Cómo proteger tu seguridad online

Formación tecnológica para todos

Test de Competencias digitales

1

FORMACIÓN TIC BÁSICA 2-4 horas

Test de Competencias digitales

2

FORMACIÓN TIC ESPECIALIZADA 2-24 horas

3

FORMACIÓN TIC AVANZADA Reskilling (350h) Upskilling (50-150h)

Presencial

Talleres dirigidos
Cibernàrium Nou Barris
Bibliotecas BCN
Canódromo
Plaza Cataluña (Movistar centro)
Sants Montjuic Activa

Coaching Digital

Cibernàrium 22@

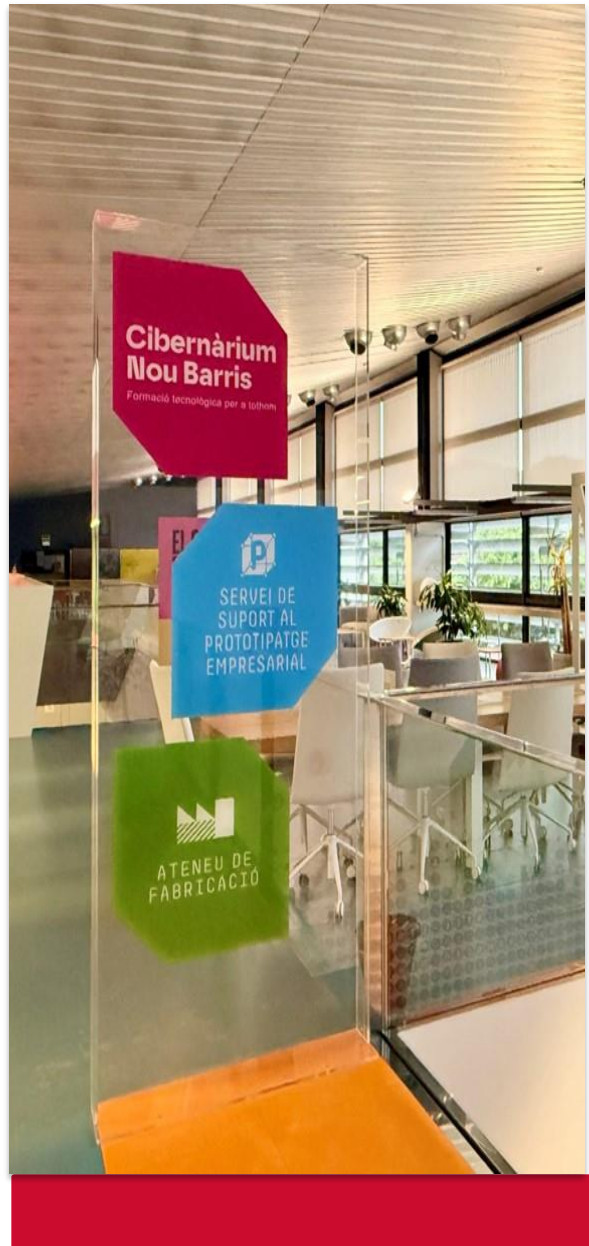
Virtual

Aulas Virtuales

VideoCápsulas

Soporte Tic

Campus Virtual, Masterclass, online...



Cómo proteger tu seguridad online

1. Software malicioso y software no deseado
2. Tipos y efectos del software malicioso
3. ¿Cómo podemos protegernos? Antivirus y Cortafuegos
4. Contraseñas y gestores de contraseñas
5. Protección de datos de carácter personal
6. Privacidad en las redes sociales
7. Privacidad en la navegación
8. ¿Quieres ampliar tu conocimiento?
9. ¿Sabías qué?

1. Software malicioso (Malware) (I)

Cuando navegamos por internet estamos **expuestos a diferentes problemas** que pueden afectar a nuestra seguridad y privacidad. Por eso es importante conocerlos para saber cuáles son, cómo actúan y qué podemos hacer para prevenirlos..

El objetivo del Malware es obtener algún beneficio económico o de otro tipo que puede suponer:

- Robo de información.
- Daños al sistema.
- Extorsión o chantaje
- Control remoto del sistema
- Molestias como mostrar anuncios no deseados, ralentizar el funcionamiento del ordenador.

1. Software malicioso y software no deseado (II)

El **software malicioso** se puede propagar de diversas maneras:

- ❑ Por correos electrónicos con adjuntos maliciosos.
- ❑ Descargas de programas no fiables.
- ❑ Vulnerabilidad del sistema a través de diferentes navegadores.
- ❑ Con dispositivos extraíbles: USB o discos duros externos.
- ❑ A través de redes sociales o mensajería instantánea.

El **software no deseado** es aquel que se instala nuestros ordenadores sin consentimiento explícito. Aunque no se malicioso como un virus puede ser molesto, porque muestra mucha publicidad, puede remplazar el ordenador o recopilar datos..

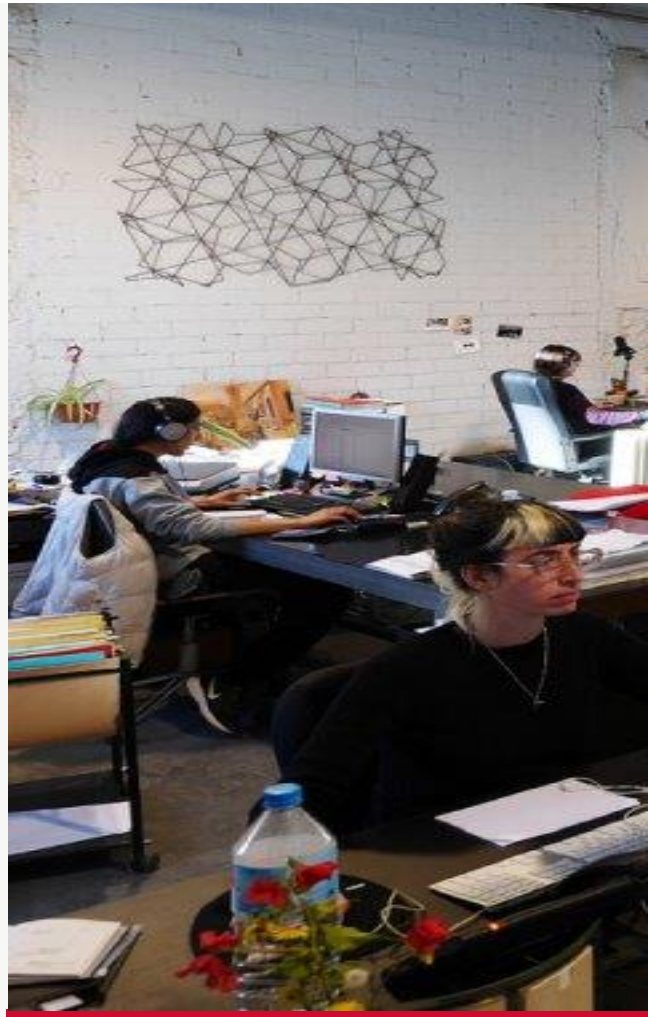
El **software no deseado** se propaga también de diversas maneras:

- ❑ A través de instalaciones de programas gratuitos
- ❑ Con anuncios engañosos.
- ❑ Descargas de sitios webs no oficiales.

2. Tipos y efectos del software malicioso

Los tipos más comunes de software malicioso son:

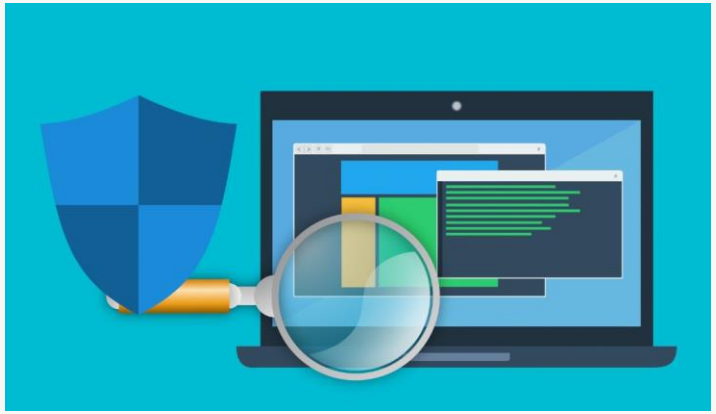
- **Virus** que se adhieren a programas o documentos cuando se usan. Incluso pueden eliminar estos documentos.
- **Gusanos**, son como los virus, pero se propagan de forma más rápida sin necesidad de abrir programas o documentos..
- **Troyanos,** parecen programas auténticos pero una vez instalados abren puertas para robar datos.
- **Ransomware,** cifran el dispositivo para que no se pueda usar y piden una recompensa a cambio.
- **Adware,** muestra publicidad no deseada.
- **Rootkits,** permiten a un tercero acceder a tu dispositivo y no se puede detectar.
- **Botnets,** son redes de ordenador afectados controlados por un atacante por envío de Spam.



3. ¿Cómo podemos protegernos?

Software malicioso

Programario malicioso



- Antivirus
- Cortafuegos
- Actualizaciones de seguridad
- Copias de seguridad
- Limitar permisos
- Sentido común

El **software malicioso** es una amenaza constante en el mundo digital y es muy importante la prevención y la vigilancia son claves para mantener nuestros sistemas seguros..

3. ¿Cómo pueden protegernos? Antivirus (II)

Un **antivirus** es un programa informático utilizado para prevenir, detectar y eliminar virus informáticos maliciosos. La mayoría de estos programas también están capacitados para detectar otras amenazas.

Antivirus

1. Gratuitos
2. Pago (más opciones de protección)

1. En línea (Menos eficaces, no hay protección permanente, sólo escaneo)
2. Escritorio

Página web de OSI (INCIBE) con análisis de antivirus gratuitos

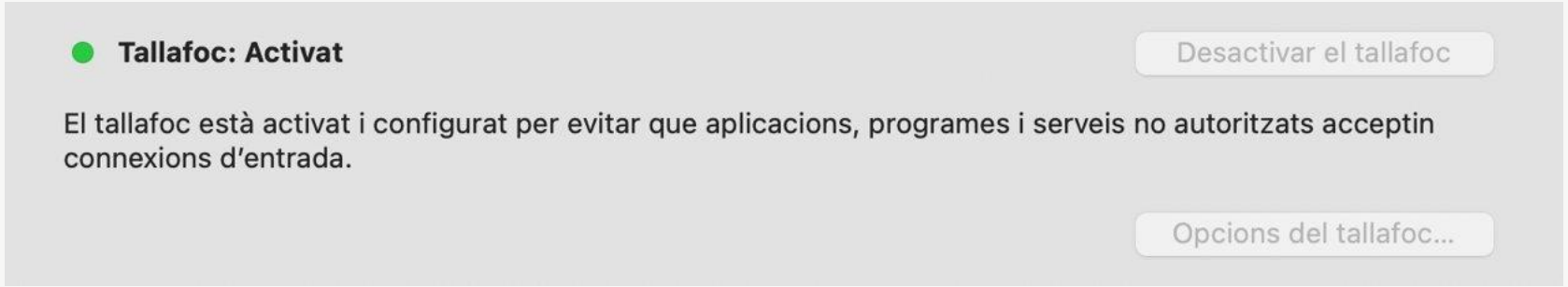
Antivirus

3. ¿Cómo podemos protegernos? Cortafuegos (III)

Un **cortafuego o Firewall** es un elemento de hardware o software utilizado en una red o equipo informático para controlar las comunicaciones, permitiéndolas o denegándolas según la configuración que le hayamos dado. Un cortafuego configurado correctamente añade protección extra.

Conseguimos:

- ✓ Proteger la información de ataques externos.
- ✓ Mantener la privacidad de la información.
- ✓ Valorada el uso abusivo de los servicios.

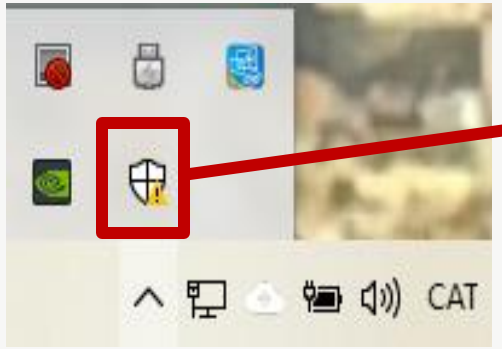


Si tenemos instalado un antivirus y lo complementamos con un cortafuegos conseguimos un buen sistema de protección.

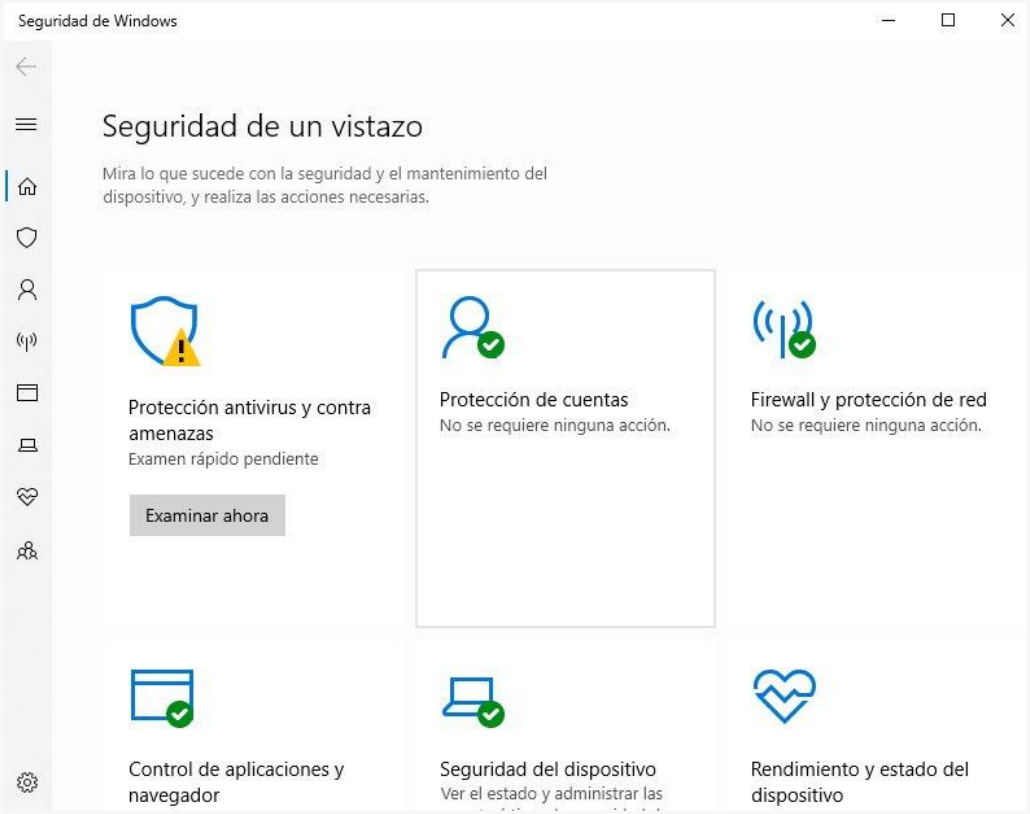
Cortafuegos

3. ¿Cómo podemos protegernos? La seguridad en Windows (IV)

La seguridad en Windows



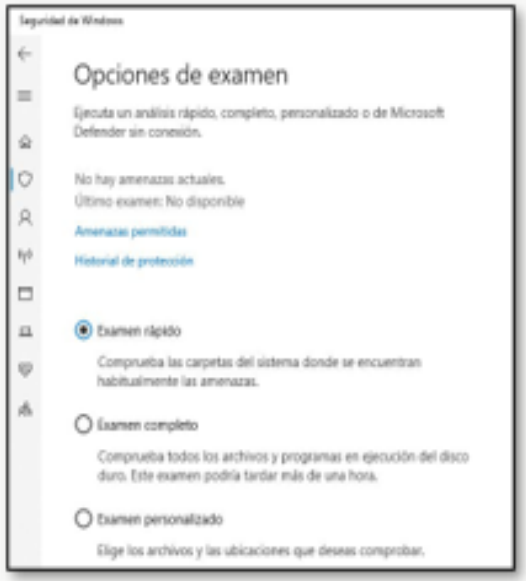
Botón para acceder a "Seguridad de Windows", desde la barra de inicio



Accedemos a este panel desde donde podemos gestionar la seguridad: Antivirus, Cortafuegos

3. ¿Cómo podemos protegernos? La seguridad en Windows (V)

La seguridad en Windows



Panel para realizar un análisis de virus. Podemos analizar todo el PC, carpetas o archivos concretos.

Panel del Cortafuegos (Firewall)

Web de Microsoft con ayuda sobre seguridad en Windows

4. Contraseñas y gestores de contraseñas

Contraseñas seguras

Otra medida de protección son las **contraseñas**, que son la primera línea de defensa para proteger nuestra información. Actualmente casi todos nuestros dispositivos y nuestras aplicaciones requieren una contraseña, por este motivo es muy importante **crear contraseñas seguras**.

CONTRASEÑA SEGURA → **entre 8 y 12 caracteres + Mayúsculas + Minúsculas + Números + Símbolos**

Las contraseñas deben ser:

ORIGINALES

No utilices información personal como el nombre, la fecha de nacimiento o el nombre de la mascota.

ALEATORIAS

Evita secuencias de números o palabras.

EXCLUSIVAS

No utilices la misma contraseña para diferentes aplicaciones o cuentas.

Vídeo Cápsula Contraseñas Seguras

4. Contraseñas y gestores de contraseñas

Contraseñas seguras

Si usamos muchas contraseñas podemos utilizar **una aplicación para gestionarlas**. Estas aplicaciones permiten almacenar varias contraseñas en una única cuenta y clave. En la tienda de aplicaciones de vuestro móvil podéis encontrar varias.

Algunos ejemplos de **Gestores de Contraseñas**

Dashlane | Keeper | LastPass | 1Password

5. Protección de datos de carácter personal

La protección de datos **es un derecho fundamental** que garantiza a las personas el control sobre su información personal. Este derecho fundamental está regulado por el **Reglamento General de Protección de Datos (RGPD)** 2016/679 del Parlamento Europeo y Consejo de 27 de abril de 2016 que en España se complementa por la **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).**

- Derecho de acceso
- Derecho de rectificación
- Derecho de oposición
- Derecho de supresión ("al olvido")
- Derecho a la limitación del tratamiento
- Derecho a la portabilidad

https://www.aepd.es/

Práctica 1 - Consulta los derechos que protegen tus datos de carácter personal a la AEPD. ¿Se mencionan en la política de privacidad de los sitios web que acostumbramos a visitar?

Datos propios

6. Privacidad en las redes sociales

Redes sociales

Es muy importante que **establezcamos el control** sobre nuestra información personal en las redes sociales, debemos controlar:

- Quién puede ver tu información personal, publicaciones y actividad
- Quién te puede encontrar, contactar y etiquetar
- Qué aplicaciones pueden acceder a tu cuenta
- Ubicación y personalización de anuncios

Práctica 2 - Revisa los ajustes de privacidad de tu cuenta en una red social que utilices habitualmente. ¿Estás compartiendo lo que pensabas?

7. Privacidad en la navegación

La privacidad a la navegación hace referencia al **grado de control que tenemos sobre nuestra información** personal mientras navegamos por las redes. En el momento que abrimos un navegador ya dejamos una huella digital que puede ser rastreada y recopila información nuestra. Es importante:

- Escoger un **navegador** centrado en la privacidad: Brave, Firefox, DuckDuckGO Browser)
- Utiliza un **buscador** también centrado en la privacidad: DuckDuckGO o Startpage.
- Gestiona las **cookies**: haz limpieza regularmente.
- Navega en modo **privado**/ **incógnito**.
- Sigues prudente con la **información que compartes**: formularios, aceptación de cookies...
- Revisa los **permisos** de los sitios webs antes de aceptar.

Navegador

Práctica 3 - Prueba las siguientes opciones de privacidad de Google Chrome. Encontrándolas también en el dispositivo móvil.

8. ¿Quieres ampliar tus conocimientos?

Saber **navegar por la red es muy útil** para nuestro día a día, pero debemos ser conscientes de que debemos hacerlo con **seguridad y protegiéndonos de posibles amenazas**, por este motivo debemos seguir los siguientes consejos:

1. **Sigues consciente de las estafas en línea** como por ejemplo el **Phishing** (robo de nuestros datos): desconfía de los correos electrónicos, SMS o mensajes que nos **piden datos personales. Verifica siempre el remitente de estos mensajes y** no te dejes llevar por las emociones.
2. **Utiliza conexión HTTPS** siempre que sea posible: asegurado que la URL empieza por https://, por lo tanto evita los lugares que sólo empiecen per http://.
3. **Mantén tus programas actualizados:** el sistema operativo, el navegador y otros programas habituales como reproductores, editores....
4. **Vigila con el Wi-Fi público**: a menudo son inseguras porque no están cifradas y cualquier persona puede acceder a tu dispositivo a través de ellas, no hagas transacciones bancarias ni compras online cuando estés conectado en estas redes..
5. **Utiliza antivirus:** una vez instalado en tu dispositivo tengas el antivirus actualizado, haz revisiones a menudo.
6. **Haz copias de seguridad** en un disco duro o nube.
7. **Revisa los permisos** de las aplicaciones y webs antes de acceder.

9. ¿Sabías qué?

El **Reglamento General de Protección de Datos (RGPD)** de la Unión Europea **es el más estricto del mundo** en materia de protección de datos.

Este reglamento se ha establecido en Europa pero afecta al resto del mundo, de esta manera **las empresas y organizaciones que quieren trabajar en Europa deben seguir esta normativa** incluso si su sede social está fuera de este territorio.

Fuente de la imagen: Universitat de Valencia

barcelonactiva.cat