Medidas de protección básicas

1 Bloquea tus dispositivos

- Configurar adecuadamente las opciones de bloqueo dificulta que alguien ajeno pueda acceder a ellos o extraer información.
- Los ordenadores de sobremesa, los portátiles y los dispositivos móviles disponen de opciones de bloqueo mediante contraseña.
- En algunos modelos de ordenadores y en la mayoría de los dispositivos móviles se puede configurar la huella dactilar.

2 Usa antivirus

- La mayoría de las amenazas que sufrimos utilizando la tecnología provienen de virus informáticos.
- Gracias a los antivirus, estos programas maliciosos, llamados malware, pueden ser detectados antes de que comiencen a ejecutarse.
- Por tanto, es importante tener instalado un antivirus no solo en tu ordenador de sobremesa o portátil sino también en móviles y tablets.

3 Descárgate aplicaciones originales

- Utilizar aplicaciones que no son originales puede suponer una seria amenaza para la seguridad de tu equipo o dispositivo.
- En el caso de los dispositivos móviles es recomendable descargar siempre las aplicaciones que instalemos de la web del fabricante o de las tiendas oficiales.

APP STORE

PLAY STORE

WEB OFICIAL

4 Controla las conexiones

- Conectarte a una red wifi sin contraseña puede facilitar el robo de nuestra información, por lo que es recomendable evitar siempre estas conexiones.
- Utiliza una contraseña tipo WPA2 en la wifi que tengas en tu vivienda.
- Controla el acceso a tu router modificando las claves de acceso que trae el dispositivo por defecto.

5 Emplea contraseñas complejas y diferenciadas

- Utiliza una contraseña diferente para cada servicio web que utilices.
- Puedes recurrir a un gestor de contraseñas para recordarlas fácilmente.
- **Para crear una contraseña segura sigue estos consejos:**
  - ✔ Alterna mayúsculas, minúsculas, números y algún carácter especial.
  - ✔ Crea contraseñas con al menos 12 caracteres.
  - ✔ No utilices datos identificativos como tu año de nacimiento, nombre, etc.
  - ✔ Evita usar palabras que aparezcan en el diccionario.