DIXITALIZACIÓN

Curso: 4º ESO

SEGURIDAD Y BIENESTAR DIGITAL

1.1 ¿Qué es la seguridad informática?

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

Al margen de las medidas de protección que se apliquen, siempre existen **riesgos potenciales,** ya que la seguridad se puede medir en función de la probabilidad de que un sistema se comporte tal y como se espera que lo haga, preservando los siguientes **principios básicos:**

- **Autenticación.** Verifica la identidad de las personas o entidades, para asegurar que no están siendo suplantadas.
- **Confidencialidad.** Garantiza que la información solo sea accesible a aquellas personas que tienen privilegios para ello.
- **Disponibilidad.** El sistema mantiene un funcionamiento eficiente, para garantizar el acceso a las personas autorizadas, y es capaz de recuperarse rápidamente si se produce un ataque o un fallo.
- **Integridad.** Asegura que la información no sea modificada sin permiso o manipulada. Los datos recibidos o recuperados deben ser iguales a los que fueron enviados o almacenados.

1.2 Proteger un sistema informático

Al proteger un sistema informático, se deben tener en cuenta todos sus **componentes,** analizando el nivel de vulnerabilidad y protección necesario para cada uno de ellos ante las posibles amenazas. Los elementos fundamentales que requieren protección son:

- El **hardware,** constituido por los **componentes físicos** que integran el ordenador, especialmente aquellos que almacenan la información (discos duros, unidades SSD, memorias USB, etc.), así como los **dispositivos de red,** que pueden utilizar personas malintencionadas para acceder a ella (rúter, tarjetas de red, antenas...). Puede verse afectado por accesos no autorizados, caídas de tensión, averías o cualquier otro accidente.
- El **software,** integrado por los **componentes lógicos,** entre los que se incluyen el **sistema operativo,** los **programas** y los **datos.** Hay que considerar que las brechas de seguridad comprometen el sistema operativo o los programas, por lo que es importante mantenerlos actualizados y protegidos con soluciones antivirus, si bien la información suele ser el objetivo de los ataques y, por tanto, el elemento más vulnerable. En caso de pérdida, el sistema operativo y los programas se pueden reinstalar pero, en ocasiones, los datos son irrecuperables.

Las tecnologías emergentes, como el *big data,* IoT o *cloud computing,* suponen nuevos retos a la protección de la información, por lo que muchas empresas recurren a **centros de procesamiento de datos (CPD),** para almacenar sus datos de forma segura.

1.3 Tipos de seguridad

El conjunto de **mecanismos** y **procedimientos** de **protección** de los sistemas informáticos diferencian entre:

- **Seguridad activa.** Tiene carácter proactivo, es decir, su objetivo es intentar **prevenir** que no se produzcan incidentes de seguridad, tales como infecciones de *malware*, ataques, robo de información...
- **Seguridad pasiva.** Actúa de manera reactiva, adoptando **soluciones** una vez que se ha producido un **incidente,** para minimizar su repercusión y facilitar su recuperación, por ejemplo, restaurando la última copia de seguridad.

1.4 Medidas de seguridad

Los planes de acción para mantener la seguridad suelen incorporar una combinación de medidas de los siguientes tipos:

- **Prevención.** Protegen el sistema a nivel de software y hardware, así como las redes. Algunas de las más frecuentes son:
  - **Autentificación:** implantación de políticas de contraseñas, técnicas biométricas o certificados digitales, para **identificar** a las personas que acceden al equipo.
  - **Permisos de usuario:** gestión de los privilegios que tiene cada persona dentro de un sistema informático, definiendo **roles** de administrador, usuario estándar o invitado.
  - **Actualizaciones:** corrección de los **fallos** de seguridad y adición de **nuevas funcionalidades** a los dispositivos. Esto incluye el sistema operativo, las aplicaciones informáticas y el *firmware*.
  - **Seguridad en las instalaciones y comunicaciones:** prestación de las medidas de **acceso** y protección necesarias a los dispositivos, así como la **privacidad** de los datos, cuando se transmiten a través de las redes (encriptación, VPN...).
  - **Formación de personal:** aseguramiento de que las **personas** que utilizan los sistemas informáticos conocen el verdadero significado y el valor de la información, las herramientas a utilizar, los protocolos a seguir ante situaciones anómalas, etc.

- **Detección.** Analizan el sistema para identificar cualquier indicio que revele una infección por software malicioso, un ataque en curso o una vulnerabilidad en el sistema. Una buena gestión de esta fase y la eliminación de la amenaza suponen una reducción significativa de su impacto final. Para ello, se emplean herramientas como los antivirus, cortafuegos, programas antiespías, etc.
- **Recuperación.** Restauran el funcionamiento del sistema cuando se ha producido alguna alteración por virus, fallos, ataques de personas, averías, etc. Algunas de las medidas más importantes que se suelen adoptar son la eliminación del software malicioso; la restauración de la información anterior, utilizando copias de seguridad; la sustitución del hardware que pueda haberse visto afectado, o la realización de análisis forenses digitales.

2

Amenazas

Las **amenazas** son incidentes que pueden **dañar** un **sistema informático,** por lo que es importante conocerlas para utilizar **contramedidas** que minimicen la probabilidad de que ocurran.

2.1 Tipos de amenazas

La seguridad se puede ver comprometida por diferentes tipos de amenazas, siendo las más habituales las siguientes:

Humanas. Provienen de una persona que suele ser:

- ***Hacker.*** Alguien experto en informática, que accede a los sistemas informáticos, redes o sitios web para **verificar su seguridad,** con objeto de avisar de los fallos, desarrollar técnicas de mejora o, simplemente, como desafío. Su objetivo no suele ser causar daños.
- **Pirata informático** (del inglés, ***cracker***). Persona que accede ilegalmente a los sistemas informáticos ajenos para apropiárselos, obtener información confidencial o causar **daños.**
- **Personal.** Alguien con malas intenciones, que dispone de información privilegiada para atacar un sistema informático. Por ejemplo, una programadora que, habiéndose encargado del diseño del sistema de seguridad en una empresa, lanza un ataque como venganza, tras ser despedida.

2

Amenazas

Lógicas. Relacionadas con el software, que suelen estar provocadas por:

- **Software malicioso:** virus, gusanos, troyanos y todo un conjunto de programas diseñados para comprometer la integridad, disponibilidad y confiabilidad de la información.
- **Vulnerabilidades:** programas o sistemas operativos que no están actualizados, están mal configurados o incluyen errores, que pueden ser aprovechados para lanzar ataques.

Físicas. Ocasionadas, generalmente, por:

- **Fallos en los dispositivos:** averías en los equipos, roturas de cableado, deterioro de discos...
- **Accidentes:** provocados de forma involuntaria por descuidos, desconocimiento, etc. Por ejemplo, una persona empleada del departamento de mantenimiento corta el suministro eléctrico, sin previo aviso.
- **Catástrofes naturales:** incendios, inundaciones, terremotos...

2

Amenazas

2.2 Software malicioso

El **software malicioso** es un **programa o fragmento** de su código, **diseñado para ejecutar acciones no deseadas** en un sistema informático. También se lo conoce por su denominación inglesa, *malware*, acrónimo de *malicious* y de software.

Existen diversos tipos, en función de cómo se propagan, cómo actúan o cuáles son sus efectos, siendo algunos de los más populares los siguientes:

- **Virus:** altera el **funcionamiento** para el que un dispositivo ha sido programado. Se propaga a través de archivos infectados de cualquier tipo, que suelen proceder de descargas de internet, del correo electrónico, de memorias USB, etc. Cuando se ejecuta el archivo, infecta el equipo y puede provocar todo tipo de efectos.
- **Gusano:** crea copias de sí mismo indefinidamente, con la finalidad de **colapsar** un dispositivo o, incluso, toda una red.
- **Troyano:** se oculta en un archivo, para pasar desapercibido mientras ejecuta **acciones ocultas.** A diferencia de los virus y gusanos, no puede reproducirse por sí mismo ni infectar archivos.
- ***Ransomware:*** secuestra los datos de un dispositivo, cifrándolos y solicitando un **rescate** económico, a cambio de la clave para poder descifrarlos. En la mayoría de los casos, se solicita el pago en **criptomonedas,** lo que dificulta a las autoridades el rastreo de este delito.

2

Amenazas

- **Programa espía o *spyware:*** obtiene **información** de forma no autorizada, ya sea controlando las acciones realizadas, recabando los hábitos de navegación, capturando lo que se escribe en el teclado, etc., para enviarla al atacante, a través de la red.
- ***Adware:*** muestra automáticamente **publicidad no deseada** o engañosa, bien a través de ventanas emergentes o de mensajes que aparecen durante la ejecución de los programas. Se suele instalar de manera involuntaria, al aceptar acuerdos de licencia de programas gratuitos.
- ***Rogue:*** simula ser *antimalware*, pero en realidad ocasiona los efectos contrarios. Muestra, en la pantalla del dispositivo, advertencias de **falsas infecciones,** tratando de engañar a la persona usuaria para que pague por la licencia para realizar la supuesta desinfección.
- ***Hoax:*** persuade para que se realice alguna acción que no se debería, utilizando **información falsa** que se envía a través de correo electrónico o de mensajería instantánea. Un ejemplo característico suelen ser las peticiones de colaboración económica para ayudar, supuestamente, a una persona enferma.
- ***Spam:*** envío masivo de mensajes de correo electrónico no deseados, no solicitados y con remitente desconocido, cuyo contenido suele ser **publicitario.** Además de ser molestos y consumir recursos de los equipos, pueden ocultar otras amenazas.

3

Protección del sistema informático

3.1 Antivirus

Un **antivirus** es un **programa** que tiene como finalidad **prevenir, detectar** y **eliminar software malicioso** u otros **ataques** en el sistema.

Su nombre se debe a que, inicialmente, solo protegían de virus informáticos pero, con el paso del tiempo, estos han evolucionado y son capaces de proteger el sistema frente a las amenazas de todo tipo. Algunos ejemplos son Avast, Panda, Norton, McAfee, Kaspersky, Bitdefender, ESET, BullGuard, etc.

Su funcionamiento consiste en **comparar los archivos** analizados con su base de datos de **firmas o definiciones de virus,** por lo que es necesario que permanezcan **actualizados.** También advierten de comportamientos sospechosos, que pueden corresponder a nuevos virus no reconocidos. Para ello, residen en la **memoria,** ejecutándose en segundo plano y analizando constantemente los archivos ejecutados, los correos entrantes, las páginas visitadas, las memorias USB introducidas, etc.

Actualizar la base de datos de un antivirus.

3

Protección del sistema informático

La mayoría de los sitios web oficiales de los antivirus ofrecen la posibilidad de realizar un **chequeo en línea** de un dispositivo. Son muy útiles para analizar el equipo cuando se sospecha que este, e incluso el propio programa antivirus, pueden estar infectados.

Su uso es imprescindible para prevenir los ataques, en cualquier tipo de dispositivo informático, debiendo utilizarse en toda clase de ordenadores.

Antivirus Kaspersky en un portátil.

3

Protección del sistema informático

3.2 Cortafuegos

Cuando se navega por la web, se descargan ficheros o se lee el correo electrónico, por ejemplo, se produce una continua **entrada y salida de datos** entre las aplicaciones e internet. Esto puede ser aprovechado por los atacantes, 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,** que determinan qué tipo de conexiones puede realizar cada aplicación (navegador web, correo electrónico, juego, antivirus...).

Cuando un cortafuegos detecta que una aplicación intenta comunicarse con internet sin tener permiso, este muestra un mensaje en el que se pide al usuario o la usuaria que autorice o deniegue esta trasferencia de datos. Así, los cortafuegos evitan que las personas intrusas tengan acceso a las redes privadas o a los equipos conectados a internet. No obstante, no protegen a los dispositivos frente a otros tipos de software malicioso, por lo que suelen ser un **complemento adicional** a las soluciones antivirus.

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 característico de que un equipo está infectado es su **ralentización,** debida a que los datos recopilados (historial de navegación, búsquedas realizadas, datos privados, etc.) se envían a quienes realizan el ataque. Por lo general, el *adware* usa la información recolectada para mostrar publicidad personalizada a quien utiliza el equipo.

3.4 Copias de seguridad

Los datos almacenados en un dispositivo pueden resultar dañados por software malicioso, ataques externos, fallos en el hardware, accidentes, etc. Para evitarlo, es posible realizar una **copia de seguridad** o *backup*. Esta contiene todos los **datos** que se desean **proteger** y permite **recuperarlos** en el momento necesario. Así, garantiza dos de los cuatro principios básicos que persigue la seguridad informática: la integridad y disponibilidad.

El sistema operativo permite planificarlas, para que se hagan de forma **automática** periódicamente o de forma **manual.** Se debe almacenar la información en soportes externos o en la nube, a fin de preservarla en caso de avería o accidente.

4

Identidad digital

4.1 Identidad personal y digital

La identidad de una persona, tradicionalmente, ha estado asociada al **conjunto de datos y rasgos** que la hacen única, como su huella dactilar, aspecto físico, lugar de nacimiento, etc. En la sociedad del conocimiento, estos se complementan con su identidad digital, que está vinculada unívocamente a cada una, y requiere de mecanismos para acreditarse y firmar documentos como el DNIe, los certificados digitales, las firmas electrónicas, técnicas biométricas, etc.

La **identidad digital** es el conjunto de **información sobre una persona,** que está expuesta **en internet.** Está formada por los datos personales, vídeos, comentarios, gustos, las imágenes, noticias, amistades, aficiones, etc.

Todos ellos **describen** a alguien en internet y **determinan** su trayectoria.

4

Identidad digital

4.2 Huella digital y marca personal

Las **acciones que se realizan en internet,** como navegar, crear listas de reproducción, comprar, retuitear, etc., **junto con la información** que se publica en la web, **van dejando una huella digital** a lo largo del tiempo, que se denomina ***marca personal.***

Cada persona debe ser consciente de la importancia de **gestionar** adecuadamente su identidad digital y su marca personal, teniendo en cuenta que no dependen solo de ella, ya que también están definidas por la información que publican otras personas.

Por otra parte, es importante **configurar** adecuadamente los dispositivos, las aplicaciones y los sitios web, para mantener la privacidad. Aunque existe la posibilidad de solicitar a ciertas plataformas que eliminen la información personal, una vez que se encuentra en internet, se pierde el control sobre ella, y se desconoce quién o cuándo la verá.

4

Identidad digital

4.3 Reputación *online*

La **reputación *online*** es la **opinión o consideración social** de una persona o una empresa **en internet,** basándose en los datos publicados, es decir, en su identidad digital o su marca personal.

Esta no siempre coincide con la real, pero contar con una buena reputación *online* puede ser esencial para tener éxito, tanto en el ámbito personal como en el mundo profesional.

Algunos de los **riesgos** a los que queda expuesta son la suplantación de identidad, el etiquetado por terceras personas en redes sociales, las publicaciones falsas o la falta de privacidad.

4

Identidad digital

4.4 DNIe

El **DNIe,** DNI electrónico o documento nacional de identidad electrónico es el documento emitido por la Dirección General de la Policía que, además de acreditar físicamente la identidad de su titular, permite:

- **Certificar, de forma electrónica e inequívoca, la identidad de la persona.**
- **Firmar digitalmente documentos electrónicos,** confiriéndoles una validez jurídica equivalente a la que les otorga la firma manuscrita.

Es un **instrumento de impulso** de la sociedad del conocimiento, dado que permite trasladar, al mundo digital, las mismas certezas del mundo físico. Para ello, incorpora un pequeño **circuito integrado o chip,** que contiene, digitalizados, los datos personales, la fotografía, firma y huella dactilar, junto con el **certificado digital** y de **firma electrónica.**

Para su **utilización,** es imprescindible contar con un lector de tarjetas inteligentes o un dispositivo inalámbrico con tecnología *near-field communication* (NFC); un PIN, para efectuar trámites, y el software, con el que acceder a su chip, disponible en www.dnielectronico.es.

4

Identidad digital

4.5 Certificado digital

El **certificado digital** permite **autentificar y garantizar la confidencialidad** de las comunicaciones entre las personas, empresas u otras instituciones, **a través de las redes abiertas** de comunicación.

Gracias a él, se asegura que únicamente su propietario o propietaria puede acceder a la información, evitando suplantaciones.

Actualmente, en España, además del incluido en el DNIe, hay otros certificados digitales emitidos por diversas autoridades de certificación, entre ellas la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM).

4.6 Firma electrónica

La **firma electrónica** es un **conjunto de datos** que acompañan o que están **asociados a un documento digital, para identificar** a la persona firmante, de manera inequívoca, **y velar por** que **un documento firmado** se mantenga fiel al original.

Tiene el mismo propósito que la manuscrita, sin que la persona firmante esté presente físicamente para plasmarla.

Para firmar un documento, es necesario disponer de un certificado digital o DNIe y una aplicación, como AutoFirma, VALIDe, Adobe Acrobat, etc.

5

Protección de la información

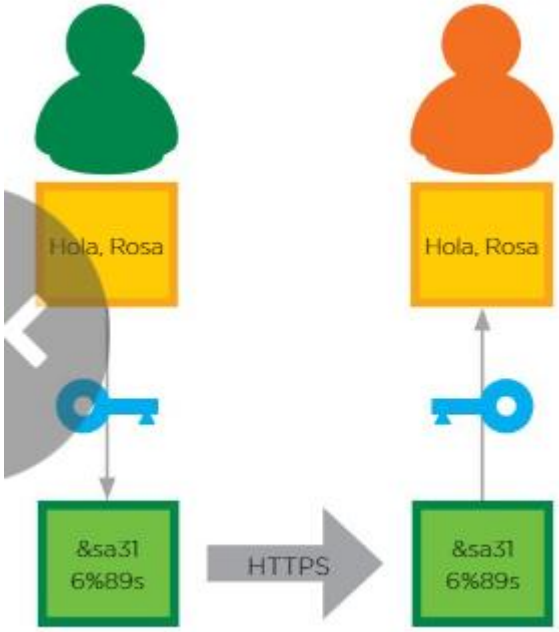
5.1 Crear contraseñas seguras

El método habitual para identificarse, y poder acceder a la información personal que se almacena en los dispositivos o en internet, es mediante el uso de **contraseñas.** Para evitar que personas malintencionadas consigan descifrarlas, es importante que sean **seguras.** Algunas **pautas** que deben tenerse en cuenta para ello son:

- **Utilizar, como mínimo, ocho caracteres, combinando mayúsculas, minúsculas, números y símbolos.**
- **Cambiarla periódicamente,** para reducir la probabilidad de que se vea comprometida con el paso del tiempo.
- **Evitar incluir datos personales,** como el nombre, la edad, la fecha de nacimiento, el teléfono, etc.
- **Aportar los datos necesarios para recuperarla** en caso de olvido, tales como el número de teléfono móvil o una cuenta de correo alternativa. Si hay que añadir una pregunta de seguridad, **nunca** se debe utilizar una cuya **respuesta** sea **fácil** de averiguar.
- **Emplear contraseñas diferentes** para evitar que, si se vulnera la de alguna aplicación o web, el resto también se vean afectadas.

5

Protección de la información



Comunicación encriptada.

5.2 Criptografía

El término ***criptografía,*** derivado de las palabras griegas *kryptós* ('oculto') y *graphé* ('escritura'), designa a una **técnica** utilizada **para ocultar datos,** de manera que **solo las personas autorizadas puedan entenderlos.**

Así, la **encriptación de datos** consiste en hacer incomprensible la información, aplicándole **algoritmos matemáticos** antes de almacenarla o enviarla a través de la red. Se utiliza al navegar por páginas con protocolos seguros, al utilizar los certificados y las firmas digitales, etc.

5.3 Protocolos seguros

Internet es una red pública, por lo que cualquier información que se envía por este medio podría ser interceptada.

Los **protocolos de seguridad** son un conjunto de **normas** comunes **que facilitan** la **comunicación** de forma **confidencial** a través de las redes.

En la navegación por internet, se utiliza el **protocolo seguro de transferencia de hipertexto (HTTPS),** que permite establecer una conexión segura utilizando la encriptación, para impedir el acceso a los datos intercambiados entre un dispositivo y el servidor al que se conecta.

No obstante, muchos sitios de internet utilizan el **protocolo de transferencia de hipertexto (HTTP)** y envían información **sin codificar,** por lo que es muy importante comprobar que su URL cambia a HTTPS, cuando se realizan operaciones que requieran privacidad.

5

Protección de la información

Consejos para usar la red de forma segura

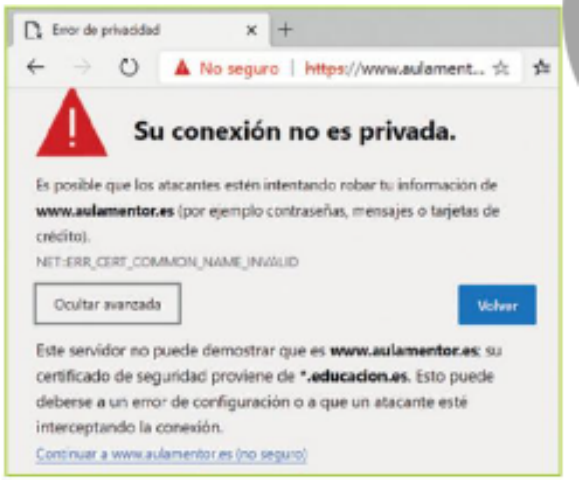
- Proteger el dispositivo con contraseñas y bloquear la pantalla cuando deja de utilizarse, para evitar que lo utilicen personas desconocidas.
- No facilitar datos personales, si no se conoce a la persona destinataria y el uso que hará de ellos.
- No enviar información importante cuando la conexión no sea segura (protocolo HTTP) o no esté encriptada.
- Mantener actualizado el sistema operativo y los programas, para evitar ataques que aprovechen sus vulnerabilidades.
- Utilizar herramientas de seguridad, como antivirus y cortafuegos, para mantener el equipo protegido.
- Realizar copias de seguridad con frecuencia, para recuperar la información en caso de pérdida.
- Emplear contraseñas seguras, que no deben ser reveladas a nadie y cambiarlas periódicamente.
- Verificar la legitimidad de los sitios web antes de proceder a la descarga de archivos, hacer compras, etc.
- Eliminar mensajes sospechosos sin abrirlos. Nunca hay que responder ni abrir sus enlaces o archivos adjuntos.
- Respetar los derechos de autoría. Las descargas ilegales y el software pirata pueden causar graves daños.
- Activar la verificación en dos pasos, siempre que sea factible, para que, además del usuario y la contraseña, se solicite algún dato biométrico, código enviado al teléfono, confirmación en una *app*, etc.
- Utilizar el sentido común y mantener una actitud crítica, para detectar software malintencionado o posibles fraudes.

5.4 Verificar la legitimidad de una página web

Una forma de evitar ser estafados en internet es asegurarse de que la página web visitada **no es fraudulenta.** Algunas **técnicas** para verificar su legitimidad son las siguientes:

- **Examinar su certificado digital.** Las páginas con certificado válido incluyen un **candado** a la izquierda de la dirección y, haciendo doble clic sobre él, se pueden comprobar sus detalles.
- **Comprobar que la página sea HTTPS.** Especialmente, en caso de utilizarla para enviar información o datos personales. Todas las páginas certificadas son HTTPS y, aunque en el navegador se suelen mostrar de forma acortada, cuando se hace doble clic sobre su URL, se despliega completa y se puede verificar.
- **Revisar que la URL sea correcta.** Podría existir una página fraudulenta con una dirección casi idéntica, pero en la que se ha cambiado algún símbolo o su extensión no se corresponde con la original. Por ejemplo, www.anayaeducaci0n.es.
- **Activar las herramientas de seguridad del navegador.** Permiten controlar la información que pueden usar y mostrar los sitios web (ubicación, cámara, tipo de contenido, etc.), además de proteger la navegación frente a eventos o sitios peligros.
- **Reconocer las señales de software malicioso.** Suelen ser sitios web en los que se despliegan muchas ventanas emergentes, al colocar el ratón sobre un enlace aparece una dirección diferente a la indicada, se realizan redirecciones maliciosas, se inician descargas no solicitadas, hay errores ortográficos, existen advertencias del motor de búsqueda al acceder, etc.

Página web sin certificado electrónico.



Advertencia del navegador al intentar acceder a una página web no segura.

6

Riesgos y precauciones en el uso de la red

6.1 Correo electrónico y mensajería instantánea

El correo electrónico y la mensajería instantánea son dos de los **servicios de comunicación más utilizados** en internet. Su popularidad también los convierte en medios habituales para la difusión de software malicioso y contenidos no solicitados, por lo que quienes deseen propagarlos cuentan con la ventaja de poder hacerlo **de forma masiva e inmediata.**

Algunos de los riesgos relacionados con el uso de estas tecnologías son, principalmente, la recopilación de contactos o direcciones de correo, la suplantación de identidad, la difusión de noticias falsas y la propagación de software malicioso.

Para mejorar la seguridad en su uso, es conveniente utilizar contraseñas robustas, descartar los mensajes sospechosos, no abrir archivos adjuntos, hacer clic únicamente en enlaces confiables y no enviar información que comprometa la privacidad de otras personas.

6

Riesgos y precauciones en el uso de la red

6.2 Descarga de contenidos

La red está plagada de todo tipo de contenidos, fácilmente accesibles y con disponibilidad inmediata, por lo que muchas personas la utilizan para leer, escuchar música, ver películas y toda clase de contenidos a la carta, ya sea en *streaming* o descargándolos en sus dispositivos.

Muchos de estos contenidos se ofrecen en **sitios de descargas gratuitas** que, además de no respetar los derechos de autoría en algunos casos, pueden ser una **fuente de riesgos,** ya que los piratas informáticos los utilizan, precisamente, para atraer a sus víctimas. Por tanto, se debe evitar descargar contenidos de internet y, siempre que se haga, hay que asegurarse de que se está utilizando un **sitio oficial,** que ofrezca **garantías de seguridad.**

6.3 Intercambio de archivos

Todos los días, millones de personas intercambian una gran cantidad de archivos de diferentes tipos (música, vídeos, juegos, etc.) en la red, a través de programas específicos para esa función.

El **procedimiento** es sencillo; se instala un **programa P2P** *(peer to peer),* generalmente gratuito, que se utiliza tanto para compartir como para localizar los archivos que contienen la información deseada.

Los riesgos de esta práctica son muy elevados, ya que, además de existir la posibilidad de estar **infringiendo** los **derechos de autoría** de los contenidos, podrían descargarse **materiales ilegales** o **infectados por software malicioso.** Por otra parte, estos programas pueden **exponer** toda la **información** de las personas que los utilizan, si no se configuran adecuadamente.

6

Riesgos y precauciones en el uso de la red

6.4 Precauciones en la navegación web

A la hora de navegar de forma segura por internet, se deben adoptar ciertos **hábitos saludables** basados en el sentido común, además de contar con herramientas de protección actualizadas como antivirus. Algunas pautas que ayudarán a estar protegidos son las siguientes:

1 **Mantener el software actualizado.** Tener el antivirus, el navegador y el sistema operativo actualizados confiere más seguridad.

2 **Usar páginas seguras.** Antes de iniciar sesión o introducir datos personales en una página, confirmar que sea segura (HTTPS). En ningún caso es recomendable acceder a sitios de dudosa reputación.

3 **Evitar iniciar sesión en ordenadores de uso público.** En caso de utilizar ordenadores de bibliotecas, cibercafés, etc., es recomendable iniciar la navegación de incógnito y no acceder a páginas que requieran el uso de contraseñas o datos privados.

4 **No acceder a wifis desconocidas.** Las redes de cafeterías, centros de ocio, hoteles, etc., no suelen ser seguras, por lo que se deben evitar.

5 **No descargar ni abrir archivos desde sitios sospechosos.** Pueden contener código potencialmente malicioso.

6 **Desactivar la ubicación en la navegación.** Es importante no compartir la localización o dejar rastros de los trayectos habituales.

7 **Tapar la cámara web cuando no se use.** El ordenador podría tener *malware* instalado con la funcionalidad de activar la cámara en cualquier momento y recopilar escenas o conversaciones privadas.

8 **Activar las herramientas de control parental o filtros de contenidos.** Así se evitan contenidos sexuales o de violencia explícitos.

6

Riesgos y precauciones en el uso de la red

6.5 Protección de la privacidad en las redes sociales

Las redes sociales ponen al alcance de las personas usuarias recursos para que estas puedan interactuar y compartir información, pero hay que ser prudentes, con el fin de que esa información solo llegue a las personas deseadas. Algunas recomendaciones son:

1 **Publicar solo la información necesaria.** Los datos personales, comportamientos inapropiados, fotos personales, etc., podrían comprometer la privacidad o perjudicar a las personas implicadas, en el presente o el futuro. Desde el instante en el que se realiza una publicación, se pierde todo el control sobre su contenido, ya que, aunque se borre, otras personas pueden haberla copiado o difundido.

2 **Privatizar el perfil.** Por seguridad, solo deberían ver la información las personas que se desee y siempre que sean conocidas. Hay que pensar bien qué información se comparte y valorar qué podrían hacer otras personas con esos datos.

7

Preservar el bienestar digital y evitar fraudes en internet

7.1 Bienestar digital

El **bienestar digital** hace referencia a la búsqueda de un **equilibrio** entre el **uso de las tecnologías** informáticas y el **resto de las actividades** que se desarrollan a diario.

Actualmente, las herramientas digitales están muy presentes en las actividades diarias y contribuyen al bienestar de las personas, pero es necesario hacer un uso responsable de ellas y conocer sus límites. No obstante, esta relación puede volverse tóxica, debido a la hiper-conexión de la sociedad actual, provocando que muchas personas estén continuamente pendientes de mensajes instantáneos, llamadas, correos electrónicos, redes sociales, notificaciones, etc.

7

Preservar el bienestar digital y evitar fraudes en internet

Consecuencias de un uso inadecuado de la tecnología

El **mal uso tecnológico** impacta en el bienestar de las personas y puede derivar en problemas tan diversos como los siguientes:

- **Trastornos en la salud,** como el estrés, el insomnio, la ansiedad, la depresión o la fatiga, que provocan, entre otras muchas cosas, mal humor, desmotivación y un menor rendimiento.
- **Tecnoadicciones,** experimentando la necesidad incontrolable de utilizar redes sociales, videojuegos, chats, dispositivos tecnológicos, etcétera. Se caracterizan por la aparición de los síntomas de tolerancia, abstinencia y dependencia.
- **Aislamiento,** disminuyendo la capacidad de relación con los demás y deteriorando las relaciones con la familia, las amistades, etc.
- **Pérdida de tiempo,** al pasar largos períodos delante de dispositivos, que repercutirá en los estudios y en el resto de las actividades.

Es importante saber utilizar los dispositivos para conseguir su objetivo, que es mejorar la vida de las personas, no para apartarlas de ella.

7

Preservar el bienestar digital y evitar fraudes en internet

Hábitos saludables para preservar el bienestar digital

Para preservar el bienestar digital, es importante adoptar hábitos saludables como los siguientes:

1 Utilizar la **tecnología con fines funcionales** y prácticos.

2 **Dedicar tiempo a actividades presenciales** con otras personas.

3 **Organizar y planificar** conscientemente las tareas diarias.

4 **Focalizar la atención** en lo que se realiza en cada momento, evitando distraerse por los estímulos tecnológicos.

5 **Desconectar** de la tecnología, practicar ejercicio físico, descansar y dormir las horas necesarias.

6 Utilizar alguna **herramienta de bienestar digital** que monitorice y ayude a controlar la actividad con dispositivos digitales.

El uso adecuado de la tecnología permite aprovechar todo su potencial y disfrutar de sus beneficios, logrando un equilibrio entre cantidad y calidad.

7

Preservar el bienestar digital y evitar fraudes en internet

7.2 Fraudes en internet

El uso de las nuevas tecnologías e internet incrementan el riesgo de ser víctimas de fraudes cibernéticos. Si se toman en consideración algunas medidas de seguridad, es posible limitar la exposición a estos delitos, preservando el bienestar digital.

Las **amenazas** más importantes suelen afectar a los servicios que requieren una **especial confidencialidad:** la banca *online*, el comercio electrónico, los trámites con la Administración, etc.

Suplantación de identidad

Uno de los principales fraudes sufridos por las personas menores es la suplantación de identidad. En este grupo de edad, es frecuente un **exceso de confianza,** lo que les hace más vulnerables.

La **suplantación de identidad** es un **delito** que tiene lugar cuando **alguien se hace pasar por otra persona** y utiliza sus datos para realizar acciones ilegales.

7

Preservar el bienestar digital y evitar fraudes en internet

Ingeniería social

Para llevar a cabo los fraudes, una de las prácticas habituales suele ser la ingeniería social, consistente en **obtener información confidencial, a través de engaños.** Los piratas informáticos se aprovechan del desconocimiento y la confianza de sus víctimas, para emplear técnicas como el *baiting, phishing, vishing,* etc. Pueden utilizar correos electrónicos y sitios web falsos, con los que **simulan pertenecer** a organizaciones legítimas.

Detección del fraude

Existen varios **indicios** que alertan de este tipo de fraudes, tales como:

- **Ofertas inverosímiles.** Hay que sospechar de artículos o viajes exageradamente baratos, trabajos en los que se ganan grandes cantidades de dinero con facilidad, etc.
- **Correos inesperados.** Incluyen archivos adjuntos con software malicioso y suelen redactarse usando un traductor automático. Pueden enviarse desde contactos conocidos que han sido infectados, por lo que hay que prestar atención a su contenido.
- **Sorteos en los que se gana un premio sin participar.** La estafa suele consistir en obtener los datos personales de la víctima y solicitar el pago por adelantado de los costes de envío o aduana de artículos que nunca llegan.
- **Comentarios sobre tiendas fraudulentas.** En tiendas *online,* los comentarios de otros compradores y compradoras sobre su experiencia pueden ayudar a detectar un posible fraude.

8

Consecuencias del uso prolongado de las tecnologías