# Introducción a la seguridad informática

Contenido

[Introducción a la seguridad informática 1](#_Toc371518018)

[Presentación del tema 1](#_Toc371518019)

[Sistemas de información y sistemas informáticos. 2](#_Toc371518020)

[Sistema de información: 2](#_Toc371518021)

[Sistema informático: 2](#_Toc371518022)

[Seguridad 3](#_Toc371518023)

[Medidas de seguridad. Clasificaciones. 4](#_Toc371518024)

[SEGURIDAD ACTIVA / SEGURIDAD PASIVA: 4](#_Toc371518025)

[SEGURIDAD FÍSICA / SEGURIDAD LÓGICA 4](#_Toc371518026)

[PROPIEDADES DE UN SISTEMA DE INFORMACIÓN SEGURO. 5](#_Toc371518027)

[INTEGRIDAD: 5](#_Toc371518028)

[CONFIDENCIALIDAD: 5](#_Toc371518029)

[DISPONIBILIDAD: 5](#_Toc371518030)

[NO REPUDIO: 6](#_Toc371518031)

[Otras propiedades de seguridad. 6](#_Toc371518032)

[Análisis de riesgos 6](#_Toc371518033)

[Elementos de estudio... ¿En qué tenemos que fijarnos? 7](#_Toc371518034)

[El proceso del análisis de riesgos: 10](#_Toc371518035)

[Políticas de seguridad 12](#_Toc371518036)

[Plan de contingencias 12](#_Toc371518037)

[Auditorías de seguridad 14](#_Toc371518038)

# Presentación del tema

En este tema hablaremos de los conceptos básicos de la Seguridad Informática.

No son conceptos nuevos ni creados a propósito para ésta disciplina.

La mayor parte de ésta terminología ha sido adoptada de terminología ya existente en el ámbito empresarial, referida a la seguridad en un concepto amplio.

La Seguridad Informática se encarga de los aspectos relacionados con la seguridad de los equipos informáticos, pero también de todo lo que le rodea de manera más o menos directa: personas, datos, software, instalaciones...

## Sistemas de información y sistemas informáticos.

### Sistema de información:

Un sistema de información es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos.

Esos elementos son:

* Recursos, como ordenadores, componentes, periféricos, conexiones, aplicaciones, sistemas operativos, y otros recursos no necesariamente informáticos, desde un teléfono a una grapadora.
* Equipo humano
* Información: datos organizados que tienen un significado. Pueden estar en un soporte informático o no.
* Actividades: muy importante... toda organización realiza varias actividades en su negocio. (Ej.: una pequeña tienda tiene varias actividades: vender productos a los clientes, hacer pedidos a los proveedores, controlar la cantidad de productos almacenados, gestionar los gastos, ingresos, impuestos, etc...)

### Sistema informático:

Un Sistema informático está formado por un conjunto de elementos físicos (hardware, conexiones, cables...) lógicos (Software de aplicación, de base, protocolos) y también podemos considerar con frecuencia al componente humano.

Un sistema informático **da soporte a las actividades de los sistemas de información**. Las empresas diseñan sus actividades conforme a la información que manejan... Nunca pensando en el sistema informático que les va a dar soporte. Lo importante para ellas, lógicamente, es que esas actividades se desarrollen de manera ordenada, eficaz y eficiente. Los sistemas informáticos, cuando están bien diseñados y utilizados, contribuyen en esos aspectos. (INFORMÁTICA=Tratamiento autoMÁTICO de la INFORmación).

No necesariamente todas las actividades de la empresa requieren de sistemas informáticos.

## Seguridad

La seguridad es la disciplina que se ocupa de diseñar las **normas, procedimientos, métodos y técnicas** destinados a conseguir un sistema de información seguro y confiable.

Todos los elementos que participan en un sistema de información pueden verse afectados por factores de diversa índole que pueden poner en peligro su estabilidad y normal funcionamiento.

Con respecto a la Seguridad Informática, debemos tener en cuenta, que de todos esos elementos, debemos poner especial atención en la **información,** pues es el elemento más sensible de la empresa, y la que tiene un valor *incalculable[[1]](#footnote-2)*... pero siempre por detrás, por supuesto, de la seguridad de las personas.

Reflexiona sobre ésto: ¿Tendría sentido anteponer la seguridad de la información o de cualquier otro elemento a la seguridad de las personas?

Nuestro trabajo se centrará en la seguridad de los sistemas informáticos, pero siempre teniendo en mente que la protección va encaminada hacia las **actividades** de una empresa... a intentar que no se vean vulneradas o afectadas por ninguna circunstancia, y por supuesto, tampoco la información que manejan. Es decir, a que los *sistemas de información* continúen su ritmo con la máxima normalidad posible. Para ello actuamos sobre los sistemas informáticos que les dan soporte.

Nuestra disciplina se encarga poco de la seguridad de las personas, por eso no tendrá especial relevancia. Eso no significa que sea, sin duda, el aspecto clave de la seguridad... simplemente, que ésta disciplina se enfoca principalmente hacia la seguridad de los sistemas de información.

Para afrontar la seguridad de un sistema, deberemos conocer los elementos del sistema, los peligros que pueden acechar y las medidas que deberían adoptarse para lograr esa seguridad. No obstante, lo estudiaremos desde un punto de vista formal, utilizando terminología estándar del sector de la seguridad.

Reflexiona sobre ésto: ¿Se puede lograr la seguridad total? Es decir... estar totalmente protegido contra cualquier cosa.

Hay un dicho en el sector de la seguridad:

***La cadena siempre se rompe por el eslabón más débil.***

A menudo se dice también que ese eslabón suele implicar al factor humano.

Reflexiona sobre ésto:¿Crees que en efecto, el factor humano es el eslabón más débil?

## 

## Medidas de seguridad. Clasificaciones.

Para proteger la información, es necesario establecer una serie de medidas. Las medidas de seguridad pueden clasificarse de varias maneras. Nosotros vamos a mencionar dos:

### SEGURIDAD ACTIVA / SEGURIDAD PASIVA:

Atendiendo al carácter que tenga, hablamos de medidas de seguridad

* **Activas**: aquellas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. Podemos decir que tienen un carácter **preventivo.** es decir, intentan *impedir* que ocurra un incidente.  
  Por ejemplo, en un coche, el ABS es una medida de seguridad activa, ya que es un mecanismo electrónico que ayuda al conductor a frenar el coche... intenta evitar, prevenir un incidente.
* **Pasivas**: aquellas cuyo objetivo es minimizar la repercusión de un incidente de seguridad una vez producido. Podemos decir que tienen un carácter **correctivo.**Es decir, no intentan evitar un incidente, sino reducir sus posibles efectos adversos. Por ejemplo, en un coche, un cinturón de seguridad es una medida de seguridad pasiva: no intenta evitar un accidente, sino que, de producirse, los daños para el ocupante del vehículo sean menores.

Una determinada medida de seguridad casi siempre cae en uno de los dos grupos. Es poco frecuente encontrar medidas de seguridad que simultáneamente puedan considerarse activas y pasivas... no obstante, como haberlas, haylas. Por ejemplo, cualquiera de los antivirus modernos, por un lado intenta *impedir* la entrada de virus y malwares, y por otro lado, si entran y el antivirus los detecta intentará minimizar su impacto.

### SEGURIDAD FÍSICA / SEGURIDAD LÓGICA

Referido ya al ámbito exclusivo de la seguridad informática, podemos hablar de

* **Seguridad lógica**: cuando la medida va destinada a la protección de la información o del software.
* **Seguridad física**: cuando la medida va destinada a la protección del hardware.

Quizá estés pensando en el hecho de que el hardware, a veces es soporte del software y los datos... Por ejemplo... Si protejo un ordenador servidor con un SAI (el ordenador es hardware), pero el servidor en su interior contiene datos... entonces ¿el SAI es una medida de seguridad física o lógica? Es física... protege de manera directa al hardware... y los datos del servidor también, pero de manera indirecta.

En general, el hardware en sí no es un recurso demasiado valioso. Hay medidas de seguridad física dirigidas a él porque prácticamente siempre es el soporte de los datos.

## PROPIEDADES DE UN SISTEMA DE INFORMACIÓN SEGURO.

¿Qué le pedimos a un sistema de información seguro? ¿Que no se cuelque? ¿Que no nos borre cosas? ¿Que no lo puedan hackear?.... Si... por supuesto. Estas cosas y muchas otras más. Formalmente hablando, hay tres *propiedades* básicas que un sistema de información debe mantener al máximo que sea posible. Prácticamente todo lo que le pidamos a un sistema de información que consideremos seguro cae dentro de mantener estas tres propiedades altas:

### INTEGRIDAD:

Garantizar la autenticidad y precisión de la información, sin importar el momento en que se solicita.

Dicho de otra forma, que los datos no son alterados ni destruidos de modo no autorizado, ni accidentalmente. Si los datos se pierden, se borran, se modifican, se corrompen, o se añaden datos nuevos fraudulentos o erróneos consideramos que se ha perdido la integridad de un sistema de información. Esto puede ocurrir con datos que están almacenados (“quietos”, en un fichero, o base de datos, o manejados por una aplicación...) o con datos que se está en un sistema de comunicaciones (se están “moviendo”... y llegan a su destino en un estado diferente al que fueron emitidos.

### CONFIDENCIALIDAD:

Garantizar que los datos almacenados estén únicamente al alcance de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada.

Es decir, no sólo que se pueda acceder a información si se está autorizado, sino que se además, debe hacerse dentro de la actividad correspondiente.

Si un sistema de información permite que un dato cualquiera llegue a ser visto por alguien que no está autorizado supone una pérdida de la confidencialidad. El concepto va todavía más lejos... Si el dato llega a una persona que sí es un destinatario legítimo de la información, pero llega por un mecanismo no autorizado, o un momento no autorizado, o utilizando algún procedimiento no autorizado, también consideramos que se ha producido una pérdida de la confidencialidad.

### DISPONIBILIDAD:

El grado en que un dato está en el lugar, momento y forma en que es requerido por un usuario autorizado.

Dicho de otro modo, que la información que se solicite esté disponible en un periodo de tiempo "razonable" desde que se solicita por un usuario autorizado.

La pérdida de la disponibilidad sólo implica en sí misma que en un momento dado, una información que se solicita no es devuelta por un sistema. Esto no implica que la información haya perdido la integridad... sólo que no se puede proporcionar en ese momento.

### NO REPUDIO:

La capacidad de determinar quién creó, modificó o accedió a cierta información, de forma que ni el emisor/creador pueda negar su participación, ni el receptor pueda negar que tuvo dicha información disponible.

Esta característica de la seguridad cobra importancia a la hora de realizar transacciones seguras en un sistema informático, con aplicaciones variadas. Por ejemplo, en la administración electrónica, es vital que el ciudadano pueda probar que ha tramitado en plazo sus obligaciones tributarias, y que el estado no pueda alegar que no recibió la documentación.

### Otras propiedades de seguridad.

Además de las tres propiedades fundamentales de un sistema de información seguro (la disponibilidad, confidencialidad e integridad), y del la cualidad de no-repudio, a menudo se utilizan otras propiedades de seguridad en algunos sistemas, según sean útiles o no:

* **Autenticación**: Más allá de la confidencialidad, las medidas o servicios de autenticación intentan garantizar la identidad de las personas o entidades que intentan acceder a la información. Se puede exigir la autenticación en el origen de los datos, en el destino o en ambas. Está ligada a la **confidencialidad**, ya que el sistema informático necesita saber quién accede al sistema para garantizar esta última. Se necesita para el **no-repudio**.
* **Control de acceso**: Son las medidas o servicios que no sólo permiten o impiden el acceso de personas o entidades a la información, sino que además, suelen registrar constancia del hecho del acceso o el intento de acceso. Relacionado con la **confidencialidad** y el **no-repudio**.

# Análisis de riesgos

Hasta ahora, hemos planteado algunos conceptos básicos de la seguridad.... utilizando una terminología informal.

En el ámbito de la seguridad, se utiliza sin embargo, una terminología formal y común para todas las disciplinas de seguridad (la seguridad informática incluida, por supuesto).

El **Análisis de riesgos** es una acción extremadamente común en el estudio de la seguridad de un sistema. Consiste en estudiar, analizar, reflexionar y proponer medidas de seguridad fijándose en algunos aspectos de un sistema de información. Es decir, es un estudio dirigido, acotado... destinado a reflexionar sobre una parte o unos aspectos concretos de la seguridad.

Podría hacerse referido a la seguridad de un sistema informático al completo, pero esa es una tarea titánica... mejor enfocarse. Si es necesario hacer un análisis de riegos de todo un sistema es mejor descomponerlo en partes o aspectos y hacer análisis de cada uno de ellos.

Este análisis suele dar como resultado **documentación escrita**. Es decir, el análisis tiene valor en sí mismo, pero es necesario darlo a conocer.

Aunque tiene un carácter ciertamente esquemático y técnico, debe estar lo suficientemente redactado y razonado como para que cualquier persona entienda su contenido... de qué va, qué es lo que se está estudiando, qué elementos se ven afectados, por qué se está realizando el estudio, por qué se proponen según qué medidas, etc.

Existen modelos formales que nos ayudan a saber qué pasos realizar para hacer un análisis de riesgos de calidad y exhaustivo (ej MAGERIT). Nosotros, en la asignatura, lo haremos algo más informalmente, adecuado para análisis de sistemas o subsistemas en la pequeña o mediana empresa... pero eso no es excusa para descuidar su aspecto, profundidad e incidencia.

## Elementos de estudio... ¿En qué tenemos que fijarnos?

Ya hemos comentado que un **análisis de riesgos** suele ir dirigido, es decir... se motiva por la presenta de supuestos peligros que queremos estudiar, o bien... porque directamente se ha producido un incidente y queremos evitar que se repita uno igual o similar.

Nos fijaremos en éstos elementos:

#### ACTIVOS:

Se denomina así a cualquier recurso de la empresa (exceptuando el dinero). Son activos elementos de los datos, el software, el hardware, el personal, las redes, las instalaciones e incluso los servicios y actividades de la empresa. En un análisis de riesgos los enumeraremos y explicaremos lo que son.

#### AMENAZAS:

Se entiende por amenaza la presencia de uno o más factores de diversa índole que -de tener la oportunidad- afectarían al sistema objeto de estudio produciéndole daños.

Hay muchos tipos de amenazas... cortes eléctricos, fallos en hardware, riesgos ambientales, acciones intencionadas, software malicioso, robo, destrucción de información, modificación de información... seguro que se te ocurren un montón.

Pero en función del daño o manipulación que puedan hacer sobre la información, suelen caer en uno de éstos grupos:

* De **interrupción**: se deshabilita el acceso a la información, se cortan comunicaciones o accesos.
* De **interceptación**: se capta la información por personas o elementos no autorizados
* De **modificación**: La información se altera, bien definitiva o bien circunstancialmente
* De **fabricación**: se genera información nueva y fraudulenta o errónea.

Como ya comentamos, según su origen pueden ser:

* Fortuitas (o accidentales)
* Fraudulentas (o intencionadas)

#### VULNERABILIDADES:

Cada activo es vulnerable en cierto grado a algunas amenazas. Las amenazas sólo afectan a los activos vulnerables. Es necesario estudiar qué activos son vulnerables a qué amenazas.

Ej: (Un tanto exagerado). Imaginemos la siguiente amenaza: "Lluvia de meteoritos desde el espacio exterior que caen sobre nuestra población".

Si los activos que pueden verse afectados son "Yo mismo" y "Superman"... El primer activo es totalmente vulnerable a la amenaza... El segundo activo es prácticamente invulnerable.

Otro ejemplo: (Menos exagerado). El famoso virus "Sasser" estaba programado para aprovecharse de algunas vulnerabilidades de algunos sistemas operativos de la serie Windows. Algunos sistemas Windows eran totalmente vulnerables... otros sólo parcialmente o eran completamente invulnerables. Todos los sistemas tipo unix eran invulnerables.

#### RIESGOS

Riesgo es la probabilidad de que se materialice una amenaza y produzca un daño sobre un activo aprovechando su vulnerabilidad ante dicha amenaza. Es decir... la definición de **riesgo** está íntimamente ligada por un lado a los activos y sus vulnerabilidadades, y por otro a las amenazas.

Ej.: Siguiendo con el ejemplo anterior... el **riesgo** de que se produzca una lluvia de meteoritos sobre ésta población y me afecte a mí (el activo) es muy bajo. (No se conocen lluvias de meteoritos en los últimos siglos sobre ésta población).

El el riesgo de que se produzca una lluvia de meteoritos sobre ésta población y afecte a Superman (el activo) es practicamente inexistente. (Además de que no se conocen lluvias de meteoritos en los últimos siglos sobre ésta población, tampoco Superman suele estar por aquí, con lo cual, si se produjera una lluvia de meteoritos es poco probable que le pillara, y en caso de que le pillara, es invulnerable a los meteoritos).

El riesgo de un virus tipo "I loveyou" afecte a un sistema Windows es muy alto, ya que están diseñados específicamente para propagarse y aprovechar vulnerabilidades de éstos.

Lo importante de los riesgos es **estimarlos...** hacer una estimación de la probabilidad de que aparezca la amenaza y afecte a un determinado activo.

La estimación no es más que eso: una forma de intentar "adivinar" en qué grado de probabilidad una amenaza afectaría a un activo.

A menudo, se diseñan herramientas (estadísticas, matemáticas, probabilísticas...) para intentar evaluar los riesgos de la manera más cuantificada posible (es decir, con números)... Si utilizamos alguna de éstas herramientas para evaluar un riesgo, es necesario citarla *siempre*.

Ante la detección de un riesgo, se puede optar por tres alternativas:

* **Asumirlo, y no prevenirlo**. Ésto resulta lógico cuando el perjuicio esperado tiene poco valor o cuando el coste de la aplicación de medidas preventivas supera el de la reparación del daño. (Véase "**Plan de contingencias**". En éste caso, es útil. Si no prevengo un riesgo, al menos, saber cómo afrontarlo).
* **Prevenirlo**: Aplicar medidas de seguridad activa para disminuirlo o anularlo.
* **Transferirlo**. Traspasar a un tercero la gestión de ese riesgo: típicamente, **contratar un seguro** para ese riesgo. Tiene sentido cuando el coste de la prevención es elevado, también el de la reparación... pero el riesgo de que ocurra es bajo.

#### ATAQUE:

Llamamos **ataque** a la materialización de una amenaza, independientemente de que su origen sea fortuito o intencionado.

En función del impacto causado y la propiedad del sistema vulnerada, los ataques se clasifican en:

* **ataques activos**: Si se modifica, daña o suprime información o si se bloquean los canales de comunicación (Es decir, se compromete la *integridad* o la *disponibilidad* del sistema
* **ataque pasivo**: Si solamente se accede a información de manera no autorizada o por canales no autorizados (Es decir, se compromete la *confidencialidad* del sistema).

Un ataque también puede ser **directo** si se produce directamente desde el atacante hasta el activo, o **indirecto** si se hace a través de recursos o personas intermediarias.

#### IMPACTO:

El impacto es la consecuencia de un ataque (producido ya o supuesto). Dicho de otra forma, son los daños causados por un ataque, existente o no.

Los impactos se puede estimar:

* De forma **cuantitativa**, cuando se puede expresar en términos económicos.
* De forma **cualitativa**, cuando esos daños no se pueden cuantificar (ej: pérdida de derechos fundamentales, pérdida de vidas, daños morales, de imagen...)



### 

## El proceso del análisis de riesgos:

Para realizar un análisis de riesgos, en primer lugar estudiaremos el caso que tengamos entre manos, tratando de encontrar sus elementos.

Después, deberíamos seguir un cierto esquema, que, sin duda pasa por estos puntos:

* **Enumerar y valorar los activos**: decir cuáles son los implicados en el caso, cuál es su función, qué contienen, en qué actividades se ven involucrados, quién los utiliza... etc.
* **Identificar y valorar las vulnerabilidades**de cada activo ante cada amenaza: dadas las amenazas a estudiar, algunos activos presentarán vulnerabilidades, otros no, y otros sólo en cierto grado o aspecto: reflexionar sobre ello y plasmarlo.
* **Identificar y valorar las amenazas que pueden afectar a los activos**: definir qué amenazas pueden tener impacto sobre los activos enumerados... en qué consisten, en qué circunstancias se producirían
* **Determinar la medida de los riesgos:** Cada amenaza tendrá una cierta probabilidad de aparición, y, según las vulnerabilidades de cada activo a cada amenaza, supondrá un cierto nivel de riesgo. Es necesario *estimarlo,* si es posible, con datos o herramientas que lo refrenden, y plasmarlo convenientemente.
* **Identificar y evaluar las medidas de seguridad existentes**: qué medidas hay ya tomadas en el sistema. Cómo afectan a las amenazas, activos y vulnerabilidades descritas.
* **Identificar los objetivos de seguridad de la organización**. ¿Qué es lo que queremos lograr? ¿Para qué estamos haciendo éste análisis?
* **Determinar el impacto de un ataque:** Si el ataque se ha producido, describirlo y evaluar su impacto. De las posibles amenazas no materializadas, intentar *estimar* su supuesto impacto.
* **Identificar y seleccionar las medidas de seguridad propuestas**: proponer medidas de seguridad, tanto activas como pasivas para reducir los riesgos. Es conveniente estimar sus costes, tanto de implantación como de mantenimiento.
  + Es necesario establecer un orden en las medidas propuestas. Dar alternativas... Un análisis de riesgos debe concluir con varias aportaciones de seguridad activa o pasiva, que deben quedar perfectamente definidas.
  + Si algunas de las aportaciones son excluyentes (ej.... optar por una o por otra), debe quedar perfectamente claro para el que lo lee, y cuál es la prioritaria y por qué.
  + Las medidas de seguridad no siempre se proponen "sueltas"... normalmente se combinan de forma ordenada y lógica... en ese caso, forman un **mecanismo de seguridad**. Seguro que muchas de las mejores propuestas se expresan normalmente en forma de mecanismos, y no de medidas sueltas.

Es importante resaltar que las medidas de seguridad activas intentan eliminar una **vulnerabilidad**, mientras que las medidas de seguridad pasivas mitigan los impactos de un daño producido por una **amenaza**



En conclusión.... el **análisis de riesgos** es mucho más que un documento... ES UN **ANÁLISIS**: un estudio y reflexión del profesional que lo realiza, y se refiere la seguridad de algún aspecto de un sistema informático, con aporte de soluciones para reducir los riegos, y estudio y evaluación de todos los elementos implicados, desde los puntos de vista más amplios posible.

Es la herramienta clave de la SEGURIDAD, tanto informática como de cualquier otro aspecto, y es el punto de partida hacia el aporte de soluciones. Lo emplearemos intensiva y extensivamente en los casos que veamos a lo largo del curso.

[más[Análisis de riesgos](http://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo) en Wikipedia]

# Políticas de seguridad

Llamamos así a las directrices u objetivos de una organización con respecto a la seguridad.

Toda organización debe tener recogidas esas directrices, que todas las personas involucradas de alguna manera con la empresa deben conocer y cumplir.

Las políticas de seguridad se refieren a todos los aspectos de seguridad de la empresa, pero por supuesto, habrá medidas referidas a los sistemas informáticos. Las medidas en ese sentido deben proponerse a partir de los análisis de riesgos.

Un análisis de riesgos es un documento técnico y exhaustivo. Si a partir de uno o varios análisis de riesgos se llega a una medida o mecanismo de seguridad que deba ser conocido y respetado por todos, debe estar plasmado en las **políticas de seguridad** de la empresa.

Las políticas de seguridad no son un documento técnico ni exhaustivo. Es un documento generalista y es para que todas las personas de la empresa lo conozcan y velen por el cumplimiento de las normas que exhibe.

Es un documento que debe ser aprobado por la dirección de la empresa y conocido por todos.

La parte referida a los sistemas informáticos será propuesta sin duda por personal técnico a partir de uno o más análisis de riesgos.

Existen estándares para realizar las políticas de seguridad de las empresas. Por ejemplo el ISO (International OrganizationforStandarization) define uno. MAGERIT también.

Entre los puntos que debe cubrir la política de seguridad podemos destacar:

* Identificar las necesidades de seguridad y riesgos
* Relación de todas las medidas de seguridad
* Reglas y procedimientos que deben aplicarse en los diferentes departamentos de la organización, y los que deben aplicarse con carácter general.
* Mecanismos de detección de vulnerabilidades y fallos
* Definir planes de contingencias para amenazas posibles.

## Plan de contingencias

Un plan de contingencias intenta describir los pasos a seguir ante la materialización de un amenaza.

Ante muchas amenazas, se pueden poner medidas preventivas (seguridad activa) que impidan que se materialicen en un ataque.

A menudo, esas medidas no se pueden poner (porque su coste es caro con respecto al riesgo que supone la amenaza) o a veces, a pesar de las medidas de seguridad activa, el ataque se produce.

Ante un ataque, algunas actividades de la empresa se verán afectadas, impidiendo su normal desarrollo.

Un plan de contingencias intenta organizar la manera de actuar ante la presencia de un ataque, de manera que el desarrollo de la actividad empresarial afectada pueda continuar.

Es decir, está enfocado a continuar con la actividad de la empresa aunque se produzca un ataque... NO a la continuidad del funcionamiento del sistema informático.

En ese sentido, para cada contingencia previsible (cada posible amenaza), debería existir un plan de contingencias (que se anexa a las políticas de seguridad), y que contenga cada uno al menos tres planes independientes:

* **El plan de emergencia:** el que contempla qué hacer **cuando se está produciendo** un ataque o acaba de producirse: qué se debe hacer para continuar con las actividades empresariales afectadas. Debe ser una descripción clara y sencilla: debemos intentar que cada persona actúe de acuerdo al plan (sea bueno o menos bueno), de esa manera se intenta evitar la desorganización y el caos.
* **Plan de respaldo**: Contempla las contramedidas preventivas **antes**de que se materialice una amenaza. Su finalidad es evitar dicha materialización.
* **Plan de recuperación**: Contempla las medidas necesarias **después**de materializada y controlada la amenaza. Su finalidad es **restaurar** el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Los planes de contingencia forman parte de las políticas de seguridad de una empresa.

[más: [Planes de contingencia](http://es.wikipedia.org/wiki/Plan_de_Contingencias) en wikipedia]

## Auditorías de seguridad

En nuestro ámbito, una auditoría es un análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan.

Su finalidad es **verificar** que se cumplen los objetivos de la **política de seguridad** de la empresa.

Proporciona una idea actual del estado de seguridad e un sistema de información.

No obstante, la auditoría en sí misma se ha convertido en una parte importante de la seguridad.

Hablando en concreto de la Seguridad Informática, la auditoría tiene su propia dinámica.

[más[Auditoría informática](http://es.wikipedia.org/wiki/Auditoria_inform%C3%A1tica) en wikipedia]



1. Valor incalculable puede significar dos cosas:

   * que es muy valioso
   * que no se puede calcular.

   En nuestro contexto, nos referimos a la segunda acepción. [↑](#footnote-ref-2)