# Tema 1: Ética en la interacción en la red.

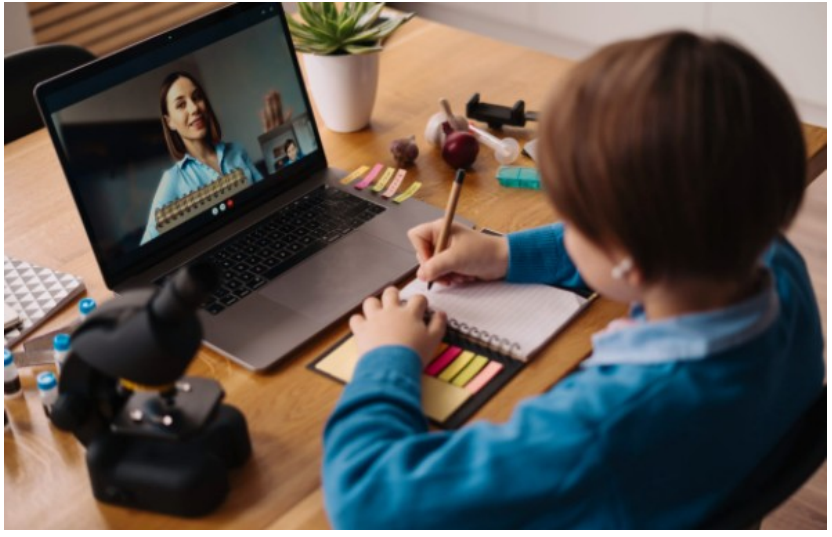
CUESTIONES SOCIALES, ÉTICAS, LEGALES Y DE LA SALUD

Los ordenadores son parte de la vida personal, laboral, social y política. Más allá de aquellas que vemos, encontramos una gran cantidad de computadoras invisibles que utilizamos a diario, como las que controlan importantes funciones en lavarropas, juegos electrónicos, ascensores, automóviles.

Como otras aplicaciones tecnológicas (por ejemplo, la energía atómica), la tecnología de los sistemas de información puede ser usada para elevar la calidad de vida del ser humano, o en su contra.

El gran desafío que vive la humanidad es el de asimilar esta tecnología para el bien general evitando los efectos negativos que puede provocar.

Muchos son los impactos sociales de esta tecnología, resultando necesario orientar y motivar la búsqueda y profundización de sus efectos positivos.



# Responsabilidad ética y legal

Existen comportamientos en el uso de la tecnología informática que infringen la ley, estos son delitos asociados a la informática.

- El uso de una clave restringida, por algún empleado de una organización, para obtener y divulgar información privada.

- El fraude en un banco, adulterando movimientos o saldos de cuentas.

- El fraude con tarjetas de crédito y de débito en cajeros automáticos.

- La realización de copias ilegales de software, violando los derechos de autor, con el consiguiente efecto negativo, tanto en el autor como en el financiamiento de futuros desarrollos.

No se puede estimar la cantidad de dinero que se pierde por delitos telemáticos, pero sí puede afirmarse  que es significativo. Esto aunque —lamentablemente no hay información cierta— debido a que:

-Muchos de estos delitos no son denunciados por los damnificados, pues su divulgación puede ser nociva para la marcha de sus negocios. Tal el caso de bancos que sufren estos delitos y no los denuncian, para que su imagen de seguridad no se vea afectada.

-Otros tantos, como la venta de información, son de difícil cuantificación.

Por ejemplo los conocidos hackers, personas que utilizan sus conocimientos con fines ilícitos y/o amorales, tales como acceso ilegal a sistemas para obtener información para su divulgación, modificación, realizar chantajes y otras actividades delictivas en beneficio personal o crear virus con el solo objeto del daño. Han entrado, por ejemplo, en sistemas de aerolíneas, consiguiendo pasajes a su favor; en sistemas bancarios, sustrayendo fondos; y en sistemas de compras con tarjetas de crédito, utilizando nombres y números de terceros.

# Investiga (actividad en aula virtual)

Investiga de qué se tratan los siguientes delitos telemáticos, y cómo dañan a las personas o instituciones y empresas afectadas:

- Ciberbullying.
- Sexting (divulgación de mensajes y fotos privadas).
- Bulos / Fake news.
- Grooming.
- Sextorsión.
- Ciberterrorismo.
- Fraude financiero.
- Scamming.

# Seguridad informática

Una vez vistas algunas de las amenazas que nos acechan cuando nos conectamos a internet, vamos a profundizar más en estos conceptos.

Entendemos por **seguridad informática** el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad.

**Virus informáticos.** Los virus de ordenador adquieren mucha importancia en una sociedad informatizada, pero no son los únicos enemigos contra los que nos debemos proteger.

# Sistema Íntegro y Sistema Confidencial

Un **sistema es íntegro** si impide la modificación de la información a cualquier usuario que no haya sido autorizado con anterioridad.

**Un sistema es confidencial** si impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.

Estas características que restringen el uso de la información deben ir unidas siempre al concepto de disponibilidad, pues los sistemas deben estar disponibles para que los usuarios autorizados puedan hacer un uso adecuado de ellos.

Según todo esto, ¿crees poseer un sistema informático seguro en tu casa o en tu aula de informática? ¿Puede ver tus archivos cualquier usuario que trabaje con tu mismo ordenador? ¿Proteges tu identidad usando contraseñas y claves de acceso?

A menudo restamos importancia a la seguridad de nuestro ordenador excusándonos en reflexiones como estas: «mi ordenador no es importante», «¿quién va a querer entrar en mis archivos?», «mientras no introduzca discos con virus, mi ordenador estará seguro». La práctica nos demuestra que todo ordenador debe estar protegido en mayor o menor medida y los usuarios deben acostumbrarse a prácticas que aumenten la seguridad de sus equipos.

### *Malware*

Software creado para instalarse en un ordenador ajeno sin el conocimiento del usuario. Su finalidad consiste en obtener información y en ralentizar el funcionamiento o destruir archivos. En esta categoría de software se encuentran los virus, los gusanos, los troyanos y los espías.

# ¿Contra quién debemos protegernos?

- **Contra nosotros mismos,** que en numerosas ocasiones borramos archivos sin darnos cuenta, eliminamos programas necesarios para la seguridad o aceptamos correos electrónicos perjudiciales para el sistema.
- **Contra los accidentes y averías** que pueden hacer que se estropee nuestro ordenador y perdamos datos necesarios.
- **Contra usuarios intrusos** que, bien desde el mismo ordenador, bien desde otro equipo de la red, puedan acceder a datos de nuestro equipo.
- **Contra software malicioso o *malware,*** es decir, programas que aprovechan un acceso a nuestro ordenador para instalarse y obtener información, dañar el sistema o incluso llegar a inutilizarlo por completo.

# Seguridad Activa y Pasiva

Podemos diferenciar dos tipos de herramientas o prácticas recomendables relacionadas con la seguridad:

- Las **técnicas de seguridad activa**, cuyo fin es evitar daños a los sistemas informáticos:

  1. El empleo de **contraseñas adecuadas.**
  2. La **encriptación de los datos.**
  3. El uso de **software de seguridad informática.**

- Las **técnicas o prácticas de seguridad pasiva,** cuyo fin es minimizar los efectos o desastres causados por un accidente, un usuario o *malware.* Las prácticas de seguridad pasiva más recomendables son estas:

  1. El **uso de hardware adecuado** frente a accidentes y averías (refrigeración del sistema, conexiones eléctricas adecuadas, utilización de dispositivos SAI, etcétera).
  2. La realización de **copias de seguridad de los datos** y del sistema operativo en más de un soporte y en distintas ubicaciones físicas.

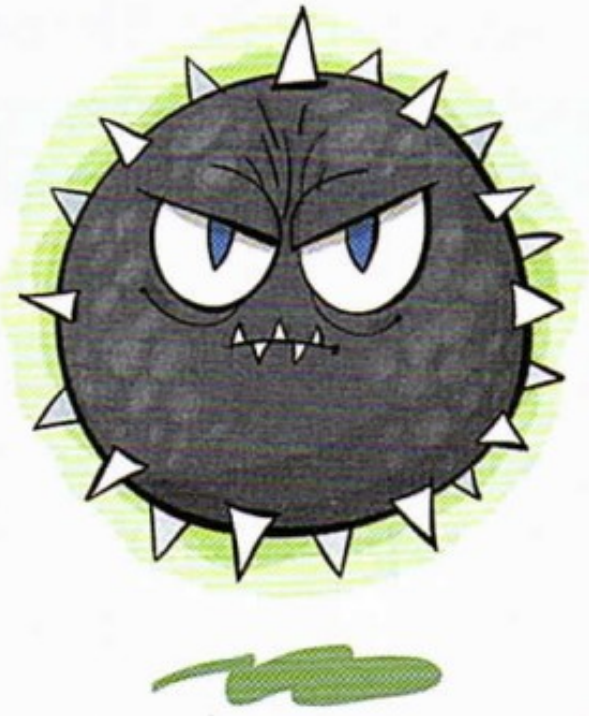
Una práctica muy aconsejable ya explicada anteriormente es la creación de **particiones lógicas en el disco duro** para poder almacenar archivos y *back-up*[1] en una unidad distinta que el sistema operativo.

# Las amenazas silenciosas

Nuestro ordenador se encuentra expuesto a una serie de **pequeños programas o software malicioso** que puede introducirse en el sistema por medio de los correos electrónicos, la navegación por páginas web falsas o infectadas, la transmisión de archivos contaminados desde soportes como discos magnéticos, unidades de memoria, CD, DVD, etcétera. Podemos encontrar los siguientes tipos de software malicioso:

- Virus
- Gusano
- Troyano
- Dialer
- Espía
- Spam
- Pharming
- Miner (Cryptomonedas)

- **Virus informático.** Es un programa que se instala en el ordenador sin el conocimiento de su usuario y cuya finalidad es propagarse a otros equipos y ejecutar las acciones para las que fueron diseñados. Estas funciones van desde pequeñas bromas que no implican la destrucción de archivos, pasando por la ralentización o apagado del sistema, hasta la destrucción total de discos duros.



- **Gusano informático.** Es un tipo de virus cuya finalidad es multiplicarse e infectar todos los nodos de una red de ordenadores. Aunque no suelen implicar la destrucción de archivos, sí ralentizan el funcionamiento de los ordenadores infectados y de toda su red.
  Suelen acompañar a un correo electrónico malicioso y muchos tiene la capacidad de enviarse automáticamente a todos los contactos del programa gestor de correo. Independientemente de los sistemas de protección que utilicemos en nuestro ordenador, siempre es recomendable ser cauteloso a la hora de abrir correos electrónicos.

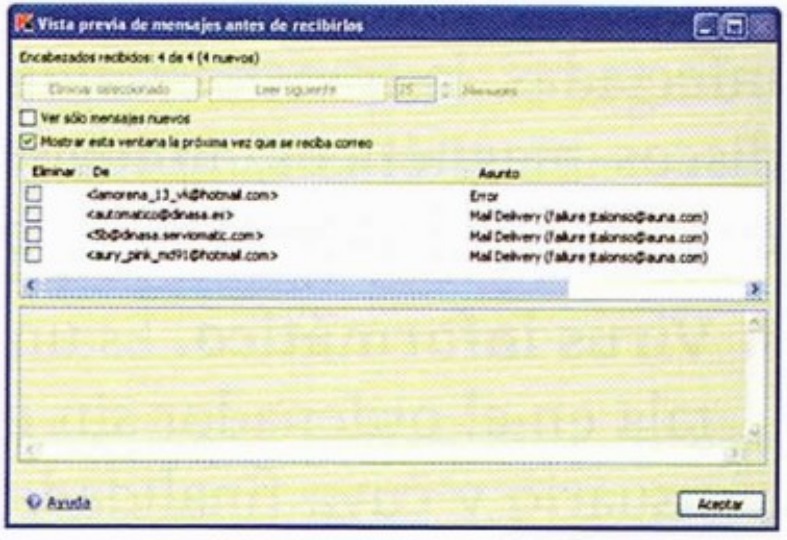
- **Troyano.** Es una pequeña aplicación escondida en otros programas de utilidades, fondos de pantalla, imágenes etc., cuya finalidad no es destruir información, sino disponer de una puerta de entrada a nuestro ordenador para que otro usuario o aplicación recopile información de nuestro ordenador o incluso tome el control absoluto de nuestro equipo de una forma remota. Los sistemas de transmisión que utilizan son el acompañamiento con software y medios como la web, el correo electrónico, los chats o los servidores ftp.

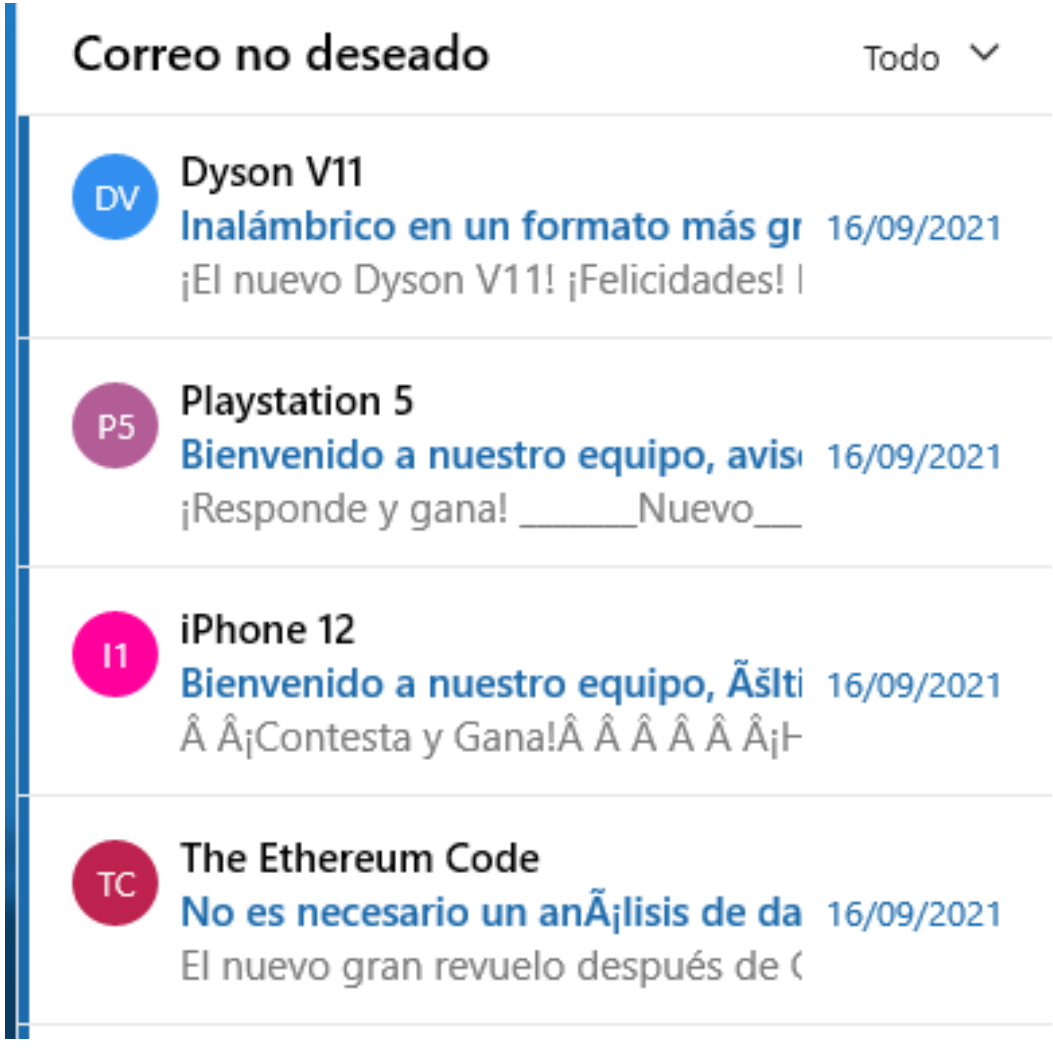
- ***Dialers.*** Son programas que se instalan en el ordenador y utilizan el módem telefónico de conexión a Internet del usuario para realizar llamadas telefónicas de alto coste, lo que provoca grandes gastos al usuario y beneficios económicos al creador del *dialer.* Si la conexión a Internet se realiza mediante un *router* ADSL, se evita este problema. Es aconsejable indicar a nuestro proveedor telefónico que nos bloquee las llamadas a servicios telefónicos de pago (teléfonos 803,806 y 807).

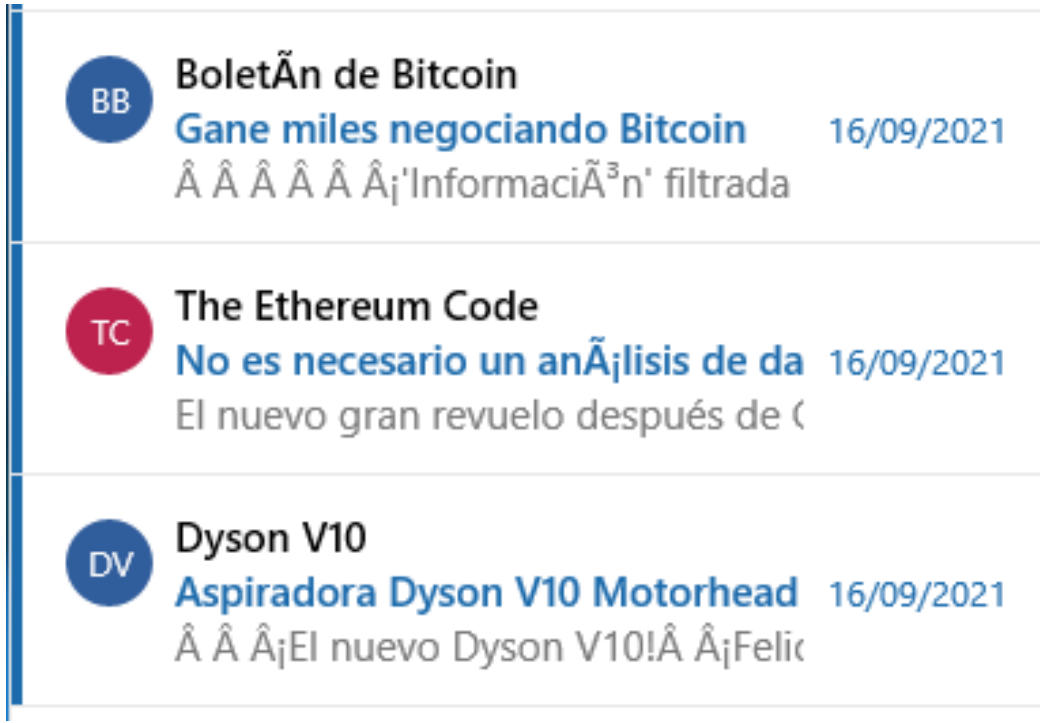
- **Espía.** Un programa espía o *spyware* es un programa que se instala en el ordenador sin conocimiento del usuario y cuya finalidad es recopilar información sobre el usuario para enviarla a servidores de Internet que son gestionados por compañías de publicidad. La información que recopila un espía suele ser utilizada para enviarnos *spam* o correo basura. Los ordenadores infectados con *spyware* ven muy ralentizada su conexión a Internet.

- ***Spam.*** También conocido como **correo basura,** consiste en el envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico existente. Tiene como finalidad vender sus productos. Los principales perjuicios que nos ocasiona es la saturación de los servidores de correo y la ocultación de otros correos maliciosos. Muchos de los paquetes de software de seguridad actual incluyen filtros contra el correo no deseado.

  Aparte de los **filtros antispam,** la opción **Vista previa de encabezados** (antes de su descarga) nos evita descargar correo no deseado desde el servidor.




Correo no deseado
Todo
DV
Dyson V11
Inalámbrico en un formato más gr
16/09/2021
¡El nuevo Dyson V11! ¡Felicidades! I
P5
Playstation 5
Bienvenido a nuestro equipo, avis
16/09/2021
¡Responde y gana! _____Nuevo__
I1
iPhone 12
Bienvenido a nuestro equipo, Ãšlti
16/09/2021
Â Â¡Contesta y Gana!Â Â Â Â Â Â¡H
TC
The Ethereum Code
No es necesario un anÃ¡lisis de da
16/09/2021
El nuevo gran revuelo después de (


BB
BoletÃn de Bitcoin
Gane miles negociando Bitcoin
16/09/2021
Â Â Â Â Â Â¡'InformaciÃ³n' filtrada
TC
The Ethereum Code
No es necesario un anÃ¡lisis de da
16/09/2021
El nuevo gran revuelo después de (
DV
Dyson V10
Aspiradora Dyson V10 Motorhead
16/09/2021
Â Â Â¡El nuevo Dyson V10!Â Â¡Felic

- ***Phishing*** (*pesca* de datos). Práctica delictiva que consiste en obtener información confidencial de los usuarios de banca electrónica mediante el envío de correos electrónicos que solicitan dicha información. Esta estafa se disimula dando al correo el aspecto oficial de nuestro banco y utilizando la misma imagen corporativa.

Phishing.

Correos españa <[redacted]@bradfordskips.com>

Carta Certificada CD 61278791640

CORREOS

Su paquete ha llegado a **30 de agosto de 2016**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

CD 61278791640

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de 9,79 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado

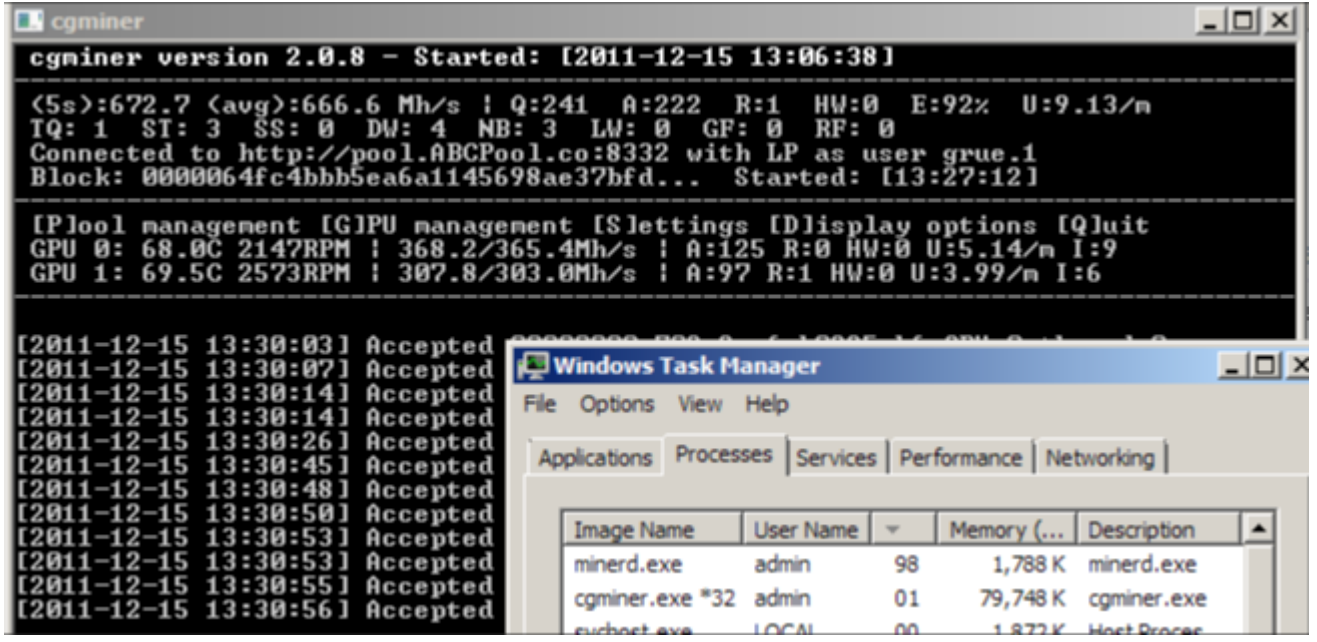
- ***Pharming.*** Consiste en la suplantación de páginas web por parte de un servidor local que está instalado en el equipo sin que el usuario lo sepa. La suplantación suele utilizarse para obtener datos bancarios de los usuarios y cometer delitos económicos.

El Pharming nace del Phishing, sin embargo es MÁS PELIGROSO.

En el Phishing el atacante pone el cebo (email falso simulando ser una empresa respetable) y espera a que la víctima caiga; en el Pharming el delincuente identifica y persigue activamente al usuario manufacturando malwares o llevando a cabo manipulaciones conscientes de la red.

Mientras que en el phishing la diferencia entre el éxito y el fracaso del robo de datos dependen de si la víctima hace clic en un enlace determinado e introduce sus datos bancarios, en el pharming, la simple presencia en la red ya es sinónimo de peligro.

- **Miners:** con el auge de las cryptomonedas han aparecido programas maliciosos que se instalan en tu equipo sin tu consentimiento y se dedican a utilizar el procesador, memoria RAM y tarjeta gráfica para hacer minado de cryptomonedas en segundo plano, sin que te des cuenta, ralentizando el funcionamiento del ordenador y haciendo que consuma mucha más energía, con el consecuente aumento del gasto en la factura eléctrica.

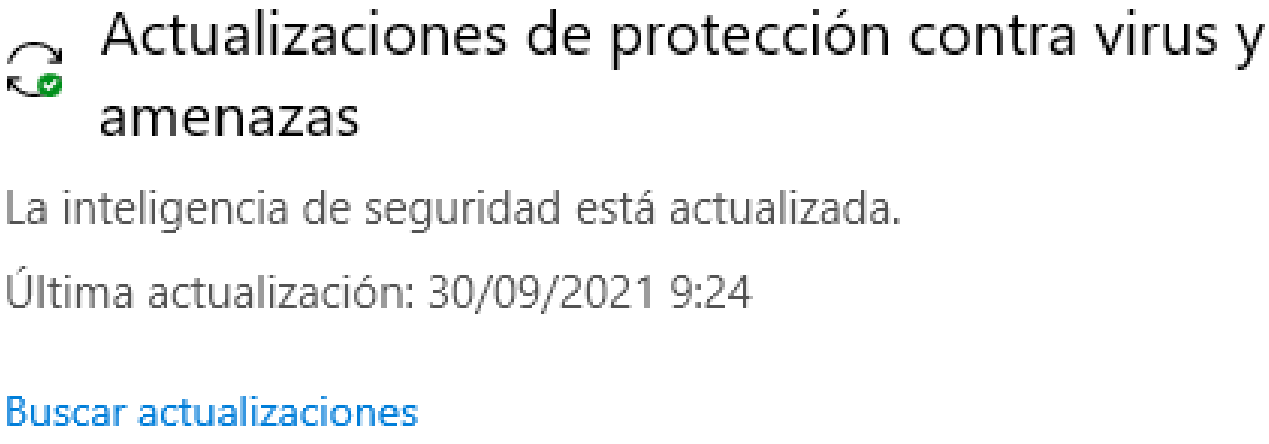


# Protección ante amenazas

- Antivirus

Un programa **antivirus** es un programa cuya finalidad es detectar, impedir la ejecución y eliminar software malicioso como virus informáticos, gusanos, espías y troyanos.

El funcionamiento de un programa antivirus consiste en **comparar los archivos** analizados con su base de datos de archivos maliciosos, también llamados **firmas.** Para que su funcionamiento sea efectivo, la base de datos debe estar actualizada, ya que aparecen nuevos virus constantemente. Los antivirus modernos disponen de servicios de actualización automática por Internet.




Base de datos del antivirus que trae incluido Windows 10

Muchos programas antivirus también funcionan con **sistemas heurísticos.** La técnica heurística[1] de un antivirus consiste en analizar el código interno del archivo y determinar si se trata de un virus aunque no se encuentre en su base de firmas maliciosas. Esta forma de trabajo es muy importante para detectar los nuevos virus que todavía no se han incluido en las bases de datos.


[1]**heurística:** Capacidad de un sistema para evolucionar positivamente en función de su creatividad y su razonamiento.

Los programas antivirus tienen distintos niveles de protección:

- **El nivel de residente,** que consiste en ejecutar y analizar de forma continua los programas que se ejecutan en el ordenador, los correos entrantes y salientes, las páginas web, etcétera. El **antivirus residente** consume recursos de nuestro ordenador y puede ralentizar su funcionamiento.
- El **nivel de análisis completo** consiste en el **análisis de todo el ordenador,** es decir, de todos los archivos de disco duro, del sector de arranque, de la memoria RAM, etc. Los antivirus interactúan con las tareas programadas para así analizar periódicamente el sistema. Los análisis completos del sistema se van haciendo más rápidos cuanto más se repitan, ya que el antivirus marca los archivos en buen estado para evitarlos en posteriores análisis.

- Cortafuegos (Firewall).

Un programa **cortafuegos** o ***firewall*** es un programa cuya finalidad es permitir o prohibir la comunicación entre las aplicaciones de nuestro equipo y la red, así como evitar ataques intrusos desde otros equipos hacia el nuestro mediante el protocolo TCP/IP.

Se encarga de controlar el tráfico entre nuestro equipo y la red local e internet. Para que el funcionamiento de un cortafuegos sea eficaz, debe tener configuradas una serie de reglas para las aplicaciones que tienen permiso de comunicación con la red, (explorador de internet, cliente de correo, aplicación de actualización del antivirus, etc.) y prohibir la comunicación de aplicaciones que no queremos que interactúen con internet.

Cuando el cortafuegos detecta que una aplicación que intenta comunicarse con internet no tiene configuradas las reglas al respecto, emerge una ventana que nos pregunta lo que debe hacer con esa comunicación.

- Software antiespía.

Como ya hemos visto, los programas espía se instalan camuflados en nuestro ordenador cuando descargamos desde Internet utilidades gratuitas aparentemente inofensivas. Los *spyware* recopilan información sobre nuestras costumbres de navegación, los programas instalados, etc. y a menudo tiene la capacidad de *secuestrar* nuestra página de inicio del navegador y mandarnos a una página en blanco, de publicidad... mediante un funcionamiento conocido como hijacking[1].

[1] **hijacking:** Significa «secuestro» en inglés y se utiliza para denominar la práctica de cambiar la página de inicio del explorador de Internet sin permiso del usuario.

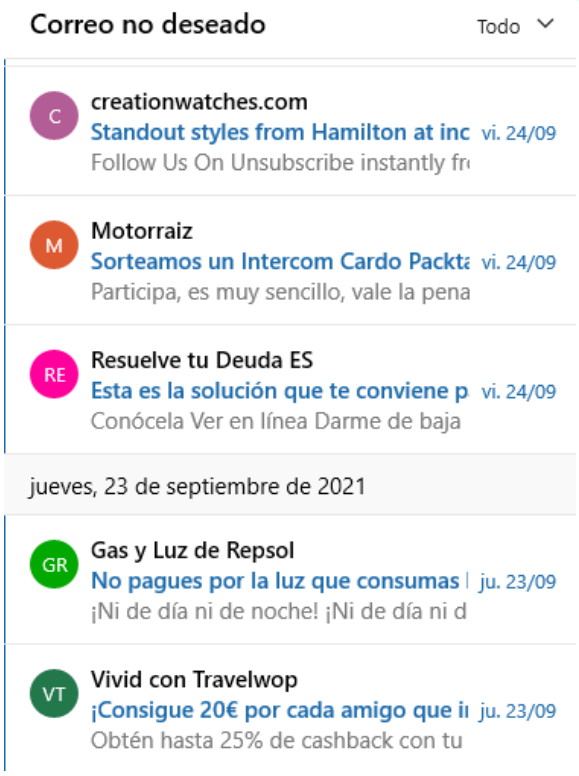
El **funcionamiento** de los programas antiespía es similar al de los antivirus, pues compara los archivos de nuestro ordenador con una base de datos de archivos espías. Por eso, también en este caso es de suma importancia mantener actualizado al programa antiespía.

Este tipo de programas es compatible con el antivirus. Es aconsejable tener instalados ambos en nuestro equipo y que se ejecuten de forma residente, es decir, que analicen el sistema de forma continua.

Los síntomas de un ordenador infectado por espías son la lentitud de funcionamiento y navegación por Internet, las excesivas ventanas emergentes en Internet y las ventanas emergentes en el sistema operativo al encender el ordenador.

- Antispam

El **software antispam** son programas basados en filtros capaces de detectar el correo basura, tanto desde el punto cliente (nuestro ordenador) como desde el punto servidor (nuestro proveedor de correo).




**Spam**

Término inglés sin traducción literal que tiene su origen en una marca de jamón enlatado americano de no muy buena calidad. Ha sido adoptado para denominar el correo masivo no deseado.

El *spam* o correo basura es enviado masiva e indiscriminadamente por empresas de publicidad. La lucha contra el correo basura resulta compleja si se pretenden respetar al mismo tiempo los correos electrónicos normales.

Estos filtros analizan los correos electrónicos antes de ser descargados por el cliente. La forma de detección está basada en listas o bases de datos de correos *spam*, en el análisis de la existencia del remitente, etcétera.

Actualmente la mayoría de los antivirus tienen integrado un filtro antispam en sus distribuciones de seguridad.

Existen dos tipos de correo electrónico: el **correo POP3,** que utiliza clientes de correo como Microsoft Outlook, Mozilla Thunderbird o Evolution de Linux Ubuntu para descargar los correos desde el servidor; y el **correo webmail,** que es visualizado a través de páginas web como Hotmail, Gmail, Mixmail o Yahoo. Los filtros antispam para estos correos actúan de la manera siguiente:

- Los filtros antispam por tecnología POP3 deben estar instalados en el ordenador cliente para interactuar con el programa de correo. Las empresas que dan servicio de *e-mail* también tienen sus propios filtros en el servidor.
- El correo webmail suele tener sus propios filtros antispam y antivirus. También puede bloquear remitentes y definirlos como *spamers*.

Algunos programas como **Kaspersky Internet Security** nos muestran los encabezamientos de los mensajes de correo electrónico almacenados en el servidor POP3 antes de descargarlos, de manera que podemos eliminar los mensajes no deseados antes de que lleguen a nuestro equipo.

Hoy en día los filtros antispam ya suelen venir integrados en la aplicación de correo electrónico que uses.

# Actividad

Para proteger tu equipo y tus datos de las amenazas de internet, realiza las siguientes tareas:

- Activa el antivirus de Windows con todos sus escudos.
- Comprueba si la base de datos de virus está actualizada.
- Activa el cortafuegos de windows.
- Crea un punto de restauración del sistema operativo.
- Añade al navegador de internet el programa MinerBlocker o NoMiner para evitar que usen tu equipo para minar cryptomonedas.

# Privacidad en la red

- La utilización de servicios de Internet como chats, programas de mensajería instantánea o redes sociales requiere ciertas precauciones para evitar problemas de privacidad. Uno de los problemas con el que nos podemos encontrar es que nuestras fotografías y vídeos sean almacenados por usuarios desconocidos que hagan un uso fraudulento de ellos, como editarlos a su manera para difamarnos, utilizarlos como suyos para confundir a otros usuarios, etc.
- A menudo, en estos sitios se nos solicitan datos personales y se asegura que se respetará nuestra privacidad, pero las redes sociales crecen a muy alta velocidad y puede que entre los amigos de los amigos de los amigos de tus amigos se cuele algún usuario malintencionado. En ese caso, tendrá acceso a tus datos, como por ejemplo tu fecha de cumpleaños, tus aficiones, tus contactos, las zonas de fiesta que frecuentas y tus próximas citas, por lo que ese usuario malintencionado podría llegar a localizarte o intentar hacerse amigo tuyo en los chats.

# Consejos de privacidad

- Nunca subas fotos ni vídeos comprometedores a Internet; pueden llegar a manos extrañas y utilizarse para hacerte daño.
- Nunca facilites datos exactos en tus perfiles; pueden terminar en manos de desconocidos. Siempre debes proteger tus datos personales: nombre y apellidos, dirección, DNI, teléfono, fotografías, etc.
- Configura tus perfiles para que solo los vean tus amigos directos.
- No te des de alta en estos servicios si eres menor de 14 años.

- Desconfía de los datos que te dan usuarios desconocidos; puede que no sean ciertos y que las imágenes no sean realmente suyas.
- Consulta a un adulto cuando conozcas por Internet a una persona que quiere que acudas a una cita a ciegas. Informa a tus padres de las amistades que tienes por Internet.
- Utiliza estos medios respetando a los demás; todo lo que haces y dices en Internet queda almacenado y se puede llegar a identificar. Piensa y pide permiso antes de etiquetar o subir una fotografía de alguien.
- Seguramente utilizas un nombre de usuario y una contraseña en numerosos sitios de Internet. No debes repetir estos datos en todos ellos, pues corremos el riesgo de que alguien llegue a conocer estos datos y los utilice para hacerse pasar por nosotros. Esta práctica es conocida como suplantación de la identidad y puede causarnos muchos problemas, desde conflictos con nuestros contactos, estafas en nuestro nombre o cualquier tipo de fraude.
- Utiliza la copia oculta cuando envíes un mismo correo electrónico a varios de nuestros contactos; no debemos jugar con la privacidad de estas personas, ya que puede que no se conozcan entre ellas o que no quieran que se difunda su dirección de correo electrónico. La opción CCO (con copia oculta) de los correos electrónicos nos permite escribir las direcciones de los destinatarios de un correo sin que ninguno de ellos pueda ver la dirección de los demás.

# Uso de contraseñas seguras

- Debido al amplio uso de las nuevas tecnologías, muchas personas manejan de forma habitual varias claves o contraseñas: el número pin del teléfono móvil, las contraseñas de correos electrónicos, las contraseñas bancarias (de las tarjetas de crédito, de banca electrónica). Todas son códigos secretos que solamente debe conocer el propio usuario.

# Prácticas erróneas en la elección de contraseñas.

Con el fin de recordar mejor nuestras contraseñas personales, cometemos muchos errores:

- Solemos utilizar la misma contraseña para todos los servicios. Así, cuando hackean alguno de nuestros servicios, estamos permitiendo que accedan a los demás.

- Utilizamos casi siempre contraseñas cortas. Cuanto más largas sean, más difíciles serán de desencriptar. Se recomienda que tengan al menos ocho caracteres.

- Las contraseñas que utilizamos suelen tener que ver con nosotros. Es habitual usar fechas de cumpleaños o aniversarios, nombres de familiares, etc. Cualquier ataque malintencionado realiza pruebas de contraseña con este tipo de datos.

- Acostumbramos a utilizar sólo números o sólo letras en nuestras contraseñas, lo que facilita mucho la desencriptación.

# Consejos para elegir una contraseña segura

- No utilices la misma contraseña para distintos servicios.
- Cambia tus contraseñas cada cuatro o seis meses.
- Utiliza contraseñas de más de ocho caracteres.
- Mezcla números, letras mayúsculas y minúsculas y caracteres especiales de tu teclado como @, #, $, & entre los caracteres de tu contraseña.
- Evita que el contenido de tu contraseña tenga que ver con fechas y nombres relacionados contigo.
- Sigue los consejos de los formularios que te indican la fortaleza de tu contraseña.