1 Seguridad informática

1.1 ¿Qué es la seguridad informática?

La seguridad informática es la disciplina que se ocupa de diseñar normas, procedimientos, métodos y técnicas destinados a proteger los sistemas informáticos y la información contenida en ellos.

Al margen de las medidas de protección que se apliquen, un sistema informático siempre tiene riesgos potenciales. Su seguridad se puede medir en función de lo fiable que resulte, es decir, de la probabilidad de que se comporte tal y como se espera que lo haga.

La seguridad informática consiste en preservar estas características:

- **Disponibilidad.** El sistema mantiene un funcionamiento eficiente para garantizar el acceso a los usuarios autorizados y es capaz de recuperarse rápidamente si se produce un ataque o fallo.
- **Integridad.** Asegura que la información no sea modificada o manipulada. Los datos recibidos o recuperados deben ser iguales a los que fueron enviados o almacenados.
- **Confidencialidad.** Garantiza que la información solo sea accesible a aquellas personas que tienen privilegios para ello.

1.2 Proteger un sistema informático

A la hora de dotar de seguridad a un sistema informático, se deben tener en cuenta todos sus componentes, analizando el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas. Los elementos fundamentales que requieren protección son:

- **El hardware.** Componentes físicos de un sistema (por ejemplo, monitor, unidad de disco duro...) que contienen las aplicaciones que permiten su funcionamiento, a la vez que almacenan la información. Pueden verse afectados por un acceso no autorizado, una caída de tensión, una avería o cualquier otro accidente.
- **El software.** Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información. El software puede fallar por errores de programación o ser atacado por usuarios malintencionados.
- **Los datos.** La información es el elemento más valioso y, por tanto, el más amenazado. El funcionamiento de una empresa u organización depende de sus datos, que pueden ser de todo tipo: económicos, fiscales, de Recursos Humanos, etc.

Si se produce un ataque, el hardware se puede reemplazar y el software, reinstalar. Sin embargo, a veces, los datos son irrecuperables.

Protección... ¿total?

La cadena de seguridad siempre se rompe por el eslabón más débil. Imaginemos una empresa que mantiene su servidor de red en un búnker protegido con un software diseñado a prueba de piratas informáticos. Aun así, es posible que su sistema quede inutilizado al verter accidentalmente un líquido sobre el equipo.

Comprende, piensa, aplica...

1 Visita la Oficina de Seguridad del Internauta, explora sus contenidos y lee alguna de las historias reales que contiene. Pon a prueba tus conocimientos con su cuestionario de seguridad en http://www.osi.es/es/cuanto-sabes.

2 Explica las medidas de prevención, detección y recuperación que aplicas para proteger tus ordenadores (sobremesa, tableta, portátil o teléfono). ¿Alguna vez has perdido información por culpa de un virus o fallo informático?

1.3 Medidas de seguridad

Son muchos los factores que se deben considerar en el momento de proteger un sistema. Las medidas de seguridad deben ser tanto activas como pasivas.

- **Seguridad activa.** Tiene como objetivo prevenir y detectar amenazas para evitar daños en los sistemas informáticos.
- **Seguridad pasiva.** Tiene como finalidad recuperar un sistema informático que haya sido infectado por software malicioso o atacado por personas, o que haya sufrido algún accidente.

De este modo, las medidas de seguridad pueden ser de prevención, detección o recuperación de los sistemas.

Prevención

Las medidas de prevención tratan de proteger el sistema durante su funcionamiento normal para evitar que se produzcan violaciones de seguridad. Los mecanismos más habituales son:

- **Control de acceso.** El usuario ha de identificarse a través de una clave, técnicas biométricas, el DNI electrónico, un certificado, etc.
- **Permisos de acceso.** Los permisos establecen a qué recursos puede acceder un usuario determinado (lectura, ejecución, escritura, etc.). Estos permisos se suelen gestionar a través de las cuentas de administrador del sistema operativo.
- **Seguridad en las comunicaciones.** Garantiza la privacidad de los datos cuando se transmiten a través de la red. Se utilizan mecanismos basados en la encriptación de datos, como los protocolos seguros, la firma digital y los certificados.
- **Actualizaciones.** Sirven para mantener actualizado el sistema operativo y las aplicaciones, lo cual supone una garantía para el funcionamiento correcto y eficiente del sistema.
- **SAI** (sistema de alimentación ininterrumpida). Permite guardar la información y apagar el equipo correctamente cuando hay un fallo eléctrico.

Sistema biométrico en iPhone.

Detección

Una de las principales funciones de la seguridad es identificar y eliminar las vulnerabilidades y los ataques. Para ello, se emplean herramientas como antivirus, cortafuegos, antiespías, etc. Existe una gran variedad de herramientas de seguridad para detectar y erradicar las posibles amenazas.

Recuperación

Se emplean medios de recuperación cuando se ha producido alguna alteración del sistema por virus, fallos, intrusos, etc., y se quiere restaurar su correcto funcionamiento.

Cuando se trabaja en red, se utilizan métodos como la réplica de información, equipos con varios procesadores, etc. En cualquier caso, una medida imprescindible para redes y ordenadores personales es la realización frecuente de copias de seguridad.

Comprende, piensa, aplica...

1 Busca información sobre los virus más famosos de la historia de la informática. Explica brevemente cuáles eran sus efectos y cómo se difundían.

2 Amenazas

2.1 Ataques y amenazas

Los elementos que pueden comprometer la seguridad de un sistema informático se agrupan en:

Personas

Muchas de las acciones contra los sistemas informáticos provienen de personas que, de manera accidental o intencionada, pueden causar enormes pérdidas. Algunos de los ataques más habituales son:

- ***Hackers.*** Usuarios cuyos conocimientos informáticos avanzados les permiten entrar en los sistemas por desafío o para verificar su seguridad. Generalmente, no causan daños.
- ***Crakers.*** Personas que poseen amplios conocimientos en informática, gracias a los cuales burlan los sistemas de seguridad y perjudican los equipos informáticos causando daños.
- **Personas familiarizadas con el sitio atacado.** Puede tratarse de empleados descontentos, antiguos programadores u otras personas malintencionadas que cuentan con información privilegiada para atacar un sistema. Por ejemplo, el programador que diseñó el sistema de seguridad en una empresa.
- **Otros usuarios.** Cualquier persona que utiliza herramientas diseñadas para atacar sin necesidad de tener conocimientos de seguridad.

Amenazas lógicas

Algunos de los programas que se instalan en un sistema informático pueden dañarlo. Por ejemplo:

- **Software malicioso.** Virus, gusanos, troyanos, espías y todo un conjunto de programas que atacan los equipos y comprometen, así, la integridad, disponibilidad y confiabilidad de la información.
- **Vulnerabilidades del software.** Cualquier error en su diseño, configuración o funcionamiento puede poner en peligro la seguridad del sistema informático si este es descubierto por un atacante o, directamente, provoca un fallo.

Amenazas físicas

Principalmente, existen tres tipos de amenazas físicas:

- **Fallos en los dispositivos.** A veces, surgen problemas en discos, cableados, el suministro de energía u otros componentes que pueden provocar la caída del sistema.
- **Catástrofes naturales.** Los incendios, las inundaciones y los terremotos, por ejemplo, pueden provocar un fallo grave en el sistema informático.
- **Accidentes.** Sucesos provocados de forma involuntaria por descuidos, malas prácticas o desconocimiento. Por ejemplo, si un empleado de mantenimiento corta el suministro eléctrico.

Detección del ataque de un troyano.

Comprende, piensa, aplica...

1 Chema Alonso, ingeniero informático de sistemas, es considerado uno de los mejores *hackers* de nuestro país. Busca información sobre este experto en ciberseguridad y visualiza alguno de sus vídeos en YouTube.

2.2 Virus y *malware*

Los virus son uno de los principales riesgos de seguridad para los sistemas informáticos. Su objetivo es alterar el funcionamiento del dispositivo sin el permiso ni el conocimiento del usuario. Al ejecutar un archivo infectado por un virus, este se aloja en la memoria, toma el control de algunos servicios del dispositivo e infecta los programas que se ejecutan a partir de ese momento.

Con el uso generalizado de las nuevas tecnologías, han ido apareciendo otras amenazas de software que pueden resultar muy dañinas.

Se denomina *«malware»* a cualquier amenaza o programa que pueda resultar perjudicial para un dispositivo, tanto por causar pérdidas de datos como de productividad. Este término procede de la contracción de *«malicious»* y «software», es decir, 'software malicioso'

La propagación del software malicioso se realiza a través de las redes informáticas, de Internet y del intercambio de archivos. Este se reproduce e infecta ficheros en los equipos conectados.

Informe de amenazas y vulnerabilidades.

Tipos de *malware*	
Virus clásicos	Software que infecta otros programas añadiéndoles su código malicioso para alterar el funcionamiento normal del dispositivo sin el permiso ni el conocimiento del usuario.
Gusanos	*Malware* que usa los recursos de red para propagarse rápidamente. Localiza los contactos para enviar copias de sí mismo a través del correo electrónico, programas de mensajería, redes locales, etc.
Troyanos	Código dañino que se camufla en programas gratuitos, juegos, etc., para pasar desapercibido cuando el usuario los instala. Puede secuestrar el equipo por control remoto, destruir datos y realizar otras acciones dañinas.
Spyware	Programas espía que obtienen información sobre un usuario de forma no autorizada. Su objetivo puede abarcar desde averiguar los hábitos de navegación en la web hasta robar información financiera.
Rootkit	Colección de programas usada por ciberdelincuentes para evitar ser detectados mientras obtienen acceso no autorizado a un dispositivo, que pueden utilizar para encubrir ataques ilegales.
Adware	Programa que despliega publicidad no solicitada utilizando ventanas emergentes o páginas de inicio no deseadas. El usuario suele instalarlo de manera involuntaria al aceptar acuerdos de licencia de programas gratuitos.
Phishing	Suplantación de identidad para obtener información confidencial de modo fraudulento. Los ataques suelen consistir en enviar correos electrónicos que incitan a usar enlaces falsos para averiguar los datos bancarios del usuario.
Spam	Conjunto de mensajes, cuyo remitente es desconocido, que son enviados masivamente para intentar estafar a los destinatarios, robar sus direcciones de correo o difundir publicidad no solicitada.
Hoax	Información falsa enviada por correo electrónico y difundida con la ayuda de público desinformado. Está diseñada para persuadir al usuario de que realice una acción que no debería ejecutar.
Rogue	Programas que simulan ser aplicaciones *antimalware*, pero que ocasionan efectos negativos. Muestran en la pantalla advertencias llamativas respecto a infecciones o amenazas que, en realidad, no existen.
Bromas	Programas que no causan ningún perjuicio a los equipos que infectan, pero que intentan asustar al usuario informándole sobre supuestos daños sufridos en el equipo o amenazas actuales o futuras.
Vulnerabilidades del software	Fallos y puertas traseras del sistema operativo o aplicaciones que aprovechan algunos programas para lanzar ataques automáticos contra el sistema. La mejor protección es mantener actualizado el software.
Otros software maliciosos	Programas que no afectan directamente a los dispositivos, pero que se suelen usar para crear *malware* o realizar actividades ilegales, como ataques de denegación de servicio o DoS, *spoofing*, *hacking*, etc.

3 Protección del sistema informático

3.1 Antivirus

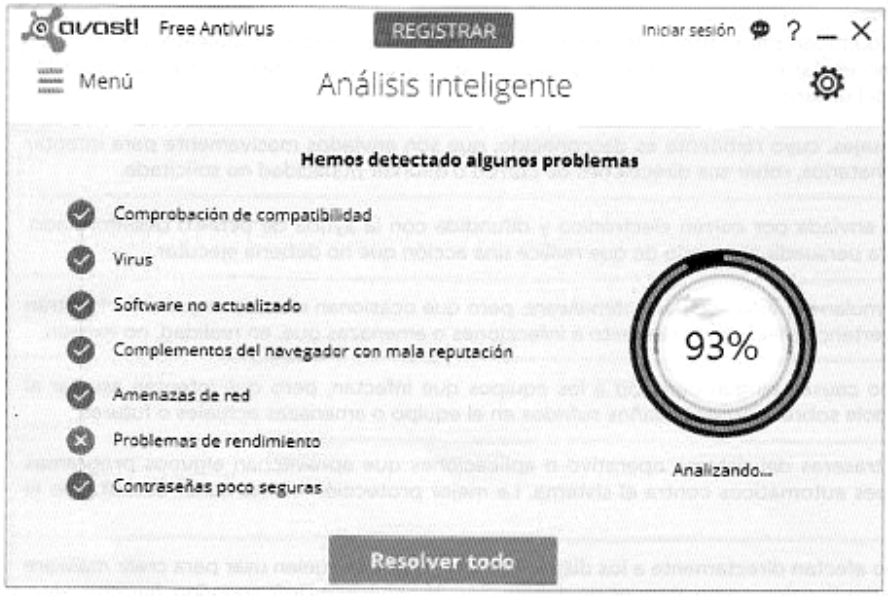
Un antivirus es un programa cuyo objetivo es detectar y eliminar virus informáticos. Con el paso del tiempo, estos programas han evolucionado y, aunque se siguen llamando «antivirus», son capaces de proteger el sistema frente a las amenazas de todo tipo de *malware*. Algunos ejemplos de antivirus son Avast, Panda, Norton, McAfee, Kaspersky, Bitdefender, etc.

El funcionamiento de un programa antivirus consiste en comparar los archivos analizados con las bases de datos de virus. Esta base de datos, que se conoce como «firmas» o «definiciones de virus», ha de ser actualizada periódicamente con el fin de evitar que un virus nuevo pase desapercibido.

Actualizar la base de datos de un antivirus.

Los antivirus advierten de comportamientos sospechosos y utilizan algoritmos heurísticos para reconocer códigos maliciosos que no se encuentran en su base de datos, bien porque son nuevos, bien porque no han sido muy difundidos.

La mayoría de los sitios web oficiales de los programas antivirus ofrecen la posibilidad de realizar un chequeo online gratuito de nuestro equipo. Son muy útiles para analizar el ordenador cuando se sospecha que este, e incluso que el propio antivirus, pueden estar infectados. Su uso es imprescindible para prevenir los ataques en cualquier tipo de dispositivo informático.



Antivirus en un ordenador.

Antivirus en segundo plano

Los antivirus permanecen residentes en la memoria de un sistema y avisan de posibles infecciones que detectan al abrir documentos, ejecutar programas, descargar archivos de Internet, etc.

En la barra de notificaciones, se muestra el antivirus que está activo.

Antivirus en un teléfono móvil.

3.2 Cortafuegos

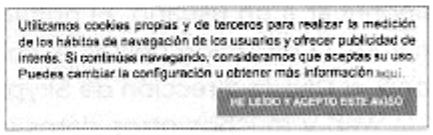
Mientras se trabaja en red, por ejemplo, navegando, descargando ficheros o leyendo el correo, se produce una continua entrada y salida de datos. Los intrusos pueden utilizarlos para infiltrarse en el dispositivo y acceder a la información, borrar archivos, etc.

Un cortafuegos o *firewall* es un sistema de defensa que controla y filtra las conexiones entrantes y salientes del sistema informático con el fin de bloquear el tráfico no autorizado. Para que su funcionamiento sea eficaz, se configuran una serie de reglas para las aplicaciones que tienen permiso de comunicación con la red (navegador web, correo electrónico, protocolos de transferencia de archivos o FTP, etc.).

Cuando un cortafuegos detecta que una aplicación intenta comunicarse con Internet sin tener permiso, se muestra un mensaje en el que se pide al usuario que autorice o deniegue su entrada. Así, los cortafuegos evitan que los intrusos tengan acceso a las redes privadas o a los equipos conectados a Internet. No obstante, no protegen el equipo frente a otros tipos de *malware*, por lo que se deben complementar con antivirus.

¿Qué es una *cookie*?

Es un fragmento de información que se almacena en el disco duro cuando se visitan determinadas páginas web, a petición de los creadores de las mismas. Se emplea para llevar un control sobre el número de visitantes u obtener información sobre los hábitos de navegación del usuario. No suelen generar problemas de seguridad, pero se consideran intrusiones en el ámbito de la privacidad, por lo que los navegadores incorporan la opción de permitirlas o no.



Advertencia del uso de *cookies*.

3.3 Antiespías

Las aplicaciones antiespía detectan, bloquean y eliminan dos tipos de *malware* que suelen actuar de forma conjunta: el *sypware* y el *adware*. El síntoma de que un dispositivo está infectado es su ralentización, debida a que los datos recopilados (historial de navegación, búsquedas realizadas, datos privados, etc.) se envían a los atacantes. Por lo general, el *adware* utiliza la información recolectada para decidir qué publicidad mostrará al usuario.

3.4 Copias de seguridad

Los datos almacenados en un dispositivo pueden resultar dañados por *malware*, ataques externos, fallos en el hardware o descuidos del usuario.

Para evitarlo, se puede realizar una copia de seguridad o *backup*. Esta contiene todos los datos que queremos proteger y permite recuperarlos si es necesario. Así, garantiza dos de los tres objetivos básicos que persigue la seguridad informática: integridad y disponibilidad.

El sistema operativo permite planificar la realización automática de copias de seguridad periódicamente, aunque el usuario puede realizarlas de forma manual cuando lo desee. En cualquier caso, se debe almacenar la información en soportes externos o en la nube. La copia debe incluir todos los documentos y la información difíciles de recuperar en caso de pérdida.

Comprende, piensa, aplica...

1 Realiza un chequeo de tu ordenador utilizando el antivirus instalado.
   a) ¿Ha detectado alguna amenaza?
   b) ¿Incluye algún cortafuegos para filtrar la actividad de la red y garantizar la seguridad?

2 Imagina que, al llegar a casa, tu ordenador ha dejado de funcionar.
   a) ¿Has perdido información importante?
   b) ¿Cómo podrás disponer de una copia actualizada de tus datos en la nube?

Comprueba cómo progresas

Aplica tus conocimientos

1 La principal fuente de ingresos de los buscadores es la publicidad. Al conocer los perfiles y gustos de cada uno de sus usuarios, pueden mostrarles los anuncios que más se adecúen a sus preferencias y, así, captar su atención e interés.

a) Después de haber buscado un producto varias veces, ¿suele coincidir la publicidad de las páginas web con la búsqueda? ¿Es casualidad?

b) Elimina las *cookies* almacenadas en el navegador que utilizas. Recuerda hacerlo regularmente.

c) Consulta lo que Google conoce sobre ti en https://www.google.com/dashboard y deshabilita el historial de búsquedas.

2 Imagina que, a pesar de haber pasado varios años desde que publicaste unos vídeos sobrepasando con tu moto la velocidad permitida, continúan apareciendo al buscar tu nombre en Internet.

a) ¿Crees que podrían tener un efecto negativo a la hora de buscar empleo como profesor de autoescuela?

b) Introduce tu nombre en el buscador y, si no deseas que parte de la información que aparece sea pública, pide a Google que la elimine y cambia las opciones de privacidad de la página donde está publicada.

3 Crea un póster, una infografía o una presentación e incluye indicaciones para utilizar las nuevas tecnologías (dispositivos, redes sociales, navegación web, etc.), promoviendo una interacción de forma ética y segura con la red.

Investiga

1 Un antivirus muestra el siguiente resultado tras analizar un dispositivo:

a) ¿Qué tipo de *malware* se ha detectado?

b) ¿Cómo se ha solucionado el problema?

c) ¿Cuál era el medio de transmisión del virus?

2 Elabora una tabla con una relación de las principales herramientas de prevención y detección de *malware*. Escribe varios ejemplos de programas de cada tipo y sus sitios web oficiales.

Herramienta	Nombre	Sitio web
Antivirus	Kaspersky ESET NOD32	http://www.kaspersky.es http://www.eset.es
Cortafuegos		
Antiespías		

3 Las cadenas de correo pueden ser, básicamente, de dos tipos:

- De broma o *hoax*, término inglés ampliamente utilizado en Internet.
- De «captación» de correos electrónicos. Quien origina la cadena tendrá, al final, una colección de direcciones de correo electrónico para enviar publicidad, *malware*, etc.

Consulta tu correo web y responde:

a) ¿Recibes mensajes de personas desconocidas o empresas a las que no has autorizado a utilizar tu correo?

b) ¿Tienes activado el filtro *antispam*?

c) Algunos mensajes son identificados como *spam* erróneamente, de manera que pasan inadvertidos al usuario. Por ello, conviene que revises la bandeja de *spam* cada cierto tiempo. Para que no tengas que hacerlo muy a menudo, establece que el correo no deseado se borre a los diez días.