NAVEGA SEGURO POR INTERNET... Y MUCHO MÁS

LECTURA FÁCIL

Me @dministro 2.0

Federación Nacional aspaym

Subvencionado por:

Fundación Vodafone España

Colabora:

POLICÍA NACIONAL

Edita: Federación Nacional ASPAYM

Subvencionado por: Fundación Vodafone España

Coordinación y elaboración de contenidos:
- Federación Nacional ASPAYM
- ASPAYM Castilla y León
- Dirección General de la Policía. Comisaria General de Seguridad Ciudadana. Unidad Central de Participación Ciudadana

Adaptación de textos a lectura fácil:
Servicio Adapta - Plena Inclusión Madrid

Validación de textos:
Servicio Adapta – Fundación Alas Madrid

Diseño y maquetación:
Grafox Imprenta

Disponible esta publicación en: www.aspaym.org

¿QUÉ VAS A ENCONTRAR EN ESTA GUÍA?

PRESENTACIÓN DE ESTA GUÍA

Federación Nacional ASPAYM colabora
con Fundación Vodafone España
para dar cursos de formación sobre trámites en internet.
Por ejemplo, hicimos un proyecto de formación
llamado "Me @dministro 2.0: la e-Administración
para la inserción laboral".
En este proyecto, enseñamos a personas con discapacidad
a utilizar herramientas como el DNI electrónico
o los certificados electrónicos, entre otros muchos temas.

En ese proyecto nos dimos cuenta de que muchas personas
tenían problemas para protegerse en internet, por ejemplo,
evitar que les roben sus datos
o que les entre un virus informático en su ordenador.

Esta guía titulada "Navega seguro por internet… y mucho más"
cuenta cómo puede cualquier persona protegerse en internet
y en las redes sociales de muchos peligros.
Esta guía está en lectura fácil para explicar esta información
a personas que tienen más dificultades para leer.

Lo más importante es conocer cómo protegerse en internet
y saber bien lo que hay que hacer.
Por ejemplo, en caso de tener dudas,
nunca debemos aceptar un mensaje o un nuevo contacto.
Estamos seguros de que esta guía va a ser muy útil
para que muchas personas puedan saber
qué hacer para protegerse en internet.

¿CÓMO PUEDO PROTEGER MI ORDENADOR, MI MÓVIL Y MI TABLET, CUANDO USO INTERNET?

Hoy tenemos diferentes dispositivos
para conectarnos a internet.
Un dispositivo es un ordenador, un teléfono móvil o una tablet.
Las personas utilizamos estos dispositivos
para visitar páginas web, para leer, para comprar,
para ver fotografías y vídeos o para escribir correos electrónicos.

Pero internet puede ser peligroso.
Hay personas que pueden ver qué lees, qué compras,
qué vídeos y fotografías ves
o qué escribes en tus correos electrónicos.
Puedes evitar este peligro de estas formas:

- ✓ Debes proteger bien tu dispositivo.
- ✓ Debes conocer bien qué herramientas puedes utilizar.
- ✓ Debes utilizar internet con cuidado.

Los antivirus y los cortafuegos

Utiliza estas dos herramientas para proteger tu dispositivo cuando está conectado a internet:

✓ Los antivirus

Un antivirus es un programa informático.
Este programa informático sirve
para proteger tu dispositivo
de ataques de otros programas informáticos.
Los programas informáticos
que pueden atacar tu dispositivo pueden ser de 2 tipos:

- Los virus informáticos

  Un virus informático entra en tu dispositivo
  y puede tener muchos efectos.
  Por ejemplo, puede provocar que vaya más lento
  o puede dejarlo sin funcionar.
  Algunos virus pueden destruir tu ordenador
  y te impiden volver a utilizarlo.

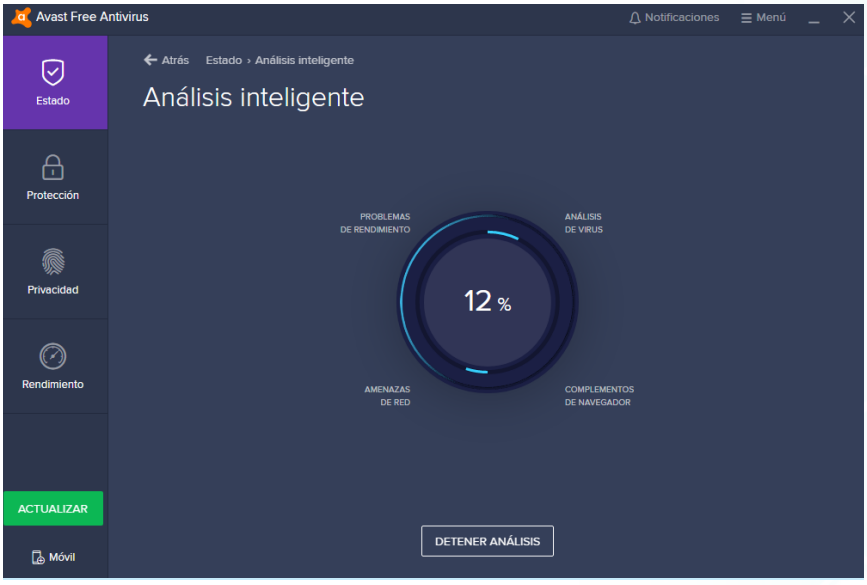
- El malware

  La palabra malware es inglesa
  y significa programa malicioso.
  El malware puede entrar
  en tu ordenador o tu móvil
  y toma nota de tus mensajes de correo electrónico
  o de las páginas web que visitas.
  Algunos malware son todavía más peligrosos
  porque bloquean tu ordenador
  y te piden dinero para desbloquearlo.

Debes proteger tu ordenador, tu móvil o tu tablet con un antivirus.

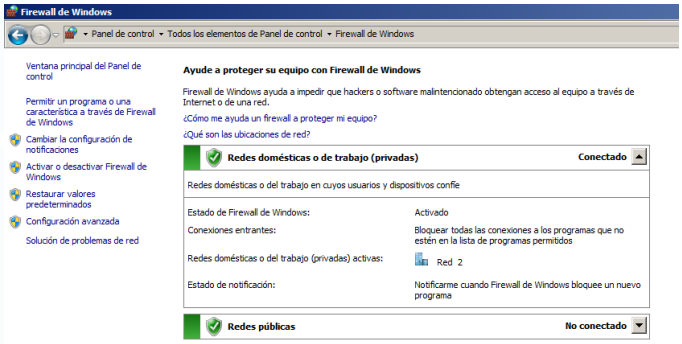
Sigue estas recomendaciones:

1. Actualiza siempre tu antivirus.
   El antivirus debe tener siempre al día el listado de posibles virus y malware.
   Así podrá reconocerlos y bloquearlos.
2. Utiliza el antivirus de vez en cuando para comprobar que tu dispositivo no tiene virus.
   Los antivirus suelen tener un botón llamado escanear, que revisa todo el dispositivo, encuentra los virus y los elimina.



✓ Los cortafuegos

Un cortafuegos es una barrera
que impide que otra persona entre en tu dispositivo
sin tu permiso.
A veces, lo encontrarás en tu dispositivo
con el nombre de firewall,
que significa cortafuegos en inglés.
Por ejemplo, un cortafuegos impide
que un pirata informático pueda entrar a tu ordenador
a través de la conexión de internet.
Un cortafuegos puede ser un aparato
o un programa informático.
Lo más habitual es que tu ordenador o tu móvil
tengan programa informático de cortafuegos ya instalado.



Sigue esta recomendación:

Una buena idea es que configures el cortafuegos.
Esto quiere decir que puedes elegir las opciones
que protegen más tu dispositivo, por ejemplo,
para proteger tu ordenador cuando te conectas
a internet en un lugar que no es tu casa o tu trabajo.

Otros peligros que debes vigilar

Los virus y el malware son 2 peligros cuando estás en internet.
Hay otros 2 peligros más que debes vigilar
cuando uses tu dispositivo:

✓ Cuidado con los archivos que descargas de internet

Un archivo puede ser un libro, un vídeo o una canción.
Cuando descargas un archivo de internet, quiere decir
que el archivo de internet pasa a tu dispositivo.
Por ejemplo, imagina que ves una página web
que te permite descargar un vídeo.
Cuando lo descargas, puedes ver el vídeo
desde tu ordenador sin estar conectado a internet.

Descargar un archivo de internet puede ser peligroso.
Algunos archivos parecen un libro, una canción o un vídeo,
pero ocultan un virus.

Sigue estas recomendaciones:

1. Fíjate quién ha puesto ese archivo en internet.
   Mira si puedes encontrar quién es el propietario
   de la página web o si hay información
   sobre el propietario del archivo.
2. ¡Ten cuidado! Descargar un archivo
   sin permiso de su propietario puede ser un delito
   y podrías tener problemas
   con la policía o los jueces.
   Mira si puedes encontrar información en la página web
   sobre las posibilidades de descargar el archivo.

3. Nunca descargues un archivo,
   si tienes alguna duda de su seguridad.
   Así evitarás infectar tu dispositivo con un virus.

✓ Cuidado con los pendrives de otras personas

La palabra pendrive es inglesa.
Un pendrive es un dispositivo
que te permite guardar tus archivos
y verlos en un ordenador.
Muchas personas los llaman USB o pinchos.
Los pendrives pueden tener virus
cuando los utilizamos en varios ordenadores.

Sigue estas recomendaciones:

1. Ten cuidado con los pendrives de otras personas
   que conectas a tu ordenador.
   Los pendrives pueden tener virus
   que pasan a tu ordenador.
2. Ten cuidado cuando utilizas tu pendrive
   en otro ordenador.
   El ordenador puede tener un virus
   que puede pasar a tu pendrive.
3. Revisa los pendrives con tu antivirus.
   Esa revisión se llama escanear.
   También puedes configurar tu antivirus
   para que revise los pendrives de forma automática
   cuando los conectes a tu ordenador.

¿CÓMO PUEDO PROTEGER MIS DATOS Y MIS ARCHIVOS?

Todos utilizamos dispositivos,
como ordenadores, teléfonos móvil y tablets,
donde guardamos muchos archivos personales.
Por ejemplo, guardamos fotos con familiares y amigos, facturas,
los números de teléfonos de conocidos o correos electrónicos.
Todos estos archivos tienen datos personales,
como tu nombre, tu dirección o tu número de cuenta bancaria.

Por eso, debes proteger tus archivos y evitar que otras personas
puedan entrar en tus dispositivos y robarlos.
Hay muchas situaciones en las que te pueden robar los datos.
Es necesario que conozcas estas situaciones
y sepas cómo evitar los robos.

Utiliza contraseñas seguras

Una contraseña es un conjunto de letras y números
que solo conoces tú para entrar en tu teléfono,
en tu correo electrónico o en tus redes sociales.
Las contraseñas deben ser seguras
para que otras personas no puedan adivinarlas.
Las contraseñas más seguras son las complicadas.
Por ejemplo, debes evitar poner tu nombre, tus apellidos
o tu fecha de nacimiento como contraseña.
Eso puede ser fácil de adivinar.

Sigue estas recomendaciones:

1. Crea una contraseña que tenga una mezcla
   de letras mayúsculas, letras minúsculas,
   números y otros signos.
2. Esta contraseña debe tener más de 8 letras,
   números y signos.
3. Utiliza contraseñas diferentes para cada red social,
   banco, aplicación o correo electrónico.
   Tener la misma contraseña para todo puede ser peligroso.
4. Cambia tus contraseñas cada 3 meses.
   Esos cambios mejoran mucho la seguridad de tus datos.
5. Nunca guardes tus contraseñas en tu ordenador,
   tu móvil o tu tablet.
   Puedes anotarlas en una libreta
   y guardarlas en un cajón u otro sitio que solo tú conozcas.

Puede parecerte complicado
que tengas que utilizar diferentes letras, números y signos
en las contraseñas y cambiarlas cada cierto tiempo.
Pero estas decisiones te ayudan a proteger mucho más tus datos.

Una idea es hacer una variante complicada de palabras sencillas.
Por ejemplo, esta contraseña es muy fácil: vivoenmadrid
Puedes hacerla difícil de esta forma: V1v03nM@dr1d
Esta contraseña mezcla letras mayúsculas, letras minúsculas,
números y signos como la @.
Puedes hacerlo con el título de una canción o un libro
o con otras palabras que elijas.

Ten cuidado con el wifi

La palabra wifi es inglesa
y se refiere a la conexión a internet sin cables.
Muchas veces vamos a sitios que tienen wifi gratis.
En este caso, el wifi te permite estar conectado a internet
y no gastar de tus datos para ver internet o utilizar Whatsapp.
Las conexiones wifi gratis abiertas sin contraseña
pueden ser peligrosas para la seguridad
de tus dispositivos y tus datos.

✓ La wifi privada

En tu casa puedes tener conexión wifi privada a internet.
Es importante que esa conexión wifi sea cerrada,
es decir, que necesites una contraseña para utilizarla.

Sigue estas recomendaciones:

- Cambia las opciones que vienen de fábrica en el router o llama a la compañía para que te ayuden a cambiarlas.
  El router es el aparato que nos permite conectarnos a internet y que nos da la wifi.

  La wifi tiene un nombre de usuario y una contraseña.
  El nombre de usuario suele tener alguna palabra que nombra a la compañía telefónica.
  Cambia el nombre de usuario y la contraseña que te da la compañía para tu wifi con las recomendaciones que te hemos dado para hacer contraseñas seguras.
- Apaga el router cuando no estés en casa o cuando no utilices la conexión a internet.
- Comprueba si un desconocido utiliza tu wifi sin tu permiso.
  Desconecta el ordenador, la tablet, el móvil y todos los aparatos de casa que utilicen internet.
  Si las luces del router parpadean, alguien está usando sin permiso tu wifi.

Consulta de nuevo las recomendaciones para hacer contraseñas seguras de la página 14

Es muy importante que vigiles
que alguien está usando en ese momento tu wifi.
Si una persona sin tu permiso comete un delito
mientras usa tu wifi, tú eres el responsable
y puedes tener problemas con la policía y los jueces.

✓ La wifi pública

En algunos sitios públicos, como museos, hoteles,
oficinas o estaciones, hay wifi de uso público.
Estas conexiones wifi a internet pueden ser peligrosas
cuando no piden una contraseña para utilizarlas.
Si te conectas a estas wifis, tus dispositivos
pueden estar en peligro de que les roben los datos.

Sigue estas recomendaciones:

- Utiliza estas wifis
  solo cuando lo necesitas de verdad.
- En el caso de que utilices estas wifis,
  debes tener un buen antivirus, un buen cortafuegos
  y todos los programas deben estar actualizados
  con las últimas mejoras.
- Existe un tipo de conexión segura a wifis abiertas
  sin contraseña llamado VPN.
  Este tipo de conexión dificulta que otra persona
  pueda robarte tus datos.
  Comprueba en tu dispositivo si tienes esta opción.
- Quita la opción de sincronizaciones automáticas
  con wifi.

Esta opción actualiza los programas
de tu ordenador o las aplicaciones de tu móvil
de forma automática
cuando te conectas a cualquier wifi.
Esto es peligroso en wifis públicas sin contraseña.
En estas actualizaciones pueden entrar virus
sin que te des cuenta.

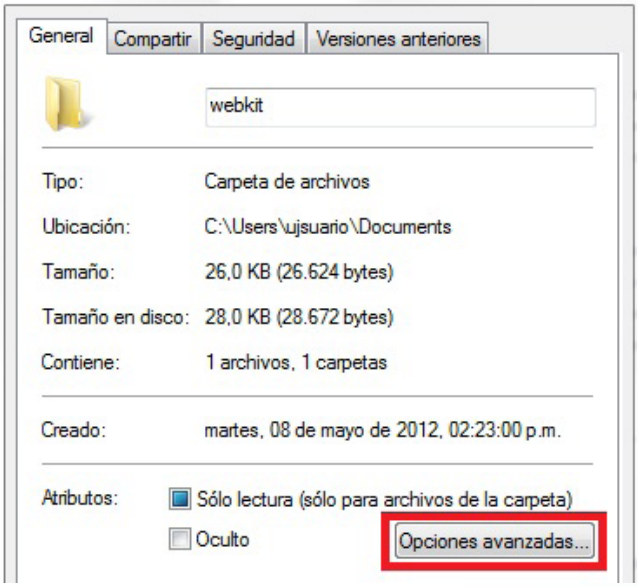
- Bloquea la opción de conexión automática a wifis.
  Muchos sitios tienen una wifi pública abierta.
  Si tienes la conexión automática activada,
  tu móvil se conecta cuando pasas por un sitio
  que tiene wifi abierta sin contraseña.
  Los piratas informáticos pueden utilizarla
  para robar tus datos.
- No entres en aplicaciones o páginas webs
  donde tengas tus datos y utilices una contraseña,
  cuando estás conectado en una wifi pública abierta.
  Por ejemplo, no entres en tu correo electrónico,
  tu cuenta bancaria ni hagas compras por internet.
- Entra solo en páginas web
  que empiezan por HTTPS.

La S significa que las páginas son seguras.
Evita las páginas que empiezan por HTTP
sin la S al final.

- Borra el nombre de la wifi de la lista de wifis de tu ordenador, tu móvil o tu tablet, cuando dejes de utilizarla.
  Borra todas las páginas web que has visitado cuando estabas conectado a la wifi pública.

Haz que tus archivos sean ilegibles para personas no autorizadas

Imagina que una persona no autorizada
entra en tu ordenador o en tu móvil.
En ese momento, puede ver todos tus documentos,
tus fotos y tus datos.
Puedes evitar ese peligro con el cifrado.



El cifrado es una forma de proteger todos tus archivos y tus datos.
El cifrado hace que la información de tu ordenador, tu tablet
o tu móvil sea ilegible para otras personas,
es decir, no pueden leer su contenido de ninguna forma.
En este caso, ilegible quiere decir que una máquina
no puede leer o comprender la información.
Para poder ver esa información, la persona no autorizada
necesitará una contraseña que tú has puesto.

Puedes poner una contraseña para el cifrado en:

- ✓ Tu ordenador, tu móvil, tu tablet
  Es necesario conocer la contraseña
  para ver toda la información.
- ✓ Los archivos, los documentos
  o las carpetas de información
  Puedes proteger con una contraseña solo algunas partes,
  pero el resto de la información
  quedará abierta para cualquiera.

Consulta de nuevo las recomendaciones para hacer contraseñas seguras de la página 14

Sigue estas recomendaciones:

- Crea una contraseña de cifrado
  con las recomendaciones que te hemos dado
  para hacer contraseñas seguras.
- Recuerda la contraseña siempre
  o anótala en un sitio seguro
  Si la olvidas, nunca más podrás volver a ver tus archivos
  ni la información que guardas.

Protege tus datos personales en los dispositivos que puedes llevar a cualquier sitio

Hace unos años solo había ordenadores de gran tamaño
que solo estaban en nuestra casa o en nuestro trabajo.
Hoy hay muchos dispositivos que almacenan información
y puedes llevar a cualquier sitio,
como, por ejemplo, un móvil, una tablet o un ordenador portátil.

En esos dispositivos guardas mucha información personal.
Por ejemplo, guardas fotos con familiares y amigos, facturas,
los números de teléfonos de conocidos o correos electrónicos.

Un pirata informático puede entrar
en cualquiera de estos dispositivos
si no los proteges de forma adecuada.
Los piratas informáticos son personas que roban tus datos,
tus contraseñas o tus documentos de tus dispositivos.
Esta situación es muy peligrosa.
Además de copiar tus datos, puede utilizarlos
para hacerse pasar por ti en internet o en las redes sociales.

Sigue estas recomendaciones:

- Crea una contraseña para entrar en el dispositivo con las recomendaciones que te hemos dado para hacer contraseñas seguras.

Consulta de nuevo las recomendaciones para hacer contraseñas seguras de la página 14

- También puedes crear un patrón,
  que es un dibujo que haces con los dedos.
  Por ejemplo, si creas un patrón, deberás hacer ese dibujo
  para desbloquear el móvil o la tablet
  y poder ver la información.
  Cifra la información que tengas en el dispositivo
  con las recomendaciones que te hemos dado
  para cifrar los archivos.

Limpia las cookies cada cierto tiempo

La palabra cookies es inglesa.
Esta palabra nombra unos pequeños archivos
que se guardan de forma automática en nuestro ordenador
cuando entramos en una página web.
Las cookies guardan datos tuyos, por ejemplo:

- ✓ El idioma que utilizas para entrar en internet.
- ✓ Las páginas que has visto.
- ✓ Los anuncios que has visitado.
- ✓ El tiempo que has estado en la página.
- ✓ La hora a la que has entrado.
- ✓ Si has dado tu correo electrónico por alguna razón.

En España, la ley obliga a que las páginas webs
avisen de que tienen cookies
y de la información que pueden ver de ti esas cookies.
La ley también les obliga a las páginas web
a que puedas aceptar o rechazar las cookies.
Por eso, aparece un aviso de que tienes que aceptar
o rechazar las cookies cuando entras en una página web nueva.

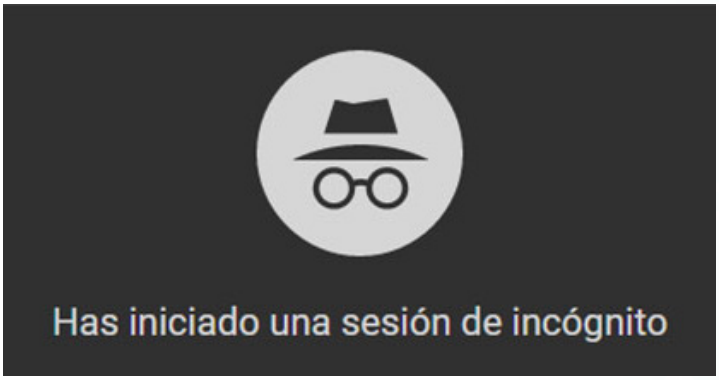
Los piratas informáticos pueden utilizar las cookies
para robar tus datos o para llevarte a páginas webs piratas
donde robarte tus datos o sacarte dinero.
Una web pirata es una página web que parece segura,
porque es muy parecida a una página web conocida.
Pero es falso, es una página web muy peligrosa.
Puedes descubrirlas porque el nombre de la página web
es muy parecido, pero tiene alguna diferencia.
Por ejemplo, una página pirata que quiere imitar a Google
podría poner goooogle en su dirección.
Es parecido, pero tiene más letras o.
Por ese motivo, debes tener cuidado con las cookies.

Sigue estas recomendaciones:

- Actualiza tu navegador de internet.
  El navegador es el programa que utilizas
  para entrar en páginas web,
  por ejemplo, Firefox, Safari, Chrome o Explorer.
  Mantén este programa al día
  y deshabilita los complementos que ya no se actualicen.
  Un complemento es un pequeño programa
  que se instala en el navegador para alguna función.
  Cuando lo deshabilitas, lo dejas desactivado.
- Entra en la configuración de tu navegador de internet
  para elegir las opciones sobre las cookies.
  Selecciona que aceptas las cookies propias de la página
  y el tiempo que permites que las cookies
  estén en tu dispositivo.

Por ejemplo, puedes elegir que duren unos días,
o hasta que dejes de navegar por internet ese día
o hasta la fecha en que las cookies se borran
de forma automática.
Elige también que aceptas las cookies de terceros
solo de las páginas webs que visitas.
Por ejemplo, las cookies de terceros son
las de los anunciantes en un periódico por internet.

- Borra la información de las páginas webs que has visitado
cada cierto tiempo.
Esa información incluye las cookies,
los datos de la página web
o las imágenes que has descargado.
- Lee siempre los mensajes de aviso
que aparecen en la página web.
Nunca aceptes el mensaje hasta que no lo hayas leído
y entendido bien.
- Elige la opción de navegar de incógnito
o navegar de forma privada para proteger tus datos.



La navegación de incógnito
o la navegación de forma privada
es una opción de los navegadores para evitar
que las páginas webs que visitas se queden con tus datos.

- Haz un escaneo de tu dispositivo con el antivirus
cada cierto tiempo.

¿CÓMO PUEDO PROTEGER MIS DATOS PERSONALES Y MIS IMÁGENES PERSONALES?

Casi siempre, los problemas de las personas en internet vienen por sus propios errores.
Tú puedes tener todo tipo de protección, pero es inútil:

- ✓ Si descargas un programa o un archivo de internet por tu propia decisión y tiene un virus dentro.
- ✓ Si pones una contraseña muy sencilla de adivinar para entrar en tu correo electrónico o tus redes sociales.
- ✓ Si compartes información personal en tus redes sociales, por ejemplo, fotos personales.

Por eso, debes evitar compartir datos personales.

Cuida tus datos personales

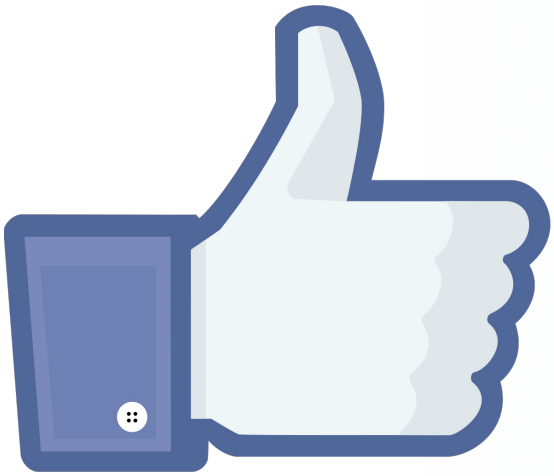
Un dato personal es una información
que solo compartirías con una persona de confianza.
Tu nombre y tus apellidos, tu número de teléfono,
tu correo electrónico, tu número de DNI o tu currículum
son datos personales.
Se llaman datos personales porque te permiten identificarte,
es decir, reconocerte y diferenciarte del resto de las personas.

Sigue estas recomendaciones:

- Recuerda que las empresas que tienen una página web deben cumplir las leyes de protección de datos. Estas páginas web deben explicar de forma clara qué datos personales guardan de ti, para qué los utilizan y qué leyes de protección de datos deben cumplir.
- Evita subir datos personales a las redes sociales. Cuanta más información compartas, más personas con malas intenciones podrán aprovecharse de ella.
- Lo mejor es compartir los datos personales en persona en vez de a través de internet.
- Comprueba qué páginas web visitas y a qué correos electrónicos respondes antes de dar cualquier dato personal.

Cuida tu imagen digital

La imagen digital es la forma que tenemos
de mostrarnos en internet o en las redes sociales.
Cada persona crea su imagen digital en internet.
cada vez que sube una foto o un vídeo,
da un "me gusta" en Facebook o retuitea en Twitter,
o escribe un comentario a una noticia publicada en un periódico.



La reputación se refiere a la fama que tiene una persona.
Tener buena reputación es tener buena fama,
es decir, los demás tienen una buena opinión de una persona.
La reputación digital es la forma que tienen de vernos
los demás en internet.
Las fotos, los vídeos o las opiniones que publicas
van a afectar a cómo te ven los demás.
Esto influirá en cómo se comporten o se comuniquen
los demás contigo en internet y también cara a cara.

La huella digital es el rastro que dejas en internet
cada vez que publicas una foto, un vídeo o un comentario.
La huella digital es difícil de borrar.

Sigue estas recomendaciones:

- Ten mucho cuidado con todo lo que publicas en internet o en las redes sociales, porque:
  - ✓ Una mala imagen en internet o en las redes sociales puede hacerte mucho daño en tu vida personal y social.
  - ✓ Todo lo que publicas en internet o en las redes sociales deja de pertenecerte. Cualquier persona puede utilizarlo para bien o para mal, a tu favor o en tu contra.

¿CÓMO DEBO PROTEGERME EN LAS REDES SOCIALES?

Las redes sociales son lugares de reunión
y para compartir información en internet.
Hay muchas muy conocidas, como Facebook, Twitter o Instagram.
Los usuarios de estas redes abren una cuenta
y publican a través de un perfil.
El perfil es la forma de presentarse en la red social,
por ejemplo, la foto, mis gustos, datos personales.

En las redes sociales hay muchas personas
que participan con perfiles y nombres falsos.
Es difícil saber quién tiene un nombre verdadero
y quién tiene un nombre falso.
Muchas personas se hacen pasar por otras
y pueden robar tus datos o sacarte dinero.
Por eso, debes tener cuidado con las personas
que te contactan por redes sociales.
Una forma de evitar estos problemas es limitar
quién puede ver los mensajes o imágenes que publicas.

Sigue estas recomendaciones:

- Elige el nivel privado en tus redes sociales
  dentro de la configuración de privacidad.
  En el nivel público, cualquier persona puede ver
  lo que publicas.
  En el nivel privado, solo las personas
  que tú permites y conoces pueden ver lo que publicas.
  Si das permiso a desconocidos,
  puedes tener los mismos problemas.
- Evita compartir tus datos personales de forma pública.
  Si los compartes pueden saber, por ejemplo,
  dónde estás en cada momento, a qué sitios vas,
  por dónde paseas.
- Comparte datos de otras personas solo con su permiso.
  Compartir datos de otras personas sin permiso
  puede ser un delito.
- Trata a los demás como quieres que te traten a ti.
  Antes de publicar un comentario, hazte esta pregunta:
  ¿Le diría lo mismo si estuviera delante de él o de ella?
  Los insultos o las amenazas son malos comportamientos
  y también pueden ser delitos.
- Desconfía de los perfiles de redes sociales
  de los que tengas dudas.
  Por ejemplo, desconfía de los perfiles de personas
  que aparecen con un nombre muy raro,
  o que publican mensajes que no tienen mucho sentido,
  o que solo ponen enlaces sin ningún texto.

Las redes sociales tienen formas de averiguar
si los perfiles son falsos o no
en el caso de personas famosas o de empresas.
Pero no pueden comprobar lo mismo
con el resto de los perfiles de personas.

- Puedes pedir que borren los datos
que has publicado en internet o en las redes sociales.
También puedes pedir que borren los datos
que otros han publicado por ti de forma incorrecta.
Este derecho a que borren esos datos
se llama derecho al olvido.

¿QUÉ PUEDO HACER CUANDO SUFRO ACOSO POR INTERNET?

Una persona acosa a otra cuando le altera su día a día sin permiso y de forma continua con malas intenciones, por ejemplo:

- ✓ El acosador vigila o persigue al acosado.
- ✓ El acosador busca estar siempre cerca del acosado.
- ✓ El acosador se pone en contacto con el acosado por cualquier medio, como teléfono, cartas o incluso a través de otras personas.
- ✓ El acosador utiliza los datos personales del acosado para hacer compras o se los da a otras personas para que se pongan en contacto con el acosado sin su permiso para que también le acosen.
- ✓ El acosador impide que el acosado se sienta libre o daña su casa u otras posesiones.

El acoso es un delito grave.
Un juez puede castigar a un acosador con hasta 2 años de cárcel.

El acoso a través de internet se llama ciberacoso.
Hay varias formas de ciberacoso:

- ✓ Ciberacoso general

  Un adulto acosa a otro adulto o un menor de edad acosa a otro menor de edad sin relación con el colegio.

- ✓ Ciberacoso sexual

  Un adulto acosa a otro adulto
  con la intención de tener relaciones sexuales.

- ✓ Ciberacoso sexual a menores de edad

  Un adulto acosa a un menor de edad
  con la intención de tener relaciones sexuales.
  El ciberacoso sexual a menores de edad también se conoce
  por la palabra inglesa grooming.

- ✓ Ciberacoso escolar

  Un menor de edad acosa a otro menor de edad
  relacionado con el colegio.
  El ciberacoso escolar también se conoce
  por la palabra inglesa ciberbullying.

El ciberacoso es grave por varias razones:

- ✓ El acosador puede acosar a la persona sin estar cerca,
  por ejemplo, con mensajes de móvil,
  a través de las redes sociales,
  en juegos por internet o en chats.
- ✓ Es difícil ver el problema porque el acosado no lo cuenta,
  por ejemplo, por miedo o por vergüenza
- ✓ El acosador se aprovecha de que puede ocultar
  su identidad verdadera a través de internet
  o de las redes sociales.

Soy víctima de un acosador por internet, ¿qué puedo hacer?

Sigue estas recomendaciones:

1. Cuéntale a un adulto de tu confianza que sufres acoso, si tienes menos de 18 años.
2. No respondas a los mensajes del acosador.
3. Bloquea las llamadas y mensajes del acosador.
4. Cambia las contraseñas de tu correo electrónico, tus redes sociales, tus aplicaciones, tu banco y cualquier otra.
5. Reúne todas las pruebas que puedas contra el acosador.
   Por ejemplo, los mensajes que te envía, las conversaciones por el chat, fotografías y vídeos.
6. Denuncia que sufres acoso a la empresa propietaria de las redes sociales.
7. Denuncia el acoso a la policía y en los juzgados.

Soy testigo de un caso de acoso por internet, ¿qué puedo hacer?

Sigue estas recomendaciones:

1. Nunca participes en el acoso a otra persona
   Serás parte del delito.
2. Si te enteras de esta situación, defiende al acosado.
3. Denuncia el acoso en las redes sociales y a la policía o pide ayuda a un adulto para denunciar.

MÁS INFORMACIÓN SOBRE EL CIBERACOSO:

Mira en la web

www.policia.es

Pide información en el correo electrónico

participa@policia.es