

TEMA 4: Seguridad informática.

Conceptos

1. Concepto de seguridad informática.
2. Tipos de amenazas.
3. Medidas de seguridad.
4. Virus y malware.
5. Antivirus y cortafuegos.
6. Copias de seguridad.
7. Seguridad en Internet.
8. Protección de la intimidad.
9. La ingeniería social y la seguridad informática.
10. Protección de la información.

Actividades

Actividades de introducción.

1. Los virus afectan, sobre todo, al sistema operativo Windows, y no a Linux, por lo que la mayoría de los sistemas de protección están desarrollados para Windows. Según esto, ¿es Linux más seguro que Windows?, ¿cuál es la razón/es para que no haya virus en Linux?

Respuesta: Efectivamente, hasta el momento Linux no es objetivo de virus y atacantes. Además, este sistema operativo se caracteriza por ser bastante estable, fiable y seguro, por lo que es posible tenerlo sin ningún tipo de antivirus, antispyware, etc., instalados y estar tranquilos. No obstante, Linux corre los mismos riesgos de perder la información por errores en software y hardware que cualquier otro sistema operativo, por eso hay que realizar obligatoriamente copias de seguridad.

2. Si te descuidas y bajas la guardia, tu ordenador corre el riesgo de convertirse en un coladero para hackers y troyanos. ¿Qué programas te ayudan a protegerte de ellos?, ¿tienes alguno instalado en tu equipo?

Respuesta: La solución es tener instalado un firewall. Este programa impide el acceso no autorizado a tu ordenador o a la red. Windows ya lleva un firewall instalado y algunos antivirus dan la opción de instalar el suyo propio.

3. Es fundamental realizar con regularidad tareas de mantenimiento del equipo. Hay que instalar actualizaciones, analizarlo en busca de virus, realizar copias de seguridad, etc. ¿Cuál es la última copia de seguridad de tus datos que has realizado?

Respuesta: Por descuido o pereza, la mayoría de usuarios no realizan ningún tipo de copia de seguridad de sus archivos, o lo hacen con muy poca frecuencia. Un fallo en el equipo o una infección por virus puede provocar la pérdida de información de meses o años de trabajo.

4. Además de los virus informáticos, los troyanos y otros programas maliciosos, los ordenadores corren otros riesgos. ¿A qué otras amenazas está expuesto tu ordenador?

Respuesta: Las amenazas pueden ser:

- De otras personas: hacker, cracker, etc.
- A nivel de software: virus, malware o bugs.
- A nivel de hardware: con todo tipo de fallos.

5. Los piratas informáticos desarrollan constantemente nuevos medios, tanto técnicos como psicológicos, para conseguir sus objetivos. Uno de estos métodos es la llamada ingeniería social. ¿Sabes en qué consiste?

Respuesta: El concepto de ingeniería social aplicado a la informática hace referencia a todas aquellas conductas que permiten obtener información confidencial de otras personas, sin que éstas se den cuenta de que la están revelando.

6. Para evitar que la información que viaja a través de internet sea conocida por otras personas, es necesario utilizar métodos de cifrado. ¿En qué consiste el método de encriptación en clave pública y clave privada?

Respuesta: Las claves privada y pública se basan en el cifrado de la información utilizando algoritmos matemáticos. El emisor cifra el mensaje con la clave pública del destinatario, éste descifrará el mensaje con su clave privada, que únicamente conoce él.

1. **Concepto de seguridad informática.**

Se entiende como **seguridad informática**, la característica de cualquier sistema informático que indica que está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esto es muy difícil de conseguir, en lugar de hablar de seguridad, se habla de **fiabilidad**, como probabilidad de que un sistema se comporte tal y como se espera de él. Así pues se habla de sistemas fiables y no de sistemas seguros.

La seguridad persigue tres objetivos básicos:

- **Confidencialidad:** garantiza que la información sea accesible exclusivamente a aquellas personas autorizadas.
- **Integridad:** protege la exactitud y totalidad de la información y sus métodos de proceso.
- **Disponibilidad:** garantiza a los usuarios autorizados acceso a la información y recursos.

Los tres elementos principales a proteger en cualquier sistema informático son:

- **Hardware:** puede verse afectado por caídas de tensión, averías, etc.
- **Software:** al que pueden afectar virus,...
- **DATOS:** sin duda el más importante ya que si una máquina se rompe se puede comprar otra y si un programa deja de funcionar correctamente puede reinstalarse, pero si se pierden datos como documentos, fotografías, etc., sólo se recuperarán si se ha realizado previamente una copia de seguridad.

2. Tipos de amenazas.

Los elementos que pueden amenazar a un sistema informático son:

- **PERSONAS:** La mayoría de ataques van a provenir de personas que, intencionada o accidentalmente, pueden causar grandes pérdidas. Pueden darse dos tipos de ataques.
 - **Pasivos:** aquellos que fisgonean el sistema pero no lo modifican ni lo destruyen. Suelen ser:
 - **Accidentes del personal.** Ejemplo: un empleado de mantenimiento que corta el suministro eléctrico.
 - **Curiosos, estudiantes o personal:** intentan conseguir mayores privilegios que los que tienen intentando acceder a sistemas a los que oficialmente no tienen acceso. Ejemplo: leer el correo de un amigo, enterarse de cuánto cobra un compañero, etc.
 - **Hackers:** intrusos que pueden acceder al sistema sin permiso para practicar, por desafío, diversión, etc., pero un hacker no es un delincuente informático (pese al empeño de los medios de comunicación y películas). Un hacker es alguien con muchos conocimientos informáticos que le colocan en la cúspide de la pirámide tecnológica. Lo que haga con ese conocimiento, no tiene que ser necesariamente malo o ilegal aunque el sólo hecho de acceder sin permiso puede ser constitutivo de delito (comentar caso EEUU).
 - **Activos:** aquellos que dañan a su objetivo o lo modifican en su favor.
 - **Crackers:** atacan el sistema con el único fin de provocar daños.
 - **Antiguos empleados:** aprovechan debilidades de un sistema que conocen perfectamente para dañarlo por venganza.
 - **Piratas informáticos:** trabajan a sueldo a cambio de robar material confidencial, dañar la imagen, etc.
 - **AMENAZAS LÓGICAS:** son programas que pueden dañar el sistema. Pueden ser:
 - **Intencionadas:**
 - **Virus y malware.**
 - **Herramientas de seguridad:** utilizadas para detectar fallos y aprovecharlos para atacar.
 - **Puertas traseras:** accesos no autorizados aprovechando backdoors que se crean durante el desarrollo de aplicaciones grandes o de sistemas operativos para facilitar el mantenimiento posterior y que son descubiertas por los atacantes (como una puerta de servicio en un piso).
 - **Software incorrecto:** los bugs (agujeros, fallos) provienen de errores cometidos de forma involuntaria por los programadores de sistemas o aplicaciones (comentar la importancia que tienen las versiones alfa y beta).
 - **AMENAZAS FÍSICAS:** pueden darse por fallos en los dispositivos (fallo de discos, de cableado, de suministro de energía, etc.) o por catástrofes naturales (terremotos, inundaciones...).
1. La página web: <http://alerta-antivirus.es>, informa de manera permanente de las últimas amenazas. Esta página recoge, además, una recopilación de herramientas gratuitas que son útiles para la prevención de ataques e infecciones. Visita la página y anota los nombres y porcentajes de incidencias de los 5 virus más activos en las últimas 24 horas. ¿Qué zonas de España presentan mayores porcentajes?,

3. **Medidas de seguridad.**

Las medidas de seguridad evitan o previenen de las amenazas y los ataques contra los recursos de la red y preservan la privacidad de los usuarios. Se dividen en tres grandes grupos:

- **PREVENCIÓN:** tratan de aumentar la seguridad de un sistema durante su funcionamiento normal, para prevenir que se produzcan violaciones a la seguridad. Los mecanismos de prevención más habituales son:
 - **Contraseñas:** el usuario ha de introducir una contraseña para acceder a recursos.
 - **Permisos de acceso:** establecen a qué recursos puede acceder un usuario y qué permisos tienen los usuarios sobre los recursos (lectura, ejecución, escritura, etc.). Estos permisos se suelen gestionar en el S.O. a través de grupos.
 - **Seguridad en las comunicaciones:** se utilizan mecanismos basados en la criptografía (cifrado de contraseñas y firmas digitales) para garantizar la seguridad y privacidad de los datos cuando se transmiten a través de la red.
 - **Actualizaciones:** tener un S.O. correctamente actualizado es una garantía para el correcto y eficiente funcionamiento del sistema. Igualmente sucede con el resto del software, especialmente con el relacionado con la seguridad.
 - **S.A.I. (Sistema de Alimentación Ininterrumpida):** dispositivo que gracias a una batería puede proporcionar energía en caso de fallo en el suministro eléctrico. Además mejora la calidad de la señal eléctrica evitando las subidas y bajadas de tensión que podrían ocasionar daños en el sistema informático.
 - **DETECCIÓN:** se emplean herramientas específicas para cada tipo de amenaza como antivirus, firewalls, antispyware, etc.
 - **RECUPERACIÓN:** Se aplica cuando ya se ha producido alguna alteración del sistema por cualquiera de las causas expuestas anteriormente para restaurar el sistema a su correcto funcionamiento. En redes sensibles se emplean métodos como duplicación de datos en la red, etc. En pequeñas redes y ordenadores personales la medida imprescindible a adoptar con las backups.
1. Analiza lo expuesto en este apartado con el objeto de comprobar el grado de cumplimiento de estas medidas básicas de seguridad informática.

4. Virus y malware.

La palabra **malware** proviene de la contracción de las palabras *malicious* y *software*. Así, el malware es cualquier programa o mensaje que pueda resultar perjudicial para un ordenador, tanto por causar pérdida de datos como por pérdida de productividad.

Clasificación de malware:

Nombre	Descripción	Solución
Virus Gusanos Troyanos Backdoors Sniffer	Programas habitualmente ocultos dentro de otros programas, emails, ficheros, etc. Se ejecutan automáticamente, haciendo copias de sí mismo dentro de los programas a los que infectan. Dependiendo del modo en que atacan y se propagan reciben distintos nombres.	Antivirus
Adware Pop-ups	Software que despliega publicidad de distintos productos o servicios. Utilizan ventanas emergentes o barras que aparecen en la pantalla.	Antivirus
Intrusos Hackers Crackers Keylogger Phone Fhreaker	Utilizan herramientas de hacking para poder acceder a un ordenador desde otro equipo, obtener información confidencial, lanzar ataques, etc. Según el tipo tendrán distintos objetivos y serán más o menos dañinos.	Firewalls
Spam	Correo basura no solicitado con el que se bombardean los emails y que suelen estar relacionados con publicidad.	Anti-spam
Spyware	Software que, de forma encubierta, utiliza la conexión a internet para extraer datos e información sobre el contenido del ordenador, páginas visitadas, programas, etc.	Anti-spyware
Dialers	Cuelgan la conexión telefónica utilizada y establecen otra utilizando una conexión de tarificación especial, que se reflejará en la factura telefónica	Anti-dialers
Bugs Exploits	Errores de programación que pueden provocar daños en la información. También códigos que se aprovechan de las vulnerabilidades del software para lanzar ataques de forma automática y sin la intervención del usuario.	Actualización del software
Jokes Hoaxes	No son virus sino mensajes con falsas advertencias de virus, o de cualquier otro tipo de alerta o de cadena distribuida por correo electrónico (comentar graves perjuicios económicos en caso de empresas cotizadas en bolsa, etc.).	Ignorarlos y borrarlos

5. Antivirus y cortafuegos.

1. Puede que tras lo expuesto en el apartado anterior algunos piensen que la situación no es tan grave y que si se tiene un buen antivirus se está a salvo. Pues bien, vamos a demostrarlo con un ejercicio práctico. Consiste en llevar a cabo una serie de acciones que serían necesarias en el caso de existir alguna infección grave y que podría solucionar el problema. Aún así, algunas infecciones son tan maliciosas, que habría que recurrir a métodos más exhaustivos o herramientas específicas pero con esto tendremos bastante para cubrir nuestros objetivos. Será necesario instalar algunos programas (todos ellos gratuitos) y llevar a cabo una serie de pasos ordenados. El documento en el que se explican dichos pasos se puede encontrar en la web indicada por el profesor y se deberán enviar el correo del profesor capturas de pantalla con algunos de los resultados tras los análisis (borrando previamente con un programa de dibujo como el Paint cualquier dato sensible o personal y guardando la imagen en formato jpg para que ocupe el mínimo espacio).

Un antivirus es un programa que detecta, bloquea y elimina malware. Aunque se sigue empleando la palabra antivirus, estos programas han evolucionado y son capaces de detectar y eliminar, no solo virus, sino también otros tipos de códigos maliciosos como gusanos, troyanos, espías, etc.

Para ello, el antivirus compara el código de cada archivo con una base de datos en la que dispone de datos de los códigos de los virus conocidos. Es lo que se conoce como "firmas o definiciones de virus" y es imprescindible actualizarla periódicamente (idealmente cada vez que accedamos a internet). Ejemplos: Karpesky, McAfee, Norton, Panda, Nod32, Antivir, Spyware Doctor, etc.

La mayoría de los sitios web oficiales de las empresas dedicadas a comercializar antivirus disponen de la opción de chequeo on-line gratuito, algunas incluso permiten eliminarlo (comentar cuales).

Un cortafuegos o firewall es un programa o dispositivo hardware que se utiliza para controlar las comunicaciones e impedir accesos no autorizados a un ordenador o a una red. Para ello, filtra los datos de la conexión, dejando pasar sólo los que están autorizados.

Mientras se trabaja en red, se produce una continua entrada y salida de datos por lo que los intrusos pueden utilizar estos datos para colarse en el ordenador.

Algunos sistemas operativos como Windows incluyen su propio cortafuegos aunque es posible instalar alguno específico.

2. ¿Por qué es peligroso tener un puerto abierto?, ¿piensa si utilizas programas que requieran alguna medida así?, sería interesante que utilizases alguna herramienta que te permitiese averiguar si qué puertos tienes abiertos en tu equipo (ver herramientas de la página de alerta antivirus).

6. Copias de seguridad.

Las copias de seguridad o backups son copias de todos los datos que nos permitirán recuperar la información original en caso de ser necesario. Para realizarlas se utilizan dispositivos externos de almacenamiento: DVD, disco duro externo, cinta, etc...

Lo más sencillo es llevar a cabo una planificación periódica de copias de seguridad. Cuanto más reciente sea la copia, menor será la pérdida de datos. Se aconseja:

- Copia semanal de los archivos nuevos y con los que se ha trabajado recientemente.
- Copia mensual o trimestral de toda la información del equipo.

El usuario es quien determina los elementos a copiar. Se realizan solamente de los datos no de los programas. De modo general, suelen incluir:

- Carpetas y archivos del usuario.
- Favoritos.
- Correo electrónico.
- Otra información relevante: certificados digitales, agenda de direcciones, etc.

Para realizar estas copias se pueden utilizar herramientas específicas que proporciona el mismo S.O. (ver Centro de copias de seguridad y restauración), programas específicos o incluso copiar la información deseada en el soporte de almacenamiento. El uso de herramientas facilita la tarea automatizando el proceso. El inconveniente es que para restaurar la información necesitaríamos disponer de dicha herramienta mientras que utilizando una copia directa sería accesible desde cualquier equipo.

7. Seguridad en Internet.

El email es una de las mayores fuentes de virus aunque se debe en la mayoría de los casos a imprudencias o malas prácticas del usuario que podrían evitarse siguiendo unos sencillos consejos: no se deben ejecutar ficheros, abrir presentaciones, ver vídeos, abrir fotos, etc. Si no se conoce al remitente. Cuidado que sin abrir ningún archivo adjunto podrían infectarnos si, como la mayoría de los usuarios, tenemos activada la vista previa de los mensajes o la descarga automática de las imágenes que contenga. Los buenos antivirus, realizan análisis en tiempo real y analizan el correo entrante y saliente.

Algunos ejemplos de emails peligrosos son: mensajes simulando proceder de entidades bancarias (técnicas de phishing); email que contienen cadenas solidarias de ayuda o denuncia y que acumulan miles de direcciones con ánimo de lucro; mensajes con archivos como fondos de pantallas, imágenes, programas, etc. de usuarios desconocidos; premios, bonos descuento, viajes regalados, etc.

Las cookies (galletas) son sencillos ficheros de texto que se graban en el ordenador al navegar por la red. Recopilan datos de acceso del usuario como su nombre, contraseña, dirección, etc., y quedan guardados para que éste no tenga que volver a introducirlos al navegar y que así, las páginas se carguen más rápido. No pueden considerarse maliciosos pero no conviene almacenarlos. Consejo: configurar navegador para que los elimine cada vez que lo cerremos y ejecutar periódicamente un limpiador.

La criptografía se utiliza para proteger la información enviada a través de internet. Algunas de las ocasiones en que se emplea son:

- Cuando se navega por páginas seguras tipo https://...
- Al utilizar certificados digitales.
- Si se encripta el correo electrónico.
- Cuando los usuarios se identifican con firmas electrónicas.

En las redes WIFI la información se transmite utilizando ondas de radio por lo que hay que tomar medidas de seguridad adecuadas:

- Se debe cambiar la contraseña por defecto de acceso a la administración del router.
- Usar encriptación WEP/WPA. La clave se codifica utilizando 64 bits, 128 bits, etc.
- Para los usuarios más avanzados existen medidas más restrictivas como activar el filtrado de direcciones MAC, desactivar el DHCP, etc.

1. Busca en internet en qué consiste la biometría y haz un listado de cinco situaciones en las que podría aplicarse. Busca también el significado de "discos RAID".

RESPUESTA: La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para "verificar" identidades o para "identificar" individuos.

En las tecnologías de la información (TI), la autenticación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autenticación.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

En informática, el acrónimo RAID (originalmente del inglés Redundant Array of Inexpensive Disks, 'conjunto redundante de discos baratos', en la actualidad también de Redundant Array of Independent Disks, 'conjunto redundante de discos independientes') hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor throughput (rendimiento) y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.

En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAIDs suelen usarse en servidores y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad. Debido al decremento en el precio de los discos duros y la mayor disponibilidad de las opciones RAID incluidas en los chipsets de las placas base, los RAIDs se encuentran también como opción en los ordenadores personales más avanzados. Esto es especialmente frecuente en los computadores dedicados a tareas intensivas de almacenamiento, como edición de audio y vídeo.

8. Protección de la intimidad.

¿QUEDAN IMPUNES LOS DELINCUENTES INFORMÁTICOS? Aunque la dirección IP con la que se accede a la red sea dinámica y cambie cada vez que se accede a internet, el proveedor conoce y mantiene un fichero de quién y a dónde se conecta cada equipo por lo que a partir de una dirección IP es posible identificar al usuario y comunicarlo a la autoridad competente ante un requerimiento judicial.

Los datos personales forman parte de la intimidad de las personas. La mayoría de los países poseen sus propias normativas pero es necesario un marco legal internacional dado el carácter mundial de internet.

Normativa de la U.E.

- Los datos deben recopilarse con fines claros y lícitos y nunca deben ser excesivos en relación con los fines para los que se vayan a emplear.
- Los datos deberán ser exactos y, cuando sea necesario, estar actualizados.
- Los responsables del tratamiento deberán proporcionar a los interesados medidas razonables que les permitan rectificar o suprimir los datos incorrectos sobre su persona.
- Los datos de identificación no se deberán mantener un periodo de tiempo superior al necesario.
- Los estados de la Unión Europea designarán una o varias autoridades de control que vigilen la aplicación de estas medidas.
- En principio, todos los responsables del tratamiento de datos han de notificar a las autoridades de control si están tratando datos.
- Los estados miembros podrán solicitar controles previos, que deberá realizar la autoridad de control, antes de que se inicien tratamientos que puedan suponer riesgos específicos.

1. ¿Crees que no tener malas intenciones justifica o exime de responsabilidad legal intentar invadir la intimidad de otra persona?

9. La ingeniería social y la seguridad informática.

Aplicado a la informática, el significado del término ingeniería social hace referencia a todas aquellas conductas que permiten obtener información confidencial de otras personas manipulándolas para que no se den cuenta de que están revelándola.

Por razones de seguridad, nunca mejor dicho, evitaré comentar las estrategias existentes aunque sí comentaré las que permiten prevenir o evitar los ataques.

Estrategias de la ingeniería social (sólo las más sencillas, excluyendo seguimientos, etc.):

- **ELIMINADO**

Estrategias para prevenir o evitar los ataques:

- Comprobar la autenticidad de las personas que soliciten información.
- Analizar convenientemente el correo antes de abrirlo.
- No responder a solicitudes de información personal a través de email (las empresas fiables nunca solicitan contraseñas, números de tarjetas, etc. por este medio).
- Nunca ejecutar un programa de procedencia desconocida.
- Nunca se debe tirar documentación sensible sin destruirla previamente.

Consejos para la elección de contraseñas:

- Deben ser fáciles de recordar para nosotros pero difícil de adivinar a otras personas.
- Debe ser larga, mínimo 8 caracteres aunque lo ideal es que tenga 14 o más.
- Deben ser alfanuméricas e incluso que combine minúsculas o mayúsculas y utilizando caracteres diversos.
- Evitar utilizar secuencias de números o letras ni caracteres repetidos. Tampoco conviene emplear nombres o datos relacionados con nuestra persona.

10. Protección de la información.

Ya hemos comentado lo que significa el término encriptación.

La forma de proteger la información transmitida a través de internet, es utilizar **métodos de cifrado**. El método más sencillo es que emisor y receptor tengan conocimiento de una clave para poder cifrar/descifrar el mensaje. Pero si una de las partes revela o pierde la clave, compromete a ambos y además, no puede emplearse cuando la operación se realiza entre personas o empresas que no han tenido una relación previa.

Para solucionar este problema se emplea un sistema de cifrado con dos claves: una **pública** y una **privada**. La primera puede enviarse a cualquier persona (incluso hay servidores en los que estas claves están disponibles) pero la segunda sólo la conoce su dueño y nunca debe ser revelada. Ambas claves están coordinadas.

Las claves se obtienen mediante operaciones matemáticas sencillas de realizar en un sentido pero complejas en el contrario (descomposición factorial del producto de dos números muy altos; comentar la importancia de ordenadores cuánticos, etc.)



La **firma digital** es un método criptográfico que asegura la identidad del remitente de un mensaje. Puede ser de tres tipos:

- **Simple:** sirve para identificar al firmante.
- **Avanzada:** además garantiza que el mensaje no se ha modificado durante su recorrido.
- **Reconocida:** además está garantizada por un certificado digital emitido por un organismo reconocido.

Dado que las claves públicas no garantizan que la persona que envía la clave pública sea la persona a la que realmente le pertenece, la autoridad de certificación se encarga de emitir un certificado digital, que garantiza que la clave pública enviada realmente pertenece a la persona o entidad que la envía.

Cualquiera puede emitir un certificado digital pero sería inútil si no está reconocido por las autoridades pertinentes, en España, el Ministerio de Industria, Comercio y Turismo. Aplicaciones de los certificados digitales: contratos comerciales electrónicos, factura electrónica, transacciones comerciales electrónicas, invitación electrónica, dinero electrónico, notificaciones judiciales electrónicas, voto electrónico, etc.

Acceso fácil | Mapa del Sitio | RSS

Alerta-Antivirus

Centro de Alerta Temprana sobre Virus y Seguridad Informática

Virus más extendidos: últimas 24h

Mapa	Nombre	Incidencias
	Netsky.Q	(32.9 %)
	MIME_Overflow	(30.7 %)
	Renos.AIG	(18.4 %)
	Netsky.P	(13.1 %)
	Spy.AT	(1.6 %)

Muestra: 118.818.175 - Detecciones: 132.106 (0.1 %)

[Estadísticas detalladas...](#)

Últimos virus encontrados

Nombre	Peligrosidad	Fecha
Agent.czj	1 - Mínima	10/09/2008 21:26
OnLineG.BC	1 - Mínima	10/09/2008 13:29
Losabel.K	1 - Mínima	10/09/2008 07:14
Tibs.KMN	1 - Mínima	09/09/2008 20:41
Agent.HOQ	1 - Mínima	09/09/2008 10:55

[Más virus...](#)

Boletines de Seguridad MS - Septiembre 2008

Microsoft ha publicado cuatro nuevos Boletines de Seguridad en Septiembre (en inglés), que proporcionan parches para vulnerabilidades descubiertas recientemente.

- MS08-052: **Critica** (Microsoft Windows GDI+)
- MS08-053: **Critica** (Windows Media Encoder 9)
- MS08-054: **Critica** (Windows Media Player 11)
- MS08-055: **Critica** (Microsoft Office)

Instale en su equipo aquellos parches que sean de aplicación al software que utiliza en su sistema.

Para mantener la seguridad de su sistema recomendamos a todos los usuarios de Windows que visiten el sitio web de **Windows Update** (para actualizaciones automáticas).

Nuevo Portal del proyecto: Impulso a la Implantación y Certificación de SGSI en

Acceso fácil | Mapa del Sitio | RSS

Alerta-Antivirus

Centro de Alerta Temprana sobre Virus y Seguridad Informática

Índice

- Antivirus Gratuitos
- Cortafuegos gratuitos
- Escaneadores de Puertos
- Mata-Emergentes (popup-killers)
- Anti-Marcadores (anti-dialers)
- Herramientas de Desinfección
- Anti-espías (Anti-spyware)
- Anti-Spam
- Copias de Seguridad
- Test de Velocidad
- Anti Fraude
- Herramientas Avanzadas
- Control Parental
- Análisis de ficheros
- Herramientas Test
- Análisis URLs

Antivirus Gratuitos

Un antivirus es un programa informático específicamente diseñado para detectar bloquear y eliminar códigos maliciosos.

Aunque se sigue utilizando la palabra antivirus, estos programas han evolucionado y son capaces de detectar y eliminar, no sólo virus, sino también otros tipos de códigos maliciosos como gusanos, troyanos, espías...

Los antivirus detectan que un programa es malicioso empleando diferentes técnicas, las más comunes están indicadas en el siguiente artículo: [técnicas antivirus](#).

En el listado de antivirus, ofrecemos dos tipos de antivirus diferentes, los de escritorio y en línea.

Los antivirus de escritorio se suelen utilizar en modo residente para proteger al ordenador en todo momento de cualquier posible infección, ya sea al navegar por Internet, recibir algún correo infectado o introducir en el equipo algún dispositivo extraíble que esté infectado. No necesitan que el ordenador esté conectado a Internet para poder funcionar, pero sí que es necesario actualizarlos frecuentemente para que sean capaces de detectar las últimas amenazas de virus. Desde INTECO-CERT recomendamos tener sólo un antivirus de escritorio en el ordenador, ya que tener varios antivirus puede ocasionar problemas de incompatibilidad entre ellos.

Por otro lado, los antivirus en línea son útiles para analizar el ordenador con un segundo antivirus cuando sospechamos que el equipo puede estar infectado. Para ejecutarlos es necesario acceder con el navegador a una página de Internet. Si bien son muy útiles para realizar un escaneo del ordenador y, de este modo, comprobar que no está infectado, no sirven para prevenir infecciones, esto sólo lo hacen los antivirus de escritorio.

Si está buscando una solución rápida para una infección, visite nuestra página de [Herramientas Gratuitas de Desinfección](#), donde encontrará programas de varios fabricantes de antivirus que eliminan los virus más comunes.

Antivirus de escritorio

En inglés



Grisoft ofrece **AVG Antivirus Free edition** un antivirus completo para pc de escritorio, con las funciones habituales de protección residente, exploración de correo electrónico y actualización periódica de los patrones de virus. Es *gratuito sólo para usuarios domésticos*.

Plataformas: Windows 98/2000/NT/XP/Vista.



La empresa alemana Avira GmbH ofrece **Avira Antivir Personal Edition**, un antivirus de escritorio gratuito para fines personales. Incluye escudo residente, detección de virus de macro y asistente de actualización. Disponible en Inglés y en Alemán.

Plataformas: Windows 98/2000/NT/XP/Vista.



Clam Antivirus es un escáner anti-virus escrito desde cero. Se distribuye con licencia GNU GPL2 (gratuito, código abierto). Está escrito en C y cumple con la norma POSIX. Funciona en múltiples arquitecturas como Intel, Alpha, Sparc, Cobalt MIPS boxes, PowerPC, RISC 6000. En Linux se puede correr como un demonio, proporcionando protección permante.

Instalación algo compleja.

Plataformas: Linux, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, Mac OS X, y en Windows (98/2000/NT/XP) con Cygwin B20.



BitDefender Free Edition v8, antivirus para ordenadores con S.O. Windows con todas las funciones habituales excepto el servicio de protección residente. Esto implica que el usuario debe explorar manualmente cualquier archivo sospechoso (basta con hacer clic derecho con el ratón sobre el archivo y seleccionar la opción de exploración con el antivirus).

Plataformas: Windows 98/2000/NT/XP.






Alwil Software ofrece la versión doméstica de su antivirus, **Avast Home**, gratuito para *uso doméstico sin ánimo de lucro*. Está disponible en español, aunque en la versión analizada aquí, la ayuda en línea estaba en inglés. Dispone de protección residente, y su característica más relevante es que el filtrado de correo electrónico es independiente del cliente de correo, ya que implementa un servidor de correo SMTP, donde realiza la exploración el correo. Simplemente hay que configurar cliente de correo para que use como servidor de correo entrante y saliente el del antivirus. Como curiosidad, dispone de un interfaz personalizable mediante pieles (*skins*).

Plataformas: Windows 98/2000/NT/XP/Vista.



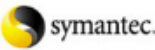

Antivirus en Línea

Estos antivirus no se instalan en el PC como un programa convencional, sino que se accede mediante un navegador web. El tiempo de escaneo varía en función de la velocidad de su conexión, la carga momentánea de los servidores o el volumen de datos que usted quiera rastrear. La mayoría de estos servicios descargan un subprograma (ActiveX o Java), por lo que la primera vez que se accede tardan unos minutos en arrancar.

En español

	Descarga un control ActiveX y realiza el escaneo, desinfección y eliminación de virus, gusanos y troyanos por todas las unidades del sistema, incluyendo los ficheros comprimidos y el correo electrónico y realiza la detección de software espía. Es actualizado diariamente.
	Utiliza un applet de Java, lo que permite que sea soportado por todos los navegadores. Presenta una estructura de árbol de directorios con las unidades del sistema, para escoger aquellas de las que se desea realizar el escaneo de virus. La página de descarga de Internet está en inglés, pero el producto está en castellano y tiene incorporada una herramienta de chequeo de puertos.
	Tras aceptar la descarga de un control ActiveX, comienza el escaneo de la parte del sistema elegida: unidad de disco duro, directorio "Mis documentos" o ficheros de Windows. Al finalizar el proceso, se muestra un listado con los ficheros infectados y el virus que los afecta.

En inglés

	Tras la descarga de un subprograma ActiveX, se puede seleccionar las opciones de configuración del análisis del sistema, permite escanear la memoria de su sistema, todos los archivos, carpetas, discos y sectores de arranque, ofreciéndole no sólo la opción de detectar infecciones, sino también de desinfectar o, incluso, eliminar los archivos infectados.
	Tras la instalación de unos ficheros, nos ofrece la posibilidad de realizar tres chequeos diferentes del sistema. Escaneo total de la máquina, escaneo rápido (solamente examina los ficheros que son objetivo frecuente de virus: sector de arranque, directorio raíz,...) o escaneo de los directorios y ficheros que se le sean especificados.
	Descarga un subprograma ActiveX y realiza el escaneo de todas las unidades del sistema sin dar opción a elegir un subconjunto. La búsqueda no se realiza en ficheros comprimidos.
	Descarga un subprograma ActiveX y realiza el escaneo de todo el equipo sin ofrecer la posibilidad de seleccionar un subconjunto o unos ficheros concretos. Permite eliminar los archivos que haya detectado como maliciosos.

Características de los antivirus en línea

	Idioma	Navegador*	¿Elección de datos?	¿Escanea directorios?	¿Escanea fich. comprimidos?	Desinfección
Panda Sw.		IE	✓	✓	✓	✓
Trend Micro		IE, FF	✓	✓	✓	✓
McAfee		IE	✓	✓	✓	✗
BitDefender		IE	✓	✓	✓	✓
PC Pitstop		IE	✓	✓	✓	✗
Symantec		IE	✗	✓	✗	✗
ESET		IE	✗	✓	✓	✓

Navegador*: IE = Internet Explorer; FF = Mozilla Firefox.

Nota: Debido a que Internet Explorer 7 en Windows Vista funciona como una 'caja de arena' (*sandbox*), los antivirus no pueden eliminar los ficheros infectados del ordenador. La columna de "Desinfección" de la tabla anterior, no es válida para Windows Vista.

Nota2: Una 'caja de arena' (*sandbox*) es un ambiente virtual, creado por emulación, que permite al código ejecutarse dentro de un ambiente controlado sin que las acciones del código que se ejecuta afecten al entorno real del ordenador.

Actualizado: Septiembre 2007