CIBER EXPERT@

FORMACIÓN EN EL USO SEGURO DE INTERNET


POLICÍA
NACIONAL

CIBER EXPERT@

ÍNDICE

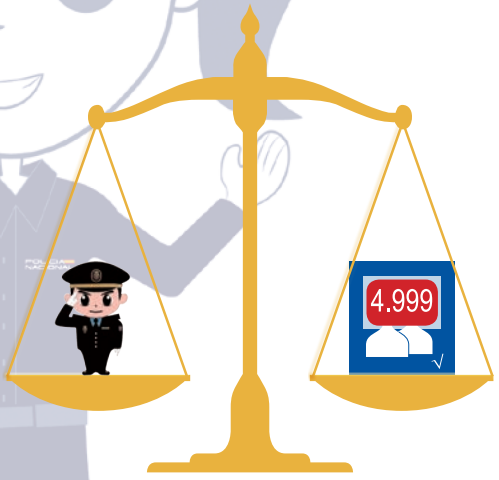
1. IDENTIDAD DIGITAL: CÓMO AFECTA A LA VIDA REAL

¿QUÉ ES?

Las publicaciones en los perfiles de nuestras redes sociales, las fotos, los vídeos, las personas a las que seguimos, nuestros seguidores, los "me gusta", los comentarios que hacemos... Todo lo que hacemos en internet conforma nuestra Identidad Digital.

En una balanza, colocamos a un lado la popularidad, el número de seguidores, amigos, comentarios, etc. Al otro, situamos la seguridad de nuestra privacidad.

Somos nosotros los que decidimos a cuál de los dos factores otorgamos más peso.



DERECHOS EN LA RED

Las distintas leyes de Protección de Datos existentes reconocen una serie de derechos conocidos como «derechos **ARCO**».

Acceso: derecho a solicitar y obtener gratuitamente información de nuestros propios datos de carácter personal.

Rectificación: derecho a que se modifiquen los datos que resulten ser inexactos o incompletos.

Cancelación: derecho a que se supriman los datos que resulten ser inadecuados o excesivos.

Oposición: derecho a que no se lleve a cabo el tratamiento de nuestros datos de carácter personal.

Y por encima de todos ellos, existe el **derecho al olvido**, a que no se difunda nuestra información personal en internet.

Debemos cuidar la imagen que damos en internet igual que cuidamos la imagen real.

2. NETIQUETA: COMPORTAMIENTO EN LÍNEA

¿QUÉ ES?

Es el conjunto de normas de buen comportamiento que utilizamos en el ciberespacio para comunicarnos con otros usuarios, siendo de especial importancia relacionarse de manera empática y respetuosa.

¿QUÉ HAGO? ¡OJO!

En caso de ser víctima de un mal comportamiento *online*, cuéntaselo a un adulto.

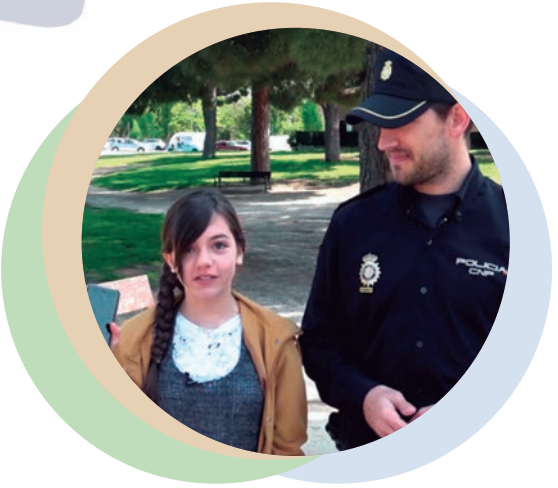
Contesta siempre de acuerdo a las normas de la *netiqueta*, aunque quien te ataque no lo haga.

Finaliza las discusiones con una frase breve e ignora los siguientes mensajes.

Bloquea a la persona que realiza el ataque y denúncialo a la red social en caso de ser necesario.

En caso de ser el autor de un mal comportamiento en la red, busca ayuda, asesórate y pide disculpas.

En caso de ataques graves, denuncia ante las Fuerzas y Cuerpos de Seguridad.



3. REDES SOCIALES Y GESTIÓN DE LA PRIVACIDAD

¿QUÉ SON?

Son lugares en Internet en los que todo el mundo puede participar (normalmente muchos usuarios al mismo tiempo) y que se centran en las relaciones entre las personas (de familia, de amistad, de trabajo, por algún interés en común...).

CONDICIONES DE USO

¡OJO!

Cuando se hace un perfil en una red social, aparece una pantalla en la que nos indican las **normas** y las **condiciones de uso** de la misma.

- Propiedad intelectual de la red
- Obligación de actualizar los datos
- Rastreo de tu ubicación
- Limitación de contenidos
- Publicidad personalizada
- Edad mínima de 14 años para usarlas

GESTIÓN DE LA PRIVACIDAD

La **privacidad** es la protección que le damos a los datos que introducimos en los perfiles de nuestras redes sociales.

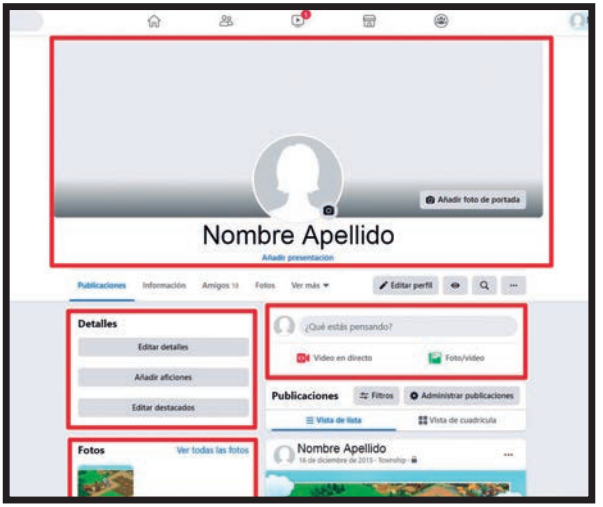
Podemos dividir la privacidad en dos: **pública y privada**.
Sin embargo, por el uso que se le da, podemos hablar de tres categorías:

- Privado: asegurándonos de que todos a los que agregamos son quienes dicen ser.
- Privado: pero con desconocidos agregados.
- Público: todo el mundo puede ver nuestras publicaciones.

REGALAR INFORMACIÓN

Es importante tener cuidado con los datos que aportamos a las redes sociales.

DATOS PRIVADOS



- Nombre
- Apellidos
- DNI
- Domicilio
- Ideas
- Sentimientos
- Pensamientos
- Documentos
- Fotografías
- Vídeos
- Relaciones

CONTRASEÑAS

Para acceder a los correos electrónicos o
a las redes sociales, es muy importante saber crear
contraseñas con mayor nivel de seguridad.

Débil	• mesaroja • luisruiz • alba2005	• Palabras de diccionario • Nombre y apellidos • Nombre y año de nacimiento
Fuerte	• mEsArOJA • lUiSrUIZ • 20aLBa05	• Agregar números • Agregar mayúsculas y minúsculas
Muy fuerte	• ME$ArOJ4 • [U¡5rU1Z • 2º@Lb40S	• Más de ocho caracteres • Mayúsculas y minúsculas • Símbolos y números

Es necesario, para aumentar la seguridad,
el cambio periódico de contraseñas,
así como el uso de un *password* diferente
para cada cuenta (red social, correo, etc.) que poseamos.

**Podemos guardar por escrito
nuestras contraseñas,
pero no en el móvil, sino en papel,
para evitar robos de identidad.**

4. SUPLANTACIÓN DE IDENTIDAD

¿QUÉ ES?

Acción de apropiarse de los derechos y facultades de otra persona, bien sea creando un perfil falso o hackeando una cuenta existente en la Red para hacerse pasar por esa persona y utilizar sus derechos y facultades con distintos fines.

CONSECUENCIAS

- Vulneración de la intimidad a través del acceso a datos personales.
- Daños a la reputación a través de la publicación de información inapropiada en su nombre.
- Perjuicios económicos cuando se suplanta la identidad para realizar transacciones económicas.

¿ME ESTÁ PASANDO?

¡OJO!

Cuéntaselo a un adulto de confianza.

Denuncia los hechos en el servicio correspondiente (sitios webs, servidores de correo, etc.) o ante la Agencia Española de Protección de Datos.

Si la problemática continúa, denuncia ante las Fuerzas y Cuerpos de Seguridad o el Ministerio Fiscal.

Recopila todo tipo de pruebas en relación a la suplantación de identidad.

5. CIBERBULLYING

¿QUÉ ES?

Acoso producido entre menores de manera continuada e intencional, a través de dispositivos electrónicos, consistente en amenazas, humillaciones, vejaciones, etc., con graves consecuencias para su desarrollo personal.

CÓMO DETECTARLO

No existe un perfil definido de víctima de ciberacoso, si bien hay circunstancias que pueden ser indicadores de que el menor está siendo víctima de esta situación.

- Pueden producirse alteraciones del sueño y de la alimentación, sentimiento de soledad, tristeza y enfado.
- El menor parece nervioso cuando usa algún dispositivo tecnológico o deja de usarlos inesperadamente.
- Descenso en su rendimiento escolar por falta de concentración y rechazo a asistir al centro educativo.
- Aislamiento social, apatía y problemas para relacionarse.

Y SI ME PASA ¡OJO!

Habla con quien está ejerciendo dicho acoso para intentar que cese en el mismo.

Pide ayuda a algún familiar o profesor.

Busca apoyo en tu grupo de amigos.

No respondas a las provocaciones.

Usa la configuración de privacidad y si es necesario, ¡bloquea!

¡No borres las evidencias del ciberacoso y denuncia!

6. SEXTING

¿QUÉ ES?

El *sexting* consiste en enviar o publicar imágenes o vídeos de contenido sexual, realizados por el propio remitente, a otras personas, utilizando el teléfono móvil u otros dispositivos.
El principal riesgo del *sexting* es la pérdida de control de las fotografías con las consecuencias que puede tener.

CÓMO DETECTARLO

Posibles señales de alarma:

- El menor se aísla en su habitación o lleva el móvil al baño.
- Demuestra dependencia del móvil.
- Se conecta principalmente por la noche.
- Cuida su aspecto físico, le gusta hacerse selfies y subirlos en redes sociales.
- Cambios en su comportamiento; observar si tiene desórdenes alimenticios, no sale de casa, conductas disruptivas, etc.
- Está teniendo o está empezando su primera relación de pareja.

ALGUNOS CONSEJOS PREVENTIVOS

¡OJO!

A LOS MENORES:

Cuida tu imagen *online*.

Sé consciente de a quién le envías las imágenes.

Si te llega una imagen por difusión, dañina hacia otra persona, ponlo en conocimiento de una persona adulta.

NUNCA reenvíes este tipo de imágenes.

A LOS PADRES

- Reconoce el problema y habla con el menor sobre el tema.
- Informa sobre el peligro y consecuencias negativas.
- Conoce sus contactos en el ciberespacio.
- Revisa su presencia en la red.
- Ponle límites de uso del móvil y del ordenador.
- No juzgues al menor.
- Incúlcale el respeto a la propia imagen y hacia los demás.

Informa a la Policía, ya que la difusión de dichas imágenes puede tener consecuencias legales.

7. GROOMING

¿QUÉ ES?

Conjunto de técnicas de engaño que utiliza un adulto para conseguir la confianza de un menor con el objetivo de obtener de él un beneficio de carácter sexual, pudiendo buscar contacto sexual u obtener material pornográfico.

CÓMO DETECTARLO

Posibles señales de alarma:

- El menor recibe regalos o posee dinero de origen desconocido.
- Se aparta para usar el teléfono móvil.
- Se muestra poco atento o desconcentrado en clase.
- Presenta cambios de humor, aislamiento o apatía.
- Problemas de sueño, ansiedad.
- Tiene ideas suicidas o conductas autodestructivas

¡No descargues archivos de desconocidos!

CÓMO PREVENIRLO

¡OJO!

No facilites imágenes y vídeos de carácter comprometedor.

Protege el equipo con antivirus y contraseñas seguras.

Configura las opciones de privacidad.

Limita el uso de las redes abiertas.

¿Y SI ME PASA?

- No cedas al chantaje y cesa cualquier relación con el *groomer*.
- Pide que se retire del servidor la información vejatoria.
- Bloquea o elimina al acosador.
- Cuéntaselo a tus padres, familiares cercanos o alguien del entorno escolar.
- Recopila pruebas del delito y denuncia SIEMPRE.

PADRES O PROFESORES DE POSIBLES VÍCTIMAS

- Comunicación entre padres y profesores para confirmar nuestras sospechas.
- Habla con el menor para que cuente su situación y se deje ayudar.
- Proporciona al menor el apoyo necesario, no lo juzgues.
- Motívale para que cuente todos los detalles del desarrollo de su relación con el *groomer*.
- DENUNCIA la situación.

8. TECNOADICCIONES

¿QUÉ ES?

Uso excesivo e incontrolado de dispositivos tecnológicos, afectando de manera nociva a la vida del menor y su entorno.

CÓMO DETECTARLO

Posibles señales de alarma:

- Cada vez pasan más tiempo haciendo uso de las tecnologías.
- Revisan constantemente las redes sociales y mensajería instantánea.
- Se presentan más irritables y tienen problemas para relacionarse.
- Se sienten angustiados si no pueden conectarse.
- Pierden interés por otras opciones de ocio.
- Están conectados de manera continuada, incluso en horarios de dormir o comer.
- Presentan una vida sedentaria, con consecuencias como sobrepeso, cansancio, dolor de espalda, de cabeza, etc.
- Su rendimiento escolar disminuye.

¿ME ESTÁ PASANDO? ¡OJO!

Pide ayuda a padres, familiares y profesores.

Vuelve a practicar actividades que hacías anteriormente o a empezar otras nuevas.

Queda nuevamente con tu grupo de amigos y busca ocio alternativo.

Controla el tiempo de conexión mediante un horario que no incumplas.

Respeta las horas de sueño y de comida.

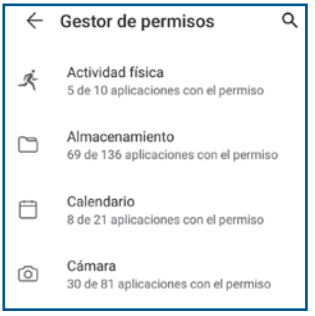
A LOS PADRES

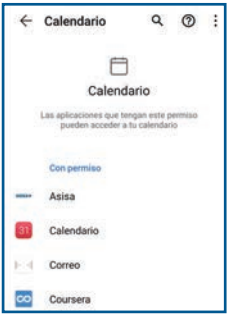
- No prohíbas, pero sí gestiona los tiempos de uso.
- Fomenta las relaciones interpersonales.
- Instala los aparatos electrónicos en estancias comunes de la casa.
- Haz uso de las aplicaciones de control parental.
- Si es necesario, pide ayuda a un especialista.

9. APP'S, JUEGOS Y CONTENIDOS INAPROPIADOS

APP'S

Las aplicaciones para móvil o tableta solicitan una serie de permisos para conectarse a los dispositivos. La primera vez que se abre la aplicación aparece un texto que lo advierte y solicita dicho permiso. También a través de los ajustes podemos controlar las aplicaciones a las que le hemos dado acceso a las distintas funciones.





JUEGOS

Los juegos de ordenador, consola o tableta,
no tienen por qué ser inadecuados para los niños.
La clave de su buen uso es la moderación.
Sin embargo, no todos los juegos que salen al mercado
son adecuados. Para distinguir cuáles lo son,
se ha creado una catalogación conocida como PEGI.

CONTENIDOS INAPROPIADOS

Todo aquel material que, percibido por un menor de edad, puede causarle un perjuicio psíquico o físico. Este material puede ser ilegal, perjudicial, o no ser entendido por motivos de su desarrollo madurativo.

Contenidos nocivos

- Pornografía entre adultos.
- Violencia.
- Juegos de azar.
- Trastornos alimenticios (Pro-Ana, Pro-Mía).
- Ideas autolíticas.
- Vídeos virales sobre actividades lesivas.
- Publicidad engañosa.
- Sectas.

Contenidos ilícitos

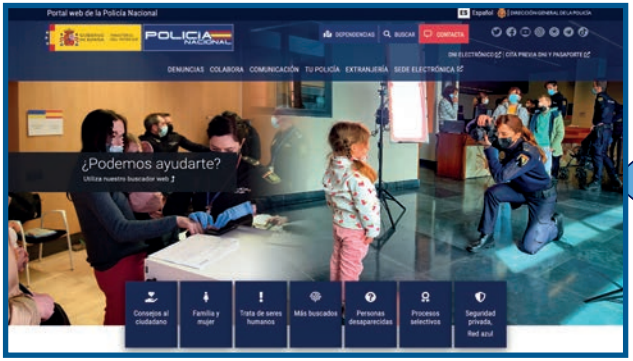
- Apología del terrorismo.
- Pornografía infantil.
- Provocar e incitar a delitos de odio.
- Difamación en internet.
- Distribución de material que vulnera la dignidad humana.

COMUNIDADES PELIGROSAS

Las comunidades *online* son grupos de personas con intereses comunes que no tienen un lugar físico dónde reunirse, contactan por Internet.
No son malas en general, pero pueden llegar a serlo si se cumple una de las siguientes condiciones:

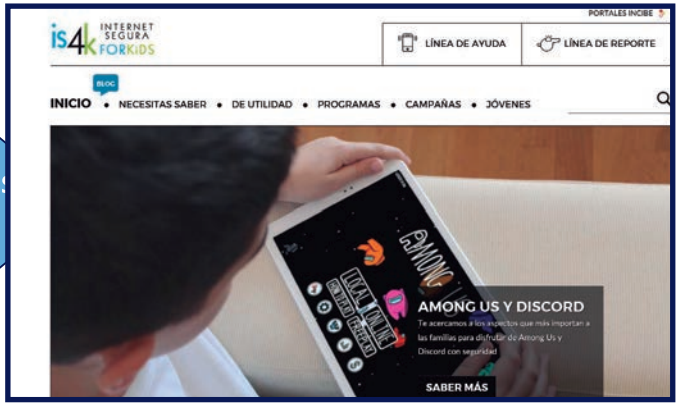
- Tienen contenidos inapropiados.
- Pueden empujar a los miembros a consecuencias trágicas.

10. RECURSOS Y LINKS



Policía Nacional
https://www.policia.es

Internet Segura FOR KiDS
http://www.is4k.es/



Tú decides en Internet
https://www.tudecideseninternet.es


POLICIA
NACIONAL

www.ciberexperto.org

seguridadescolar@policia.es

UNIDAD CENTRAL
DE
PARTICIPACIÓN CIUDADANA

POLICÍA NACIONAL

GOBIERNO DE ESPAÑA | MINISTERIO DEL INTERIOR | DIRECCIÓN GENERAL DE LA POLICÍA

NIPO (papel): 126-22-053-8 NIPO (en línea): 126-22-055-9
DEPÓSITO LEGAL: M-20450-2022