# Software y hardware, redes y seguridad: Administración de la seguridad

Estamos rodeados de virus, bacterias y hongos que producen enfermedades. Pero los seres humanos disponemos de mecanismos de defensa tanto internos, el sistema inmunológico, como externos, las medicinas y las vacunas.

Ya hemos visto en los temas anteriores que los ordenadores son máquinas que "imitan" a las personas en aspectos tales como la constitución, el funcionamiento y la comunicación. Del mismo modo, también sufren los ataques de programas, archivos y mensajes que atacan sus sistemas, pero también disponen de mecanismos que les permiten minimizar estos ataques.

La administración de la seguridad trata de conseguir la integridad y la protección de los procesos, de los recursos y los datos. Debemos distinguir por tanto entre **seguridad informática** y **seguridad de la información.**


Img 0. La seguridad informática

Imagen de producción propia

# 1. La seguridad informática

**Importante**

La **seguridad informática** se define como el conjunto de métodos y herramientas destinados a proteger los sistemas computacionales ante cualquier amenaza.

La seguridad de los sistemas informáticos se suele comparar con una cadena, la cual es segura si el eslabón más débil también lo es. Para encontrar ese eslabón y protegerlo se tiene que tratar la seguridad desde distintos puntos de vista:

- Establecer la seguridad física que afecta a la infraestructura y al material.
- Establecer la seguridad lógica para proteger datos, aplicaciones y sistemas operativos.
- Concienciar a los usuarios de la importancia de la seguridad del equipo, del sistema y de la información.
- Proteger los sistemas de comunicación, especialmente en las redes.


Seguridad informática

Imagen de producción propia

## Objetivos de la seguridad

El objetivo principal de la seguridad informática es garantizar que los recursos y la información estén protegidos y para protegerlo son necesarios conseguir los siguientes aspectos:

1. **Integridad**.- sólo los usuarios autorizados podrán modificar la información.
2. **Confidencialidad**.- sólo los usuarios autorizados tendrán acceso a los recursos y a la información que utilicen.
3. **Disponibilidad**.- la información debe estar disponible cuando se necesite.
4. **Irrefutabilidad.-** el usuario no puede refutar o negar una operación realizada.

## Autoevaluación

Antes de comenzar a estudiar los contenidos del tema, busca la definición de los siguientes términos. Seguro que muchos de ellos los conoces, pero intenta relacionarlos con la seguridad informática.

- Amenaza
- Impacto
- Riesgo
- Vulnerabilidad
- Ataque
- Contingencia

# 1.1. Seguridad física y seguridad lógica

**Importante**

La **seguridad física** de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.
- Disturbios internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes.

La seguridad informática

Imagen obtenida en pdatugsteno.com



**Importante**

La **seguridad lógica** de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y al información contenida en él.

El activo más importante de un sistema informático es la información y, por tanto, la seguridad lógica se plantea como uno de los objetivos más importantes.


La seguridad lógica

Imagen de flickrcc

La seguridad lógica trata de conseguir los siguientes objetivos:

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

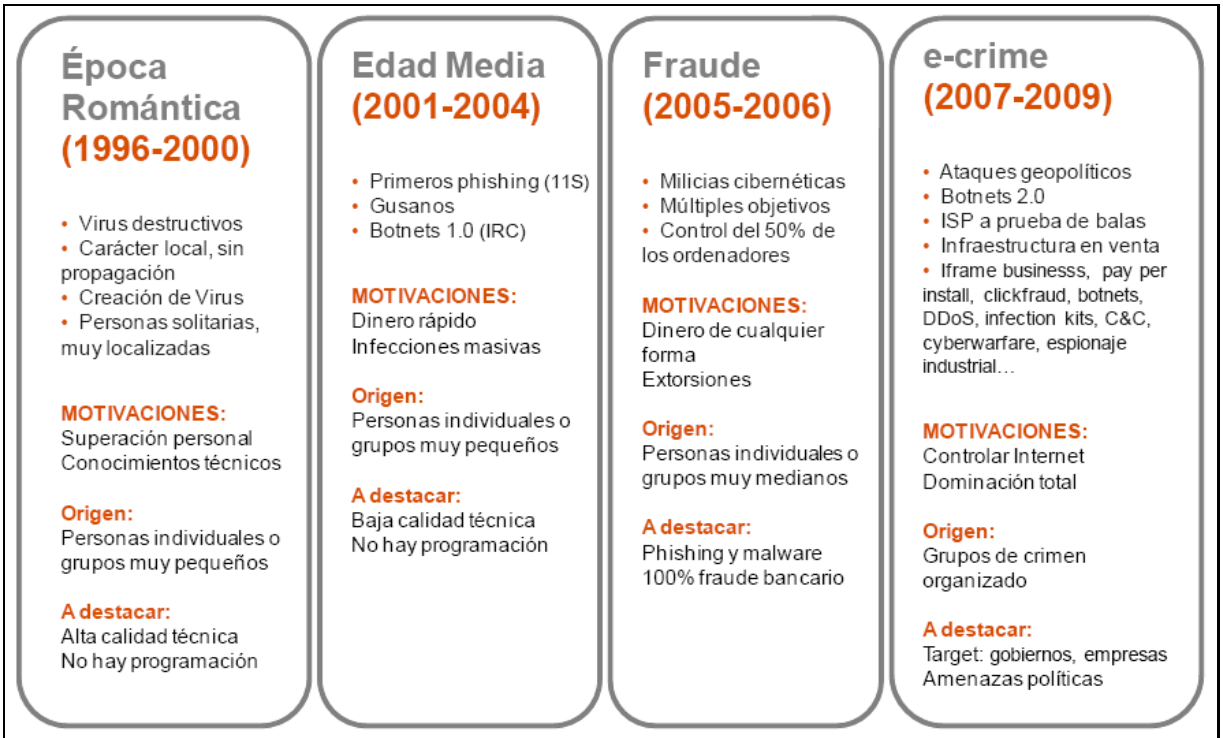
## Autoevaluación

Indica a qué tipo de seguridad, física o lógica, pertenece cada uno de los siguientes sistemas:

1. Uso del procedimiento correcto.
2. Blindaje contra robos.
3. Comprobación de la veracidad de una información transmitida.
4. Creación de usuarios restingidos.
5. Sistema de protección contra incendios.
6. Control de acceso a los recintos donde se sitúan los ordenadores.

## 1.2. Delitos informáticos y legislación

La implantación y desarrollo de las TIC ha creado nuevas posibilidades de delincuencia antes impensables. El delito informático es aquel que se refiere a actividades ilícitas realizadas por medio de ordenadores o de internet. También incluye delitos tradicionales como fraude, robo, estafa, chantaje, falsificación y malversación de caudales públicos. Los perjuicios ocasionados por este tipo de delitos son superiores a la delincuencia tradicional y también es mucho más difícil descubrir a los culpables.




Evolución de los delitos informáticos

Imagen de producción propia

Información obtenida del Informe sobre el Cibercrimen 2.008 de la empresa S21sec.

Te interesa saber:

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de ordenadores.
2. Manipulación de los datos de entrada.
3. Daños o modificaciones de programas o datos computarizados.

Cuando se comete un delito informático, siempre hay dos tipos personas involucradas:

- Sujeto activo: aquella persona que comete el delito informático.
- Sujeto pasivo: aquella persona que es víctima del delito informático.

En algunos casos, un ordenador intermedio puede ser correa de transmisión del virus o incluso del ciberdelito sin saberlo el propio usuario.

En España está en vigor la Ley Orgánica de Delitos Informáticos, basada fundamentalmente en la Decisión Marco de la Unión Europea.

También existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el CERT/CC (*Computer Emergency Response Team Coordination Center*) del SEI (Software Engineering Institute).

## Para saber más

Si te interesa conocer la legislación vigente sobre delitos informáticos, aquí tienes algunos enlaces interesantes.

Decisión Marco de la Unión Europea nº 2005/222/

Proyecto de Ley Orgánica de 15 de enero de 2.007

Aprobación del proyecto de ley de delitos informáticos de 7 de mayo de 2.008

## Autoevaluación

Llegados a este punto, no hemos mencionado todavía dos palabras que te sonarán: hacker y cracker. Realiza una pequeña investigación para conocer su definición y las diferencias que existen entre las dos.

¿Cuales son estas diferencias? ¿Cuáles fueron sus orígenes? ¿Quienes son considerados los primeros hackers?
Puedes encontrar información en los artículos de wikipedia y de la vanguardia.

# 1.3. Malware


El término *Malware* fu
computacional Klaus Brun
"maliciosos" que podían
actualidad, el término ti
cualquier software que at
sistema operativo, un orde

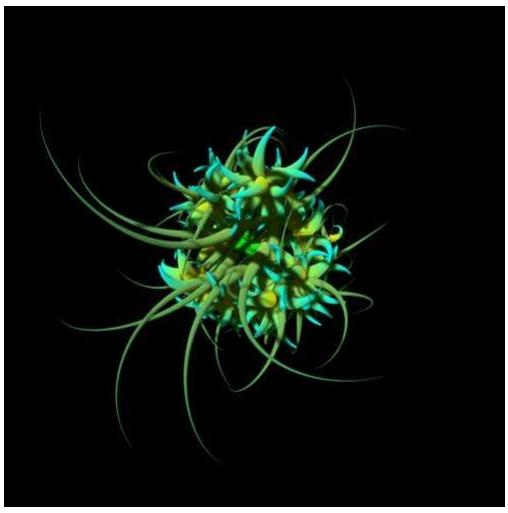
Seguro que te suena el nombre de algunos de estos programas: virus, troyanos, gusanos, espías y phishing.

## Virus

Se llama virus informático a aquel programa cuyo objetivo es alterar el normal funcionamiento del ordenador sin el permiso del usuario. Se denominaron así ya que se propagan como una enfermedad infecciosa.

Una de las principales características de los virus es el consumo de recursos, lo que puede producir daños en diferentes aspectos, tales como pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos. Una de las grandes facilidades de los virus son las redes, incluída internet, que permiten su propagación muy rápidamente.

Dependiendo del medio que utilicen para infectar el ordenador se clasifican en: virus residente, de arranque, de fichero y de macro. Cada virus plantea una situación distinta y, por tanto, también hay diferentes soluciones para enfrentarse a ellos. Los métodos más comunes para enfrentarse a los virus son la instalación de firewalls (pared cortafuegos) y de antivirus. Los estudiaremos en el punto de protección junto con algunos métodos más.



Virus MyDoom

Imagen de 20minutos.es

(Licencia Creative Commmons)

Galería de imágenes: "así crecen los virus"

## Para saber más

Una empresa de seguridad ha recopilado los 20 virus más importantes de la historia. Desde que se creó el que se considera el primer virus informático en 1.971, el *Creeper*, hasta el famoso *Italian Job*, que infectó en 2.007 más de 10.000 sitios web. En el siguiente artículo de la revista "20 minutos" lo puedes encontrar todos:

20minutos: virus más importantes

Y ya que estás aquí, echa también un vistazo a los virus más peligrosos de la historia. Seguro que has oído alguna vez estos nombres:

20minutos: virus más peligrosos

## Troyano

También denominados "caballos de Troya", son códigos maliciosos que se alojan en el ordenador y permiten el acceso a usuarios externos. Normalmente tienen dos fines: recabar información o controlar el ordenador de forma remota. Su nombre deriva de la Odisea de Homero, en la que el Caballo de Troya se hacía pasar por un regalo, pero escondía a las tropas griegas. Del mismo modo, un troyano suele ser un programa alojado en otro archivo o aplicación que se instala en el sistema al ejecutar el archivo y, una vez instalado, realiza otra función.

La diferencia entre un virus y un troyano es su finalidad, ya que el primero provoca daños en el ordenador y el segundo trata de pasar inadvertido en el ordenador para acceder la información. Por tanto, el mejor sistema para evitar este tipo de malware es no ejecutar archivos o programas que no tengan una fuente conocida y tener instalado algún programa anti-troyanos y firewall. Hoy en día, los troyanos se transmiten a través del correo electrónico y de los archivos P2P.

Hay troyanos de muchos tipos, por ejemplo, las llamadas “bombas de tiempo”, que se activan en fechas determinadas; las “bombas lógicas”, que se activan cuando el ordenador infectado cumple unos requisitos especificados por su programador; o los "troyanos sociales", incluidos por las empresas en los programas para obtener más información sobre su uso.


Virus troyanos

Imagen de Aprendegratis.com

## Autoevaluación

1. El término "malware" se refiere a:

- a) Hardware mal instalado.
- b) Software mal instalado.
- c) Programas maliciosos.

2. Los virus se propagan como una enfermedad infecciosa ¿Qué daños pueden causar?

- a) Consumo de recursos y pérdida de productividad.
- b) Daños en los sistemas de información y de datos.
- c) Todos los anteriores.

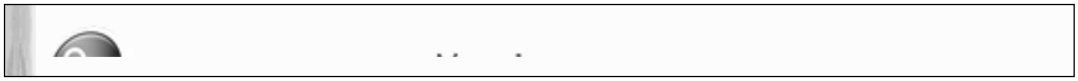
3. La finalidad de un troyano es:

- a) Acceder a la información del ordenador atacado.
- b) Provocar daños en los sistemas de información.
- c) Consumir los recursos del ordenador.

**Gusano**

Un gusano informático es un programa malicioso que tiene la propiedad de reproducirse por sí mismo sin necesidad de hardware o software de apoyo. Suelen distribuir códigos maliciosos como troyanos. La diferencia con los virus es que no pretenden dañar los archivos del ordenador, sino que habitualmente lo que hacen es consumir los recursos de la red. Se instalan en la memoria y desde ahí se reproducen indefinidamente.

El primer gusano informático se lanzó en 1.988 y fue el gusano *Morris*, el cual colapsó a Arpanet infectando a gran parte de los servidores existentes hasta esa fecha. Los gusanos actuales utilizan el correo electrónico mediante el envío de adjuntos que contienen instrucciones para recolectar todas las direcciones de correo electrónico de la libreta de direcciones y enviar copias de ellos mismos a todos los destinatarios. Estos gusanos son scripts o archivos ejecutables enviados como un adjunto. Uno de los más extendidos es el *Conficker*, del cual puedes encontrar información en páginas de microsoft y wikipedia.



Esquema de funcionamiento del gusano Conficker obtenido en la página de Microsof Corporation.

### Curiosidad

Hoy en día, los gusanos informáticos lo tienen fácil, han encontrado en internet su medio ideal de propagación y reproducción en la red. Si buscas en la prensa especializada encontrarás prácticamente a diario noticias relacionadas con programas maliciosos. Te mostramos a continuación un vídeo sobre un gusano que se extendió en MySpace y su creador.

## Programa espía

Son programas maliciosos que se instalan en el ordenador para obtener alguna información con o sin consentimiento del usuario. Se conocen más con la traducción inglesa de su nombre: ***spyware***. Se instalan a través de internet y suelen afectar a la velocidad de transferencia de datos. Se utilizan para diferentes fines, desde empresas publicitarias hasta organismos oficiales. Pueden instalarse a través de troyanos, visitando páginas web o con aplicaciones con licencia shareware o freeware.

Cuando se utilizan con propósitos de mercadotecnia suelen ser el origen de otra plaga como el ***SPAM***. En ocasiones, los programas espías provienen de otro tipo de software denominado ***adware***, que son programas que despliegan publicidad, bien en ventanas emergentes, bien en barras. Cuando incluyen códigos para obtener información de los usuarios, son considerados *spyware*.

A diferencia de los virus, no se traspasan a otros ordenadores por medio de internet o por unidades de almacenamiento masivo. Para eliminarlos se utilizan programas antiespías que además suelen detectar y eliminar otros códigos maliciosos como adware, spybot, spam, etc..

### Autoevaluación

Acabas de ver tres términos nuevos: spyware, adware y SPAM. Dos de ellos los hemos explicado ya, pero ¿qué es el SPAM? ¿cuál es su origen? ¿para qué se utiliza? ¿existen programas anti-SPAM?

Si investigas un poco, encontrarás toda esta información.

## Phishing

El nombre proviene del termino inglés "fishing" que significa "pescando". Se produce cuando se intenta adquirir información confidencial de forma fraudulenta. Se realiza de muchas formas, dependiendo del fin que se quiera conseguir: se puede duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original; se envía información solicitando un número de cuenta porque no ha llegado correctamente el original para obtener datos bancarios o financieros.

Normalmente, se utiliza con fines delictivos enviando SPAM e invitando acceder a la página señuelo. A continuación puedes ver uno gráfico de los caso de phishing por países.

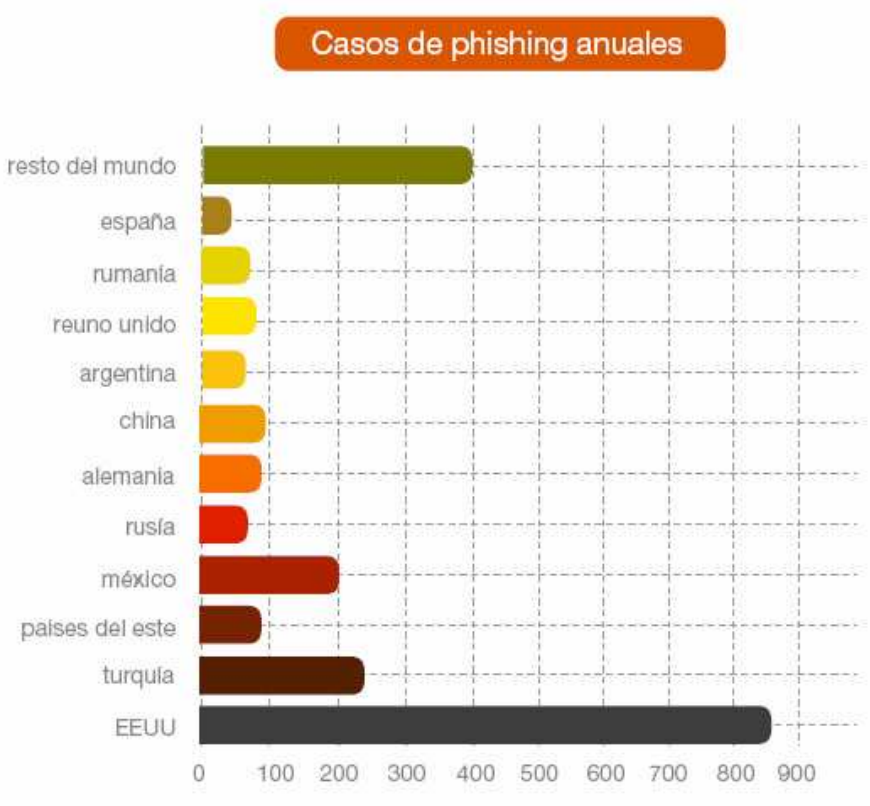



Gráfico obtenido del Informe del Cibercrimen 2.008 realizado por la empresa S21sec.

Imagen de producción propia

## Para saber más

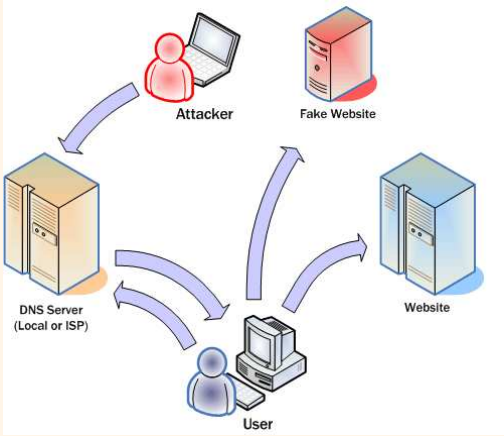
La aparición de malware diferentes es constante, ya que a medida que se producen avances tecnológicos en los ordenadores, también se crean programas maliciosos para atacarlos. La función de este tema no es que seas un experto en seguridad informática, pero si que conozcas los problemas más importantes que se pueden dar y cómo se pueden resolver. Has aprendido los cinco tipos de malware más comunes y más extendidos, pero hay muchos más. A continuación te mostramos algunos de ellos:

El **pharming** es el aprovechamiento de una vulnerabilidad en el software de los servidores DNS que permite a un atacante adquirir el nombre de dominio de un sitio, y redirigir el tráfico de una página Web hacia otra página Web.

Un **Hoax** (del inglés: engaño, bulo) es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Los objetivos del hoax son captar direcciones de correo y saturar la red o los servidores de correo.

Un **Exploit** es un programa o código que "explota" una vulnerabilidad del sistema para aprovechar esta deficiencia en beneficio del creador del mismo. Aunque no es un código malicioso en sí mismo, generalmente se utiliza para otros fines como permitir el acceso a un sistema o como parte de otros malware, es decir, los exploits son utilizados como "componente" de otro malware.

Como su nombre lo indica un **Keylogger** es un programa que registra y graba la pulsación de teclas o los clicks del ratón. Actualmente existen dispositivos de hardware o bien aplicaciones que fucionan como keylogger.




Cómo se hace un pharming

Imagen de producción propia

## Autoevaluación

4) ¿Cuál es el medio más utilizado por un gusano informático para propagarse?

- a) Otros tipos de malware.
- b) Mediante archivos adjuntos a través del correo electrónico.
- c) Ethernet.

5) Un programa espía es aquel que se instala en el ordenador para...

- a) obtener alguna información con o sin consentimiento del usuario.
- b) obtener la licencia de programas.
- c) ver lo que hace el usuario.

6) ¿Cuál es una de las formas más comunes de realizar un phishing?

- a) Grabando la pulsación de las teclas.
- b) Duplicar una página web para hacer creer al usuario que es el sitio oficial.
- c) Poniendo el salvapantallas de peces.

7) ¿Qué tipo de malware es aquel en el que se envía un mensaje de correo electrónico con contenido falso distribuido en cadena?

- a) Keylogger.
- b) Pharming.
- c) Hoax.

# 2. Seguridad de la información


Se entiende por seguridad de la información a las medidas tanto **proactivas** (aquellas que se toman para prevenir un problema) como **reactivas** (aquellas que se toman cuando el daño se produce, para minimizar sus efectos) que se toman por parte de las personas, organizaciones o sistemas tecnológicos.

Su objetivo es resguardar y proteger la **información** buscando siempre mantener la *confidencialidad*, la *disponibilidad* e *integridad* de la misma.

## Confidencialidad

Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado. Implica por tanto la no divulgación de información a personas o sistemas no autorizados.

Cualquier persona, empresa u organización debe velar por la **protección de los datos** sensibles que residen en su sistema.

Una técnica desarrollada para garantizar la confidencialidad es la criptografía:

Se ocupa del cifrado de mensajes para que no pueda ser leído por ningún agente intermedio. El mesaje será cifrado por su emisor y sólo podrá descifrarlo el receptor del mismo.

## Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La tecnología actual facilita la integridad de un mensaje a través de la **firma digital**.

La firma digital sirve para demostrar la autenticidad de un documento electrónico dando al destinatario la seguridad de que fue creado por el remitente, y que no fue alterado durante la transmisión.

Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar tanto la falsificación como la manipulación del documento emitido.

## Disponibilidad

Es la característica de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La criticidad en este sentido viene derivada fundamentalmente de la necesidad de mantener los datos operativos el mayor tiempo posible, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, actualizaciones del sistema u otro tipo de caídas de los servicios.

En este sentido, garantizar la disponibilidad implica también la prevención de ataques del tipo Denegación de servicio _**DoS** (del inglés ***D**enial **o**f **S**ervice*): un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, provocado normalmente por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

### Para saber más

En el marco de las directivas de la Unión Europea, el Estado español ha aprobado un conjunto de medidas legislativas que son de interés para el usuario de Internet:

- Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)
- Ley de Firma Electrónica
- RD sobre el Documento Nacional de Identidad electrónico

## Servicios de seguridad

Para contrarrestar posibles ataques a la seguridad se hace uso de mecanismos y servicios de seguridad estandarizados, entre los que se encuetran el no repudio y la autenticación.

Si la autenticidad prueba quién es el autor de un documento y cual es su destinatario, el "no repudio" prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

### No repudio

Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2.

No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

### Autenticación

Es una validación de identificación de usuarios: técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

Para garantizar la confidencialidad y autenticidad de las comunicaciones entre ciudadanos, empresas u otras instituciones públicas a través de Internet, evitando fraudes y suplantaciones, se han generado mecanismos de seguridad como el Certificado digital y el Documento Nacional de Identidad electrónico (DNIe).

# 3. Sistemas de seguridad informático

**Importante**

Un sistema de seguridad informático es aquel cuyo objetivo es proteger la información, los equipos y los usuarios.

Hoy en día es imposible hablar de un sistema cien por cien seguro, ya que el costo de la seguridad total es muy alto. Sin embargo, es posible controlar una gran parte de la vulnerabilidades acotando aspectos relativos a procedimientos y estrategias. Organizaciones gubernamentales y no gubernamentales internacionales han desarrollado una serie de directrices y recomendaciones sobre el uso adecuado de las nuevas tecnología, evitando el uso indebido de las mismas y obteniendo el máximo aprovechamiento.


La seguridad informática

Imagen de SEGURINFO
Licencia Creative Commons

Surgen así, las llamadas Políticas de Seguridad Informática (PSI) como una herramienta para concienciar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y su seguridad. Hacen referencia también a los equipos que la soportan, incluyendo hardware y software, y a los usuarios que la manejan.

**Para saber más**

Para ampliar la información sobre seguridad y estar al día de las vulnerabilidades más extendidas pueden consultarse las siguientes páginas web:

- Centro de Respuesta a Incidentes en Tecnologías de la Información
- Enciclopedia de seguridad Intypedia

# 3.1. Políticas de seguridad

**Importante**

La política de seguridad define una serie de reglas, procedimientos y prácticas óptimas que aseguren un nivel de seguridad que esté a la altura de las necesidades del sistema.

Se basa, por tanto, en la minimización del riesgo, el cual viene definido por la siguiente ecuación:

$$RIESGO = \frac{AMENAZA \times VULNERABILIDAD}{CONTRAMEDIDAS}$$

En esta ecuación, la amenaza representa el tipo de acción maliciosa, la vulnerabilidad es el grado de exposición a dicha acción y la contramedida es el conjunto de acciones que se implementan para prevenir o evitar la amenaza. La determinación de estos componentes indica el riesgo del sistema.

## Etapas

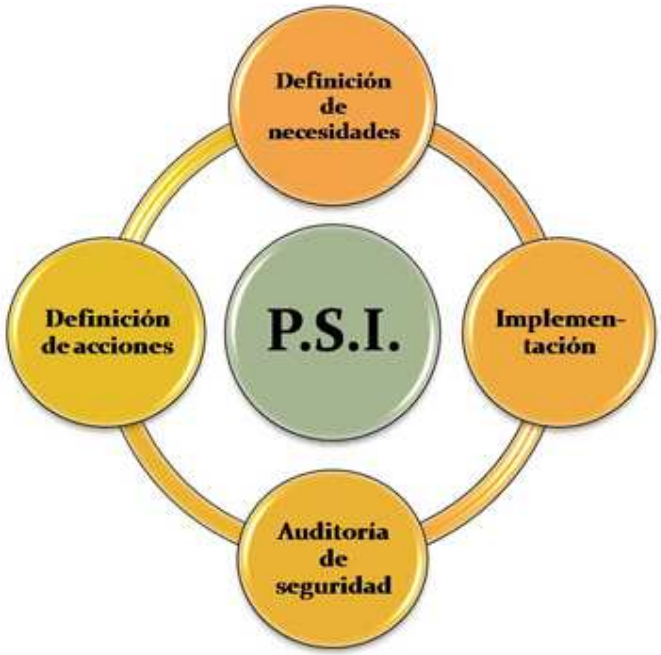
La política de seguridad de un sistema informático se define en cuatro etapas:

La definición de las necesidades de seguridad y de los riesgos informáticos del sistema así como sus posibles consecuencias, es el primer escalón a la hora de establecer una política de seguridad. El objetivo de esta etapa es determinar las necesidades mediante la elaboración de un inventario del sistema, el estudio de los diferentes riesgos y de las posibles amenazas.

La implementación de una política de seguridad consiste en establecer los métodos y mecanismos diseñados para que el sistema de información sea seguro, y aplicar las reglas definidas en la política de seguridad. Los mecanismos más utilizados son los sistemas firewall, los algoritmos criptográficos y la configuración de redes virtuales privadas (VPN). Los estudiaremos en profundidad en el siguiente punto.

Realizar una auditoría de seguridad para validar las medidas de protección adoptadas en el diseño de la política de seguridad. Cuando se trata de compañías, organismos oficiales o grandes redes, suelen realizarlas empresas externas especializadas. También se llama etapa de detección de incidentes, ya que éste es su fin último.

La definición de las acciones a realizar en caso de detectar una amenaza es el resultado final de la política de seguridad. Se trata de pever y planificar una las medidas que han de tomarse cuando surga algún problema. Esta etapa también es conocida como etapa de reacción puesto que es la




Política de seguridad informática

Imagen de producción propia

## Métodos

Para definir una política de seguridad informática se han desarrollado distintos métodos, diferenciándose especialmente por la forma de analizar los riesgos. Algunos de ellos son:

- Método MEHARI *(Método armonizado de análisis de riesgos*), desarrollado por CLUSIF *(Club de la Sécurité de l'Information Français)*, se basa en mantener los riesgos a un nivel convenido mediante un análisis riguroso y una evaluación cuantitativa de los factores de riesgo.
- Método EBIOS *(expresión de las necesidades e identificación de los objetivos de seguridad*), desarrollado por la DCSSI *(Direction Centrale de la Sécurité des Systèmes d'Information,* permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información.
- La norma ISO/IEC 17799 es una guía de buenas prácticas pero no especifica requisitos para establecer un sistema de certificación.
- La norma ISO/IEC 27001 es certificable ya que especifica los requisitos para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad según el PDCA, acrónimo de "plan, do, check, act" (planificar, hacer, verificar, actuar).

### Autoevaluación

Para repasar este punto, te proponemos que completes el siguiente texto con las palabras que faltan. Encontrarás todas las respuestas en los contenidos antes explicados.

Una de las claves de los sistemas de seguridad informáticos es definir una [ ] de seguridad basada en la minimización del [ ] . Para ello, es necesario llevar a cabo [ ] etapas: definición de [ ] , [ ] , [ ] de seguridad y definición de [ ] . Se han desarrollado distintos [ ] para definir una política de seguridad los cuales se diferencian en la forma de [ ] el [ ] .

**Comprobar**

## 3.2. Medios de protección

Chip no entiende cómo ha podido coger la gripe: está vacunado contra un montón de virus, siempre va bien abrigado y tiene una buena higiene. Tantas medidas de protección y no se ha escapado. Es cierto, nunca estamos protegidos al cien por cien de las enfermedades. Lo mismo ocurre con los sistemas informáticos, por muchos medios de protección que se utilicen, nunca se conseguirá una seguridad total.

Ya hemos visto en los puntos anteriores que muchas de las vulnerabilidades de un sistema son debidas a la falta de políticas de seguridad y a problemas ocasionados por los usuarios. A continuación vamos a estudiar los medios más utilizados para evitar o eliminar estas vulnerabilidades.

## Antivirus

Son programas que detectan códigos maliciosos, evitan su activación y propagación y, si es posible, incluso eliminan el daño producido. Se llaman antivirus porque surgieron para eliminar este tipo de malware, pero hoy en día han evolucionado y detectan otros tipos de malware como troyanos, gusanos o espías, y cuentan además con rutinas de recuperación y reconstrucción de archivos dañados.

El funcionamiento de los antivirus se basa en un programa residente que se instala en la memoria del ordenador y analiza cualquier archivo, programa o aplicación mientras está encendido. Para ello, tienen una base de datos actualizada con los códigos maliciosos. Hoy en día, disponen de la función de escaneado para revisar cualquier sistema de almacenamiento interno o externo y también los hay que realizan este análisis desde internet.


Pantalla de detección de virus

Imagen de producción propia

Las técnicas más utilizadas por los antivirus son las siguientes:

- Detección de firma.- cada código malicioso se caracteriza por una cadena de caracteres llamada firma del virus. Los antivirus tienen registradas estas cadenas y las buscan para detectar los virus.
- Búsqueda de excepciones.- se utiliza en el caso de que el virus cambie de cadena cada vez que realiza una infección (virus polimorfos). Son difíciles de buscar, pero hay antivirus especializados.
- Análisis heurístico.- se basa en el análisis del comportamiento de las aplicaciones para detectar una actividad similar a la de un virus ya conocido. Es la única técnica automática de detección de virus.
- Verificación de identidad o vacunación.- el antivirus almacena información de los archivos y, cada vez que se abren, compara esta información con la guardada. Cuando detecta una anomalía, avisa al usuario.

## Actividad de lectura

Hay muchos antivirus en el mercado y es difícil elegir el más adecuado para proteger nuestro ordenador. En la siguiente página web encontrarás una comparativa de los mejores antivirus.

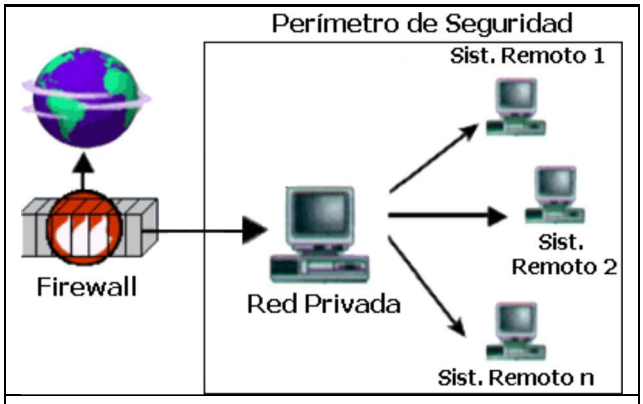
- Comparativa antivirus: pc a salvo
- Comparativa antivirus freeware


Tipos de antivirus

Imagen de producción propia

## Firewall

Un firewall (pared cortafuegos) es un elemento de hardware o software ubicado entre dos redes y que ejerce la una política de seguridad establecida. Protege una red confiable de una que no lo es (por ejemplo, internet) evitando que pueda aprovechar las vulnerabilidades de la red interna.




Funcionamiento del Firewall

Imagen de segu-info.com

Licencia Creative Commons

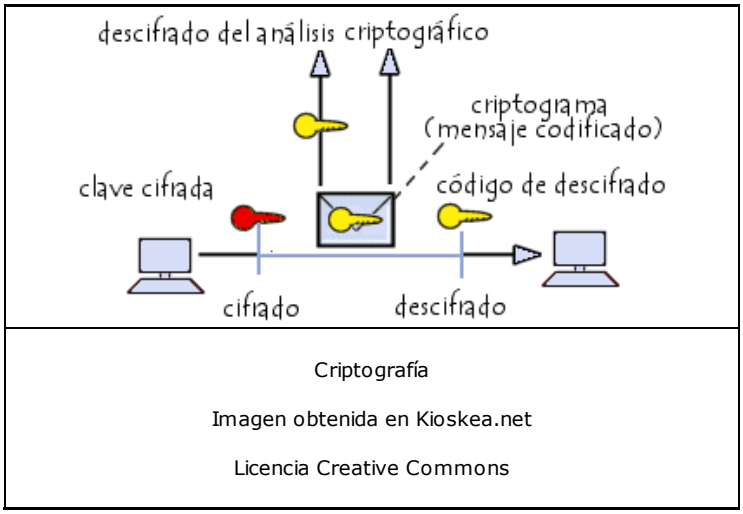
El uso de firewall se ha convertido en algo fundamental ya que es el elemento que controla el acceso entre dos redes y, si no existiera, todos los ordenadores de la red estarían expuestos a ataques desde el exterior.

Sin embargo, el firewall no es un sistema inteligente ya que actúa según los parámetros establecidos y si un paquete de información no está definido dentro de estos parámetros como código malicioso, lo deja pasar. Normalmente se suele complementar con otro medio de protección, por ejemplo un antivirus, ya que no contiene herramientas para filtrar los virus.

Existen muchos tipos de firewall (filtrado de paquetes, servidor proxy-gateway, personales) y su elección dependerá de las limitaciones y capacidades del sistema por un lado, y de las vulnerabilidades y las amenazas de la red externa por otro.

## Criptografía

Cómo ya hemos visto en un vídeo anterior, la criptografía es una ciencia utilizada desde la antigüedad que consiste en transformar un mensaje inteligible en otro que no lo es utilizando claves que sólo el emisor y el destinatario conocen, para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

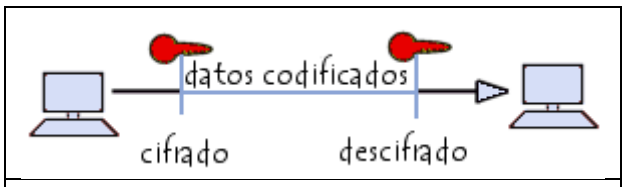



Criptografía

Imagen obtenida en Kioskea.net

Licencia Creative Commons

La criptografía simétrica permite establecer una comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado una clave llamada "clave simétrica" que se utiliza para cifrar y para descifrar.




Criptografía simétrica

Imagen obtenida en Kioskea.net

Licencia Creative Commons

La criptografía tiene en la actualidad multitud de aplicaciones en informática, entre las cuales destacan las siguientes:

- Seguridad de las comunicaciones.- permite establecer canales seguros sobre redes que no lo son.
- Identificación y autentificación.- se emplean las firmas digitales y otras técnicas criptográficas para garantizar la autenticidad del remitente y verificar la integridad del mensaje recibido.
- Certificación.- se basa en la validación por agentes fiables (como una entidad certificadora) de la identidad de agentes desconocidos.
- Comercio electrónico.- es un sistema muy utilizado ya que reduce el riesgo de fraudes, estafas y robos en operaciones realizadas a través de internet.

## Antiespías

Son programas diseñados para detectar, detener y eliminar los códigos maliciosos de programas espías (spyware). A veces, vienen incluidos en los antivirus, pero son más efectivos los diseñados específicamente para eliminar este tipo de malware.

Al igual que los antivirus, es necesario que el módulo residente esté activado para detectar el código malicioso antes de que se instale en el sistema. También es importante mantener actualizadas las bases de códigos.


Programas antiespías

Imagen de producción propia

### Curiosidad

**¡OJO CON LOS ANTI…!**

Los creadores de malware no paran nunca. Lo último ha sido utilizar los medios de protección para acceder a los sistemas. De este modo, han aparecido en internet cantidad de antivirus y antiestpías que en realidad son otro tipo de malware.

En las siguientes páginas web puedes encontrar listas actualizadas de dichos programas.

Antivirus falsos

Antiespías falsos

## Autoevaluación

Para conocer los medios de protección de los sistemas informáticos lo mejor es utilizarlos. Pero esta será tu tarea en este tema. Ahora, te proponemos que contestes a las siguientes preguntas sobre ellos. Encontrarás las respuestas en el contenido de este punto del tema.

1. Los antivirus son programas que detectan virus y evitan su activación y propagación.

Verdadero ○ Falso ○

2. El análisis heurístico consiste en la detección de la "firma del virus".

Verdadero ○ Falso ○

3. Un firewall es una medida de seguridad física para evitar incendios en los equipos informáticos.

Verdadero ○ Falso ○

4. La criptografía simétrica utiliza la misma clave para cifrar y descifrar una información.

Verdadero ○ Falso ○

5. Uno de los métodos para verificar la autenticidad de un mensaje en la firma digital.

Verdadero ○ Falso ○

6. Los antiespías son programas que utilizan una webcam para vigilar la información del ordenador.

Verdadero ○ Falso ○