

Unidad 4. Seguridad Informática





Seguridad y privacidad. Accesos restringidos, contraseñas, privacidad de la información, consecuencias legales de la vulneración de la privacidad.

¿Qué es la seguridad informática?

Área de la informática encargada de asegurar el buen uso de los recursos informáticos y la información como activos de una organización, manteniéndolos libres de peligros, daños o riesgos.

La seguridad informática se puede clasificar en seguridad lógica y seguridad física y busca con la ayuda de políticas y controles mantener la seguridad de los recursos y la información manejando los riesgos, sin embargo cuando se habla de seguridad se debe tener en cuenta que no existe la seguridad 100%.

No hay una fórmula matemática que nos indique que un sistema de información o proceso es 100% seguro, pero si existen tres principios que deben mantenerse para decir que existe seguridad en la información.

Principios de la Seguridad de la Información

- **Integridad:** la información debe ser protegida de modificaciones no autorizadas.
- **Disponibilidad:** la información y servicios deben estar disponibles siempre que se necesiten.
- **Confidencialidad:** se debe garantizar que la información es conocida únicamente por a quien le interese.

Garantizar la seguridad de la información requiere la construcción de una Política.

Política de Seguridad

Toda estrategia se basa en unos principios y objetivos claramente definidos. En el caso de seguridad de la información no es diferente, estos objetivos se agrupan en un documento de alto nivel llamado Política de Seguridad que contiene el conjunto de normas, procedimientos y prácticas de seguridad de la organización orientadas a mantener un ambiente informático seguro.

La construcción de una política de seguridad inicia con el entendimiento de los objetivos de la organización, seguida por la redacción de las normas y procedimientos que sean requeridos, el establecimiento del apoyo por parte de la dirección de la organización para finalmente declarar las políticas de seguridad y su publicación.

Estas políticas pueden cubrir desde las buenas prácticas para mantener la seguridad de un computador hasta proveer las normas que deben cumplir los usuarios de una organización para proporcionar un ambiente seguro de la información y los recursos informáticos en cuyo caso debe estar apoyada por la normatividad de seguridad de la organización.

Peligros de seguridad informática

Conceptos Básicos

Para entender porque existe la seguridad informática, es importante conocer los siguientes conceptos:

- **Amenaza:** todo aquello que represente la posibilidad o probabilidad de ocasionar un daño.
- **Vulnerabilidad:** oportunidades que existen a nivel de sistema operativo y/o hardware de ser explotadas para hacer daño mediante ataques o intrusiones. Una vulnerabilidad facilita la materialización de una amenaza.
- **Daño:** es la consecuencia de una vulnerabilidad, amenaza o ataque.
- **Riesgo:** daño potencial que puede surgir por un proceso presente o evento futuro. Combina la probabilidad de que ocurra un evento negativo con cuánto daño causaría dicho evento.
- **Ataque:** acción exitosa o no, cuyo objetivo es causar daño a un sistema, robar información o utilizar un recurso informático de forma no autorizada.

Documento de Políticas de privacidad de una empresa que opera por Internet:

- **Políticas de Privacidad**
- **¿Qué son los Cookies?**
- **Confidencialidad de la Información.**
- **Modificación / actualización de la información personal.**
- **Protección de la Información Personal.**
- **Aceptación de los términos.**

Este es un ejemplo más de que algunas empresas si que están preocupadas por la seguridad de los datos personales, pero hay que tener claro que lo que provoca esto es la actuación de la AGP (Agencia de Protección de Datos) con sus exigencias de cara a la legislación y con la actuación de los propios usuarios, ya que somos nosotros con nuestra desconfianza los que obligamos a las empresas, que solicitan nuestros datos a través de Internet (o cualquier otro medio), a ofrecer garantías de seguridad a la hora de adquirir, tramitar, utilizar... nuestros datos.

La principal inseguridad que sufren los usuarios, sobre todo en nuestro país, es la que va asociada al tráfico de datos personales a través de Internet, bien sea por la impersonalidad de la red, por sus características no físicas (en ocasiones hay entidades que no tienen domicilios postales fuera de Internet), o por la inmunidad del anonimato. El caso es que esta desconfianza no es infundada, ya que, tal y como veremos a continuación, la inseguridad que existe asociada a Internet resulta, en muchos casos, bastante razonable.



Busca cualquier página en Internet y observa el documento “Políticas de privacidad de una empresa.

¿Qué amenazas existen en Internet?

Las acciones más frecuentes de los virus son:

- Unirse a un programa instalado en el ordenador permitiendo su propagación.
- Mostrar en pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir espacio en el disco.

Las amenazas en Internet se pueden clasificar en varios grupos, veamos los más representativos:



Virus: es un programa que al instalarse en el PC puede causar daño al software o hardware del mismo. Requiere de un medio para propagarse a otros PCs.



Gusanos: trabajan de forma parecida a los virus, sin embargo, pueden fácilmente aprovechar una vulnerabilidad para propagarse o hacer daño a otros PCs remotos.



Trojanos: "El Maestro del Disfraz". Son programas que disfrazan una amenaza, simulando ser una aplicación indefensa, como por ejemplo protectores de pantalla, para ingresar y hacer daño.



Hoax: "El Manipulador". Falsos virus. Es un truco utilizado para molestar al lector y crear congestión en la red, se asocia con bromas, engaños y en su mayoría juegan con los sentimientos de las personas.



Phishing: "La Pesca Milagrosa". Es un mecanismo de engaño al usuario basado en la suplantación de identidad.



Spyware: "El Espía". Son programas informáticos que espían todo lo que hace el usuario en su computador, facilitando el robo de información y el conocimiento de preferencias para posteriormente convertirlo en víctima de spam, phishing, adware y otros



Adware: "El Vendedor Intenso". Corresponde a programas informáticos asociados con el envío y notificación de publicidad no deseada. En esta categoría se encuentran los pop-up o ventanas que se abren sin ser llamadas cuando navegamos en Internet.



Spam: "El Cartero Indeseado". Envía información no solicitada de forma masiva. El spam no se encuentra solamente en el correo electrónico, también existe el spam telefónico, en foros de Internet, en el correo convencional entre otros.

Mejores prácticas de seguridad informática

Para evitar el contagio de virus, gusanos y/o troyanos

- No iniciar sesión en el computador con el usuario Administrador de Windows a menos que sea estrictamente necesario.
- No navegar en Internet con los privilegios del usuario Administrador de Windows.
- Revisar con un antivirus cualquier medio de almacenamiento externo que vaya a ser conectado o leído.
- No abrir archivos adjuntos a los correos electrónicos y/o mensajería instantánea solo por curiosidad, cuando no se espera dicho archivo.
- Cuando use mensajería instantánea no acepte mensajes de contactos desconocidos.

Para evitar el phishing

- No ingresar información personal privada en formularios de Internet o enviados por correo electrónico.
- Confirmar la veracidad de comunicados de entidades bancarias por correo electrónico, solicitando actualización de datos.

Para evitar el spyware y adware

- No instalar herramientas desde Internet cuando cualquier sitio lo solicite.
- No instalar herramientas libres ofrecidas en Internet sin antes averiguar sobre ellas.
- Evitar los sitios de descargas gratuitas de software, música, vídeos y otros.

Para evitar el spam

- No continuar cadenas de mensajes de correo electrónico.
- No entregar la lista de correos electrónicos de nuestros contactos.
- No enviar correos a una lista de correos electrónicos extensa, se recomienda enviar correo a máximo cinco buzones y utilice la opción enviar con copia oculta.
- No responda correos solicitando que lo retiren de la lista, esto en la mayoría de correos spam lo único que hace es confirmar que existe la cuenta de correo.
- No inscribir la cuenta de correo en todos los sitios de Internet que nos solicitan una cuenta de correo.

Formas de prevención de virus informáticos

Existen diferentes formas de prevención:

- **Copias de seguridad:** Se deben realizar copias de seguridad de la información almacenada y mantenerlas en un lugar diferente al ordenador.
¿Qué hay que copiar: carpetas y archivos del usuario, Favoritos, correo electrónico y otras informaciones relevantes, como certificados digitales, agendas, etc.
- **Copias de programas originales:** Es recomendable hacer una copia del original para evitar que el disco original se dañe.
- **Rechazar copias de origen dudoso:** La mayoría de las infecciones provocadas por virus proceden de discos de origen desconocido.
- **Uso de contraseñas:** Es necesario poner una contraseña al ordenador para que puedan acceder a él.

Medidas de seguridad activas y pasivas

Las medidas de seguridad evitan las amenazas y los ataques contra los recursos de la red y 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:
 - ✓ **Contraseñas.** Hay que introducir una contraseña para acceder a los recursos.
 - ✓ **Permisos de acceso.** Los permisos establecen a qué recursos puede acceder un usuario y qué permisos tienen sobre los recursos (lectura, ejecución, escritura, etc.).
 - ✓ **Seguridad en las comunicaciones.** Se utilizan mecanismos basados en la criptografía (cifrado de contraseñas y firmas digitales).
 - ✓ **Actualizaciones.** Tener actualizado el sistema operativo como los programas antivirus, será una garantía para el correcto funcionamiento del sistema.
 - ✓ **SAI.** Permite guardar la información cuando existe un apagón de la corriente.
- **Detección.** Para detectar y evitar acciones contra la seguridad se emplean herramientas como **antivirus, firewall, anti-spy-ware**, etc. Prácticamente hay una herramienta asociada a cada tipo de amenaza.
- **Recuperación.** Se aplica cuando ya se ha producido alguna alteración del sistema, por virus, fallos, intrusos, etc., para restaurar el sistema a su correcto funcionamiento. En pequeñas redes y ordenadores personales la medida imprescindible a adoptar es la copia de seguridad.

Antivirus informáticos

El antivirus es un programa de software que permite a través de la consulta en bases de datos (llamada firmas o definiciones de virus), identificar y determinar la existencia de un posible código malicioso en un sistema o computador y además de esto, tomar acciones para evitar la activación de dicho código, dando de esta manera protección a los diferentes sistemas antes de que sean afectados.

Hoy en día existen muchos antivirus en el mercado, algunos de uso libre, con estos hay que tener especial cuidado, pues la eficiencia de un antivirus esta en su posibilidad de mantenerse actualizado con las últimas firmas de virus existentes, es decir con los patrones de los últimos códigos maliciosos que han aparecido y para los cuales ya hay una vacuna, de lo contrario no habría protección ante las nuevas amenazas. Por otra parte no se debe confundir la función de antivirus con la función de un anti-spyware, anti-adware o anti-spam, cada uno tiene su funcionalidad específica, en el caso del antivirus este se encarga de virus, gusanos y troyanos, estos últimos en ocasiones no pueden ser eliminados pero si detenidos de tal manera que no causen daño. En el caso de otros tipos de código malicioso como keylogger, keystroke, pop-up, etc. existen programas de software específicos para protegernos de ellos, por ejemplo el anti-spyware protege de programas orientados a espiar todo lo que hacemos, el anti-adware protege de las molestas pop-ups o ventanas emergentes y así otros programas existentes en el mercado.

En la actualidad los proveedores han querido unir todas las protecciones en un solo producto, encontrándose de esta manera software antivirus, antispyware, antiadware y antispam en un solo paquete y de forma modular con la posibilidad de habilitar los módulos según la necesidad del cliente. Es posible habilitar todas las protecciones pero vale la pena aclarar que en la medida que se activan más protecciones se va a requerir mayor poder de cómputo ya que todos los módulos revisan minuciosamente la información y cada proceso que se inicia en el computador.



Realiza un análisis del sistema con varios antivirus en línea (on-line) y comprobar si el sistema contiene algún tipo de amenaza.

<http://alerta-antivirus.es>

Filtros de correo o correo no deseado

El correo no deseado (también conocido como correo pesado) es una molestia frecuente en Internet, que resulta difícil de controlar. Grandes cantidades de correo comercial no deseado viajan por Internet, ofreciendo cosas como métodos de obtener dinero fácil, pornografía, crédito ilimitado y calificaciones falsas, entre otros.

Para reducir el volumen de “correo basura” que recibe, puede utilizar los filtros incluidos en el software y servicio de correo, sin embargo, el mejor consejo es no responder, ya que hacerlo sólo confirma al remitente que su mensaje ha llegado a alguien, y entonces es probable que reciba aún más correo de este tipo. También debe tener cuidado si da su dirección de e-mail en formularios de registro en sitios web y si coloca su dirección de e-mail en zonas públicas como los “libros de visita”, dado que esto puede contribuir a que reciba más correo basura.

La forma más habitual de propagar los virus es incluirlo como adjunto en un mensaje de e-mail. Si lee un e-mail como estos y descarga el archivo adjunto, el computador abre el archivo y el virus empieza a producir sus efectos nocivos; por ejemplo, puede que envíe una copia de él mismo, más un enlace a un sitio web pornográfico, a todas las personas de su libreta de direcciones. La mejor defensa ante los virus es instalar un programa de antivirus en el computador, y mantenerlo actualizado (normalmente hay actualizaciones regulares en línea).

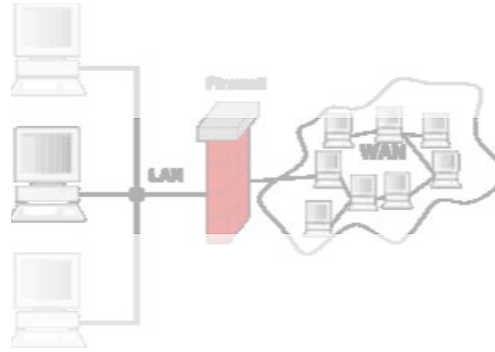


Si tienes correo on-line, comprueba las opciones de correo no deseado, así como las opciones de remitentes bloqueados.

Cortafuegos (Firewall)

Un cortafuegos o firewall es un programa o dispositivo hardware de seguridad, es decir una herramienta de protección que restringe la información o solicitudes que puede recibir un computador desde otro, ubicado en su misma red o en una red diferente. Se encarga de bloquear o permitir el paso de información al computador de acuerdo con una configuración por defecto o establecida por el usuario.

Por ejemplo, un computador puede estar configurado para aceptar solicitudes de conexión de aplicaciones como Messenger MSN o actualizaciones de Windows, pero no acepta ninguna conexión de Yahoo Messenger; en este caso se debe ingresar al firewall y configurar el equipo de tal forma que las conexiones de Yahoo Messenger sean aceptadas de lo contrario serán bloqueadas.



Comprueba si tienes o no activado el cortafuegos de Windows.

Programas Espías

Los programas espías o spywares son aplicaciones que recogen datos privados de una persona u organización sin su consentimiento.

Estos programas pueden llegar al ordenador mediante un virus que se distribuye por correo electrónico o puede estar oculto en la instalación de un programa.

Pueden tener acceso por ejemplo al correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, qué tiempos se está en ellas y con qué frecuencia se regresa; qué software está instalado en el equipo y cuál se descarga; qué compras se hacen por internet; tarjeta de crédito y cuentas de banco.

Los principales **síntomas de infección** son:

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto,
- Barras de búsquedas de sitios como la de Alexa, Hotbar, MyWebSearch, FunWeb, etc., que no se pueden eliminar.
- Creación de carpetas tanto en el directorio raíz, como en "Archivos de programas", "Documents and Settings" y "WINDOWS".
- Modificación de valores de registro.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda más en iniciar el computador debido a la carga de cantidad de software spyware que se inicia una vez arrancado el ordenador.

- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- Aparición de un mensaje de infección no propio del sistema, así como un enlace web para descargar un supuesto antispyware.
- Denegación de servicios de correo y mensajería instantánea.

Las cookies son archivos en los que se almacenan información sobre un usuario que puede acceder a Internet. Se usan para identificar, mediante un código, al usuario de modo que pueda ser reconocido en las sucesivas conexiones a la página correspondiente.



Elimina las cookies de tu ordenador.

Proteger la conexión inalámbrica

En las redes inalámbricas la información viaja por ondas de radio. Esto las hace fácilmente accesibles a todos los usuarios dentro de su radio de alcance. Si no están protegidas cualquiera las puede aprovechar para conectarse a internet o acceder a los ordenadores conectados a esa red.

Para evitarlo hay que tomar las medidas de seguridad adecuadas. Algunas de estas medidas son:

1. **Cambiar la contraseña por defecto.** Todos los fabricantes establecen una contraseña por defecto de acceso a la administración del router.
2. **Usar una encriptación WEP/WPA.** El software del fabricante permite la conexión con una clave utilizando encriptación WEP o WPA, dependiendo del modelo de router.
3. **Para los usuarios más avanzados** existen medidas aún más restrictivas como activar el filtrado de direcciones MAC, desactivar el DHCP, etc.



**UNIDAD 4
ACTIVIDADES Y TAREAS**

1. Define Seguridad informática.

2. Indica los tres principios básicos de la seguridad de la Información.

3. Indica las principales amenazas que existen en Internet.

4. Indica otras amenazas que pueden existir en Internet.

5. Averigua qué antivirus tiene tu ordenador.

6. Crea un filtro para que tu correo. Ejecuta el filtro de correo y solicita a tu compañero que te envíe un mensaje. Comprueba que, una vez recibido, lo ha movido a la carpeta de correo no deseado.

7. ¿Está activado del firewall de tu ordenador?. ¿Qué opciones avanzadas ha activado?

8. Busca los significados de hacker y cracker y compáralos.

9. ¿Qué programas te ayudan a protegerte de los hackers y crackers?

10. Cuando se ha alterado la página de inicio y no se puede volver a poner la deseada o cuando se ralentiza un ordenador, es hora de realizar un análisis antispymware.

a) descarga el programa **Spybot Search & Destroy**, aplicación gratuita:

<http://www.safer-networking.org>

b) instálalo en el equipo y busca las actualizaciones.

c) analiza los problemas y soluciona los problemas detectados.

11. Las siguientes páginas web están relacionadas directamente con la seguridad informática. Entra en cada una de ellas y haz un breve comentario sobre su temática:

- <http://web.alerta-antivirus.es>

- <http://www.leydeprotecciondedatos.com>

- <http://www.hackhispano.com>

- <http://rediris.es>

12. LOPD, 18 de octubre de 2007

Multa por revelar 42 direcciones de correo

La AGPD ha multado con 600 euros a una persona por enviar 42 e-mails en los que cada destinatario podía ver las direcciones de los demás.

Recuerda que el e-mail es un dato de carácter personal sujeto a ley.

Revisa tus mensajes de correo, ¿en cuántos de ellos aparecen direcciones de e-mail de otras personas?

Si deseas mantener la privacidad, ¿qué campo debes utilizar para poner las direcciones de correo cuando envías un mensaje a varias personas?
