimización de los sistemas y subsistemas:** Como diariamente se obtiene información es necesario realizar acciones optimización. Por lo tanto, aquí es necesario verificar estas acciones son efectivas y no interrumpen la operatividad del sistema.

- **Administración de bases de datos:** Aquí se deberá de evaluar los sistemas que existen para salvaguardar las bases de datos y la integridad de los datos.

Auditoría de Seguridad: Este tipo de auditoría analiza tanto las medidas físicas como las medidas lógicas de seguridad que utilizan, es decir una auditoria global de la seguridad. A parte de poder realizar esta auditoria global, también se puede realizar por partes específicas.

Auditoría de desarrollo de proyectos (aplicaciones): En este tipo de auditoria el auditor debe de analizar las metodologías utilizadas para su elaboración, analizar las distintas fases del control interno de las aplicaciones y los procesos y ejecuciones de programas críticos.

Auditoria de comunicaciones y redes: Consiste en analizar los procesos de autentificación que se realizan en los sistemas y todos los procesos que se realizan en las redes.

ANEXO VI

ESTRUCTURA DE LA NORMA ISO 27001

Esta norma se estructura en doce puntos, siendo los que se muestran a continuación:

0. Introducción: En este punto se realiza una introducción al método PDCA.
1. **Campo de aplicación:** Se desarrollan los objetivos y aplicaciones.
2. **Normas para consulta:** Son otro tipo de normas que pueden servir de referencia.
3. **Términos y definiciones:** engloban los términos más usados a lo largo de la norma.
4. **Sistema de gestión de la seguridad de la información:** Aquí se desarrolla todo lo relacionado con el sistema de gestión de la información, es decir, como establecerlo, implementarlo, monitorizarlos, revisarlo mantenerlo y mejorarlo, así como controlarlo y los requerimientos de documentación necesarios.
5. **Responsabilidad de la dirección:** Compromiso que se tiene con el SGSI y la formación y concienciación que tiene que tener el personal de la organización
6. **Auditorías internas del SGSI:** Se indica cómo se deben de realizar las auditorias de control.
7. **Revisión del SGSI por la dirección:** Como realizar la gestión del proceso de revisión del SGSI.
8. **Mejora del SGSI:** Acciones preventivas y correctoras para mantener la mejora continua.
9. **Objetivos de control y controles:** Indica los objetivos de control y los controles que se plasman en la norma
10. **Relación con los principios de la OCDE:** Los apartados de la norma tienen correspondencia con los principios de buen gobierno de la OCDE.
11. **Correspondencia con otra norma:** Se refiere a una tabla de correspondencia de la norma con algunos puntos de la ISO 9001 y la ISO 14001.
12. **Bibliografía:** Conjunto de normas y publicaciones que se han utilizado como referencia para elaborar la norma.

ANEXO VII

DOCUMENTOS QUE FORMAN EL SGSI

A continuación mostramos los diferentes documentos que deben de formar el SGSI según la norma ISO.

- **Alcance del sistema de gestión de seguridad de la información:** Se establece el ámbito de la organización que se encuentra sometido al SGSI.
- **Política y objetivos que se tienen de seguridad:** Establecimiento del compromiso de la dirección y el enfoque que tiene la organización en la gestión de la seguridad de la información.
- **Conjunto de procedimientos y mecanismos de control que soportan al SGSI.**
- **Enfoque de la evaluación de riesgos:** Aquí se establece la metodología utilizada y los criterios de aceptación de riesgos y fijación de niveles aceptables de los riesgos.
- **Informe de evaluación de dichos riesgos:** Se plasma los resultados del estudio de aplicar la metodología.
- **Plan para el tratamiento de riesgos:** En este documento englobamos todo lo relacionado con las acciones, recursos, prioridades y responsabilidades para gestiona los riesgos en función de la evolución de los mismos, recursos disponibles…etc.
- **Procedimientos documentados:** Estos son todos lo necesarios para asegurar la planificación, operación y control de los distintos procesos de seguridad.
- **Registros:** Nos proporcionan una visión de la conformidad de los requisitos y el funcionamiento eficaz del SGSI-
- **Declaración de la aplicabilidad:** Engloba los objetivos de control contemplados por el SGSI, basándose en los resultados de los procesos de evaluación y tratamiento de riesgos.

Todos estos documentos, a su vez los podemos dividir en cuatro bloques:

1. *Manual de seguridad:* Con este documento se dirige todo el sistema, en el se determinan y exponen las intenciones, también los objetivos, el alcance, responsabilidades, políticas…etc.

2. *Procedimientos:* Estos son unos documentos en los que se garantiza que se están realizando de forma eficaz tanto las planificaciones, operaciones y el control de los distintos procesos de seguridad.
3. *Instrucciones/ formularios:* En estos documentos se describen como se efectúan las tareas y actividades que están relacionadas con la seguridad de la información.
4. *Registros:* Los registros son documentos que proporcionan una evidencia de que se están cumpliendo los distintos requisitos establecidos por el SGSI.

ANEXO VIII

RANKING DE PAÍSES EN CERTIFICADOS

A continuación mostramos la siguiente tabla, en la que podemos ver el ranking de países en certificados.

Puesto	País	Numero certificados
01	Japón	7084
02	India	1931
03	Reino Unido	1923
04	China	1710
05	Italia	901
06	Taiwán	861
07	Rumania	840
08	España	799
09	Alemania	581
10	Estados Unidos	566

ANEXO IX

ESTRCTURA ESQUEMA NACIONAL DE SEGURIDAD

Requisitos mínimos:

- Organización e implantación del proceso de seguridad
- Gestión personal
- Análisis y gestión de riesgos
- Profesionalidad
- Autorización y control de los accesos.
- Adquisición de productos
- Protección de instalaciones
- Seguridad por defecto
- Integridad y actualización del sistema
- Protección de la información tanto almacenada como la que se encuentra en tránsito.
- Prevención ante otros sistemas de la información interconectados
- Incidentes de seguridad
- Registro de actividades
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

Todos estos requisitos serán exigidos en función de los riesgos presentes en cada sistema, en algunos casos estos requisitos no será necesario requerirse si el sistema no presenta riesgos significativos.

Principios básicos

- Seguridad integral
- Gestión de riesgos
- Prevención, reacción y recuperación
- Líneas de defensa
- Reevaluación periódica
- Función diferenciada

Medidas de seguridad

Para que se puedan cumplir tanto los principios básicos como los requisitos mínimos es necesario el requerimiento de una serie de medidas de seguridad. Estas medidas variaran en función de las dimensiones del sistema que se quiere proteger y de la categoría que tiene el sistema de información que se quiere proteger. Dichas medidas las podemos encontrar clasificadas en tres grupos, siendo los siguientes, marco organizativo, marco operacional y medidas de protección. A continuación mostramos los distintos puntos a tener en cuenta dentro de cada uno de los grupos.

Marco organizativo

Conjunto de medidas que están relacionadas con la organización global de la seguridad. Dentro de este tipo de medidas podemos encontrar los siguientes apartados.

- Política de seguridad: Esta deberá de ser aprobado por el órgano superior correspondiente y deberá plasmarse en documento para poder requerir de ella en cualquier momento.
- Normativa de seguridad: Está formada por un conjunto de documentos, en los cuales se describe cual es el uso correcto de los distintos equipos, que es considerado como uso indebido de estos y la responsabilidad que tiene el personal de acuerdo al cumplimientos o violación de las normas
- Procedimientos de seguridad: Son un conjunto de documentos en los que se plasma de manera clara y precisa la forma en la que hay que realizar las distintas tareas, quien debe de realizar cada una ellas y la forma de identificar y disminuir los comportamientos que no son habituales.
- Proceso de autorización

Marco operacional

Conjunto de medidas orientas a proteger la operación del sistema considerándolo como un conjunto integral de componentes para un determinado fin. Dentro de este marco operacional encontramos el siguiente desglose.

- Planificación: Dentro de esta se tendrá en cuenta el análisis de los distintos riesgos con los que podemos encontrarnos, la adquisición de componentes nuevos para el sistema, la gestión de las distintas capacidades y los componentes certificados.

- Control de acceso: Este es considerado un conjunto de actividades para que una cierta entidad, proceso o usuario pueda tener acceso o no al sistema para realzar una acción en concreto.
- Explotación: Aquí nos referimos a la realización de un inventario de activos de sistemas, el cual, se debe de encontrar actualizado, también se deberá de configurar la seguridad de los equipos antes de que estos comiencen a utilizarse, la configuración de los distintos elementos del sistema deberán gestionarse de forma continua y será necesario realizar un mantenimiento tanto lógico como físico del sistema. Por otro lado, también será necesario controlar continuamente todos los cambios que se realicen en el sistema, proteger a este de cualquier impacto dañino que le pueda afectar como son los troyanos o los virus. En el caso de sufrir incidencias se dispondrá de un proceso determinado para su gestión, para esta gestión de incidencias será necesario un registro de las actividades de cada uno de los usuarios para de esta forma en caso de darse una poder localizarla con mayor facilidad, además todas las incidencias producidas deberán de ser registradas. También deberán de ser protegidos todos los registros de actividades, así como las claves criptográficas.
- Servicios externos: Cuando se utilice cualquier recurso que sea externo se deberá de tener en cuenta la contratación y los acuerdos realizados, también se deberá de realizar una gestión diaria del sistema, disponer de medios alternativos por si se da el caso de que el servicio que se tiene contratado no está disponible.
- Continuidad del servicio: Aquí nos referimos al análisis del impacto que de los servicios en la organización para de esta forma determinar el impacto que tendría si se interrumpe un servicio en un periodo determinado y aquellos elementos que son imprescindibles para la prestación de los servicios. También será necesario desarrollar un plan de continuidad en el que se determinen las acciones que se deberían de llevar a cabo si se interrumpiera un servicio, así como realizar una serie de pruebas periódicamente para de esta forma detectar cualquier tipo de error que pudiera haber en el plan de continuidad y corregirlo.
- Monitorización del sistema: Las actividades del sistema se encontraran monitorizadas para de esta forma poder detectar intrusos, además se determinaran una serie de indicadores para medir el desempeño del sistema en lo que se refiere a seguridad.

Medidas de protección

Este tipo de medidas está orientado a proteger una serie de activos en concreto, dependiendo de su naturaleza. Dentro de este tipo de medidas podemos encontrar las siguientes:

- Protección de las instalaciones e infraestructuras
- Gestión del personal
- Protección de las comunicaciones
- Protección de los equipos
- Protección de los soportes de la información
- Protección de la información
- Protección de las aplicaciones informáticas
- Protección de los servicios

ANEXO X

MEDIDAS DE SEGURIDAD OBLIGATORIAS PARA ENTIDADES DE CRÉDITO, CAJAS DE AHORRO Y BANCOS

Las Cajas de Ahorro, entidades de Crédito y Bancos están reguladas por la Orden INT/317/2011, de 1 de Febrero, sobre las Medidas de Seguridad Privada. En el Capítulo II de dicha Orden podemos encontrar las medidas específicas de seguridad que tienen que cumplir de forma obligatoria. Por otro lado, también tienen que cumplir las normas que se exponen en el artículo 112 del Real Decreto 2364/1194, del 9 de Diciembre, por el que se aprueba el Reglamento de Seguridad privada. . En el Capítulo II de dicha Orden podemos encontrar las medidas específicas de seguridad que tienen que cumplir de forma obligatoria. Por otro lado, también tienen que cumplir las normas que se exponen en el artículo 112 del Real Decreto 2364/1194, del 9 de Diciembre, por el que se aprueba el Reglamento de Seguridad privada.

Capítulo II Orden Ministerial INT/317/2011

Artículo 3. Medidas de seguridad que son obligatorias

1. "En los establecimientos u oficinas de las entidades de crédito o que actúen en nombre o representación de éstas, donde se custodien fondos o valores, se instalarán con carácter obligatorio las medidas de seguridad especificas en los párrafos, a),b),c) y f) del apartado primero del artículo 120 y las previstas en el apartado primero del artículo 12 del Reglamento de Seguridad Privada.

El efectivo disponible en los establecimientos referidos en este artículo deberán ser custodiados en alguno de los contenedores provistos de retardo, prevenidos en los artículos 121 y 122 del Reglamento de Seguridad Privada y en los artículos 8 a 13, ambos inclusive, de esta Orden."

2. " Los establecimientos u oficinas mencionados en el aparto anterior, situados en localidades con población superior a 10.000 habitantes, deberán contar, además, con una de las tres medidas de seguridad que se citan a continuación:

a) El reciento de caja a que se refiere el párrafo d) del apartado primero del artículo 120 del Reglamento de Seguridad Privada, con el nivel de blindaje que se señala en el artículo 6 de esta Orden.

Se considerará recinto de caja el destinado a disponer de las cajas auxiliares en su interior.

b) El control de accesos previsto en el párrafo e) del aparto primero del artículo 120 del citado Reglamento, con el nivel de blindaje que se determina en el apartado segundo del artículo 6 de esta Orden.

c) Dispensadores de efectivo o recicladores adecuados a lo dispuesto en el apartado tercero del artículo 122 del Reglamento de Seguridad Privada y en el artículo 13 de esta Orden, cuando su instalación sustituya a todas las cajas auxiliares. En caso de mantenerse alguna caja auxiliar, será preciso que ésta se encuentre dentro del recinto de caja.

   Las cajas auxiliares o submostradores no podrán ser utilizadas fuera del recinto de caja salvo en los casos y forma prevista en el artículo 12 de la presente Orden. No obstante, su ubicación y anclaje en el patio de operaciones podrá efectuarse siempre y cuando el mencionado elemento cuente con las medidas de seguridad que ya están previstas en el citado artículo, así como con un dispositivo electrónico que permita la apertura del cajón superior sólo en el caso de avería del dispensador de efectivo, limitándose su utilización a la custodia temporal, y por el menor tiempo disponible, de las sacas de dinero depositadas por las empresas de transporte de fondos en el compartimento de efectivo que existe en la parte inferior. Cuando se utilice para este fin, el retardo deberá ser, como mínimo, de diez minutos.

   Para el caso de que estos submostradores estuvieran dotados del dispositivo electrónico de apertura citado en el párrafo anterior, también se podrán utilizar para depositar, en su interior, los billetes rechazados, falsos, deteriorados y la moneda extranjera que pueda aparecer en las operaciones habituales."

3. " En virtud del artículo 111 del Reglamento de Seguridad Privada, y al objeto de proteger el efectivo que manejen, las oficinas ubicadas en poblaciones con menos de 10.000 habitantes deberán contar con las medidas enumeradas en el apartado primero de este artículo, y , además, si no disponen de alguna de las medidas de seguridad que se citan en los párrafos a),b) y c) del apartado segundo, con un caja auxiliar, que podrán ubicar en cualquier zona de la oficina bancaria, debiendo estar sujeta, conforme al apartado tercero del artículo 12 de esta Orden, y reunir las características establecidas en el apartado segundo del artículo 122 del citado Reglamento".

4. “ En las localidades que cuenten con una población entre 10.000 y 50.000 habitantes, y en función de que superen o no la media nacional sobre robos con fuerza y robos con violencia o intimidación en entidades de crédito durante los dos últimos años, a contar desde la entrada en vigor de la presente Orden, el Delegado o Subdelegado del Gobierno o, en su caso, la Autoridad autonómica competente, podrá dispensa el cumplimiento de las medidas de seguridad establecidas en el apartado segundo de este artículo”.

Artículo 4. Equipos de registro de imágenes

1. “La parte destinada a registro de imágenes de los equipos o sistemas que se instalen en las entidades de crédito deberá estar ubicada, en el interior de la sucursal, en lugares no visibles por el público; y el sistema de protección contra robo de los soportes de las imágenes ha de tener activado, durante el horario de atención al público, un retardo para su acceso de, como mínimo, diez minutos, que podrá ser técnico cuando se trate de sistemas informáticos, y físico o electrónico cuando se trate de vídeo-grabación”.
2. “El sistema retardo podrá ser sustituido por una llave de apertura del lugar en que se encuentre el equipo, que estará depositada en un elemento contenedor que cuente con el mismo tiempo de retardo”.
3. “Estos equipos de registro de imágenes deberán, además, estar conectados permanentemente al sistema de seguridad de la entidad, de forma que puedan ser utilizados como elemento de verificación por la central de alarmas autorizada a la que estuvieran conectados, de conformidad con lo previsto en la normativa sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada”:

Artículo 5. Dispositivos electrónicos de seguridad

“ Los dispositivos electrónicos que se instalen en las entidades de crédito, deberán tener un grado de seguridad 3, conforme a la Norma UNE 50131 – 1 y proteger, como mínimo, los elementos donde se deposite el efectivo y los puntos de acceso al establecimiento, debiendo el personal de la entidad accionar los pulsadores o medios a que se refiere el párrafo c) del apartado primero del artículo 120 del Reglamento de Seguridad Privada, ante un robo con intimidación u otras circunstancias que por su gravedad lo requieran, siempre que el accionamiento no suponga riesgo para la integridad física de dicho personal, o para terceras personas”.

Artículo 6. Blindaje de recintos de caja y del control de accesos

1. "El recinto de caja, incluida su puerta de acceso, tendrá un blindaje perimetral, como mínimo, de categoría de resistencia BR2, según la Norma UNE-EN 1063 para las partes acristaladas y de la misma clase, según la Norma UNE 108132, para las partes opacas".
2. "El control individualizado de accesos de las entidades de crédito a que se refiere el apartado segundo del artículo 3 de esta Orden, tendrá un blindaje interior, como mínimo, de categoría de resistencia BR2 y exterior, de categoría de resistencia P5A, según las Normas UNE – EN 1063 y UNE – EN 356, para los indicados niveles, respectivamente".
3. "Los dispositivos para pasar documentos o efectivo en los recintos de caja, a los cuales se refiere el párrafo d) del apartado primero del artículo 120 del Reglamento de Seguridad Privada, habrán de ser capaces de impedir el ataque directo con armas de fuego a los empleados situados en el interior".

Artículo 7. Carteles anunciadores

"Los carteles anunciadores de la existencia de medidas de seguridad tendrán un tamaño no inferior a dieciocho por doce centímetros".

Artículo 8. Cámaras acorazadas

1. "Las cámaras acorazadas de nueva instalación habrán de estar delimitadas por una construcción de muros acorazados en paredes, techo y suelo; con acceso a su interior a través de la puerta y trampón, si lo hubiera, ambos acorazados".
2. "El muro estará rodeado en todo su perímetro lateral por un pasillo de ronda con un anchura máxima de 60 centímetros, delimitado por un muro exterior con grado de seguridad II, según la Norma UNE – EN 1143 – 1".
3. "Los muros, puertas y trampón, si lo hubiere, de la cámara, habrá de estar construidos, de forma que, como mínimo, su grado de seguridad sea VII, según la Norma UNE – EN 1143 – 1".
4. "Las puertas de las cámaras acorazadas contaran con un dispositivo de bloqueo y sistema de apertura retardada de, como mínimo, diez minutos. Quedan exceptuadas del sistema de apertura retardada aquellas que contengan compartimentos de alquiler".
5. "La cámara estará dotada de detección sísmica, microfónica u otros dispositivos que permitan detectar cualquier ataque a través de las pareces, techo o suelo y detección volumétrica en su interior. Todos estos elementos, conectados al sistema de seguridad,

deberán transmitir la señal de alarma, por dos vías de comunicación distintas, de forma que la inutilización de una de ellas produzca la transmisión de la señal por la otra".

6. "Los elementos que compongan el sistema electrónico de protección, deberán tener un grado de seguridad 3, conforme a lo establecido en la Norma UNVE – EN 50131 – 1.

7. "El sistema de bloqueo de las cámaras acorazadas deberá estar activado desde la hora de cierre del establecimiento hasta la hora de apertura del día siguiente hábil".

8. "Las cámaras acorazadas cuya función sea únicamente la de contener el encaje diario de la oficina, se asimilarán a las cajas fuertes a efectos del grado de seguridad que deben cumplir, en los términos establecidos para ellas, en el artículo siguiente".

Artículo 9. Cajas fuertes

1. "Las cajas fuertes han de estar construidas con materiales con grado de seguridad 4 según la Norma UNE – EN 1143 – 1":

2. "Las cajas fuertes deberán contar, como mínimo, con la protección de un detector sísmico, que estará conectado con el sistema de alarma del establecimiento".

3. "Las cajas fuertes contarán con un dispositivo de bloqueo y sistema de apertura retardad de, como, mínimo, diez minutos. El dispositivo de retardo podrá ser desactivado, durante las operaciones de depósito de efectivo, por los vigilantes de seguridad encargados de dichas operaciones, previo aviso, en su caso, al responsable del control de los sistemas de alarma".

4. "El dispositivo de bloqueo de las cajas fuertes deberá estar activado desde la hora de cierre del establecimiento hasta la hora de apertura del día siguiente hábil".

5. "Cuando su peso sea interior a 2.000 kilogramos, deberán estar ancladas, conforme a lo establecido en la disposición adicional segunda de esta Orden".

Artículo 10. Cajas y compartimentos de alquiler

1. "Las cajas o compartimentos de alquiler deberán estar instalados en un cámara acorazada de las características determinadas en el artículo 121 del Reglamento de Seguridad Privada y en los apartados primero, segundo y cuarto del artículo 8 de esta Orden".

2. "Las cajas o compartimentos de alquiler tendrán un grado de seguridad A, según la Norma UNE 108115".

3. “Cuando los compartimentos de alquiler se ubiquen en cajas fuertes, estas últimas deberán tener un grado de seguridad 4 según la Norma UNE – EN 1143 – 1. Además, el local en que se encuentren las cajas fuertes estará protegido con dispositivos o sistemas que permitan la detección de intrusiones en el mismo, y que estarán conectados al sistema de alarma, de forma qe se transmitan las señales por dos vías de comunicación distintas, y que la inutilización de una de ellas produzca la transmisión por la otra”.

“Cuando el peso de tales cajas se inferior a 2.000 kilogramos, deberán estar ancladas, conforme a lo establecido en la Disposición Adicional Segunda de esta Orden”.

“Los elementos que compongan el sistema de alarma, deberán tener un grado de seguridad 3, conforme a la Norma UNE-EN 50131-1”.

4. “Las cámaras acorazadas que se dediquen únicamente a cajas y compartimentos de alquiles, dispondrán de un dispositivo de bloqueo, que ha de estar activado desde la hora de cierre del establecimiento hasta la hora de apertura del día siguiente hábil”.

Artículo 11. Cajas de tránsito

“Las cajas de tránsito o, en general, aquellas que tengan por finalidad el deposito transitorio de efectivo, de forma que permita su recogida o entrega sin necesidad de concurrencia física o temporal del receptor y el cedente, habrá de reunir las siguientes características”:

a) “Estarán construidas con materiales que tengan, como mínimo, un grado de seguridad 4 según la Norma UNE-EN 1143-1”.
b) “Deberán estar empotradas, de manera fija, en muros o paredes, u otros elementos, de forma que, en este segundo supuesto, el conjunto formado, en caso de pesar menos de 2.000 kilogramos, esté, a su vez, anclado a muros o paredes, en las formas previstas en la disposición adicional segunda de esta Orden”.
c) “Contarán con sistema de detección sísmica conectado con el sistema de alarma de la entidad, que permita detectar el ataque por cualquiera de sus accesos”:
d) “Dispondrán de dos puertas, una hacia el interior de la oficina o zona de acceso restringido, y otra hacia el exterior (vestíbulo de acceso, zona de autoservicio o fachada exterior), con sistema de gestión electromecánico que impida la apertura simultánea de ambas”.

e) “El sistema de apertura de la puerta interior tendrá un retardo, como mínimo, de diez minutos, y un sistema de bloqueo que impida la apertura fuera de las horas de actividad del establecimiento”.

f) “La puerta exterior estará dotada de un dispositivo de bloqueo que regule los horarios de su apertura. Éste no permitirá abrir la puerta durante el horario autorizado sin inmediatamente antes ha habido una apertura de dicha puerta y se ha efectuado un depósito de fondos. Para la apertura de la puerta exterior, será necesario el uso combinado de, como mínimo, la identificación del usuario autorizado, mediante código secreto personal; el acceso a la operación mediante clave secreta de apertura; y una llave física, que permita accionar los mecanismos de apertura”.

g) “Programación para que se accione el bloqueo durante, como mínimo, una hora, al tercer intento de apertura con el código personal incorrecto o durante, al menos, tres horas, cuando el error afecte a la clave de apertura, debiendo, en este caso, enviar una señal a la central de alarmas”.

Artículo 12. Cajas auxiliares

1. “Las cajas auxiliares se ubicarán en el interior del recinto de caja, salvo que la oficina cuente con control individualizado de accesos en la forma prevista en el párrafo e) del apartado primero del artículo 120 del Reglamento de Seguridad Privada. Los elementos con posibilidad de depósito de efectivo de dichas cajas han de estar protegidos con un sistema de retardo en su apertura de, como mínimo, cuatro minutos”.

2. “Las cajas auxiliares, cuando se instalen de forma permanente en el patio de operaciones, para sustituir a los dispensadores/ recicladores en caso de avería, como prevé el apartado tercero del artículo 122 del Reglamento de Seguridad Privada, deberán contar, en su cajón superior, con un dispositivo interno de bloqueo sobre el que solo se pueda actuar remotamente, conectado al sistema de alarma, que permita su apertura sólo en caso de avería del dispensador”.

3. “Las cajas auxiliares, independientemente de su ubicación, no podrán almacenar efectivo fuera del horario de apertura del establecimiento, y cuando se instalen en el patio de operaciones, deberán estar, en todo caso, sujetas al suelo o pared, pudiendo hacerlo por procedimientos distintos a los contemplados en la Disposición Adicional Segunda de esta Orden”.

4. “El compartimento que existen en su parte inferior, podrá ser utilizado como depósito transitorio de efectivo, limitándose su uso a la custodia, por el menor tiempo posible, de las sacas de dinero depositadas por las empresas de transporte de fondos, así como de divisas y efectivo no apto para la circulación, en cuyo caso el retardo de apertura será de diez minutos. Este retardo podrá ser desactivado, por los vigilantes de seguridad, durante las operaciones de depósito o recogida, previo aviso, en su caso, al responsable del control de los sistemas de alarma”.

Artículo 13. Dispensadores/ recicladores de efectivo

1. “Los dispensadores/ recicladores de efectivo reunirán las siguientes características:
    a) La caja fuerte en la que se ubiquen los contenedores de efectivo, estará construida con materiales cuyo grado de seguridad sea4, como mínimo, según la Norma UNE-EN 1143-1 y deberá reunir el resto de medidas recogidas en el artículo 9 de esta orden.
    b) Límite máximo de dispensación por operación, según el aprtado segundo del Anexo II de esta Orden.
    c) Sistema de bloqueo de apertura y detección de ataques conectados al sistema de alarma, cuando sean utilizados como depósito nocturno de efectivo.
    d) Deberán estar anclados cuando su peso sea interior a 2.000 kilogramos, conforme a lo establecido en la Disposición Adicional Segunda de esta Orden.
    e) Programación para transmitir directamente la señal de alarma a la central de alarmas, en caso de robo con intimidación, o cuando se tramiten tres o más operaciones consecutivas de dispensación de efectivo contra la misma cuenta, en un tiempo máximo de tres minutos”

2. “Los dispensadores/ recicladores de efectivo que reúnan estas características, podrán ser instalados fuera del recinto de caja, en la zona reservada al personal de la entidad”.

Artículo 14. Cajeros automáticos

1. “Las puertas de acceso del público y el resto de acristalamiento de la parte exterior del vestíbulo, en el que se ubican cajeros automáticos, tendrán una categoría de resistencia P5A al ataque manual, de acuerdo con lo establecido en la Norma UNE – EN 356, o clase de resistencia 5, de acuerdo con la Norma UNE-EN 1627, si las puertas fueran opacas”.

2. “La caja fuerte de los cajeros automáticos en la que ubiquen los contenedores de efectivo tendrá, como mínimo, un grado de seguridad 4 según la Norma UNE-EN 1143-1; debiendo contar, para permitir la extracción de los contenedores, con un sistema de retardo en su apertura de, como mínimo, diez minutos. Éste podrá ser desactivado durante las operaciones de depósito o retirada de efectivo por los vigilantes de seguridad encargados de dichas operaciones, previo aviso, en su caso, al responsable de control delos sistemas de alarma”.

3. “La caja fuerte donde se custodie el efectivo contará con la preceptiva detección sísmica”.

4. “Cuando los cajeros automáticos se instalen en espacios abiertos y no estén integrados o formen parte del perímetro de un edificio, la cabina a que se refiere el apartado quinto del artículo 122 del Reglamento de Seguridad Privada, estará protegida con chapa de acero de, como mínimo, tres milímetros de espesor o material de resistencia equivalente, y la puerta de acceso a la cabina tendrá una categoría de resistencia P5A al ataque manual según Norma UNE-EN 356 o clase de resistencia 5, de acuerdo con la Norma UNE-EN 1627, si las puertas fueran opacas”.

Artículo 15. Módulos bancarios transportables

1. “Los módulos bancarios transportables, o bancos móviles, tendrán un blindaje en su recinto de caja y puerta de acceso al mismo con una categoría de resistencia BR2, según la Norma UNE-EN 1063 para las partes acristaladas y de la misma clase, según la Norma Une 108132, para las partes opacas”.

2. “Los retardos de la caja fuerte y del módulo de la caja auxiliar serán de diez y cuatro minutos, respectivamente”.

3. “El recinto de caja podrá ser sustituido por la instalación de dispensador de efectivo”.

Artículo 16. Moneda fraccionaria

“A los efectos de medidas de seguridad y limitaciones de cantidad dineraria a que se refiere el presente Capítulo, la moneda fraccionaria no se tendrá en consideración”.

Reglamento de seguridad privada

Artículo 112. Enumeración de los servicios o sistemas y circunstancias determinantes

1.”Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el calor de los bienes muebles u objetos valiosos que posean o cualquier otra causa lo hiciesen necesario, el Secretario de Estado de Interior para supuestos supra provinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes:

a) Creación del departamento de seguridad
b) Establecimiento del servicio de vigilantes de seguridad, con o sin armas a cargo de personal integrado en empresas de seguridad.
c) Instalación de dispositivos y sistemas de seguridad y protección.
d) Conexión de los sistemas de seguridad con centrales de alarmas, ajenas o propias, que deberán ajustarse en su funcionamiento a los establecimientos en los artículos 46,48 y 49, y reunir los requisitos que se establecen en el apartado 6.2 del anexo del presente reglamento; no pudiendo prestar servicios a terceros si las empresas o entidades no están habilitadas como empresas de seguridad”.

2.”En todo caso deberá existir Departamento de Seguridad cuando concurran las circunstancias de los párrafos b) y c) del artículo 96.2 de este Reglamento”.

ANEXO XI

PRINCIPIOS DE LA ENTIDAD FINANCIERA LA CAIXA

A la hora de la protección de información, la entidad financiera La Caixa se basa en los siguientes principios.

Confidencialidad

- 1. “La Caixa” tiene la obligación de proteger al máximo la información personal y privada de sus clientes y empleados. Toda información verbal o escrita, incluida la electrónica, de los clientes y de los empleados se halla protegida. Debemos presumir que toda la información que recibimos es confidencial, salvo que lo contrario resulte evidente.
- 2. “Debemos salvaguardar y no revelar la información que recibimos sobre ”la Caixa”, sus clientes, proveedores y personas o entidades asociadas. Un comentario, incluso casual, sobre dicha información a terceros, incluidos parientes o amigos, puede violar el deber de confidencialidad. Cuando contratamos otras empresas para proveer servicios para nosotros, debemos exigirles que protejan igualmente la confidencialidad de la información que reciben”.
- 3. “Sólo podemos hacer uso de la información recibida de los clientes y los empleados para la finalidad para la que nos fue transmitida, todo ello de conformidad con la normativa vigente en esta materia. No podemos pretender acceder a información que no sea estrictamente necesaria para el desempeño de nuestro trabajo. Antes de transmitir información a terceros, debemos estar seguros de que estamos autorizados para ello y que lo hacemos en favor de los empleados, directivos o administradores que tengan una razón legítima para conocer o participar de la misma. Incluso en el caso de estar autorizados, es preciso limitar a lo estrictamente necesario el volumen de información a revelar. En caso de cualquier duda debemos consultar con nuestro superior jerárquico”.

- 4. “No debemos comentar ni dar información sobre “la Caixa”, aunque sea de carácter general, en conferencias, simposios, artículos, entrevistas, Internet, etc., salvo en el caso de haber sido previamente autorizados para ello. La correspondencia escrita y la entrega de documentos a clientes o terceros se limitarán a los textos establecidos con carácter general. Para el envío o emisión de documentos tales como

cartas o certificaciones que no estén previstos en las normativas internas, deberemos consultar previamente con el departamento correspondiente".

- 5. "El secreto profesional de las entidades financieras no puede alegarse frente a los tribunales de justicia y otras autoridades de conformidad con las leyes vigentes. Los requerimientos que de ellos podamos recibir debemos contestarlos a través de los circuitos establecidos con carácter general. Cuando la autoridad requirente o la información solicitada no estén contempladas en las normas internas de"la Caixa" o bien se trate de citaciones a declarar personalmente, debemos consultarlo con la Dirección de la Asesoría Jurídica".

- 6. "Debemos respetar las normas internas sobre tratamiento y confidencialidad de los datos personales aprobadas por "la Caixa", que se fundamentan en la Directiva 95/46 CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 y en la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999 de 13 de diciembre. Igualmente debemos respetar la privacidad de los datos personales de los empleados, especialmente los relativos a su salud".

Integridad

1. "Queremos actuar de forma transparente en todas nuestras actividades. La confianza de nuestros clientes y de las comunidades en las que operamos se halla en la base de nuestra actividad empresarial. La confianza sólo puede existir si la integridad de"la Caixa" queda fuera de toda duda. 2 Solamente manteniendo un elevado nivel de integridad nos hacemos acreedores de la confianza de los clientes y de la comunidad en general. 3 Creemos en la libre competencia, honesta y leal".

ANEXO XII

MEDIDAS RECOMENDADAS POR LA CAIXA A LOS USUARIOS PARA LA UTILIZACIÓN LINEA ABIERTA

1. No abrir mensajes electrónicos si no conocemos su origen.
2. No facilitar los datos personales ni los códigos PIN.
3. No abrir archivos si no conocemos su remitente.
4. No tener apuntados los códigos PIN en ningún lado y tener en lugar seguro las coordenadas de la tarjeta Línea Abierta (sistema por el que se realizan las operaciones online con Caixa).
5. No utilizar PIN triviales o que sean fáciles de deducir.
6. No confiar en promociones o regalos que nos han tocado; tampoco debemos de responder a aquellos mensajes que nos solicitan información urgentemente.
7. Tener un antivirus instalado. También es necesario tener un sistema anti-espías para ayudarnos a protegernos de los programas espías y de la publicidad no deseada.
8. Mantener actualizado el navegador y tener instalados los parches del sistema operativo.
9. Tener en cuenta las diferentes formas de proteger el ordenador.
10. Mantenerse actualizado personalmente en el uso de internet.

ANEXO XIII

AUDITORIA DE CUMPLIMIENTO DE LA LEY ORGANICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El objetivo que tenemos con la realización de este cuestionario sobre el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal es conocer si la entidad auditada cumple la normativa correspondiente, en su caso también podemos conocer qué aspectos de la ley no está cumpliendo. Además, también nos permite conocer qué tipo de medidas debemos de aplicar para su cumplimiento.

Empresa:……

Fecha:……..

Auditor:…….....

ASPECTOS GENERALES

1. ¿Cree que su entidad se encuentra al corriente de la normativa que tiene que aplicar en lo que se refiere a la protección de datos de carácter personal?
   - ☐ Sí
   - ☐ No
2. ¿Cree que cumple la ley tanto en el tratamiento de ficheros automatizados como en los que no lo son?
   - ☐ Sí
   - ☐ No
3. ¿Conoce las sanciones aplicadas por incumplimiento de la LOPD?
   - ☐ Sí
   - ☐ No

1. ¿Los ficheros que contienen datos de este tipo han sido inscritos en la Agencia Española de Protección de Datos (AEPD)?
   - ☐ Sí
   - ☐ No

2. ¿Se actualizan regularmente los ficheros?
   - ☐ Sí
   - ☐ No
3. ¿Cuándo se realiza algún tipo de cambio en los ficheros se le comunica a la AEPD?
   - ☐ Sí
   - ☐ No
4. ¿Qué se realiza con los ficheros de datos personales que ya no son necesarios?
   - ☐ Guardarlos
   - ☐ Borrarlos
   - ☐ Eliminarlos
5. ¿Conocen los derechos ARCO?
   - ☐ Sí
   - ☐ No
6. ¿Transfiere datos a terceros?
   - ☐ Sí
   - ☐ No
7. ¿Aquellos a los que le trasfiere datos cumplen con la normativa sobre protección de datos de carácter personal?
   - ☐ Sí
   - ☐ No

FUNCIONES Y OBLIGACIONES DEL PERSONAL

1. ¿Conoce todo el personal de la empresa las funciones y las medidas establecidas que deben cumplir para garantizar la seguridad de la información?
   - ☐ Sí
   - ☐ No
2. ¿Conocen las consecuencias de su incumplimiento?
   - ☐ Sí
   - ☐ No
3. ¿Se encuentran explicadas en el documento de seguridad las funciones y obligaciones del personal que trabaja con datos de carácter personal?
   - ☐ Sí
   - ☐ No

4. ¿Se mandan regularmente recordatorios o circulares para asegurarse de que todos los empleados conocen las medidas que tienen que aplicar?
   - ☐ Sí
   - ☐ No
5. ¿Cada empleado tiene determinado un perfil de usuario?
   - ☐ Sí
   - ☐ No

CONTROL DE ACCESO FÍSICO

1. ¿Qué tipo de medidas utiliza para controlar el acceso físico?
   - ☐ Video vigilancia
   - ☐ Llaves, candados…
   - ☐ Personal de seguridad
   - ☐ Ninguna
2. ¿Solo pueden acceder aquellos que están autorizados?
   - ☐ Sí
   - ☐ No
3. ¿Los ficheros no automatizados se encuentran en lugares donde el acceso está restringido?
   - ☐ Sí
   - ☐ No
4. ¿Dispone de un documento en el que se establezca la relación de personas que pueden acceder a los ficheros de datos personales y a cuáles pueden acceder?
   - ☐ Sí
   - ☐ No

COPIAS DE SEGURIDAD Y RESPLADO

1. ¿Se realizan copias de seguridad y respaldo?
   - ☐ Sí
   - ☐ No
2. ¿Se comprueba que estas se realizan de forma correcta?
   - ☐ Sí
   - ☐ No

3. ¿Se realizan frecuentemente copias de seguridad?
   - ☐ Todos los días
   - ☐ Una vez a la semana
   - ☐ Una vez al mes
4. ¿Las copias de seguridad se encuentran en el mismo lugar en que se encuentran los equipos informáticos?
   - ☐ Sí
   - ☐ No
5. En el caso de los ficheros no automatizados, ¿se realizan copias de respaldo?
   - ☐ Sí
   - ☐ No

REGISTRO DE INCIDENCIAS

1. ¿Tienen un registro de incidencias, en el que se registra cuándo se produce y quién la produce?
   - ☐ Sí
   - ☐ No
2. ¿Se registran todas las incidencias que se dan?
   - ☐ Sí
   - ☐ No
3. ¿Se analiza de manera frecuente para establecer medidas correctoras si es necesario?
   - ☐ Sí
   - ☐ No

GESTION DE SOPORTES

1. ¿Los soportes que contienen datos de carácter personal se almacenan en un lugar donde el acceso está restringido?
   - ☐ Sí
   - ☐ No
2. ¿Se realizan inventarios de dichos soportes?
   - ☐ Sí
   - ☐ No

3. ¿Registran las entradas y salidas de los soportes, así como todo lo relacionado con estas como la hora, fecha, persona que utiliza el soporte, que tipo de datos contiene…etc.?
   - ☐ Sí
   - ☐ No
4. ¿Cuándo se realiza el traslado de ficheros, se utilizan todas las medidas necesarias para impedir la manipulación, pérdida y robo de los datos?
   - ☐ Sí
   - ☐ No

REGISTROS DE ACCESO

1. ¿Cada vez que se realiza un acceso, se almacena la identificación, hora y fecha y si el acceso es autorizado o denegado?
   - ☐ Sí
   - ☐ No
2. Cuando tratan ficheros automatizados a los que hay que aplicarles altos niveles de seguridad, ¿cuánto tiempo guardan como mínimo los datos registrados?
   - ☐ 1 año
   - ☐ 2 años
   - ☐ 5 años
3. Para ficheros no automatizados y que son de alta seguridad, ¿se utiliza algún tipo de mecanismo para registrar los accesos a estos?
   - ☐ Sí
   - ☐ No

DOCUMENTO DE SEGURIDAD

1. ¿Disponen de documento de seguridad?
   - ☐ Sí
   - ☐ No
2. ¿Cumple con la normativa vigente referente a datos de carácter personal?
   - ☐ Sí
   - ☐ No

3. ¿Se actualiza regularmente?
   - ☐ Sí
   - ☐ No
4. ¿Está definido en él claramente quién es el responsable de seguridad y cuáles son sus funciones y obligaciones?
   - ☐ Sí
   - ☐ No
5. ¿El responsable de seguridad conoce claramente sus funciones y obligaciones?
   - ☐ Sí
   - ☐ No
6. ¿Hace saber al resto del personal las medidas de seguridad que hay que aplicar?
   - ☐ Sí
   - ☐ No

IDENTIFICACION Y AUTENTIFICACION

1. ¿Disponen de un registro del personal que tiene autorizado el acceso a ficheros que contienen datos personales?
   - ☐ Sí
   - ☐ No
2. ¿Disponen de sistemas de identificación de los usuarios para acceder a los distintos ficheros que contienen información de este tipo?
   - ☐ Sí
   - ☐ No
3. ¿Cada cuánto tiempo se modifican las contraseñas?
   - ☐ 3 meses
   - ☐ 6 meses
   - ☐ 1 año
   - ☐ Otro……

TRATAMIENTO DE DATOS

1. ¿Cuándo se recoge información, se le informa al interesado?
   - ☐ Sí
   - ☐ No

2. ¿Han tenido algún tipo de queja por parte de algún cliente por el tratamiento de sus datos?
   - ☐ Sí
   - ☐ No
3. ¿Cuándo se dispone de un fichero que ya no va a tener uso, lo eliminái s?
   - ☐ Sí
   - ☐ No
   - ☐
4. ¿Los datos recogidos se utilizan solamente para su finalidad inicial?
   - ☐ Sí
   - ☐ No

AUDITORÍA

1. ¿Cuándo se realizó la última auditoria?
   - ☐ Hace 6 meses
   - ☐ Hace 1 año
   - ☐ Hace 2 años
   - ☐ Otros……..
2. ¿Fue satisfactoria?
   - ☐ Sí
   - ☐ No
3. ¿Se llevan a la práctica las medidas correctoras que se han establecido una vez que se ha realizado el análisis del informe de auditoría?
   - ☐ Sí
   - ☐ No
4. Si se realizan importantes cambios en los sistemas de información, ¿se solicita una auditoria para verificar que se aplican las medidas de seguridad necesarias?
   - ☐ Sí
   - ☐ No