Introducción a la seguridad informática

Caso práctico

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.

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.”

1. Introducción a la seguridad informática.

Caso práctico

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** (acrónimo de Real Academia de la lengua Española) 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.

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.

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.

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.

3. Objetivos de la seguridad informática.

Caso práctico

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:

- **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.

4. Amenazas y fraudes en los sistemas de información.

Caso práctico

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. Sino ¿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.

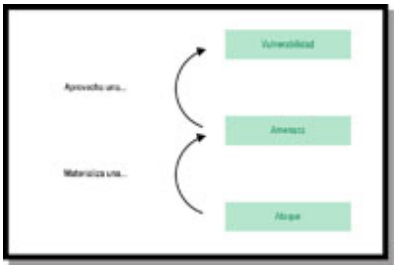
Todo ello hace que Internet sea un territorio relativamente hostil, siendo susceptible de amenazas cualquier dispositivo que esté conectado a la red.

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.



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

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.

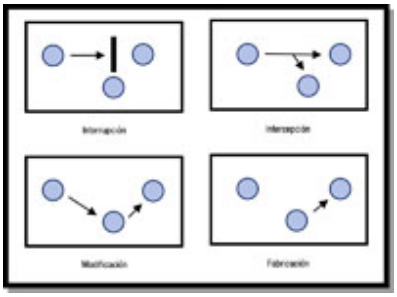
Debido a que en numerosas ocasiones, las vulnerabilidades no son descubiertas a tiempo, existe lo que se conoce como **ataques de día cero**. Estos ataques son aquellos que se producen cuando los atacantes son conocedores de la vulnerabilidad antes que el propio fabricante y, por tanto, antes de que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



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.
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.

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).
- **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 integridad.
- **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.

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

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.

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?

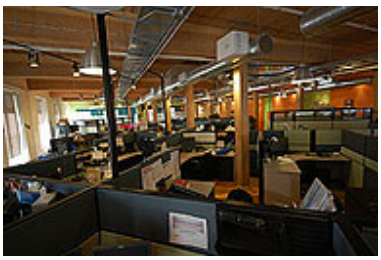
5.3 Auditorías.

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.

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

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.