Universidad Zaragoza
1542

Trabajo Fin De Grado

Título

Seguridad informática empresarial aplicada a una asesoría

Autora

Elena Lorente Bermejo

Directora

María de los Ángeles Duque Martínez

Facultad de Economía y Empresa

2020

Autora: Elena Lorente Bermejo
Directora: María de los Ángeles Duque Martínez
Título: Seguridad informática empresarial aplicada a una asesoría
Titulación: Grado en Finanzas y Contabilidad

RESUMEN

La realización de este trabajo fin de grado tiene por objeto desarrollar conceptos básicos, entidades oficiales y algunas tecnologías y herramientas útiles para cualquier trabajador que desempeñe tareas relacionadas con datos en toda su trayectoria, enfocado dentro del ámbito de la seguridad informática.

Cualquier empresa dispone de sistemas de información (ERP, Excels, ficheros de texto, bases de datos, …etc.) con algún tipo de información confidencial, por ejemplo, de clientes o proveedores. Por ello, es necesario que sea tratada de manera acorde con la ley y cumpliendo siempre unas buenas prácticas que permitan un correcto y óptimo tratamiento de los datos para la posible obtención de certificaciones.

El tema de la seguridad informática solamente centrada en los datos ya es en sí mismo una materia muy amplia en el mundo de la informática y se encuentra en una constante evolución, por lo que se ha pretendido adquirir y extrapolar de toda esa información unos conocimientos básicos y comunes que permitan conocer esta disciplina y poder reutilizar todos estos conocimientos en mi experiencia profesional.

ABSTRACT

The purpose of this bachelor degree project is to learn basic concepts, official entities and some technologies and tools useful for any worker who performs tasks related to data in all its flow, focused within the field of computer security.

Nowadays, any company has information systems (ERP, Excels, text files, databases, ...etc.) with some kind of confidential information from customers or suppliers. For this reason, it is necessary that it is processed in accordance with the law and always complying with good practices that allow a correct and optimum treatment of the data for the possible obtaining of certifications.

The subject of computer security, which is only centred on data, is already a very broad subject in the world of information technology and is in constant evolution. For this reason, I have tried to learn and extrapolate from all this information some basic and common understanding that will allow me to know a little about this topic and to be able to reuse all this knowledge in my professional experience.

Indice

1. Introducción

1.1 Motivo

Actualmente, me encuentro trabajando en una consultora tecnológica dando servicio en el ámbito del sector público y me ha parecido muy interesante para mi evolución como profesional en este sector, aprender ciertos conceptos básicos y comunes en relación a la seguridad de la información, ya que constantemente trabajo con datos confidenciales en múltiples sistemas de información.

Continuamente se ve en las noticias ataques de hackers a empresas, en concreto a sus sistemas de información, que hacen perder gran cantidad de dinero. Muchos de esos ataques se deben a una mala gestión de las contraseñas por parte de algunas empresas.

Los sistemas de hoy en día son muy seguros, pero las personas seguimos siendo muy vulnerables.

Por estos motivos, se ha pretendido desarrollar conceptos básicos acerca de los datos y ficheros con los que trabajamos a diario.

1.2 Objetivos

El objetivo de este trabajo es obtener una serie de conocimientos y conclusiones acerca de la seguridad de la información.

Para ello, he decidido desarrollar de forma práctica esta temática, ya que son conceptos estandarizados que nos encontramos a menudo en muchas materias y ámbitos, tanto en el mundo laboral como en la vida cotidiana. El contenido del proyecto se basa en unos fundamentos teóricos, pero enfocados de manera práctica y fáciles de implementar mediante sencillas herramientas.

Por ello, con este trabajo se pretenden conseguir los siguientes objetivos:

- Adquirir unos conocimientos básicos a nivel de usuario referentes a la seguridad de ficheros y datos.
- Conocer la legislación vigente relativa a términos de seguridad y protección de datos.
- Realizar una aplicación práctica de los conocimientos adquiridos.

1.3 Estructura

Debido a la gran cantidad de información sobre el tema, se ha subdividido en tres epígrafes, así como unas conclusiones finales donde se exponen algunas ideas personales que se han ido adquiriendo durante la elaboración de este trabajo.

A. Teoría básica informática enfocada al tratamiento de datos.

   Trata de aspectos clave expuestos de manera más sencilla a sistemas más complejos.

   - Ficheros
     - Propiedades básicas de los ficheros.
     - Seguridad en ficheros.
   - Comunicaciones
     - Conexiones entre diferentes máquinas.
   - Aplicaciones
     - Partes de una aplicación informática.
     - Seguridad en los datos de una aplicación.
     - Seguridad entre las comunicaciones internas entre las diferentes partes de una aplicación.

B. Legislación vigente.
   - Ley LOPD.
   - Entidades de certificación y entidades certificadoras autorizadas.
   - Certificaciones de seguridad.

C. Casos prácticos.
   - Seguridad en una tienda online.
   - Sistema de Gestión de la Seguridad de la Información (SGSI) en una asesoría.
   - Tecnologías y herramientas básicas para mantener la seguridad del trabajador.

D. Conclusiones.

2. Teoría básica

2.1 Ficheros

Si hablamos de datos e informática en general, necesitamos hablar primero del sistema primitivo para guardar información, como son los ficheros.

Todo en informática son ficheros.

- Un programa o aplicación es un conjunto de ficheros puestos en común para realizar unas tareas definidas.
- Un sistema operativo es un conjunto de ficheros puestos en común que otorgan al usuario instrucciones que estandarizan la interacción con los dispositivos hardware.

  Los drivers o controladores son más ficheros que determinan la manera de interactuar entre el hardware o periférico especifico y el sistema operativo anfitrión.

Cabe destacar la diferencia entre ficheros de texto y ficheros binarios.

Los ficheros de tipo texto son editables fácilmente mediante el Bloc de Notas o Notepad++, pero existen ficheros llamados binarios que no se pueden editar y es necesario procesarlos en sus respectivos programas.

Por ello, es muy importante identificarlos para saber cuáles podemos editar fácilmente con Notepad++ y así, identificar errores y modificarlos fácilmente.

- **<u>Ficheros de texto</u>**:

  . txt, .csv, .xml, .json, .html, .css, .js
- **<u>Ficheros binarios</u>**:

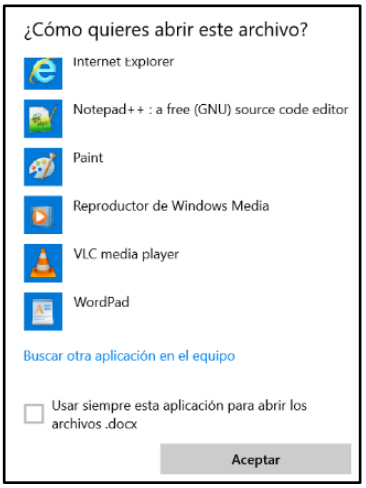
  .pdf, .zip, .doc, .xls, .avi, .jpg, .mp3, …

Ya hemos comentado que un sistema operativo se compone de ficheros. Por ejemplo, la única diferencia entre Windows y Linux es que Windows es un sistema operativo en base a ficheros y un registro *(un diccionario de claves y valores)* y Linux solo se compone o es en base solo a ficheros.

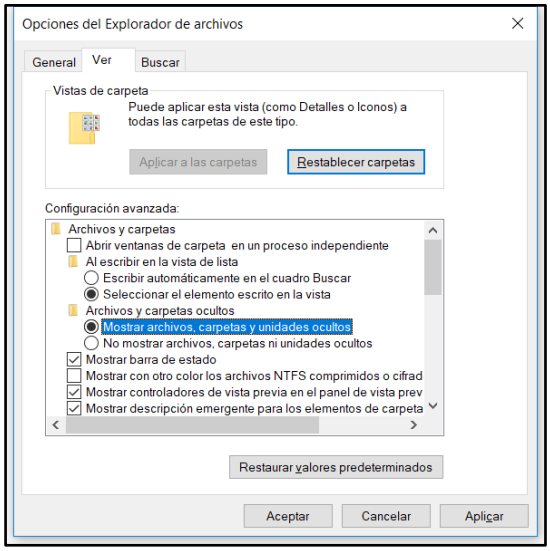
2.2 Seguridad en ficheros

Todos los ficheros de un sistema operativo disponen de una extensión de fichero, útil solo para determinar con que programa por defecto se abre ese fichero.

Por ejemplo, podemos establecer que todos los ficheros .txt se abran por defecto con el Bloc de Notas o Notepad++ o Word, pero siempre podremos editarlo con cualquiera de ellos.



Un fichero o directorio dispone de unas sencillas propiedades que no se definen con su extensión.



- Tipo de fichero:
  - Texto plano o Binario: Si se puede editar con un editor de texto.
  - Normal: Un fichero puede estar oculto o visible.
- Codificación del fichero: codificación utilizada para la representación de caracteres no pertenecientes al habla inglesa.
  - Muy importante para el correcto tratamiento de caracteres especiales, por ejemplo, ñ.
  - Se debe especificar la misma codificación en todas las aplicaciones, herramientas y sistemas operativos utilizados.
- Usuario propietario del fichero
- Permisos del fichero
- Metadatos
  - Fecha de creación.
  - Fecha de última modificación.

El cumplimiento de todas estas propiedades contribuye a una correcta política de seguridad en la empresa.

2.3 Diferencias entre Encriptación y Codificación

Estos términos son muy utilizados e importantes, ya que la seguridad en el tratamiento de la información y las comunicaciones se basa en ellos y, en ocasiones, se tiende a confundirlos.

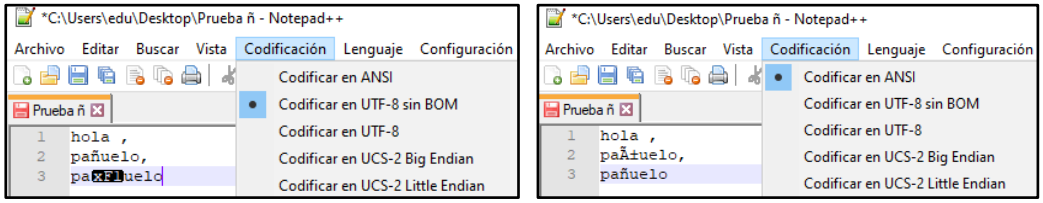
- Codificación: transformar o codificar los datos de unos caracteres o símbolos a otros usando para ello unos estándares de codificación.

  Un ejemplo, son los acentos del español. La codificación es necesaria para cualquier fichero que contenga algún carácter especial que no pertenezca al habla inglesa y, por lo tanto, necesita ser codificado internamente en el ordenador para que el procesador lo pueda tratar de manera correcta, ya que no entiende de acentos ni caracteres especiales.

  Si el fichero no contiene ningún acento, por ejemplo, un fichero de texto plano en inglés, no es necesaria ninguna codificación para ser procesado correctamente internamente en el ordenador.

  En comunicaciones en red entre ordenadores, es muy importante establecer la misma codificación tanto en emisor como en receptor porque si no aparecen errores como los llamados "caracteres extraños", fruto de una mala decodificación en el lugar del receptor al no usar la misma en ambos extremos.

  La siguiente imagen muestra, a través del programa Notepad ++ como codificamos un carácter especial como es el caso de la letra "ñ".



Fuente: Elaboración propia

  Existen muchos estándares de codificación, pero las más importantes son:

  - **UTF-8**: estándar o por defecto en muchos sistemas operativos.
  - **ISO-8859-1 (ANSI)**: codificación para países del Oeste de Europa.

- Encriptación: La encriptación o cifrado es un proceso para volver ilegible una información importante. La información una vez encriptada solo puede verse aplicándole una clave que previamente deben conocer tanto el emisor como el receptor de esa información. Normalmente se usan algoritmos complejos con

complicadas fórmulas matemáticas que usan como parámetro esa clave que debe ser conocida para recuperar la información.

- Sistema de autenticación mediante usuario/contraseña (simétrica): se utiliza un usuario y contraseña registrado en la aplicación. Esta contraseña, según la ley LOPD, se debe almacenar encriptada en base de datos. Nadie puede saber la contraseña, solo la puede resetear el usuario.
- Sistema de autenticación mediante clave privada/publica (asimétrica): Se crean dos ficheros (claves para encriptar/desencriptar la información). La clave publica es la que distribuyo y la privada es la que yo dispongo en mi ordenador y con la que cifro el contenido. Es decir, el propietario del fichero tiene la clave privada y distribuye una clave pública. Los certificados digitales de las páginas web seguras (https) contienen una clave publica con la cifrar el contenido que enviamos al servidor y que el solo pueda descifrarlo con la clave privada que el posee.

2.4 Comunicaciones

En todas comunicaciones en red entre equipos, siempre se dan en común 3 conceptos que son los 3 aspectos más importantes siempre a tener en cuenta:

- Protocolo de comunicación (como me lo mandas, por ejemplo "por correo").
  Un ordenador posee 65.000 puertos posibles de conexión por los que poder establecer una comunicación. Cada protocolo funciona por defecto por un puerto.
  - *SMTP - 25 (correo saliente), POP3 - 110 / IMAP - 143 (correo entrante)*
  - *HTTP - 80 (Web)*
  - *FTP - 21 (carpeta remota)*
  - *Servicios Web - 80 (Soap/Rest)*
  - *Oracle Base de Datos - 1521*
- Protocolo de intercambio de información (como nos entendemos, por ejemplo "texto plano, en Ingles").
  Mensaje o fichero que se manda entre en el emisor y el receptor.
  Mensajes que pueden estar encriptados y codificados.
  - Ficheros de Texto con una estructura determinada
  - Ficheros XML, JSON
  - CSV (fichero estructurado de datos)
  - Word, Excel

- Arquitectura (quien inicia el evento, por ejemplo "quien manda el correo y quien responde después"): cliente-servidor, Peer-to-Peer, ...

2.5 Aplicaciones

Las aplicaciones o programas son un **conjunto de ficheros puestos en común** para, mediante unos procedimientos, poder establecer e implementar las diferentes lógicas destinadas a cumplir las funcionalidades de esa aplicación. Cabe distinguir entre aplicaciones de Escritorio/Nativas o aplicaciones Web/Hibridas.

Aplicación Web: aplicaciones que son páginas web y que se ejecutan mediante el acceso a ellas a través de un navegador (Internet Explorer, Firefox, Chrome, …etc.).

Aplicación nativa o de escritorio: aplicaciones desarrolladas para un sistema operativo determinado en el que se va a ejecutar, accediendo a sus componentes hardware y recursos mediante una comunicación directa. (Windows, Linux, Android, IOS, …etc.).

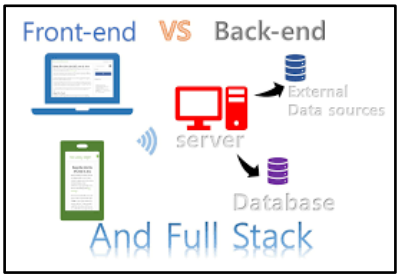
Aplicaciones Hibridas: páginas web que son encapsuladas en aplicaciones nativas, usando el mismo código desarrollado para la programación de la web para el desarrollo de una aplicación nativa.

Para ello, se desarrolla siempre usando estilos de diseño que permita una correcta visualización en todo tipo de dispositivos: teléfonos, tablets, ordenadores, tpv, etc. Diseño Responsive *(pensar para escritorio y adaptar para smartphone)* o Mobile First *(pensar para smartphone y adaptar para escritorio)*.
De esta manera, se consigue una **experiencia de usuario (UX)**, unificando interfaces de usuario entre dispositivos y reduciendo la curva de aprendizaje en el uso de la aplicación.

2.5.1 Partes de una aplicación

En todas las aplicaciones cabe distinguir tres tipos de entidades y entre ellas existen comunicaciones en las que interfiere la seguridad.

- Frontend: código ejecutado en el cliente (navegador o SO cliente). Es el encargado junto con el backend de la implementación de la lógica de la aplicación.



- Backend: código ejecutado en el servidor encargado de la comunicación entre la persistencia **(**base de datos**)** **y** el cliente **(**navegador**)**, así como de utilizar servicios de terceros *(Google maps, Google Analytics, etc.)*. Es el encargado junto con el frotend de la implementación de la lógica de la aplicación.
- Lógica de negocio: reglas de negocio destinadas a la implementación de las necesidades de la empresa. Lógica encargada de trabajar directamente con el modelo de los datos. La lógica más enfocada a la especialización del sector de cada empresa. Es muy importante concentrar toda esta lógica enfocada más a la empresa y abstraer esta de lo que es la lógica de aplicación (la manera de visualizar y trabajar con el usuario).

  Por eso, recientemente se suele implementar mucha lógica de negocio en las bases de datos. Mini Programas de Base de datos dentro de los propios programas, abstrayendo esas reglas de negocio propias de la empresa en la base de datos y permitiendo así usar diferentes Backends y Frontends con escasa lógica de negocio, permitiendo crear diferentes tipos de aplicaciones que se alimenten de estos mismos datos y programas de base de datos. Cada una con su lógica de aplicación, pero todas bajo una misma lógica de negocio.
- Lógica de aplicación: lógica encargada de interactuar con el usuario en las diferentes plataformas: móvil, ordenador…etc. Las vistas son las pantallas que se muestran al usuario y los controladores son los micro programas encargados de gestionar la interacción entre el modelo de datos y las pantallas o vistas para determinados usuarios autenticados y autorizados y dar así dinamismo a la aplicación.

2.5.2 Persistencia - Modelo

Se hace referencia a las bases de datos, pero puede ser cualquier cosa que almacene información como por ejemplo un simple fichero. De hecho, una base de datos se compone también de un conjunto

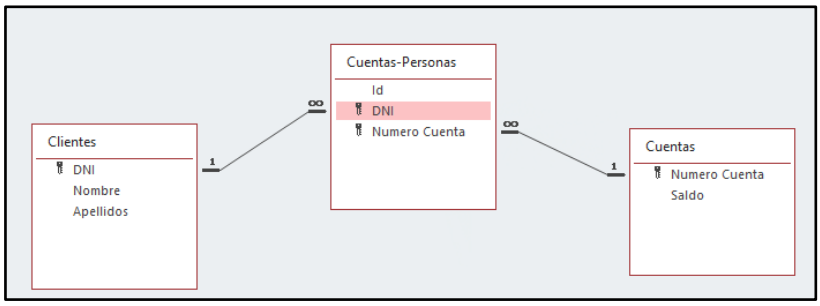
```
SELECT *
FROM nombre_tabla
WHERE condiciones búsqueda / filtros
GROUP BY agrupado por
```

de ficheros que son procesados de manera óptima y estándar mediante el lenguaje de consultas ***SQL***.

Se llama persistencia porque se almacena en el disco duro y la información no es volátil y no se borra. La diferencia entre información volátil y no volátil, es si se pierde esa información cuando se deja de alimentar con electricidad esa memoria (memoria RAM, mucho más rápida) o se mantiene (Disco Duro, más lenta).

Lo más importante de las bases de datos relacionales es lo que se denomina integridad de los datos o mantener la consistencia. En las bases de datos NoSQL no es imprescindible esa consistencia.

Se pone de ejemplo la implementación en una base de datos o en Access una relación de muchos a muchos entre clientes y cuentas bancarias.



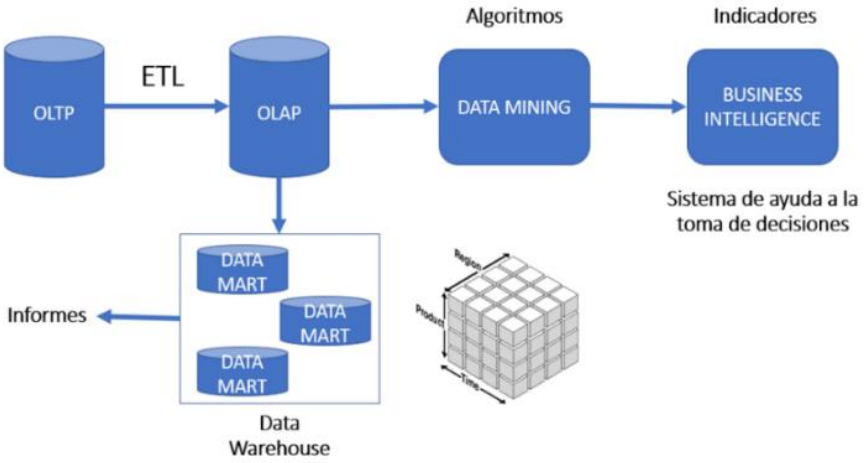
Fuente: Elaboración propia

Esta relación se implementa mediante una nueva tabla que permite establecer la relación entre ambas. La consistencia nos garantiza que esas referencias a las entidades siempre existen, nunca tendremos por ejemplo en esa nueva entidad "cuentas-personas" una referencia a la entidad cliente o la entidad cuenta que no exista.

Flujo de los datos

Cabe destacar como parte fundamental de la seguridad conocer muy bien el flujo que siguen los datos de una aplicación y algunos términos fundamentales que ayudan al correcto entendimiento de conceptos que parecen complejos como Cloud o Big Data, que lo son, pero no lo es su definición y el problema natural que soluciona.

Las tecnologías o programas surgen para solventar problemas que nos encontramos en la naturaleza. Si no se pueden explicar de manera natural cual es el problema que soluciona esa herramienta o tecnología es que no se ha entendido o esa tecnología no sirve para lo que realmente se está buscando.



- OLTP: Bases de datos transaccionales.
    - Son las bases de datos en las que trabajan los operarios cada día mediante el uso de la aplicación, realizando transacciones *(conjunto de instrucciones en una base de datos que se ejecutan todas de manera atómica correctamente o no se realiza ninguna)*.
    - Solo se almacena/mantiene el último dato valido. Si se modifica o borra se pierde, no tiene histórico.

- ETL (Extraction Transformation and Load): procesos de extracción, transformación y carga de los datos en otras tablas con un modelo de datos diferente. Son procesos que transforman datos para la adaptación a otro modelo de datos diferente.
- OLAP: bases de datos analíticas.
    - Estos esquemas OLAP o "en Estrella" no disponen de consistencia.
    - Las claves primarias son autonuméricas y se guarda histórico de cambios.
    - Se llaman Almacenes de datos o Data Warehouse.

    ➢ Cloud: el termino nube simplemente significa que no sé dónde está. Solo exploto el servicio que se me ofrece y me despreocupo donde está alojado físicamente ni soy responsable de esos servidores o CPD *(centro de procesamiento de datos)*.
        - SAAS: (software como servicio): Dropbox, Instagram, …
        - PAAS (plataforma como servicio): Sistema operativo como servicio donde poder establecer tus servidores/servicios.
        - IAAS (infraestructura como servicio): Amazon y todos sus servicios de computación en la nube.

- Big Data: almacenes de datos en la nube que son utilizados como fuentes de datos para nuestros procesos de minería de datos.
- Data Mining: algoritmos que ayudan a establecer relación entre los datos, usando como fuente de datos nuestro propio almacén de datos o usando una combinación con almacenes externos en la nube *(Big Data)*.
- Business Intelligence: indicadores o alertas sobre nuestros datos que nosotros establecemos ante los cuales se van a establecer acciones a tomar. Business Intelligence se define como un sistema de ayuda a la toma de decisiones, que permite realizar o programar acciones ante eventos producidos sobre nuestros datos o incluso establecer algún protocolo de aprendizaje automático que permita cierta autonomía o toma de decisiones automáticas.

  Se suele confundir este término y suele englobar a todos los procesos anteriores o llamar a los informes erróneamente Business Intelligence, siendo este solamente la parte final del proceso final del flujo de datos de una aplicación.

  Unos indicadores sobre una base fundamentados sobre unos malos informes no sirven de nada.

3. Legislación y Calidad en la Seguridad de la información.

En este apartado se van a tratar temas relacionados con la normativa y calidad en el ámbito de la seguridad de los datos:

- Legislación vigente y organismos públicos.
- Certificaciones que acreditan que se cumplen unos procedimientos que aseguren una calidad en el tratamiento de la información confidencial.

3.1 Reglamento General de Protección de Datos (RGPD) y Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)

La Ley Orgánica de Protección de Datos (LOPD) surgió en 1999 ante la necesidad de legislar la manera de almacenar la información personal por parte de las empresas y las entidades públicas en sus sistemas de información.

Esta ley establece procedimientos para todos los entornos, como los sistemas informatizados, el papel…etc., tanto para el sector privado como en el ámbito de la administración pública.

Periódicamente se va revisando y, recientemente, a fecha 5 de diciembre de 2018, entró en vigor la nueva Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) que adapta al entorno español el Reglamento General de Protección de Datos (RGPD) europeo que había entrado en funcionamiento el 25 de mayo de 2018.

PRINCIPALES NOVEDADES	
Sector Privado	**Sector Público**
Obligación de información a los ciudadanos sobre el tratamiento de sus datos y sobre el ejercicio de sus derechos.	Publicación del Registro de actividades de tratamiento del órgano u organismo del Sector Público.
Las bases jurídicas que legitiman el tratamiento de datos personales de los ciudadanos por parte de las organizaciones: no resulta necesario que el particular consienta el tratamiento de sus datos personales si existe otra base jurídica que legitime el tratamiento.	Obligación de información a los ciudadanos sobre el ejercicio de sus derechos.
Tratamiento de datos de menores de edad: la organización debe recabar el consentimiento del menor cuando este tenga al menos 14 años; y el de los padres o sus representantes legales en el caso de que sea menor de 14 años.	Potestad de verificación de los datos personales de los ciudadanos: sin necesidad de solicitar consentimiento del interesado.
Limitación de la actividad publicitaria: las "listas Robinson[1]": Las entidades que vayan a realizar una campaña publicitaria deben consultar con carácter previo las "listas Robinson" para evitar el envío de publicidad a todos los ciudadanos que se hayan registrado en ellas.	Nueva regulación de la aportación de documentación por parte de los ciudadanos: modificación del artículo 28 de la Ley 39/2015: eliminan la necesidad de recabar el consentimiento del ciudadano.
Datos de contacto profesionales: legitimación de su tratamiento. La Ley permite utilizar los datos personales de contacto de las personas que prestan servicios en una entidad.	Notificación de actos administrativos: identificación de los ciudadanos. La nueva Ley impide el uso conjunto apellidos, nombre y número completo del documento de identificación oficial.
Sistemas de denuncias internas: exención de responsabilidad penal de las organizaciones.	Comunicación de datos personales de los administrados a sujetos privados.
Inclusión en sistemas de información de solvencia crediticia ("ficheros de morosos").	Mayor transparencia de las sanciones impuestas al Sector Público.
Novedades sobre videovigilancia respecto a captación en vía pública, supresión de los datos y deber de información.	Tratamiento de datos personales en la notificación de incidentes de seguridad.

[1] Listas Robinson: servicio gratuito de exclusión publicitaria, a disposición de los consumidores, que tiene como objetivo disminuir la publicidad que éstos reciben.

Operaciones mercantiles: será lícito el tratamiento de datos que pudiera derivarse del desarrollo de cualquier operación.	Registros de personal del sector público: legitimación del tratamiento.
Derechos de los empleados: mayor intimidad.	Derechos de los empleados públicos: mayor intimidad.
La obligación de bloqueo de los datos personales tras el ejercicio de los derechos de rectificación o supresión.	Adaptación a la Ley Orgánica de los contratos de encargo de tratamiento de datos personales.
Tratamiento de datos personales en la notificación de incidentes de seguridad.	Tratamiento de datos personales por concesionarios de servicios públicos.
Adaptación a la Ley Orgánica de los contratos de encargo de tratamiento de datos personales.	Educación para la digitalización.
Tratamiento de datos personales en investigación sanitaria.	
Designación de un Delegado de Protección de Datos (DPD) y comunicación de la designación a la AEPD.	
Intervención del Delegado de Protección de Datos en la resolución de reclamaciones.	

Fuente: Elaboración propia según RGPD y LOPDGDD.

3.2 Ley de Servicios de la Sociedad de la Información (LSSI) y Comercio Electrónico

Establece la normativa que regula las actividades económicas a través de internet, entendiendo éstas como aquellos productos o servicios ofertados a través de páginas webs, tiendas online y correo electrónico. Quedan excluidos los productos o contenidos audiovisuales emitidos por internet.

Un aspecto importante de la ley es la obligación de indicar que se están utilizando cookies para almacenar información del usuario y la que debemos de aceptar su uso.

¿Quiénes están sujetos a esta ley?

Las personas que realicen actividades económicas por Internet u otros medios telemáticos (correo electrónico, televisión digital interactiva...), siempre que:

- La dirección y gestión de sus negocios esté centralizada en España o,

- Posea una sucursal, oficina o cualquier otro tipo establecimiento permanente situado en territorio español, desde el que se dirija la prestación de servicios de la sociedad de la información.

Por ejemplo, muchas casas de apuestas por internet que actúan en España como *Bwin, bet365*, etc., tienen ubicados sus servidores físicos en otros lugares como por ejemplo Gibraltar donde no se aplica esta ley.

3.3 Nueva normativa de doble autenticación

Desde septiembre de 2019 se ha producido un cambio en la forma de relacionarnos con nuestro banco a través de internet, es decir, el modo en que compramos online. La nueva ley europea de pagos digitales, conocida como PSD2, trata de mejorar y ajustar la forma en la que compramos y gestionamos nuestras cuentas en el mundo digital.

PSD2 es una regulación europea sobre servicios de pagos electrónicos. Su objetivo es aumentar la seguridad de los pagos en Europa, promover la innovación y favorecer la adaptación de los servicios bancarios a las nuevas tecnologías. Esta regulación ha entrado progresivamente en vigor entre el 13 de enero de 2018 y el 14 de septiembre de 2019, aunque todo comenzó en 2007, con la primera Directiva de Servicios de Pago (PSD: Payment Service Providers) con el objetivo de contribuir al desarrollo de un mercado único de pagos en la Unión Europea, fomentando la innovación y la competencia. En 2013, la Comisión Europea propuso una revisión (PSD2) que pretendía mejorar la protección del consumidor, impulsar la competencia e innovación del sector y reforzar la seguridad en el mercado de pagos, favoreciendo nuevos métodos de pago y el comercio electrónico.

Persigue reforzar la seguridad en los pagos a través de una doble autenticación, teniendo que cumplir con 2 de los 3 requisitos que exponemos a continuación:

- Algo que sabemos: es lo que venimos haciendo hasta ahora al introducir nuestro PIN o contraseña.
- Algo que tenemos: esto también se viene ya empleando, por ejemplo al pagar con tarjeta de crédito o el smartphone.

- Algo que somos: Aquí, la biometría (huella dactilar o facial, por ejemplo) va a ganar protagonismo e incluso la biometría del comportamiento, que será capaz de identificarnos solo con nuestra manera de teclear o navegar dentro de la app de nuestro banco.

3.4 Organismos Públicos

Esquema Nacional de Seguridad (ENS): Real Decreto 3/2010, de 8 de enero, por el que se regula todo lo relacionado en el ámbito de la Administración Electrónica Publica. Da cumplimiento a lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Su objeto es establecer las políticas de seguridad en la utilización de medios electrónicos públicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Tabla de organismos oficiales relacionados con la Seguridad en la Información:

Centro Criptológico Nacional (CCN)	Organismo responsable de garantizar la seguridad las Tecnologías de la Información y la Comunicación (TIC) en las diferentes entidades del Sector Público, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.
Capacidad de Respuesta a incidentes de Seguridad de la Información *(CCN-CERT)*	Contribuye a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.
Oficina Nacional de Seguridad *(ONS)*	Se crea, en 1983, como Órgano de trabajo del Secretario de Estado Director del CNI para cumplir con sus cometidos en relación a la protección de la información clasificada.

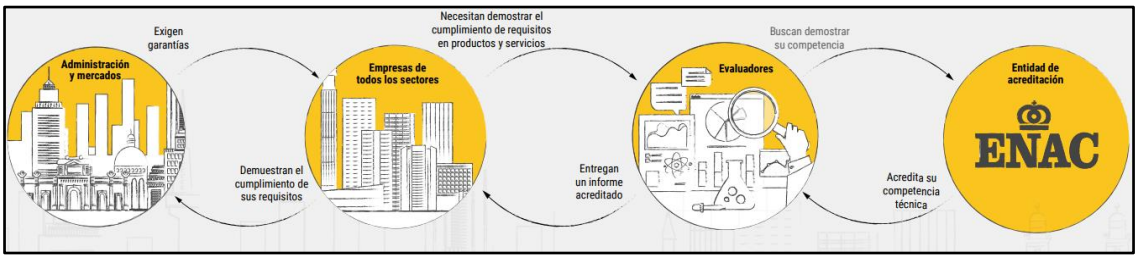
	La ONS tiene por misión fundamental la de velar por el cumplimiento de la Normativa relativa a la Protección de la Información Clasificada, tanto Nacional como aquella que es entregada a la Administración o a las Empresas en virtud de Tratados o Acuerdos internacionales suscritos por España (Artículo 4 f de la Ley 11/2002, de 6 de mayo, Reguladora del CNI).

Fuente: Elaboración propia

3.5 Entidades de Acreditación (ENAC) y Entidades Acreditadoras

A menudo, en nuestro día a día, realizamos acciones tan cotidianas como coger un ascensor, beber agua o realizar una transacción electrónica. Por ello, necesitamos tener la confianza suficiente de que todos estos actos cumplan una serie de medidas de seguridad.

Para lograr esa fe, los productos, servicios e instalaciones se someten a diferentes tipos de control, como son ensayos, inspecciones o certificaciones. La cadena de confianza es la que aporta las garantías necesarias en el mercado mediante sus diferentes agentes:



Fuente: ENAC

Explicación del flujo de la imagen:

1. El mercado y la Administración Pública exigen garantías de que los productos y servicios son fiables.
2. Por ello, las empresas necesitan asegurarse y demostrar que sus productos o servicios son seguros, fiables y cumplen con los requisitos reglamentarios que se establecen y, para ello, solicitan la realización de controles a un evaluador.
3. Los evaluadores, a través de certificados e informes que emiten a las empresas sobre la conformidad de los productos y servicios, deben demostrar su competencia técnica para la actividad que realizan. Algunos de estos evaluadores son AENOR O APP++
4. En España, La Entidad Nacional de Acreditación (ENAC) es el organismo independiente que evalúa, de forma rigurosa y conforme a normas internacionales, a los evaluadores, acreditando su competencia técnica para realizar su labor y

emitir informes y certificados fiables. ENAC es quien da la garantía y cierra la cadena de confianza.

Antes de explicar la principal actividad de una entidad certificadora, conviene definir primero que es una Certificación:

Certificación: es el proceso que lleva a cabo una entidad independiente, mediante el cual se manifiesta la conformidad de una determinada empresa, producto, servicio o persona con los requisitos definidos en normas o especificaciones técnicas. La certificación va dirigida a cualquier tipo de empresa y es un proceso voluntario.

Su tecnicismo hace referencia a la "evaluación de la conformidad" que es cualquier tipo de evaluación llevada a cabo para determinar si un producto o sistema cumple unos requisitos específicos.

Además de la certificación, existen otros tipos de evaluaciones que conceden la veracidad del cumplimiento de los requisitos como:

- Verificación: comprobación de la conformidad de los productos con arreglo a normas nacionales o su equivalente internacional.
- Inspección: acción dirigida a organizaciones que deseen asegurar que sus equipos, productos y servicios cumplen con la calidad, la seguridad y el medio ambiente.

Las entidades certificadoras o acreditadoras son las encargadas de realizar las gestiones y auditorías necesarias para determinar si se puede otorgar el certificado ISO correspondiente. Estas compañías que expiden los certificados ISO, deben estar debidamente acreditadas para el ejercicio de su labor. Son entidades totalmente imparciales e independientes.

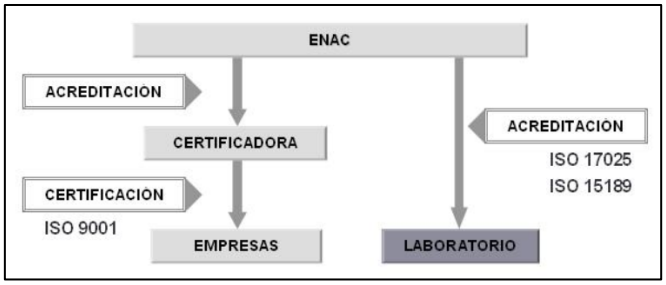
En este ámbito se va a hablar de la diferencia entre entidades de acreditación y entidades acreditadoras. Pero antes, vamos a definir el término acreditación, ya que es fundamental para poder comprender mejor la diferencia.

Acreditación: herramienta establecida a escala internacional para generar confianza sobre la correcta ejecución de determinadas actividades denominadas "Actividades de Evaluación de la Conformidad" y que incluyen ensayo, calibración, inspección, certificación o verificación, entre otras. Cualquier actividad que tenga por objeto evaluar

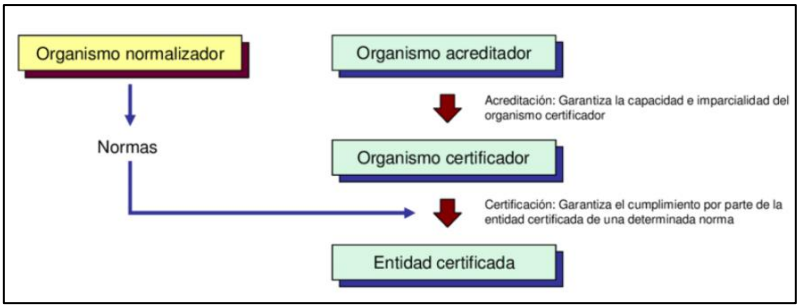
si un producto, servicio, sistema, instalación, etc., es conforme con ciertos requisitos puede estar sujeta a acreditación.

La Entidad Nacional de Acreditación (ENAC) es la entidad designada por el Gobierno, para operar en España como el único Organismo Nacional de Acreditación.

ENAC: es el organismo que establece y mantiene el sistema de acreditación nacional conforme a las normas internacionales; es decir, ENAC audita a las empresas certificadoras *(AENOR, APP+, ...)* para evaluar su competencia y asegurar que realizan las auditorías correctamente. Por lo tanto, si contratamos para nuestra auditoría de certificación a la empresa "Certificadora X" y no está acreditada, el sello emitido no está avalado por ENAC y puede ser considerado no válido por nuestros clientes o por la Administración Pública en la presentación a concursos.



Fuente: Norma ISO[2]



Fuente: ResearchGate[3]

Para saber si una certificadora se encuentra acreditada por ENAC podemos consultar su web: https://www.enac.es/web/enac/entidades-acreditadas

[2] Disponible en: *http://normaiso15189.blogspot.com/2011/01/acreditacion-vs-certificacion.html*

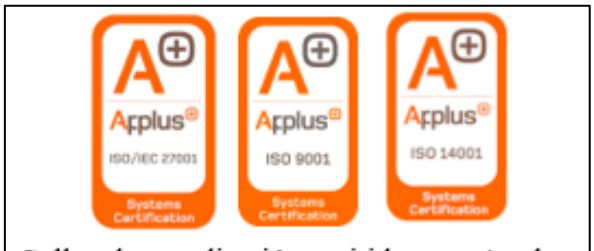
[3] Disponible en *https://www.researchgate.net/figure/Figura-1-Esquema-del-proceso-de-normalizacion-acreditacion-certificacion_fig1_268366009*

La Entidad Nacional de Acreditación (ENAC) pone a disposición de los interesados el esquema de acreditación de entidades que quieran certificar el cumplimiento con el Esquema Nacional de Seguridad (ENS). El esquema de acreditación ha sido desarrollado por ENAC en estrecha colaboración con el Ministerio de Hacienda y Función Pública (MINHAFP) y el Centro Criptológico Nacional (CCN).

AENOR: entidad privada sin fines lucrativos, cuya actividad contribuye a mejorar la calidad y competitividad de las empresas, generando un valor muy cotizado hoy en día en nuestra economía, como es la confianza. AENOR es la certificadora de referencia en España, por el rigor y la independencia que caracteriza su trabajo. Aporta a los productos, servicios y empresas un valor competitivo diferencial certificándolos, favoreciendo la cooperación internacional y las relaciones comerciales.

Sellos de acreditación emitidos por AENOR

Applus+: entidad privada líder mundial en el sector de la inspección, los ensayos y la certificación. Ofrecen una amplia cartera de soluciones que van desde la gestión de la seguridad de la información, gestión medioambiental, etc. En 1995 inició sus actividades como entidad de certificación de sistemas de gestión de la calidad, y en 1999 empezó su expansión en Latinoamérica. Ofrecen una amplia cartera de soluciones que van desde la gestión integral de activos hasta las inspecciones reglamentarias más habituales, que garantizan el cumplimiento de la normativa vigente.



Sellos de acreditación emitidos por Applus

3.6 Certificaciones de Seguridad de la Información

En este apartado se quiere repasar las normas que afectan a la Seguridad con los datos. Las normas ISO 9001 e ISO 27001, son las que más nos interesan puesto que proponen modelos de gestión de la calidad y seguridad de la información en las empresas y

organizaciones en un ámbito internacional. No se trata de normas que propongan límites cuantitativos, sino que más bien prescriben conductas o modelos de gestión cualitativos.
Certificado ISO: Conjunto de normas elaboradas por la Organización Internacional de Estandarización (ISO) con el propósito de ordenar la gestión dentro de las empresas en sus diferentes ámbitos y departamentos. Estas normas, de carácter voluntario, han logrado el reconocimiento de los consumidores y una aceptación internacional en el mundo empresarial. Gracias a este reconocimiento, las empresas certificadas en estas normas, consiguen un valor añadido frente a la competencia, además de una mejor gestión de sus recursos, repercutiendo en beneficios económicos para la empresa.

Tabla Comparativa de tipos de Certificaciones clasificadas por ámbito geográfico:

Asociación Española de Normalización (UNE: Una Norma Española)	Conjunto de normas, normas experimentales e informes (estándares) creados en los Comités Técnicos de Normalización (CTN) de la Asociación Española de Normalización. UNE es una entidad privada sin ánimo de lucro, reconocida legalmente en España como organismo nacional de normalización conforme a lo establecido en el Reglamento de la Infraestructura para la Calidad y la Seguridad Industrial (Real Decreto 2200/1995) y en el Reglamento (UE) 1025/2012 sobre Normalización Europea.
Normas Europeas (EN)	**Normas europeas (EN)** que se proponen, desarrollan y elaboran por expertos de los diferentes Estados Miembros, sectores industriales o tecnológicos implicados, reguladores, etc. dentro de la estructura de normalización del **Comité Europeo de Normalización (CEN)** y tras la oportuna tramitación son finalmente editadas como normas EN.
Normas UNE EN	Las **Normas UNE EN** son la **versión oficial en español de las normas europeas**, que son adoptadas tras la aprobación de un órgano específico dentro de la estructura de normalización nacional de AENOR. Las más conocidas en la actualidad son las normas **UNE EN ISO 9000** y **UNE EN ISO 14000** que, aunque son voluntarias se están imponiendo como requisitos fundamentales para competir con éxito debido a las demandas que está imponiendo la sociedad.
NORMAS ISO	Las Organización Internacional para la Estandarización o ISO *(International Organization for Standardization)* es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para distintos sectores industriales y comerciales. La ISO está formada por diversos institutos de normalización nacionales de 160 países, sobre la base de un instituto por país, coordinados desde una Secretaría Central. Las normas internacionales de este organismo se conocen como **normas ISO** y su finalidad es

	la **coordinación de las normas nacionales** con el objeto de facilitar el comercio, el intercambio de información y contribuir con normas comunes al desarrollo y a la transferencia de tecnologías. Las normas ISO son **voluntarias**, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país. La ISO ofrece un **catálogo** bastante extenso de normas que abarcan desde la clasificación de lenguas e idiomas (ISO 639), la gestión de la calidad (Familia de normas ISO 9000), la gestión medio-ambiental (Familia de normas ISO 14000) o la definición de un sistema de gestión de la seguridad de la información (ISO 27001).

Fuente: Elaboración propia

Tras hablar de certificaciones oficiales, vemos los mecanismos y procedimientos internos que tiene que realizar una empresa u organismo para llegar a conseguir una certificación.

Sistema de Gestión de la Seguridad de la Información (SGSI):

Conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta cualquier entidad. Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar documentalmente.

Se tienen que poder definir documentos de arquitectura que definan estos cuatro puntos que se indican.

- **Manual de seguridad**: documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.
- **Procedimientos**: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.
- **Instrucciones, checklists y formularios**: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Fuente: SGSI.

- **Registros**: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI. Están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos:

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

- Declaración de aplicabilidad: documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

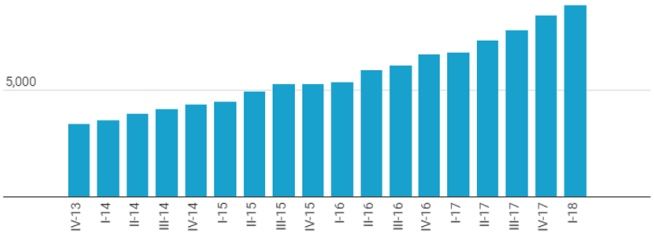
4.Casos prácticos de Seguridad en la Información

4.1 Caso práctico: Seguridad en una tienda online

En este apartado vamos a tratar de aplicar los conocimientos que hemos adquirido dentro del ámbito de la seguridad en una empresa. Para ello, vamos a conocer la normativa y las leyes básicas que regulan la seguridad en nuestras compras a través de internet. Para terminar, veremos su aplicación práctica en una web de comercio electrónico muy conocida como puede ser El Corte Inglés: *https://www.elcorteingles.es*.

El comercio electrónico es uno de los servicios que más ha crecido en los últimos años.

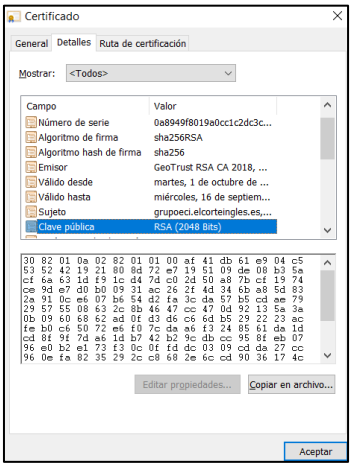
Evolución trimestral del volumen de negocio del comercio electrónico *(En millones de euros)*



Fuente: Business Insider[4]

Una cosa muy importante a la hora de realizar compras por internet es asegurarnos que estamos navegando un protocolo seguro (https) o el famoso candadito de las webs.

Secure Sockets Layer o capa de conexión segura (SSL) Estándar de seguridad global que permite la transferencia de datos cifrados entre un navegador y un servidor web. Se utiliza a fin de disminuir el riesgo de robo y manipulación de información confidencial (como números de tarjetas de crédito, nombres de usuario, contraseñas, correos electrónicos, etc.) por parte de hackers y ladrones de identidades. Básicamente, la capa SSL permite que dos partes tengan una "conversación" privada. Para establecer esta conexión segura, se instala en un servidor web un **certificado SSL (también llamado "certificado digital")** que cumple dos funciones:



[4]Business Insider. Disponible en: https://www.businessinsider.es/este-grafico-muestra-enorme-crecimiento-comercio-electronico-espana-ultimos-5-anos-311475

- Autenticar la identidad del sitio web, garantizando a los visitantes que no están en un sitio falso.
- Cifrar la información transmitida.

Cuando tratamos de acceder a una página web bajo "https" que no tiene un certificado de seguridad instalado (SSL) emitido por un emisor CA *(Entidad emisora de certificados de confianza)* válido, el navegador nos muestra un mensaje indicándonos que el sitio no es seguro e invitándonos a abandonar la página.

- Un sitio web bajo https que no tiene un certificado SSL emitido por un CA, aparecerá el siguiente mensaje:

- Si deseamos continuar, debemos hacer clic en el cuadro "Configuración avanzada", donde se desplegarán las opciones avanzadas. Aquí, haremos clic en "Acceder a sitio no seguro" para continuar navegando en la página web deseada.
- En este caso la información será encriptada, pero no se puede verificar que el origen es realmente quien dice ser. Para eso tiene que estar emitido el certificado por una CA valida.

Entidad emisora de certificados de confianza (CA)

Entidad de terceros fiable que emite certificados digitales que garantizan que la clave pública de una entidad pertenece realmente a dicha entidad.
Las funciones de una CA son:

- Al recibir una solicitud de un certificado digital, verificar la identidad del solicitante antes de crear, firmar y devolver el certificado personal.
- Proporcionar la clave pública propia de la CA en su certificado de CA.
- Publicar listas de certificados que ya no son fiables en la Lista de revocación de certificados (CRL). Para obtener más información, consulte "Trabajar con certificados revocados".

- Proporcionar acceso al estado de revocación del certificado utilizando un servidor de programa de respuesta.

Un ejemplo de entidad emisora de certificado de confianza (CA) es la Fábrica Nacional de Moneda y Timbre.

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM)

Prestador de Servicios de Certificación que pone a nuestra disposición diferentes tipos de certificados electrónicos mediante los cuales podemos identificarnos y realizar trámites de forma segura a través de Internet. https://www.sede.fnmt.gob.es/certificados

En función del destinatario de los mismos, la FNMT-RCM emite los siguientes tipos de certificados digitales que podemos solicitar a través de su SEDE Electrónica:

<table>
<tr><th colspan="2">Certificados de FNMT- RCM</th></tr>
<tr><td colspan="2">- Persona Física: se emite sin coste a cualquier ciudadano que esté en posesión de su DNI o NIE, es la certificación electrónica expedida por la FNMT-RCM que vincula a su Suscriptor con unos Datos de verificación de Firma y confirma su identidad personal.
Este certificado permite identificarse de forma telemática y firmar o cifrar documentos electrónicos.</td></tr>
<tr><td colspan="2">- Administración Pública: la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regula los sistemas de identificación de las Administraciones Públicas, así como los sistemas de firma electrónica del personal al servicio de las Administraciones Públicas y de sello electrónico para la actuación administrativa automatizada.</td></tr>
<tr><td colspan="2">- Certificados de Componente: certificados electrónicos para la identificación de servidores o aplicaciones informáticas heredando la confianza de la FNMT-RCM como Autoridad de Certificación. Dentro de esta categoría ponemos a su disposición certificados de servidor SSL, certificados de firma de código y certificados de sello de entidad.</td></tr>
<tr><td>Certificado de Representante</td><td>- Representante de Administrador Único o Solidario: certificación electrónica que vincula un firmante con unos datos de verificación de firma y confirma su identidad. El firmante actúa en representación de una persona jurídica en calidad de representante legal con su cargo de administrador único.
- Representante de Persona Jurídica: certificación electrónica que vincula un firmante a unos datos de verificación de firma y confirma su identidad. Por tanto, este certificado se expide a las personas jurídicas para su uso en sus relaciones con aquellas Administraciones públicas, entidades y organismos públicos, vinculados o dependientes de las mismas.</td></tr>
</table>

	- Representante de Entidad sin Personalidad Jurídica: certificación electrónica expedida a una entidad sin personalidad jurídica que vincula un firmante a unos datos de verificación de firma y confirma su identidad en los trámites tributarios.

Fuente: Elaboración propia según FNMT- RCM.

Consejos y buenas prácticas en compras online

A continuación, se pretende dar una serie de pautas y consejos a tener en cuenta para realizar compras de forma segura a través de internet.

Consejos para efectuar una compra online de forma segura:

- Realizar compras en páginas de confianza.
- Verificar que aparece identificado responsable de la tienda online y su ubicación.
- Comprobar que la tienda online es segura y proporciona toda la información necesaria sobre consumo y tratamiento de datos personales.
- Utilizar una tarjeta de uso exclusivo para realizar pagos online.
- Desconfiar de ofertas demasiado atractivas, ya que podría tratarse de fraude.
- Comprobar que nuestro dispositivo está configurado correctamente y la conexión a internet es segura antes de proporcionar nuestros datos personales o de pago.
- Elegir adecuadamente el medio de pago y no enviar dinero en efectivo para completar la compra que estemos efectuando.
- Tener en cuenta que un comercio con sello de confianza ofrece mayor garantía.
- En caso de renunciar a una compra o hacer uso de la garantía, tenemos que saber que no debe tener coste alguno.

Consejos ante posibles fraudes en las compras en sitios web:

- Comprar en páginas oficiales y/o de confianza o con reputación y prestigio.
- Sospechar de mensajes alarmistas o que llamen nuestra atención con el fin de que accedamos a un enlace o descarguemos un fichero adjunto.
- No responder a correos o mensajes donde soliciten nuestros datos personales.
- En caso de que se realicen compras fraudulentas con nuestra tarjeta, siempre debemos efectuar una denuncia y reclamar la devolución de los cargos efectuados. Además, es preciso anular las tarjetas en caso de pérdida o sustracción.

- Denunciar si existen razones de que el producto adquirido es una falsificación.
- Asegurarnos de que descargamos la app oficial, verificando quién es la entidad que figura como desarrollador de la aplicación, así como la política de privacidad y los permisos que solicita.
- Consultar los comentarios y valoraciones de los usuarios antes de instalar una app o comprar a través de ella.

4.2 Caso práctico: SGSI (gestión de la información) en una asesoría

En este apartado se pretende aplicar todos los conocimientos aprendidos a lo largo de este trabajo al caso de la seguridad de la información en una asesoría.

Dentro de una oficina encontramos multitud de documentación que requiere una especial atención, ya que la información que contiene es uno de los activos más importantes que poseen las asesorías. En caso de pérdida o sustracción podría ser utilizada con fines indeseados o con objeto de comercialización a todo tipo de sectores. Por ello, la mayor amenaza que sufren las oficinas y despachos es la pérdida de información, ya que el valor más preciado de este tipo de servicios es la confianza que depositan los clientes.

Hoy en día es cada vez más frecuente encontrarnos con amenazas online (botnets) que ponen en riesgo toda la información que tratamos en nuestro equipo de trabajo, lo cual obliga a tomar una serie de medidas de seguridad a la que todo profesional está obligado a cumplir. La protección frente a las ciberamenazas como virus, daños informáticos, ataques a páginas web, destrucción de información…etc. y la promoción de medidas de prevención son factores esenciales para evitar o minimizar las fugas de información y, con ello, la conservación de una buena imagen hacia los clientes.

4.2.1 Pérdida de información

En esta sección vamos a tratar de averiguar cuáles pueden ser los motivos y las causas de la fuga de información en una asesoría y de qué forma podemos prevenirlas.

Las amenazas que provocan la pérdida de información pueden tener origen interno y externo.

- Interno: son las ocasionadas por los empleados de la propia oficina, ya sea por desconocimiento, error o porque de forma voluntaria facilitan el acceso o revelan información confidencial a terceros sin autorización.
- Externo: son las que provienen de fuera de la empresa y tienen por objeto acceder de forma ilícita a información confidencial. Algunos ejemplos son los siguientes:

- El hackitivismo: terceros que quieren mostrar su desacuerdo con la actividad que realiza la asesoría.
- La venganza de clientes descontentos o de antiguos empleados.
- El robo de información confidencial: es el acceso no consentido a información privilegiada de clientes.
- El ataque de terceros que simplemente buscan el daño a la imagen de la asesoría.
- Otros cuyo objetivo es realizar actividades de competencia desleal.

Generalmente, el extravío de información se produce por ausencia o ineficiencia de algún tipo de medida de seguridad en la oficina. Las principales causas pueden agruparse en dos grupos: por un lado, causas organizativas y, por otro, causas técnicas

- Causas organizativas.

- Falta de clasificación: cuando se protege la información, suele someterse a diferentes tipos de clasificación en función del nivel de confidencialidad, del nivel de sensibilidad de la información o de si se trata de información personal o no. Por ello, si se desconoce el valor que posee la documentación dentro de la empresa, no será posible adoptar las medidas de protección adecuadas.
- Falta de delimitación del ámbito de difusión: determinar quién debe conocer la información y qué tipo de acciones puede realizar sobre esta, es lo que se conoce como principio del mínimo conocimiento.
- Falta de conocimiento y formación: la carencia de formación en materia de ciberseguridad por parte de los profesionales que integran el equipo de la oficina puede ocasionar pérdida de información.
- Ausencia de procedimientos: el establecimiento de políticas que indiquen al usuario cuáles son los límites dentro de los cuales deberá desempeñar su actividad, disminuirán el riesgo de que se produzca una fuga de información.
- Inexistencia de acuerdos de confidencialidad: es importante solicitar por escrito la conformidad de los empleados con normas internas de esta naturaleza.

- Causas técnicas.

Código malicioso o malware: es una de las principales amenazas, siendo el robo de información uno de sus objetivos más comunes. El malware está muchas veces diseñado

utilizando técnicas que permiten mantener oculto su código en un sistema, mientras recoge y envía información, lo que dificulta su localización.

- Acceso no autorizado a sistemas e infraestructuras: gran parte de estos accesos se podrían evitar si los sistemas estuvieran actualizados.
- Generalización del uso de servicios en la nube: este tipo de almacenamiento de información hace que percibamos que la información se encuentra segura cuando en realidad, la seguridad depende del grado de dureza de las contraseñas y del nivel de formación en ciberseguridad que posean los usuarios.
- Uso de las tecnologías móviles para el trabajo diario: a menudo, vinculamos a nuestros dispositivos información referente a nuestro trabajo. Por ello, se ha generalizado el uso de herramientas de cifrado de la información o el uso de VPN (redes privadas virtuales) en las comunicaciones.

En vista de que el factor humano es uno de los principales motivos de pérdida de información, es muy importante llevar a cabo campañas de concienciación en materia de ciberseguridad dentro de la oficina, sin perjuicio de que podamos hacerlas extensivas a terceros con los que mantengamos relaciones comerciales o profesionales, tales como proveedores, colaboradores u otro personal externo.

4.2.2 Consecuencias de la pérdida de información

Las consecuencias que pueden derivarse de un incidente de pérdida de información deben inquietar a cualquier empresa dentro del ámbito de la administración.

- Daños reputacionales: se genera un impacto muy negativo de la imagen de la oficina, lo que lleva aparejado la pérdida de confianza de clientes y proveedores.
- Consecuencias regulatorias: un incidente de esta naturaleza puede derivar en sanciones, tanto civiles, penales o administrativas.
- Consecuencias económicas: aquellas que suponen un impacto negativo a nivel económico, con una disminución de la inversión, negocio, etc.

Las consecuencias de una fuga de información no dependen tanto del tamaño de la empresa, sino del grado de importancia que tenga la información. Por ello, vamos a diferenciar el tipo de información que puede manejar una oficina:

- Información confidencial o restringida: aquella que consideremos crítica para los procesos de nuestra entidad. Por ejemplo: datos de nuestros clientes y de los

procedimientos que les afecten, contabilidad de la propia empresa, datos de los trabajadores, etc.

- Información no confidencial: aquella cuya revelación y divulgación impactaría en la imagen de la empresa, pero el peso del impacto económico será menor.

En base a estos factores podemos tener una aproximación que nos ayude a determinar las posibles consecuencias de un incidente. A partir de ahí, adoptaremos las medidas técnicas u organizativas adecuadas para remediarlo.

4.2.3 Gestión de la pérdida de información

El plan para la gestión de los incidentes de fuga de información que se propone a continuación recoge los principales puntos a tener en cuenta por parte de una asesoría que quiera reforzar su capacidad de prevención y reacción ante un incidente de estas características.

- Fase inicial o detección temprana del incidente

Una rápida y adecuada gestión en las primeras fases puede suponer una eficaz reducción del impacto del incidente y una minimización de sus efectos. Excepto en el caso de pérdida de dispositivos o terminales, la propia naturaleza del incidente hace que en la mayoría de las ocasiones no sea detectado hasta que la información se filtra, haciéndose pública a través de Internet o de cualquier otro medio.

En el momento que hayamos tenido conocimiento del incidente, debemos informar internamente de la situación, activando el protocolo de actuación que tengamos diseñado en nuestra organización para la gestión de estos casos.

Finalmente debemos recordar que, si la fuga de información conlleva datos personales, el Reglamento General de Protección de Datos recoge que el responsable del tratamiento tiene la obligación de notificar la violación de seguridad a la Agencia Española de Protección de Datos en las 72 horas siguientes a haber tenido conocimiento de que se ha producido la misma. Además, deberá notificar al interesado si ésta entraña un alto riesgo para sus derechos y libertades. De aquí la importancia de activar rápidamente el protocolo interno de gestión del incidente.

- Fase de lanzamiento

Cuando se activa el protocolo interno de gestión del incidente, el primer paso es el de convocar a los miembros del gabinete de crisis, aunque no todas las empresas cuentan

con un gabinete de crisis o tienen los recursos necesarios. Mantener la calma y actuar organizadamente es fundamental para evitar decisiones incorrectas.

- Fase de auditoría

Una vez se han iniciado los pasos anteriores, daría comienzo la fase de obtención de información sobre el incidente. Para ello, será necesario iniciar una auditoría interna, con el objetivo de determinar con exactitud y en el menor tiempo posible lo siguiente:

- Determinar la cantidad de información que ha podido ser sustraída.
- Establecer el tipo de datos que contiene la información que ha podido ser sustraída. Debe prestarse especial atención si se han filtrado datos de carácter personal y de qué nivel, ya que esto podrá accionar una serie de actuaciones específicas, de conformidad con la normativa sobre protección de datos.
- Determinar si la información pertenece a la propia organización o es externa.
- Establecer la causa principal de la filtración, en el sentido de determinar si tiene un origen técnico o humano. Si el origen es técnico, hay que identificar los sistemas que están afectados o se ha producido la brecha. Si es de origen humano, deberá iniciarse el proceso para identificar cómo y cuándo se ha producido la fuga y quiénes han sido los responsables.

Además de la auditoría interna, también es necesario realizar una auditoría externa. El objetivo de ésta será conocer el tamaño, gravedad y nivel de difusión de la filtración en el exterior de la organización.

- Fase de evaluación

Con la información recopilada se podrá iniciar el proceso de valoración del incidente, así como sus posibles consecuencias e impacto. Para ello es recomendable establecer las tareas a emprender para evitar nuevas pérdidas de información, así como una planificación detallada para cada una de ellas. Se debe considerar que al tratarse de una evaluación inicial las tareas se diseñan en función de la información disponible y puede ser incompleta. Algunas de las tareas a llevar a cabo en esta fase son las siguientes:

- Actuaciones para cortar la filtración y evitar nuevas fugas de información.
- Tareas de revisión de la difusión de la información, en especial si ésta contiene datos de carácter personal o se trata de información confidencial.
- Tareas para atenuar las consecuencias legales: posibles incumplimientos de normativa en materia de protección de datos de carácter personal o de otra

normativa. También aquellas tareas encaminadas a la preparación de toda la información necesaria ante posibles denuncias por los afectados, otras organizaciones, etc.

- Tareas para la determinación de las consecuencias económicas, que puedan afectar a la organización.
- Tareas a acometer en los activos de la organización afectados.

Este conjunto básico de acciones compondrá el plan de emergencia diseñado para el incidente de fuga de información. Su ejecución deberá de estar completamente coordinada y supervisada en todo momento por el gabinete de crisis.

- Fase de mitigación

Esta fase se centra en tratar de reducir la brecha de seguridad y evitar que se produzcan nuevas fugas de información. Por este motivo, en algunos casos puede ser necesario desconectar un determinado terminal, servicio o sistema de Internet. Ante esta situación, la prioridad es resolver la fuga de información en el menor tiempo posible. Más adelante se aplicarán medidas más adecuadas o menos drásticas que la desconexión, pero siempre garantizando la seguridad.

El siguiente paso se centrará en minimizar la difusión de la información sustraída, en especial si se encuentra publicada en Internet. Por este motivo, se contactará con los sitios que han publicado información, con los motores de búsqueda y se solicitará su retirada, en especial si se trata de información sensible o protegida por el secreto profesional o la LOPD.

En caso de existir personas afectadas por la fuga de información, por ejemplo, si se han filtrado datos personales de terceros, como de clientes de la asesoría, deberá seguirse el procedimiento de notificación y comunicación que contempla el Reglamento General de Protección de Datos, así como seguir las indicaciones y protocolos que establezca el organismo de control español, en este caso la Agencia Española de Protección de Datos.

- Fase de seguimiento

Una vez completadas las principales acciones del plan, se procederá a evaluar el resultado y la efectividad de las acciones realizadas, en relación con las consecuencias y su impacto. Además, en caso de ser necesario, se deberá hacer frente a otros aspectos que hayan podido generarse durante la fase de mitigación del incidente, como puedan ser consecuencias legales, económicas, reputacionales y similares.

Así mismo, se comenzará con un proceso de valoración global del mismo, que supondrá una auditoría más completa a partir de la cual se puedan diseñar e implantar medidas definitivas para evitar nuevas fugas y restablecer el normal funcionamiento de los servicios.

4.3 Tecnologías, herramientas y buenas prácticas

Este apartado trata de exponer una serie de herramientas y buenas prácticas para cualquier trabajador cuya ocupación diaria esté relacionada con datos.

4.3.1 Keepass

Se trata de una herramienta que permite centralizar todas nuestras contraseñas de manera segura mediante una contraseña maestra.

Esta herramienta quizás sea la más importante a comentar, ya que son muchos los usuarios y contraseñas diferentes que tenemos para acceder a los diferentes sistemas de información, correo, páginas web, etc. en nuestra vida diaria. Este sencillo programa nos ayuda a ser ordenados y seguros con este tema tan importante a la hora de trabajar con sistemas de información. https://keepass.info

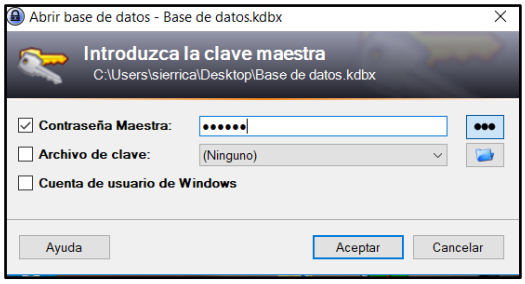


Figura 1. Entrada al programa mediante la clave maestra

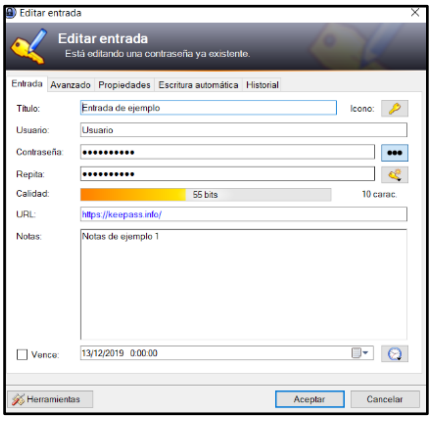


Figura 2. Vista de todas las contraseñas guardadas en el programa

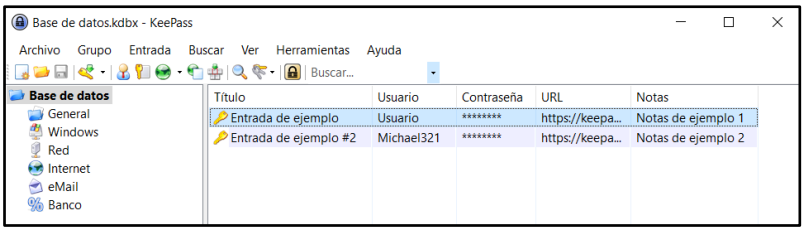


Figura 3. Vista interna de una de las contraseñas guardadas

4.3.2 Notepad++

Se trata de un procesador de textos avanzado. Existen otros que tal vez sean más complejos, pero Notepad++ es la herramienta que dispone de una interfaz gráfica y una experiencia de usuario más adecuada para enseñar a trabajar a personas no técnicas. Además, dispone de una gran cantidad de funcionalidades que lo dotan de una excelente herramienta para trabajar con cualquier fichero de texto (.txt, .xml, .html, ...).

- Permite fácilmente verificar y cambiar la codificación de los ficheros.
- Permite comparar el contenido entre 2 ficheros de texto.
- Permite una búsqueda avanzada de texto.
- Dispone de colores que ayudan a la comprensión.

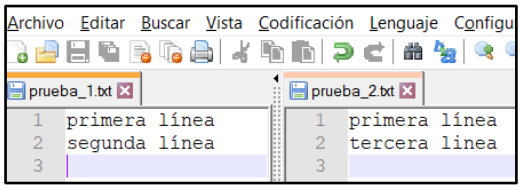


Figura 4. Vista de dos ficheros abiertos en el programa

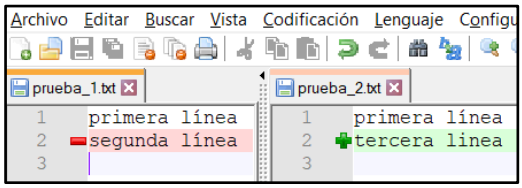


Figura 5. Comparación entre ficheros

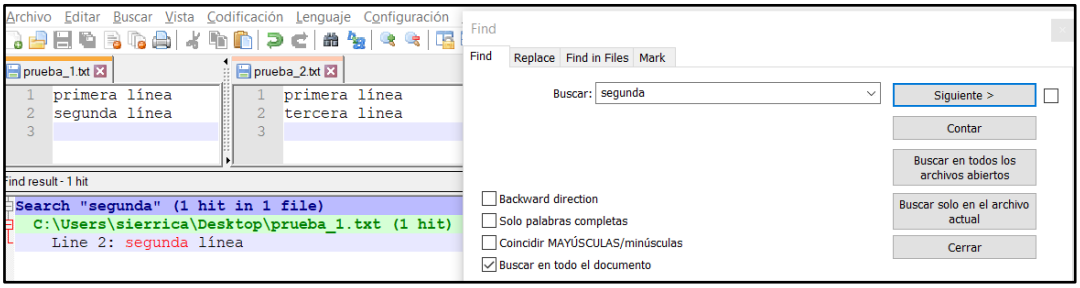


Figura 6. Vista del buscador e indicador de donde encuentra la palabra que buscamos

5. Conclusiones

En la actualidad, vivimos en un mundo globalizado en el que, de manera continua, se producen cambios relacionados con el avance de la informática y las comunicaciones. Por ello, es necesario que todos avancemos a medida que llegan más innovaciones a nuestro día a día.

Las empresas tienen la obligación de tomar las medidas necesarias conforme la tecnología va evolucionando y, todo esto llevado al terreno de la seguridad de la información, implica que cualquier negocio tiene el deber de aplicar una serie de medidas de seguridad y de concienciar a todos sus trabajadores para que se lleven a cabo las políticas adoptadas en materia de seguridad en la empresa.

Llegados a este punto, vamos a extraer una serie de conclusiones acerca de la información y su estrecha relación con la seguridad.

- Todo en informática se basa en ficheros (programas, bases de datos, etc.), por lo que resulta fundamental que cualquier usuario tenga unos conocimientos básicos.
- La seguridad por parte de los trabajadores a la hora de manejar ficheros y comunicaciones son muy importantes. No solo son necesarias unas buenas medidas de protección sino unos procedimientos definidos para todo tipo de actuaciones o incidentes que puedan producirse. Así mismo, las empresas deberían destinar parte de su capital a formar a sus empleados en materia de seguridad.
- Las leyes son muy actuales y sufren cambios continuamente. Ello repercute en que las empresas estén destinando grandes recursos para el cumplimiento de la normativa vigente.

Por todo esto, en la actualidad, es muy importante que las empresas elaboren un buen Sistema de Gestión de la Seguridad de la Información (SGSI), ya que es un buen mecanismo para proteger el negocio ante riesgos de seguridad y ayuda a minorar costes imprevistos.

En consecuencia, vuelvo a reafirmarme en la frase con la que comenzaba este trabajo, y es que "*Los sistemas de hoy en día son muy seguros, pero las personas seguimos siendo muy vulnerables"*.

6. Bibliografía

Seguridad de la información. Redes, informática y sistemas de información. Areitio Bertolin, Javier. Ed. Ediciones Paraninfo, S.A., 2008.

Enciclopedia de la Seguridad Informática. Gómez Vieltes, Álvaro. Ed. Alfaomega, 2017.

Seguridad Informática. Roa Buendía, José Fabián. Ed. Mc Graw Hill Education, 2013. Disponible en: https://www.academia.edu/8358689/Seguridad_Informatica_Mc_Graw-Hill_2013_-_www_Free_Libros_me_-_copia

Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. Luis Antonio Gómez Fernández / Pedro Pablo Fernández Rivero. Ed. AENOR INTERNACIONAL, S.A.U., 2018.

Agencia Española de Protección de Datos, Guías. Disponible en: https://www.aepd.es/es/guias-y-herramientas/guias

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de Boletín Oficial del Estado. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales – Nuevas obligaciones para el sector público. Disponible en: https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-sector-publico.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales – Novedades para el sector privado. Disponible en: https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-sector-privado.pdf

Compra segura en internet. Guía práctica, de Gobierno de España. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-compra-segura-digital-web.pdf

Compra segura en internet. Fichas prácticas, de Gobierno de España. Disponible en: http://www.aecosan.msssi.gob.es/AECOSAN/docs/documentos/para_consumidor/FICHAS_COMPRA_SEGURA_INTERNET_WEB.pdf

Entidad Nacional de Acreditación, ENAC. Disponible en: https://www.enac.es/documents/7020/15699/folleto-institucional-2019-web.pdf/708e945e-42ca-4c7a-83e0-e8154cfbfa43

Esquema Nacional de Seguridad (ENS) – Gobierno de España. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html#.Xg3MV0dKjIU

Centro Criptológico Nacional (CCN), guías e informes sobre ciberseguridad. Disponible en: https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es

Reglamento (UE) 2016/679 del Parlamento Europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf