Introducción a la Seguridad Informática.

Caso Práctico

Diego Méndez (Uso educativo nc)

Juan acaba de recibir una llamada. Era el responsable de recursos humanos de una empresa para ofrecerle un contrato durante un año como becario.

Su función, junto con la ayuda de otra persona de la empresa, que será su tutor durante la beca, es la de gestionar todo lo relacionado con seguridad en la empresa.

Juan está ilusionado con su nuevo trabajo, pero es consciente que la seguridad informática es un tema hasta ahora desconocido para él y a pesar de ser un contrato para una beca, este hecho le inquieta.

Dado que Juan es un chico previsor, ha decidido ponerse a investigar un poco sobre los conceptos básicos de seguridad informática. Quiere prepararse antes de tener la primera entrevista con su tutor. De esta forma, no será tan evidente que no tiene ni idea del tema.

Quiere, al menos, adquirir unas nociones para entender lo que le va a explicar.

A lo largo de esta unidad, daremos una serie de pinceladas a modo de introducción, sobre las diversas partes que abarca la seguridad informática.

David Goehring (CC BY)

Como sabes, el crecimiento de Internet en los últimos años ha convertido los ordenadores y las redes en algo a lo que cada vez se le da un uso más cotidiano. Precisamente, este aumento de ordenadores conectados entre si a través de Internet, supone también un incremento de peligrosidad ante ataques, propagación de virus y demás amenazas que pueden comprometer los sistemas de información.

A lo largo de esta unidad veremos los conceptos básicos de seguridad informática. Muchos de ellos te servirán como punto de partida para profundizar en unidades posteriores.

Además de comprender ciertos conceptos, esta unidad te ayudará a reflexionar sobre la necesidad de la seguridad en el ámbito informático y las consecuencias que puede acarrear el descuidar este aspecto.

Citas para pensar

Gene Spafford, experto en seguridad: "El único sistema verdaderamente seguro, es aquél que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados… y aún así tengo mis dudas."

Debes conocer

En el siguiente enlace dispones de una presentación sobre los contenidos fundamentales que se tratarán a lo largo de todo el tema. Es interesante que veas esta presentación para hacerte una idea de lo que vas a aprender en la presente unidad:

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Resumen

Clasificación de seguridad

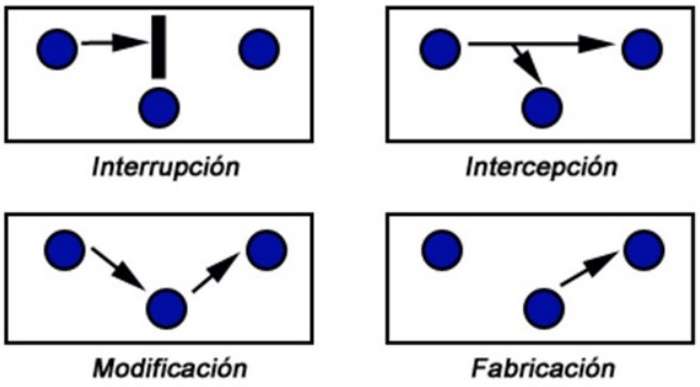
- Seguridad física (control de acceso, seguridad hardware, etc.)
- Seguridad lógica (contraseñas, antimalware, etc.)

- Seguridad activa (cortafuegos, antivirus, etc.)
- Seguridad pasiva (copias de seguridad, imágenes de respaldo, etc.)

Objetivos de seguridad

Vulnerabilidades, amenazas y ataques

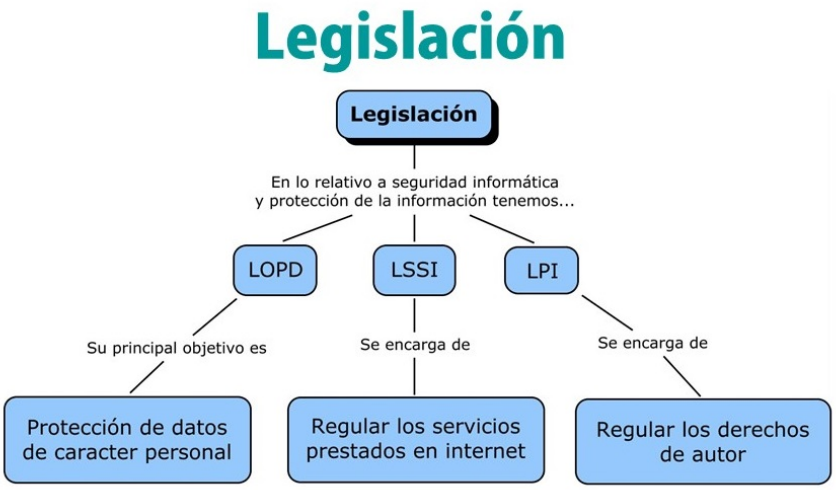
Tipos de ataque



Gestión de riesgos

- Proceso de estimación de riesgos.

- Auditorías.
- Políticas de seguridad.
- Plan de contingencias.



Descripción textual de la presentación

1.- Introducción a la Seguridad Informática.

Caso Práctico

Santiago Lopez Pina (CC BY-NC-SA)

En su proceso de investigación, Juan comienza planteándose directamente lo que es la seguridad informática y se pone a buscar en Internet información sobre el tema. El problema, es que la mayoría de los sitios que encuentra tienen información demasiado técnica y no saca demasiado en claro.

Un buen día, Juan se encuentra a Adrián, un amigo suyo que se las da de entendido en informática y éste le dice que sabe mucho del tema:

- Nada Juan, tú tranquilo que yo controlo mucho de seguridad. He trabajado en temas de vigilancia urbana y en informática será algo parecido.

- ¿En serio que hay relación?

- ¡Claro! ¿Sabes lo que es un antivirus?

- Mmmm… sí…-afirmó Juan dudando-

-Pues instalas uno en el ordenador y problema resuelto, ya te enseñaré yo, no te preocupes.

Juan agradece a su amigo su disposición para ayudarle, pero no se queda nada convencido y decide investigar un poco más sobre el tema. Pronto se da cuenta de que el término es mucho más amplio de lo que pensaba Adrián.

A lo largo de este epígrafe veremos a modo de introducción en qué consiste la seguridad informática. Comenzaremos reflexionando sobre el término de seguridad en su más amplio sentido. La RAE define seguro como:

> **“Libre y exento de todo peligro, daño o riesgo.”**

Por tanto, si trasladamos el término al ámbito informático, nos podemos referir a seguridad informática como:

“Disciplina que se encarga de proveer a los sistemas informáticos de una serie de elementos (normas, métodos, procedimientos) para conseguir que estos sean más fiables.”

La seguridad absoluta es imposible, por eso hablaremos siempre de fiabilidad.

Reflexiona

Se suele decir que la seguridad informática es un camino y no un destino. Con esta afirmación nos referimos a que, como hemos dicho, la seguridad informática consiste en una serie de medidas que debemos tomar a lo largo del tiempo buscando alcanzar la máxima fiabilidad. Pero este conjunto de medidas tendrán que mantenerse y actualizarse de forma adecuada a lo largo del tiempo.

2.- Clasificación de Seguridad.

Caso Práctico

Desde que Juan se puso a investigar sobre seguridad, ha tomado una serie de medidas en base a lo que ha ido aprendiendo: ha instalado un antivirus, ha revisado sus contraseñas comprobando que sean seguras y otra serie de medidas relacionadas con el software.

Víctor Jiménez (CC BY-NC-SA)

Lo que Juan no ha tenido en cuenta es que, en seguridad también debemos tener en cuenta muchos otros aspectos. Durante un fin de semana que ha estado de viaje una fuga en una tubería ha inundado el baño que está junto a su habitación. Como consecuencia, el equipo que estaba en el suelo, se ha visto afectado.

El equipo contenía información muy importante y además, los componentes eran de gran calidad y le habían costado bastante dinero. Nada más llegar a casa se ha apresurado en secar el equipo y comprobar si el agua había entrado hasta el interior de la caja.

Finalmente, el agua no había llegado a ningún componente crítico y no ha pasado nada, pero el susto ha hecho a Juan reflexionar sobre los diferentes elementos a tener en cuenta en la seguridad.

- Bueno, ya tengo una anécdota que contar sobre la seguridad...
- Me pregunto como sería el desastre si esto le pasa a una empresa y yo soy el responsable de seguridad. Bueno, mejor no pensarlo porque me pongo malo.

Una vez visto el concepto de seguridad, vamos a hacer una clasificación de la misma. Es importante proteger nuestro sistema con antivirus y elementos de software. Sin embargo, no hay que olvidarse de que la seguridad también consiste en una serie de medidas asociadas a elementos físicos. Por otro lado, al hablar de seguridad se tiende a pensar en mecanismos de prevención ante posibles daños, dejando de lado aquellos mecanismos que podemos emplear para minimizar los daños una vez que han ocurrido.

Cuando hablamos de seguridad informática, frecuentemente se tiende a pensar en seguridad en el software. Si bien este tipo de seguridad es importante, no debemos olvidarnos de que la seguridad informática también consiste en una serie de medidas asociadas a elementos físicos. Además, podrás comprobar que la clasificación de la seguridad también puede ir en función del momento en que los mecanismos entran en funcionamiento. De forma análoga a lo que mencionábamos anteriormente, un error común es referirse de forma exclusiva a mecanismos que actúan antes de que se produzca una catástrofe, olvidando los que se ocupan de minimizar los daños una vez

ésta ocurre.

A continuación profundizaremos un poco más sobre estos conceptos y veremos algunos ejemplos.

2.1.- Seguridad Activa y Pasiva.

Si bien se podrían establecer multitud de clasificaciones dependiendo de una serie de criterios, a continuación vamos a realizar una clasificación de la seguridad atendiendo al momento en que se ponen en marcha dichas medidas de seguridad.

Teniendo esto en cuenta, distinguimos entre:

- **Seguridad activa**: bajo esta clasificación agrupamos el conjunto de medidas que se toman para prevenir o minimizar los riesgos.
- **Seguridad pasiva**: en este caso, las medidas se enfocan a minimizar los daños una vez ha ocurrido la catástrofe.

Clasificación de diferentes técnicas de seguridad activa y pasiva

Tipo de medida	Ejemplos de medidas de seguridad
Seguridad activa.	Utilización de contraseñas. Cifrado de la información. Instalación de antivirus. Sistema de detección de incendios.
Seguridad pasiva.	Realización de copias de seguridad. Conjunto de discos redundantes. Disponer de extintores.

Ejercicio Resuelto

Los conceptos de seguridad activa y pasiva son muy utilizados en el ámbito de la seguridad automovilística. Teniendo en cuenta lo que ya sabes, ¿sabrías poner un ejemplo de mecanismos de seguridad activa y pasiva en un coche?

Mostrar retroalimentación

La iluminación, el sistema de frenado, los neumáticos, etc, serían elementos que aportarían seguridad activa. Es decir, son mecanismos de prevención.

En cuanto a la seguridad pasiva, existen elementos como los cinturones de seguridad o los airbag cuyo cometido es minimizar las consecuencias una vez hemos tenido un accidente.

Estos conceptos son análogos a los de seguridad activa y pasiva en un contexto informático.

Autoevaluación

Después de un incendio en el departamento de una empresa se queman varios equipos. Se pone en marcha un plan para restaurar las copias de seguridad que se habían realizado con anterioridad. Dichas copias, son una medida de seguridad…

- ○ Ocasional.
- ○ Activa.
- ○ Pasiva.
- ○ Permisiva.

No es correcto, las medidas son activas o pasivas.

Incorrecta, activa sería para prevenir los daños y en este caso ya se han producido.

Muy bien, has captado la idea…

No es la opción correcta, las medidas son activas o pasivas.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.2.- Seguridad Física y Lógica.

Como hemos dicho, la clasificación de la seguridad puede atender a diversos criterios. Vamos a ver otra clasificación, en este caso, dependiendo del tipo de recurso a proteger.

- **Seguridad física**: entendemos seguridad física como el conjunto de medidas que se toman para proteger el hardware, las instalaciones y su acceso y demás elementos físicos del sistema. Un fallo común, es olvidarse de este tipo de seguridad centrándose únicamente en la seguridad lógica.
- **Seguridad lógica**: complementa a la seguridad física y se encarga de proteger los elementos lógicos del sistema como son el software y la información mediante herramientas como antivirus, contraseñas, etc.

Peggy_Marco (Licencia de pixabay)

Clasificación de diferentes técnicas de seguridad física y lógica.

Tipo de medida	Ejemplos de medidas de seguridad
Seguridad física.	Mobiliario ignífugo. Control de acceso a las instalaciones. Sistemas de alimentación ininterrumpida. Detectores de humo y extintores.
Seguridad lógica.	Uso de antivirus. Cifrado de información. Cortafuegos mediante software. Filtrado de direcciones MAC (acrónimo de Media Access Control) en conexiones inalámbricas.

Autoevaluación

Teniendo en cuenta las dos clasificaciones que has visto de seguridad informática, en el caso de un antivirus ¿a qué tipos de seguridad corresponde?

- ☐ Física.
- ☐ Lógica.
- ☐ Activa.

☐ Pasiva.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Correcto
3. Correcto
4. Incorrecto

3.- Objetivos de la Seguridad Informática.

Caso Práctico

Diego Méndez (Uso educativo nc)

Por fin llega el primer día de Juan en la empresa. Le recibe, Ignacio, su tutor, con el que tendrá una pequeña entrevista.

- Hola Juan, buenos días.- Buenos días.[…]- Bueno, como sabrás, la seguridad consiste en mucho más que instalar un antivirus.- Juan asiente con la cabeza alegrándose de haber investigado previamente por su cuenta.-- En nuestra empresa es fundamental mantener la integridad, disponibilidad y confidencialidad de los datos. Aunque no vas a ser la única persona encargada de ello, será en gran parte tu responsabilidad en la empresa.

Después de hablar un poco sobre el tema, Ignacio le propone a Juan una pequeña actividad.

- Mira Juan, prepara un listado de elementos en el entorno de la oficina que pueden ser susceptibles de sufrir daños o ser destruidos.

Juan mira a su alrededor, intentando valorar a simple vista lo que se le avecina.

- Cuando ya lo tengas, haces clasificación jerárquica, ordenando cada catástrofe por las consecuencias que acarrea, de más graves a menos graves.

- Pero esa clasificación, ¿me la invento o me la dais vosotros?

- No te preocupes, la tenemos tipificada. En seguida te proporciono los criterios.

- Cuando la tenga hecha, ¿a quién se la entrego?

- Me la entregas a mí. Después nos juntamos y en base a los listados, haremos un pequeño esbozo de posibles objetivos de seguridad a cumplir.

Juan se da cuenta de que las cosas no se hacen alegremente y que son analizadas a fondo.

En este epígrafe aprenderemos a qué se refiere Ignacio con esos tecnicismos que utilizaba en su conversación con Juan y desglosaremos los objetivos que se persiguen con las medidas de seguridad informática.

Para analizar los objetivos que se persiguen con la seguridad informática, deberíamos comenzar preguntándonos ¿qué queremos proteger?

Al principio de esta unidad hemos visto que la seguridad informática consiste en llevar a cabo una serie de medidas que hacen el sistema más fiable. Además de esto, el objetivo primordial de la seguridad es proteger los activos de la empresa, especialmente la información.

Cuando hablábamos del concepto de seguridad informática, se hacía referencia a la fiabilidad de los sistemas informáticos. Si entendemos un sistema de información como un conjunto de elementos que se combinan entre sí para lograr que una empresa cumpla con sus objetivos, un sistema informático, se podría entender como un subconjunto de un sistema de información. Dicho de otro modo, un sistema informático consiste en un conjunto de elementos como son el hardware (elementos físicos), software (elementos lógicos) y además, el personal experto que maneja los elementos lógicos y físicos (elementos humanos).

3.1.- Principales Aspectos de Seguridad.

Para concretar un poco más en el objetivo que se persigue, vamos a definir una serie de características que debería cumplir un sistema seguro:

Diego Méndez (Uso educativo nc)

- **Confidencialidad**: se trata de que sólo puedan acceder a los recursos de un sistema los agentes autorizados. Por ejemplo, si yo envío un mensaje una persona, solamente el destinatario debería tener acceso al mismo.
- **Integridad**: los recursos del sistema sólo pueden ser modificados por los agentes autorizados. Garantiza que la información sea consistente. Por ejemplo, al hacer alguna transacción electrónica como pagar un artículo por Internet. Es muy importante que nadie pueda modificar los datos bancarios durante el tránsito.
- **Disponibilidad**: para que exista disponibilidad los recursos del sistema tienen que estar a disposición de los agentes autorizados. Lo contrario sería una denegación de servicio. Para ilustrar este aspecto podemos pensar en cualquier empresa que preste algún servicio a través de Internet como, por ejemplo, una empresa de comercio electrónico. El hecho de que la aplicación de comercio electrónico no esté disponible, se traduce directamente en la desaparición del servicio y por tanto en pérdidas económicas, entre otros problemas.
- **No repudio**: permite garantizar que los participantes en una transacción, no nieguen haber realizado una operación “en línea”. Por ejemplo, que una persona haga una compra y posteriormente se niegue a pagarla alegando que no fue él quien hizo la transacción.

Autoevaluación

Relaciona cada situación con el aspecto de seguridad contra el cual atentaría, escribiendo el número asociado al aspecto de seguridad que le corresponda en el hueco correspondiente.

Ejercicio de relacionar

Situación	Relación	Aspecto de seguridad
Un apagón deja un servidor inoperativo durante toda la noche.	☐	1. Confidencialidad.
Al acercar un imán a un disco, hace que se dañen parte de los datos almacenados en el mismo.	☐	2. Integridad.

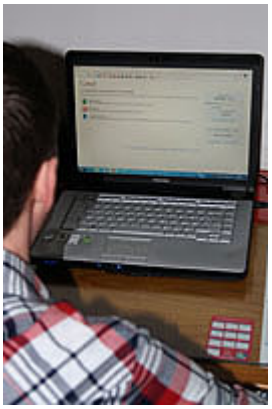
Compra de un artículo a través de Internet y posterior negativa a pagarlo alegando que es otra persona la que ha hecho la compra.	☐	3. Disponibilidad.
Un correo electrónico es interceptado y leído por una persona que no es el destinatario de dicho correo.	☐	4. No repudio.

Enviar

El apagón afectaría a la disponibilidad, la pérdida de datos a la integridad, el negarse a pagar el artículo alegando que ha sido otra persona es un caso de repudio y el correo electrónico interceptado está violando la confidencialidad.

4.- Amenazas y Fraudes en los Sistemas de Información.

Caso Práctico



Diego Méndez (Uso educativo nc)

Juan, en su vida cotidiana, acostumbra a comprar determinados artículos por Internet. Un buen día, a través de su correo electrónico recibe un anuncio publicitario con llamativas ofertas, supuestamente de una página donde acostumbraba a comprar material informático.

Cuando Juan entra a través del enlace del correo electrónico, se da cuenta de que la página se parece a la original, pero hay una serie de detalles que le hacen desconfiar y llama por teléfono a su amigo Gregorio para verificar algunos detalles.

- Hola Greg, te llamaba porque me ha llegado un correo un poco extraño. Supuestamente es del portal donde compramos los lápices de memoria la última vez, pero me piden que entre en un enlace para realizar alguna comprobaciones en mi cuenta. ¿A ti te ha llegado algo de esto?

- No que va, a mi no me ha llegado nada…

- Bueno pues creo que borraré el correo. Si es algo importante ya me llamarán por teléfono. Gracias Greg.

- No hay de qué Juan, ¡nos vemos!

Finalmente, Juan cierra la página y borra el mensaje de correo electrónico sospechoso.

- Mañana mismo le comento mi caso a Ignacio, mi tutor, porque ellos en la empresa están muy protegidos contra ataques y fraudes. Si no, ¿qué clientes confiarían en ellos?

Reflexiona

¿A qué se arriesgaría Juan si trata de introducir los datos de su cuenta en una página fraudulenta? ¿Conoces los diferentes fraudes que se pueden cometer en un entorno informático?

Como ya sabrás, en los últimos años, el número de personas que utilizan Internet de forma cotidiana ha crecido exponencialmente. Numerosos trámites que anteriormente se hacían mediante formularios en papel, ahora se realizan a través de aplicaciones web. El comercio electrónico ha ganado terreno frente al comercio tradicional siendo cada día más común hacer compras de todo tipo a través de Internet, etc. De la misma forma, en las empresas las conocidas como **TIC** (Acrónimo de Tecnologías de la Información y la Comunicación), cada vez juegan un papel más importante.

Todo ello hace que Internet sea un territorio relativamente hostil, siendo susceptible de amenazas cualquier dispositivo que esté conectado a la red.

Debes conocer

Un especialista de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional española, especialista en seguridad y la lucha contra el fraude en Internet nos da una serie de consejos y pautas a seguir para navegar por Internet de una forma más segura.

Consejos para evitar el fraude en Internet.

https://www.youtube.com/embed/2KQUvERUa-8

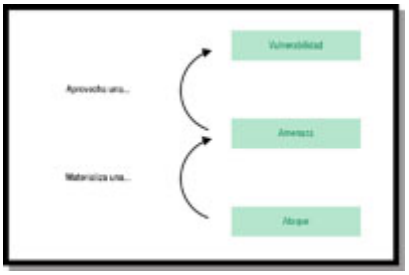
Descripción textual del vídeo

4.1.- Vulnerabilidades, Amenazas y Ataques.

En este epígrafe vamos a diferenciar entre estos términos y ver la relación que existe entre ellos.

Las vulnerabilidades y las amenazas son dos términos estrechamente relacionados. Si bien, una vulnerabilidad es la medida en que un elemento del sistema es susceptible de ser afectado por un atacante, una **amenaza** es cualquier circunstancia o evento que potencialmente puede causar un daño. Puede ser mediante la exposición, modificación o destrucción de información, o mediante la denegación de servicios críticos, aprovechándose de una vulnerabilidad.

Por otra parte, un ataque consiste en la materialización de una amenaza.



Ministerio de Educación (Uso educativo nc)

Para comprenderlo, qué mejor forma que ilustrarlo con un ejemplo…

Para saber más

En el siguiente enlace encontrarás información acerca de vulnerabilidades, actualizaciones y otros temas relacionados con seguridad.

Página sobre vulnerabilidades y otros aspectos de seguridad

Existen varias razones por las que un programa puede presentar vulnerabilidades. Una mala instalación o configuración podría ser una de esas razones, pero lo más común son errores cometidos durante el desarrollo del programa. Se dejan puertas abiertas a la entrada de intrusos.

Un **bug** (en inglés significa error) o agujero de seguridad es un fallo existente en un programa fruto de un error durante la programación del mismo que da lugar a una vulnerabilidad. En muchos casos, se detecta un bug cuando el programa ya está en explotación. Entonces, los desarrolladores implementan pequeños programas que rectifican dicho error. Estos pequeños programas se conocen como parches.

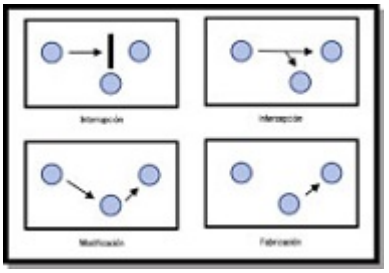
Debido a que en numerosas ocasiones, las vulnerabilidades no son descubiertas a tiempo, existe lo que se conoce como **ataques de día cero**. Estos ataques son aquellos que se producen cuando los atacantes son conocedores de la vulnerabilidad antes que el propio fabricante y, por tanto, antes de que exista un parche para reparar la vulnerabilidad.

Con respecto a los atacantes, la terminología es amplia y existen muchos términos dependiendo de las características del atacante y del ataque que efectúa. Este abanico de términos se verá en unidades posteriores, pero es interesante que te familiarices con la palabra **hacker (**en inglés pirata informático), como término genérico que se suele utilizar para referirse a la persona que efectúa el ataque informático.

4.2.- Tipos de Ataques.

Si tenemos en cuenta el objetivo del ataque, podemos distinguir entre ataques activos y pasivos.

- **Ataque activo**: Modifica o altera el flujo de datos.
- **Ataque pasivo**: Su objetivo no es alterar la comunicación sino que simplemente escucha o monitoriza para obtener información a través del tráfico.



Ministerio de Educación (Uso educativo nc)

Ejemplos de ataques

Ataque	Descripción	Tipo
Sniffing. (En inglés significa husmear).	Consiste en un análisis del tráfico, habitualmente utilizado para recabar contraseñas.	Pasivo.
Spoofing (Suplantación).	Técnicas de suplantación de identidad.	Activo.
Aprovechar agujeros de seguridad.	Como su nombre indica, son ataques que aprovechan vulnerabilidades del software.	Activo.
Denegación de servicio (DoS).	Mediante una saturación de información se causa la caída del servicio de tal forma que las usuarias o los usuarios legítimos no lo puedan usar.	Activo.
Ingeniería social.	Engloba un conjunto de técnicas en las que el atacante convence a un usuario o usuaria para obtener información confidencial.	Pasivo.
Phishing. (En inglés significa suplantación de identidad).	Es una variante de ingeniería social. El atacante se hace pasar por una persona o empresa de confianza para recabar información como contraseñas, datos bancarios, etc.	Pasivo.
Troyanos.	Consiste en un software que se instala en el equipo atacado sin que el usuario o usuaria sea consciente y permite al atacante hacerse con el control del equipo.	Se puede comportar de forma activa o pasiva.

Ataque	Descripción	Tipo
Adivinación de password. (En inglés significa contraseña).	Pueden ser ataques por fuerza bruta en los que se prueban las opciones posibles hasta dar con una contraseña válida o por diccionario, en los cuales se prueban una serie de contraseñas preestablecidas.	Pasivo.

Autoevaluación

Si enviamos un mensaje por correo electrónico y este sufre un ataque de intercepción. ¿A qué aspecto de seguridad de los vistos anteriormente afecta dicho ataque?

- ○ Confidencialidad.
- ○ Integridad.
- ○ Disponibilidad.
- ○ No repudio.

Muy bien, has captado la idea…

Incorrecta, porque el mensaje no ha sido alterado, por tanto, no afecta a su integridad.

El mensaje llega a su destino, por lo tanto, no afecta a su disponibilidad.

El hecho de interceptar el mensaje no afecta para nada al repudio del mismo.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

4.3.- Mecanismos de Seguridad.

Hasta ahora hemos visto las vulnerabilidades, amenazas y ataques que podemos sufrir. En este epígrafe veremos diferentes técnicas o mecanismos que tenemos para proteger nuestro sistema.

Teniendo en cuenta que esta unidad es una introducción a la seguridad para que te familiarices con los principales conceptos, no vamos a profundizar en lo que a medidas de seguridad se refiere, pero vamos a citar algunos consejos genéricos que será útil que conozcas. Algunas de estas técnicas o medidas son:

- **Identificación y Autenticación:** procedimiento por el que se reconocen y verifican identidades válidas de usuarios o usuarias y procesos. Tres tipos:
  - Estática (usuario/clave).
  - Robusta (claves de un solo uso, firmas electrónicas).
  - Continua (firmas electrónicas aplicadas a todo el contenido de la sesión).

Renee Silverman (CC BY-ND)

- **Control de la adquisición y actualización del software:** previene contra los virus, caballos de Troya y el robo de licencias.
- **Cifrado:** proporciona confidencialidad, autenticidad e integrigidad.
- **Actuaciones en el nivel de arquitectura:** las veremos en unidades posteriores.
- **Gestión de incidentes:** Detección de ataques, históricos, control de integridad, etc.
- **Acciones administrativas:** Identificación de responsables de seguridad, política de sanciones, políticas de privacidad, definición de buenas prácticas de uso, etc.
- **Formación:** Información a los usuarios y usuarias de las amenazas y cómo prevenirlas, políticas de la empresa frente a fallos de seguridad, etc.

Al igual que ocurría en otros aspectos, los mecanismos de seguridad se podrían clasificar en base a diferentes criterios. En este caso haremos una clasificación atendiendo al momento en que se llevan a cabo.

Devyn Caldwell (CC BY-NC-ND)

1. Si los mecanismos tratan de evitar que ocurra un desastre, decimos que se trata de un mecanismo de **prevención**.
2. Las medidas aplicadas en el momento en que se está produciendo el desastre de denominan medidas de **detección**.
3. Una vez se han producido los daños, las medidas tomadas para restaurar el estado al momento previo a que se ocasionasen los daños, son medidas de **recuperación**.

5.- Gestión de Riesgos.

Caso Práctico

Plan de Alfabetizacion Tecnológica Extremadura (CC BY-NC-ND)

Ya han pasado unos cuantos días desde que Juan comenzó a trabajar en la empresa y cada vez se desenvuelve mejor. También, a medida que va pasando el tiempo y Juan se va haciendo al puesto, sus jefes y jefas le dan más responsabilidades.

El día que Juan tuvo la primera entrevista con Ignacio, éste le explicó entre otras cosas, las directrices de la política de seguridad de la empresa. En dicha política se documenta todo lo relativo a seguridad en la empresa.

Hoy Ignacio, le ha dicho a Juan que va a tener que dar formación a los empleados y empleadas del departamento de recursos humanos en materia de seguridad informática.

- Juan tengo un nuevo trabajo para ti.

- ¿Ah sí? ¿En qué consiste? –preguntó Juan con impaciencia e ilusión a partes iguales-

- La semana que viene tendrás que dar una pequeña charla de formación a los empleados y empleadas de recursos humanos. Es muy importante que tengan unas nociones básicas de seguridad y que les transmitas lo establecido en la política de seguridad de la empresa.

- Muy bien, prepararé unas diapositivas y si me surge alguna duda ya te avisaré.

- Dedícale especial atención a los temas de auditoría, porque esta es la principal razón del curso.

Hasta ahora hemos visto el concepto de vulnerabilidad, de amenaza y de ataque. A continuación veremos lo que son los riesgos, los métodos y las herramientas que se utilizan para gestionarlos. Los objetivos de la gestión de riesgos son identificar, controlar y eliminar las fuentes de riesgo antes de que acaben materializándose en daños.

Entendemos el riesgo como la posibilidad de que una amenaza se materialice aprovechando una vulnerabilidad y viene dado por la siguiente ecuación:

Riesgo = Amenaza x Vulnerabilidad x Valor del bien

Analizando esta ecuación, vemos que el riesgo aumenta cuando aumentan tanto las amenazas como las vulnerabilidades como el valor de los bienes (o varios de ellos, lógicamente).

Por otra parte, definiremos el impacto como los daños o consecuencias que ocasiona la materialización de una amenaza. Los impactos se pueden clasificar en:

- **Impactos cuantitativos**: englobaríamos en este tipo de impactos a aquellos que se pueden cuantificar económicamente. Por ejemplo, se inunda una pequeña sala donde había 3 equipos que no contenían datos importantes y el impacto queda reducido al valor económico de los equipos.
- **Impactos cualitativos**: suponen daños no cuantificables económicamente, como por ejemplo, un ataque que no suponga pérdidas económicas pero que deja notablemente dañada la reputación de la empresa. Un daño cualitativo, por lo tanto, puede ocasionar impactos cuantitativos indirectamente.

5.1.- Proceso de Estimación de Riesgos.

Llegados a este punto, te habrás preguntado como abordar la gestión de los riesgos en la empresa. El análisis de los riesgos es el primer paso en la gestión de riesgos. Debemos dar respuesta a preguntas como:

- ¿Qué elementos necesitan protección?
- ¿Cuáles son las vulnerabilidades de esos elementos?
- ¿Qué amenazas pueden aprovechar esas vulnerabilidades?

En definitiva, valorar la magnitud del riesgo.

Aunque se podrían establecer múltiples clasificaciones, en este caso vamos a dividir el desarrollo de dicho proceso en tres subprocesos:

- **Identificación de riesgos**: lista de riesgos potenciales que pueden afectar a la organización.
- **Análisis de riesgos**: medición de la probabilidad y el impacto de cada riesgo, y los niveles de riesgo de los métodos alternativos.
- **Evaluación de riesgos**: lista de riesgos ordenados por su impacto y su probabilidad de ocurrencia

Todo este proceso está fundamentado en una base teórica. Tomando como base metodológica a, **MAGERIT** de España, se define de la siguiente manera según el ministerio de política territorial y administración pública:

> MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

Sus principales objetivos son:

- **Concienciar** a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un **método sistemático para analizar** tales riesgos.
- Ayudar a descubrir y **planificar las medidas** oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para **procesos de evaluación, auditoría, certificación o acreditación**, según corresponda en cada caso.

Como puedes ver, el enfoque que tiene MAGERIT es el de evaluar los riesgos desde el punto de vista de un sistema de información, es decir, no es algo específico de sistemas informáticos.

Para saber más

En el siguiente enlace puedes encontrar un fichero pdf con el desarrollo de la metodología MAGERIT.

Metodología MAGERIT

5.2.- Políticas de Seguridad.

Debes saber que, a la hora de gestionar la seguridad en una organización, se hace necesario reflejar de alguna manera todos los objetivos de seguridad. Entre otras cosas, para esto están las políticas de seguridad.

Teniendo esto en cuenta, una política de seguridad es el documento donde se van a plasmar todos los objetivos de la empresa en lo relacionado a seguridad de la información. Dicha política formará parte de la política general de la empresa.

Dicho de otro modo, mediante la política de seguridad, se define la manera de hacer un buen uso de los recursos hardware y software de la organización. Esto se logra:

- Concienciando a todo el personal en lo relativo a seguridad.
- Identificando las necesidades de seguridad
- Detectando las vulnerabilidades y el riesgo que entrañan en caso de ser aprovechadas por un atacante
- Estableciendo diferentes procedimientos para afrontar los problemas que puedan surgir.
- Etc.

Reflexiona

Teniendo en cuenta que uno de los principales objetivos de la política de seguridad es concienciar al personal en lo relativo a seguridad ¿te has parado a pensar en la importancia de que dicha política esté redactada de una forma clara y concisa?

Autoevaluación

Una política de seguridad…

- ☐ Recoge las directrices de la empresa en lo relativo a seguridad.
- ☐ Forma parte de su política general, por tanto debería estar aprobada por la dirección.

- [ ] El objetivo principal es concienciar a todo el personal en lo relativo a seguridad.

- [ ] En su día fue algo muy utilizado pero hoy en día es un método obsoleto.

Mostrar retroalimentación

Solución

1. Correcto
2. Correcto
3. Correcto
4. Incorrecto

5.3.- Auditorías.

Hasta ahora hemos visto la importancia de analizar los riesgos y de gestionarlos y documentarlos mediante una política de seguridad. Además, se deben aplicar una serie de técnicas y procedimientos de forma organizada para controlar el correcto funcionamiento de la organización. En otras palabras, se busca verificar que se cumplen los objetivos de la política de seguridad. Ésto, en términos generales, es lo que se conoce como auditoría.

El concepto de auditoría, inicialmente fue enfocado al terreno económico-financiero, pero hoy en día, este proceso se aplica en diversos ámbitos. En concreto y tomando como punto de partida la definición del párrafo anterior, la auditoría informática, consiste en una serie de procesos que se aplican para proteger los recursos de la empresa y asegurar un correcto funcionamiento.

Una auditoría puede llevarse a cabo por personal de la propia empresa o por personal ajeno a la misma, siendo esta opción la más aconsejable. La razón por la que es preferible que la auditoría se lleve a cabo por una persona o equipo ajeno a la empresa es de sentido común: si el encargado de los sistemas informáticos analiza los riesgos existentes con el fin de detectar deficiencias, es probable que su criterio no sea del todo objetivo. En algunos casos podría ser como “tirar piedras contra su propio tejado”.

Las **etapas** generales de una auditoría de podrían resumir a los siguientes puntos:

- Evaluación inicial del entorno auditable.
- Definición del alcance y los objetivos de la auditoría.
- Planificación.
- Puesta en marcha del proceso.
- Informe y propuestas de mejora.
- Seguimiento.

Dave MacFarlane (CC BY-NC)

Muchos de estos procesos se pueden automatizar y, por ello, existen numerosos programas destinados a auditoría de seguridad.

Para saber más

Enlace en "Monografías" sobre auditoría informática donde podrás ampliar la información al respecto:

Auditoría informática

5.4.- Plan de Contingencias.

A continuación vas a aprender en qué consiste un elemento fundamental en la gestión de riesgos: el plan de contingencias. Un plan de contingencias es un instrumento de gestión que consiste en una serie de medidas a llevar a cabo de forma complementaria al funcionamiento habitual de la empresa. Su objetivo es garantizar la continuidad del negocio de una organización en caso de se produzca un impacto.

Para ello, un **plan de contingencias** se desarrolla en tres subplanos independientes:

- **Plan de respaldo**: consiste en una serie de medidas preventivas. Su objetivo es simplemente tratar que no se materialicen las amenazas que puedan llegar a causar un impacto.
- **Plan de emergencia**: en este caso, el momento de aplicar el plan es durante el desastre, por tanto, el objetivo en este caso es paliar los daños del ataque.
- **Plan de recuperación**: como su propio nombre indica, en este caso se trata de recuperarse, restaurar el sistema y minimizar los daños tras un impacto.

Es de suma importancia que el personal de la empresa conozca perfectamente el plan de contingencias para actuar en consecuencia. De lo contrario, perdería gran parte de su sentido.

Además de especificar medidas organizativas, también recoge información acerca de las responsabilidades del personal, los materiales empleados para llevar a cabo las medidas, etc.

Ejercicio Resuelto

En este apartado hemos visto en qué cosiste un plan de contingencias. Basándote en lo anteriormente expuesto, ¿serías capaz de ilustrar el concepto con un ejemplo?

Mostrar retroalimentación

Supongamos una pequeña empresa dedicada al comercio electrónico. La infraestructura física de dicha empresa consiste en una serie de oficinas donde trabajan habitualmente sus empleados y empleadas y un par de servidores donde almacenan la mayor parte de la información. Todo ello se encuentra en la misma ubicación física.

Existen varias **amenazas** que pueden poner en peligro la integridad, confidencialidad y disponibilidad de la información, pero para este

ejemplo, nos centraremos en una: **un incendio.**

Una vez que tenemos en cuenta una amenaza en concreto podemos hacer una evaluación del **impacto** que podría llegar a causar: pérdida de clientes, caída temporal del servicio traducida en pérdidas económicas (sin contar con el efecto sobre la reputación de la empresa), inversiones en nuevo equipamiento, etc.

El plan de contingencias debería reflejar una serie de **contramedidas** para evitar o paliar el impacto en la medida de lo posible. Por ejemplo, extintores, detectores de humo, un seguro de incendios, copias de seguridad de la información (almacenadas en otro lugar), formación del personal (por ejemplo realizando algún simulacro de incendio), etc. Por último, los tres subplanes clasificarían las medidas de la siguiente manera:

- *Plan de respaldo*: revisión de extintores, simulacro de incendios, realización de copias de seguridad, etc. Como puedes ver, son medidas preventivas.
- *Plan de emergencia*: activación del sistema de extinción de incendios, restauración de las copias de seguridad, peritación del siniestro, etc. En este caso las medidas son tomadas durante el desastre o inmediatamente después.
- *Plan de recuperación*: evaluación del impacto, reanudación de la actividad, tramitar indemnización de la compañía de seguros, etc.

6.- Legislación: LOPDGDD.

Caso Práctico

La empresa donde trabaja Juan recopila numerosos datos personales de clientes. Estos datos, deben seguir un tratamiento específico que está regulado por ley. Por otro lado, en la ley también se recogen una serie de derechos que los usuarios tienen sobre sus datos.

Diego Méndez (Uso educativo nc)

Un buen día, Juan se encuentra trabajando en la oficina cuando suena el teléfono. Es un cliente que quiere rectificar sus datos:

- ¿Dígame? -responde Juan-

- Buenos días, soy Bartolomé González y llamaba por que he cambiado de domicilio y me gustaría que actualizaseis vuestro fichero con la nueva dirección postal.

- Sí, un momento por favor…

[…]

Esta era la primera vez que Juan se encontraba ante un caso como este y ha trasladado la petición del cliente a Ignacio. Ignacio, se ha disculpado con Juan por no haberle explicado antes todo lo relativo al tratamiento de los datos.

- Perdona Juan, debí explicarte antes todo esto, el tratamiento de los datos es un tema importante. Existen una serie de cosas que debemos tener en cuenta cuando manejamos datos de los clientes y clientas. Por un lado, tienen una serie de derechos y nosotros también tenemos una serie de obligaciones. En caso de no cumplir lo que marca la ley podríamos ser sancionados.

En lo sucesivo de la jornada, Ignacio continuó explicando a Juan todo lo relativo al tratamiento de los datos de su clientela.

Reflexiona

¿Sabías que la rectificación de los datos de carácter personal de un ciudadano, custodiados por una empresa o entidad, es un derecho establecido por ley junto a otros como el de cancelación u oposición?

En la constitución de 1978 ya se recoge el derecho a la protección de datos de carácter personal. En 1992 nace la **LORTAD**, primera Ley que regula de forma específica el tratamiento de los datos de carácter privado. Posteriormente, la LORTAD, fue derogada dando paso en 1999 a la **LOPD**, (acrónimo de Ley Orgánica de Protección de Datos). Actualmente, y desde 2018, está en vigor la llamada **LOPDGDD** (Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, Ley Orgánica 3/2018, de 5 de Diciembre).

En los siguientes apartados veremos lo que es la LOPDGDD y de qué manera afecta a una organización. Vas a comprobar, que dicha ley afecta principalmente a la manera en la que las empresas deben gestionar los datos de carácter personal de las personas.

Es importante conocer las directrices de esta ley, ya que, de incumplir algunos aspectos, una empresa podría enfrentarse a importantes sanciones.

6.1.- Ámbito de Aplicación.

A continuación, vamos a ver en qué ámbitos y situaciones es aplicable la LOPDGDD. Por ejemplo, de cara la protección de datos de carácter personal, no es lo mismo un entorno empresarial que desarrolle una actividad económica, que un entorno doméstico.

La **LOPDGDD** establece su ámbito de aplicación en el artículo 2, de forma que "*Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*"

Andrew Scott (CC BY-NC-ND)

Teniendo esto en cuenta, es importante distinguir a qué se refiere la Ley con el concepto de **fichero**. Un error común es pensar en un fichero como una serie de datos almacenados con formato digital en algún soporte informático. El concepto de fichero al que se refiere la LOPDGDD (como en la LOPD) consiste en un conjunto de datos almacenados en cualquier soporte e independientemente de que estén automatizados o no (en este aspecto, supuso una novedad en la LOPD con respecto a la **LORTAD**).

Teniendo esto en cuenta, se regirá por esta legislación el tratamiento de datos efectuado en territorio español o en caso de no efectuarse en territorio español, cuando le sea de aplicación la legislación española.

Por el contrario, no será de aplicación a los datos almacenados en el ejercicio de actividades domésticas. Tampoco es aplicable a los ficheros sometidos a la normativa sobre protección de materias clasificadas (asuntos relativos a secretos oficiales). Así como, los establecidos para la investigación de asuntos relacionados con el terrorismo.

Reflexiona

Hoy en día, el bombardeo de publicidad indiscriminada por muchas empresas a través de correo electrónico o de envío de mensajes a móviles, está a la orden del día. ¿Alguna vez te has planteado de qué manera podrían poner una reclamación ante estas situaciones?

Ejercicio Resuelto

Una de las directrices de la LOPD es mantener un registro de los datos de carácter personal almacenados. ¿Te has parado a pensar si sería necesario registrar en el Registro General de Protección de Datos la información de los

contactos que almacenas en tu teléfono móvil o tu ordenador?

Mostrar retroalimentación

En este caso no sería necesario, ya que se trata del almacenamiento de datos en un ámbito doméstico en cuyo caso, la obligación de registro que establece la LOPD no es de aplicación.

6.2.- Agencia Española de Protección de Datos.

Te habrás preguntado qué entidad es la encargada de gestionar todo lo relacionado con la protección de datos. La **AEPD** (**Agencia Española de Protección de Datos)** es un ente de Derecho Público cuyo principal cometido es el de velar por el cumplimiento de la legislación en lo referente a protección de datos.

Las principales funciones de la AEPD, las vamos a clasificar, por en lado, en funciones relacionadas con los usuarios y usuarias, y por otro, en relación a las organizaciones que custodian los datos de carácter privado.

Funciones en el ámbito de los **usuarios y usuarias** (siempre atendiendo a lo referente a la protección de datos):

- Garantizar sus derechos.
- Atender a posibles reclamaciones.
- Informar a los usuarios y usuarias sobre sus derechos promoviendo campañas de comunicación cuando sea oportuno.

Funciones en el ámbito de las **organizaciones** que tratan los datos. Puedes considerar:

- Velar por el cumplimiento de la Ley.
- Requerir medidas de corrección.
- Sancionar a quien no se atenga a la legislación ordenando el cese del tratamiento si fuese necesario.
- Proporcionar ayuda e información.
- Autorizar o denegar la transferencia de datos internacionales.

Otras funciones:

- Elaboración de normativa.
- Representación española en los foros internacionales.

Para saber más

Podrás ver el estatuto regulador que establece las normas por las que se ha de regir la AEPD:

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

6.3.- Derechos ARCO.

Con estas siglas **ARCO** nos referimos al conjunto de derechos ciudadanos en relación con los datos personales registrados en el Registro General de Protección de Datos.

gemawla1 (CC BY-SA)

- **Derecho de acceso**: cualquier persona puede dirigirse a una empresa u organismo público que contenga sus datos y solicitar información para saber qué datos tienen exactamente y la forma en que fueron obtenidos estos datos. La entidad que posee dichos datos tiene un plazo de un mes para atender adecuadamente la petición
- **Derecho de rectificación**: para ejercer el derecho de rectificación debes realizar un escrito acompañado de una copia de tu **D.N.I** dirigido al responsable del fichero que contiene los datos. En este caso, cuentas con un plazo de 10 días a partir del cual podrás poner una reclamación si tu petición no ha sido contestada de manera satisfactoria.
- **Derecho de cancelación**: tu como ciudadano o ciudadana tiene derecho a que tus datos sean cancelados de forma definitiva si así lo solicitas. Para ejercer este derecho, el proceso es análogo al que se sigue cuando se quiere rectificar algún dato, siendo también el plazo establecido de 10 días.
- **Derecho de oposición**: en los casos en los que no sea necesario el consentimiento del afectado o afectada y cuando existan motivos relativos a una situación personal. Si tu eres esa personal, podrías oponerse al tratamiento de tus datos. En tal supuesto el responsable del fichero excluirá el tratamiento de tus datos (siempre que una Ley no disponga lo contrario).

Además de los derechos **ARCO (**acrónimo de Acceso, Rectificación, Cancelación y Oposición.), la ley establece otros dos derechos: a la Portabilidad y a la Supresión u Olvido. Además, la AEPD establece una serie de derechos para los ciudadanos y ciudadanas como el derecho a no recibir publicidad no deseada, el derecho de exclusión de guías telefónicas, etc. En el siguiente “Para saber más” puedes encontrar un enlace a este sitio.

Para saber más

En el siguiente enlace puedes encontrar como desarrolla la AEPD cada uno de los derechos ARCO, además de otros derechos, como por ejemplo, el derecho a no recibir publicidad no deseada:

Derechos de los ciudadanos en torno a la protección de datos

6.4.- Niveles de Seguridad y Medidas Asociadas.

Marcos Guevara Rivera (CC BY-NC)

En el anterior apartado hemos hablado de algunos derechos de los ciudadanos y ciudadanas de cara al tratamiento de sus datos de carácter personal. A continuación, nos centraremos en las características de esos datos y los relacionaremos con una serie de medidas de seguridad a adoptar en función de su naturaleza.

Es importante que te des cuenta, de que no es lo mismo almacenar datos como el nombre y los apellidos de una persona, que datos relativos a su religión, orientación sexual, etc. En consecuencia, las medidas a adoptar para mantener la privacidad de dichos datos, también serán diferentes.

Teniendo todo ello en cuenta, la LOPD establecía que las medidas se clasificaban en tres niveles en función del tipo de datos:

Nivel de protección de los datos según su naturaleza con las medidas de seguridad asociadas

Nivel	Tipo de datos	Medidas
Básico	Nombre y apellidos. Números de teléfono. Dirección postal y email. Fecha y lugar de nacimiento. Etc.	Documentación de seguridad donde se reflejen las funciones de cada usuario o usuaria del fichero. Cambio de contraseñas cada año. Mantener un registro de incidencias en relación al fichero. Los datos desechados deberán ser borrados o destruidos. Realización de copias de seguridad.
Medio	Relativos a infracciones administrativas o penales. Aquellos que permitan evaluar la personalidad o comportamiento de una persona. Aquellos de los que sean responsables: ✔ Administraciones tributarias. ✔ Entidades financieras. ✔ Entidades gestoras y la Seguridad Social.	Medidas de nivel básico y además: Auditoría al menos una vez cada dos años. Establecer mecanismos de control de acceso a los datos.

Nivel	Tipo de datos	Medidas
Alto	Relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. Aquéllos que contengan datos derivados de actos de violencia de género.	Medidas de nivel medio (y por tanto básico) y además: Cifrado de los datos. Copias de seguridad almacenadas en un lugar diferente al de los datos. Mantener un registro de los accesos a los datos.

En cambio, la LOPDGDD ya no establece un conjunto de medidas de seguridad predefinidas a aplicar en función de los criterios anteriores. Lo que se plantea en la nueva Ley es que **en función del riesgo que se estime o detecte, se establecerán las medidas determinadas.** En general, si ya se estaban aplicando medidas fijadas en la LOPD, si no es necesario, pueden seguir manteniéndose, aunque también, si se detecta la correspondiente necesidad, podrían modificarse.

Para saber más

En el siguiente enlace al Boletín Oficial del estado, podrás encontrar desarrollada la clasificación de las diferentes medidas de seguridad en función de la naturaleza de los datos. Título VIII, Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Real Decreto que establece los niveles se seguridad (Título VIII)

6.5.- Infracciones y Sanciones.

Es importante que sepas que cuando una organización incumple lo establecido por la Ley, puede ser sancionada con importantes sumas de dinero. La cuantía de las sanciones que impone la LOPDGDD depende de varios parámetros como:

- La naturaleza de los derechos personales afectados.
- El volumen de los tratamientos efectuados.
- Los beneficios obtenidos.
- El grado de intencionalidad.
- La reincidencia.
- Los daños.
- El perjuicio causado.
- Etc.

Estableciendo una clasificación en cuanto a la gravedad de las infracciones y redondeando las cifras, tendríamos:

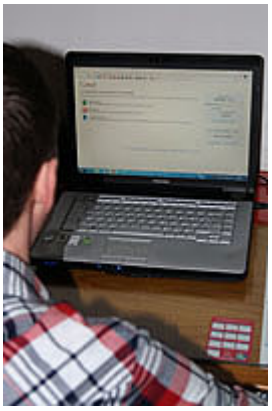
Tipos y cuantía de las sanciones en función de su gravedad

Gravedad	Infracción	Cuantía sanción
Leves	No solicitar la inscripción del fichero en la Agencia Española de Protección de Datos. Recogida de datos personales sin informar previamente de sus derechos a los afectados y afectadas. No atender a las solicitudes de rectificación o cancelación de los datos. No proporcionar la información de solicite la AGPD.	Hasta 40.000€.
Graves.	No inscribir los ficheros en la AGPD. Utilizar los ficheros con distinta finalidad al objeto legítimo de la empresa. No permitir los derechos de acceso u oposición de los ficheros. Mantener datos inexactos o no efectuar las modificaciones solicitadas. No seguir los principios y garantías de la LOPDGDD. Recogida y tratamiento de datos sin el consentimiento del afectado o afectada. No remitir a la AGPD las notificaciones previstas en la LOPDGDD. Mantener los ficheros sin las debidas condiciones de seguridad. Vulnerar el deber de secreto para datos de nivel medio.	De 40.001€ a 300.000€.

Gravedad	Infracción	Cuantía sanción
Muy graves.	Recogida de datos de manera engañosa o fraudulenta. Recabar datos especialmente protegidos sin la autorización del afectado o afectada. Desatender u obstaculizar de forma sistemática el ejercicio de los derechos de cancelación o rectificación. Vulnerar el secreto sobre datos especialmente protegidos. La comunicación o cesión de datos en los casos que no esté permitida. No cesar en el uso ilegítimo a petición de la AGPD. No atender de forma sistemática los requerimientos de la AGPD. La transferencia de datos de carácter personal con destino a países que no apliquen medidas de protección equiparables o sin autorización.	De 300.000€ a 20.000.000€. 2% al 4% facturación bruta anual

7.- Legislación: LSSI.

Caso Práctico



Diego Méndez (Uso educativo nc)

La empresa en la que Juan trabaja como becario, entre otras cosas, está a punto de ofrecer la venta de componentes electrónicos a través de una aplicación de comercio electrónico. El tutor de Juan le ha dicho que en cuanto esté terminada la aplicación la tendrían que revisar antes de subirla al servidor.

- Verás Juan, la empresa va a empezar a vender componentes electrónicos por Internet y están desarrollando un portal de comercio electrónico. Cuando lo terminen tenemos que revisar que cumpla con lo establecido por ley.

- ¿Y cuál es la Ley que regula ese tipo de cosas?

- La Ley de Servicios de la Sociedad de la Información, échale un vistazo que no se nos puede escapar nada, no vaya a ser que nos sancionen.

- Ya…sería lo que nos faltaba. En cuanto tenga un momento me pongo con ello.

- Perfecto.

Una vez que la aplicación se puso en funcionamiento, a los administradores y administradoras del portal les surgieron una serie de dudas al respecto. Decidieron que lo mejor era consultar a Ignacio y a Juan.

Por ejemplo, no tenían clara la manera de plantear la publicidad y dudaban de la legalidad de enviar correos masivos con publicidad, etcétera.

Una vez vista la LOPDGDD, seguimos con la Ley de servicios de la sociedad de la información, de aquí en adelante **LSSI**. La referencia normativa la encontramos en la Ley 34/2002 del 11 de Julio.

Como veremos a continuación, esta Ley se aplica al comercio electrónico y a aquellos servicios de Internet siempre que representen una actividad económica para el prestador o prestadora del servicio.

Hoy en día, cada vez son más las empresas que constituyen una actividad económica a través de Internet, ya sea directa o indirectamente. Con esto, nos referimos tanto a empresas de comercio electrónico, como empresas que realizan publicidad por vía electrónica o empresas intermediarias como proveedores de Internet o empresas de alojamiento. Estas empresas deberán conocer las obligaciones que establece la LSSI, pero además, los usuarios y usuarias, también están incluidos en el caso de que tengan una página con publicidad por la que perciban ingresos o simplemente, para conocer sus

derechos como usuarios y usuarias en Internet.

7.1.- Ámbito de Aplicación.

Steve Rhode (CC BY-NC-ND)

Para analizar esta Ley, comenzaremos respondiendo a la pregunta **¿a quién es aplicable?** La LSSI se centra en Internet y las nuevas tecnologías y es aplicable a los prestadores o suministradores de Servicios de la Sociedad de la Información, **siempre que representen una actividad económica** para el prestador o prestadora.

Además, el prestador o prestadora de servicios debe estar establecido en España o dicho de otro modo, su domicilio fiscal debe estar en territorio español siendo este su lugar principal de gestión de operaciones. Para aquellos no establecidos es España existen algunas excepciones, como por ejemplo, aquel que preste servicios ofrecidos a través de un establecimiento permanente en España. ¿Conoces algún caso?

Sin perjuicio de la legislación específica al respecto, la LSSI también es aplicable a los servicios de juegos de azar y apuestas.

Entonces… **¿a quién no es aplicable?** Pues no será de aplicación a aquellos servicios que no constituyan una actividad económica. Tampoco a servicios prestados por notarios o notarias y registradores o registradoras, abogados o abogadas y procuradores o procuradoras, en el ejercicio de sus funciones de representación y defensa en juicio, a quienes se le aplicará normativa específica.

Autoevaluación

Señala entre las siguientes opciones, el caso en el que no sea de aplicación la LSSI:

- ○ Un proveedor de servicios de conexión a Internet.
- ○ Una empresa de venta de artículos deportivos a través de Internet.
- ○ Un abogado en el ejercicio de sus funciones.
- ○ Una casa de apuestas por Internet.

Incorrecto, un proveedor de servicios es una empresa prestadora de un servicio que representa actividad económica.

No es correcto, una empresa de comercio electrónico es una empresa prestadora de un servicio que representa actividad económica.

Muy bien, has captado la idea…Si bien representa una actividad económica, es una excepción a la que se le aplicará normativa específica.

No es la repuesta correcta, una casa de apuestas sí dearrolla actividad

económica.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

7.2.- Obligaciones de las Empresas.

Te habrás preguntado las obligaciones que tiene una empresa de cara al cumplimiento de la LSSI. Dependiendo del tipo de actividad que desempeñe la empresa, la LSSI especifica una serie de obligaciones que debe cumplir. Para especificar estas obligaciones dividiremos las empresas en tres grupos:

Daniela Hartmann (CC BY-NC-SA)

Las empresas dedicadas al **comercio electrónico**, deben mostrar en su página Web una serie de datos que informen al usuario o usuaria, como por ejemplo:

- **NIF** (acrónimo de Número de Identificación Fiscal), domicilio, dirección de correo electrónico, teléfono o fax.
- Precios de los productos indicando impuestos y gastos de envío.
- Datos sobre la autorización administrativa necesaria para prestar los servicios que ofrezca la empresa.
- Una serie de datos relativos al contrato “en línea” en el caso que este exista.

En el caso de empresas que hacen **publicidad** a través de Internet:

- El anunciante debe identificarse con claridad.
- Debe reconocerse el carácter publicitario del anuncio de forma inequívoca.
- En caso de realizar concursos o juegos promocionales las condiciones deberán estar expresadas claramente.
- Cuando se envíe por correo electrónico o **SMS** (acrónimo de Short Message Service), se debe obtener previamente la autorización del destinatario o destinataria y proporcionar procedimientos sencillos para negar el consentimiento.

Para empresas **intermediarias** de los servicios de Internet (estas son las empresas que ofrecen alojamiento de datos, los buscadores y los proveedores de Internet):

- Colaborar con organismos públicos apara ejecutar resoluciones que precisen de su ayuda.
- Informar a los usuarios y usuarias para aumentar la seguridad en el entorno informático.

Para saber más

Enlace que recopila algunas preguntas frecuentes acerca de la LSSI:

Preguntas frecuentes sobre la LSSI

8.- Legislación: Derechos de Autor.

Caso Práctico

Diego Méndez (Uso educativo nc)

Hace unos días que Juan impartió la charla de seguridad a los empleados y empleadas del departamento de recursos humanos y se le ha ocurrido hacer un dossier para que cada uno de ellos conserve un pequeño resumen por escrito de los aspectos fundamentales de la política se seguridad de la empresa.

Para elaborar dicho dossier, Juan busca información e imágenes por Internet, pero se le plantea la duda de qué contenidos podrá utilizar.Él sabe que sabe que existen diferentes tipos de licencias, pero no le queda muy claro que restricciones impone cada una de ellas.

El caso es que Ignacio le ha comentado que tuviese cuidado con los derechos de autor de los recursos que utiliza.A Juan, eso de los derechos de autor siempre le ha sonado de las obras musicales, pero nunca se había parado a pensar en los derechos de otro tipo de obras.

Por otra parte, su conocimiento en cuanto a licencias se limitaba a si la obra incluía o no un copyright. Después de investigar un poco se ha dado cuenta que existe un amplio abanico de posibilidades a la hora de asociar una licencia a una obra.

Imágenes, música, vídeo, contenidos…en la red existe un amplio abanico de recursos y obras de todo tipo y no todas tienen los mismos permisos para su uso y difusión.

Hace algunos años, la posibilidad de hacer una copia ilegal se reducía prácticamente a copiar obras musicales o cinematográficas sobre cintas magnéticas. Hoy en día, con la globalización de Internet y el uso generalizado de los ordenadores, la existencia de todo tipo de obras digitalizadas y colgadas en la red, es algo de lo más común.

A lo largo de este epígrafe veremos las directrices de la Ley de Propiedad Intelectual (de aquí en adelante LPI) y algunos tipos de licencias que se pueden asociar a las obras.

8.1.- Ley de Propiedad Intelectual.

En este apartado conocerás las directrices de la Ley de Propiedad Intelectual. Muy pocas veces nos vemos afectados por esta ley pero quizás, tú seas un pequeño creador o creadora.

Según el Ministerio de Cultura…

> "*La propiedad intelectual es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación*."

El **Real Decreto Legislativo 1/1996**, de 12 de abril, aprueba el texto refundido de la Ley de Propiedad Intelectual.

Juan Espino (CC BY-NC-SA)

La nombrada Ley, protege todo tipo de creaciones originales de cualquier tipo y expresadas en cualquier medio, lo que abarca desde un libro, a una coreografía. Por otra parte, se excluyen las ideas, conceptos matemáticos o métodos de operación, pero no la expresión de los mismos.

Existen dos tipos de derechos sobre una obra, los derechos de autor (persona que crea la obra) y los derechos conocidos como afines, pertenecientes a productores y productoras, ejecutantes no autores de la obra, etc.

Hay quien piensa que la propiedad intelectual de una obra nace en el momento de su inclusión en el Registro de Propiedad Intelectual o que el autor o autora de la obra debe estar inscrito en alguna sociedad privada de gestión, como por ejemplo, la SGAE (acrónimo de Sociedad General de Autores y Editores), pero ninguna de estas cosas son necesarias ya que la propiedad intelectual de una obra, comienza en el momento en que se crea dicha obra sin necesidad de llevar a cabo ningún trámite especial.

Para saber más

En el siguiente enlace encontrarás un video sobre la nueva Ley de Economía Sostenible relacionada con las páginas web de descargas en Internet.

Ley de economía sostenible y descargas en Internet

Autoevaluación

Según la Ley de Propiedad Intelectual, autor es:

- La persona natural que crea alguna obra literaria, artística o científica.
- La persona natural que crea alguna obra literaria, artística o científica y procede posteriormente a su registro en el Registro de la Propiedad Intelectual.
- Quien paga por los derechos sobre la obra.
- Cualquier persona que haya divulgado alguna obra literaria, artística o científica.

El artículo 5.1 de la LPI dice lo siguiente: "Se considera autor a la persona natural que crea alguna obra literaria, artística o científica".

Incorrecta, el ser autor o autora no implica registrar la obra.

No es correcta, el autor o autora tiene los derechos sobre su obra.

No es la opción correcta, el autor o autora es quien crea la obra.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

8.2.- Copyright y Copyleft.

Posiblemente sabrás que, cuando se crea una obra, (ya sea literaria, pictórica, fotográfica, etc.) existen varias formas para proteger de forma legal el uso que se hace de dichos contenidos. Una de ellas, es el Copyright, que en España, constituye un derecho automático, aunque cada país tiene una legislación copyright aplicable con diferentes matices.

Desconocido (Dominio público)

¿Has reconocido con facilidad este símbolo?

La manera de incluir el Copyright, aunque puramente indicativa, se formaliza de la siguiente manera:

> Símbolo Copyright © + año de publicación + nombre del autor (o de la sociedad que ha depositado el copyright).
> Ejemplo: © 2011 Ministerio de Educación.

Cuando un contenido incluye Copyright ya sabes que significa que tiene los derechos reservados y, por tanto, existen una serie de restricciones sobre el uso de dichos contenidos. Como por ejemplo, la utilización o la publicación parcial o total con fines comerciales.

Como hemos dicho, el Copyright constituye un derecho automático por si mismo, pero existen instrumentos que sirven de ayuda a la hora de ejercer este derecho, como son los **depósitos de Copyright.** Un depósito de Copyright, te permite demostrar que realmente eres el autor o autora. También te permite probar en qué fecha la obra ha sido creada. Sin este instrumento no siempre es una tarea trivial.

Zscout370 (Dominio público)

Como contrapunto al Copyright, surge lo que se conoce como Copyleft. Cuando una obra tiene una licencia Copyleft implica que dicha obra o contenido, tendrá permisos de copia, modificación y redistribución, y además impone la misma licencia a las copias y a las obras derivadas.

¿Con cual de los dos identificaría al software libre?

8.3.- Licencias Creative Commons.

En el anterior apartado hemos visto las licencias Copyright. Llegados a este punto, puede que te preguntes ¿Pero las posibilidades se reducen a un Copyright o Copyleft? ¿No hay término medio?

Pues bien, como alternativa más flexible al Copyright, nacen las licencias Creative Commons que permiten reservar solamente determinados derechos de una forma muy sencilla.

Creative Commons es una corporación americana sin ánimo de lucro. En el 2004, en España se adaptan las licencias a la legislación sobre propiedad intelectual, siendo la institución afiliada a CC la Universidad de Barcelona.

Este tipo de licencias cada vez son más utilizadas y de hecho España, encabeza el ranking (en inglés, tabla de clasificación) mundial de países en su utilización.

Las licencias Creative Commons ofrecen una serie de derechos a terceras personas bajo unas condiciones concretas. A continuación vamos a ver, según Creative Commons España, las **condiciones** a partir de las cuales se forman **las licencias existentes**:

- **Reconocimiento**: En cualquier explotación de la obra autorizada por la licencia hará falta reconocer la autoría.
- **No Comercial:** La explotación de la obra queda limitada a usos no comerciales.
- **Sin obras derivadas:** La autorización para explotar la obra no incluye la transformación para crear una obra derivada.
- **Compartir Igual:** La explotación autorizada incluye la creación de obras derivadas siempre que mantengan la misma licencia al ser divulgadas.

Con estas cuatro condiciones combinadas podrías generar las seis **licencias** que se pueden escoger:

César Poyatos (CC BY-NC-SA)

- **Reconocimiento (by):** Te permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación de obras derivadas. La distribución de las mismas también está permitida sin ninguna restricción.
- **Reconocimiento - NoComercial (by-nc):** Te permite la generación de obras derivadas siempre que no hagas un uso comercial. Tampoco se puede utilizar la obra original con finalidades comerciales.
- **Reconocimiento - NoComercial - CompartirIgual (by-nc-sa):** No te permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales la debes hacer con una licencia igual a la que regula la obra original.
- **Reconocimiento - NoComercial - SinObraDerivada (by-nc-nd):** No te permite un uso comercial de la obra original ni la generación de obras derivadas.
- **Reconocimiento - CompartirIgual (by-sa):** Sí te permite el uso comercial de la obra y de las posibles obras derivadas. Su distribución la debes hacer con una licencia igual a la que regula la obra original.
- **Reconocimiento - SinObraDerivada (by-nd):** Te permite el uso comercial de la

obra pero no la generación de obras derivadas.

Para saber más

En el siguiente enlace encontrarás un formulario que te permite configurar una licencia Creative Commons y generar un código HTML para incluirla en tu página Web.

Pon una licencia a tu obra