Tu huella digital:

date una pausa y conéctate con responsabilidad

Proyecto educativo para la ciudadanía digital y la prevención del ciberdelito

Guía de Apoyo

para la prevención del ciberdelito para equipos docentes y familias

Presidencia Uruguay | agesic

ANEP Administración Nacional de Educación Pública

Centro de Estudios Judiciales del Uruguay

inau Instituto del Niño y Adolescente del Uruguay

Fiscalía General de la Nación

Presidencia Uruguay | Junta Nacional de Drogas

Ministerio del Interior

PantallasAmigas

Global Programme on Cybercrime

Naciones Unidas Oficina contra la Droga y el Delito

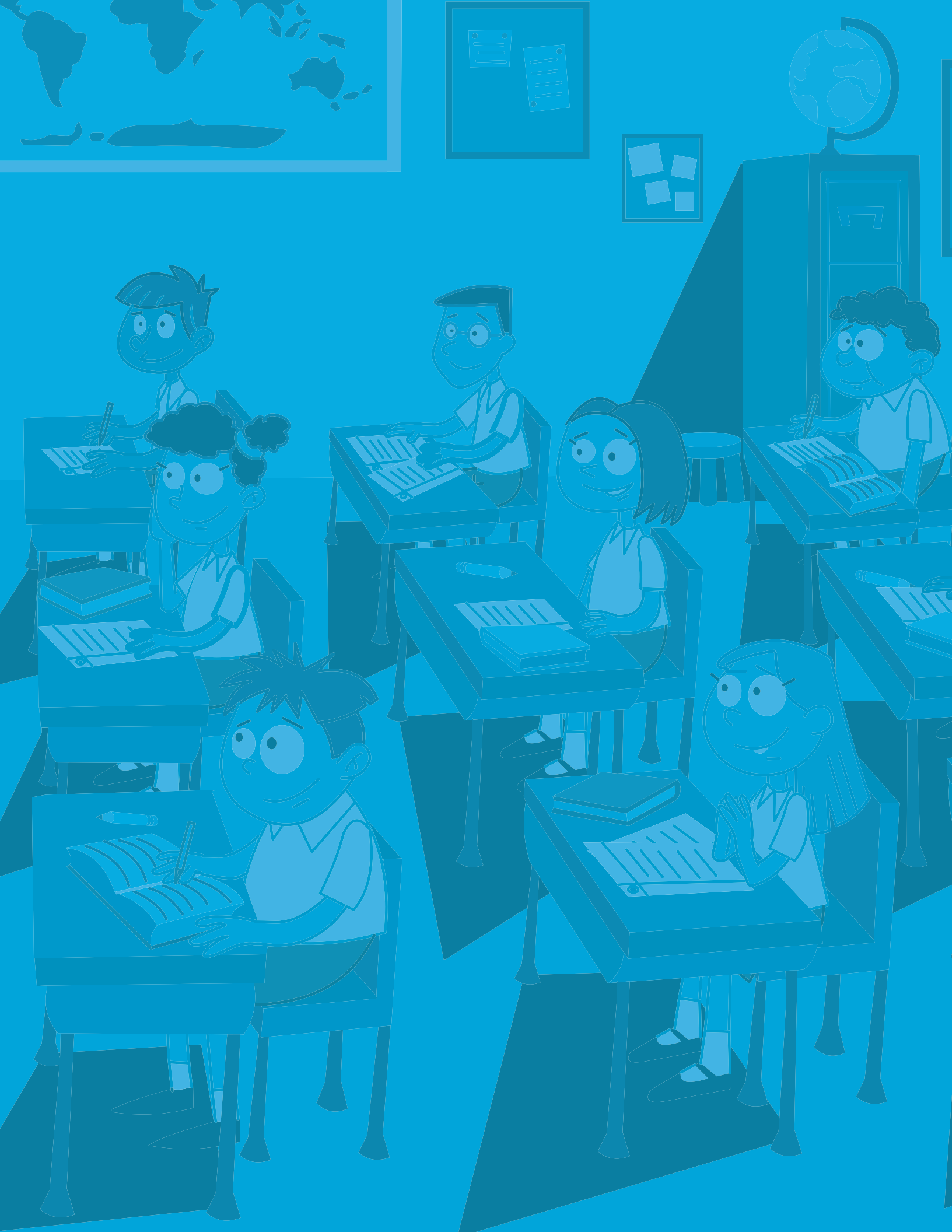
Naciones Unidas
Oficina contra
la Droga y el Delito

Oficina de las Naciones Unidas contra la Droga y el Delito

El Programa Global de Ciberdelito de UNODC tiene como misión proporcionar liderazgo global en la formulación de políticas y la construcción de capacidades para combatir el delito cibernético y los delitos financieros. Para lograrlo, el Programa está diseñado para responder de manera flexible a las necesidades identificadas en los Estados Miembros para prevenir y combatir estos delitos de manera integral. El Programa realiza acciones en África, Latinoamérica y el Caribe, Medio Oriente y el Sudeste de Asia y el Pacífico con los objetivos de:

Generar mayor eficiencia y eficacia en la investigación, enjuiciamiento y sanción del delito cibernético, especialmente los vinculados a la explotación y abuso sexuales de niños, niñas y adolescentes, desde un marco sólido de derechos humanos. Facilitar respuestas eficientes, eficaces, sostenibles, articuladas y de largo plazo de todas las instituciones del Estado para el abordaje del delito cibernético a través de la coordinación nacional, la recopilación de datos y fortalecimiento de los marcos normativos. Fortalecer la comunicación y coordinación nacional e internacional entre el Estado, sus instituciones y el sector privado para generar alianzas y mayor conocimiento en la población sobre los riesgos en Internet y cómo hacer un buen uso.

ISBN: 978-84-17774-85-1
Autor: Jorge Flores Fernández (PantallasAmigas)



Prólogo

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) es la Agencia del Sistema de las Naciones Unidas encargada de brindar asistencia técnica a los Estados Miembros en la lucha contra el tráfico de drogas, la delincuencia organizada y la corrupción y los desafíos planteados por estos fenómenos. En ese marco de trabajo, el Programa Global de Ciberdelito de UNODC se especializa en ejecutar acciones para responder de manera flexible a las necesidades identificadas en los Estados Miembros para prevenir y combatir los ciberdelitos de manera integral.

Bajo esta intervención global, Uruguay prioriza trabajar en la prevención de las ciberamenazas y el ciberdelito en el ámbito escolar y familiar, en el marco de la protección a la niñez y adolescencia. Es por ello por lo que la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), la Administración Nacional de Educación Pública (ANEP), el Instituto del Niño y Adolescencia (INAU), el Centro de Estudios Judiciales del Uruguay (CEJU), la Fiscalía General de la Nación, el Ministerio del Interior, la Junta Nacional de Drogas, la Unidad de Cibercrimen de la Policía Nacional y UNODC trabajan conjuntamente para fortalecer las capacidades de las y los educadores para la prevención y el abordaje del fenómeno del ciberdelito en las familias y escuelas, partiendo de las siguientes áreas temáticas: ciberseguridad; privacidad en Internet; sexting; grooming; sextorsión; ciberacoso; sexualidad y consumo de pornografía en Internet; desinformación y malinformación; ciberviolencias hacia las mujeres y niñas; huella, reputación e identidad digital.

A fin de cumplir con los objetivos propuestos, se contemplan acciones de formación especializada a docentes; la elaboración de materiales audiovisuales e impresos para los centros educativos y la elaboración de guías de apoyo para educadores, niños, niñas y adolescentes. La presente guía, que ha sido posible gracias a la contribución financiera de INL -Estados Unidos de América-, constituye un apoyo pedagógico para que las personas a cargo del cuidado de niños, niñas y adolescentes aprendan y orienten sobre las amenazas en el ciberespacio, y contribuyan en desarrollar acciones para prevenir que sean víctimas de algún ciberdelito o tengan comportamientos que los pongan en riesgo en Internet. Esta guía ha sido pensada para trabajar focalmente con menores de 18 años, en el entendimiento de los riesgos presentes en esta población per se.

Es imprescindible promover el involucramiento, acompañamiento y vigilancia de los referentes adultos, como correlato de la corresponsabilidad existente por parte de los distintos actores, en garantizar la conformación de espacios protectores en todos los ámbitos, educativo, familiar y comunitario, entre otros.

Presentación

La presente guía de apoyo se encuentra dirigida a docentes, educadores, padres y madres de familia para la prevención del ciberdelito en las aulas y en casa. Es un material de referencia para que aborden el fenómeno del ciberdelito y las prácticas digitales saludables entre la población de niños, niñas y adolescentes. Realizar estas labores preventivas es más importante que nunca debido al incremento constante del uso de Internet y de la virtualización de la educación que ha iniciado un camino que no tiene marcha atrás. La Oficina de las Naciones Unidas contra la Droga y el Delito, junto con la comunidad educativa, han adquirido el compromiso de procurar una sociedad digital más segura para los más pequeños, complementando el papel educativo que tienen las familias.

Internet para niños, niñas y adolescentes es sin duda una gran oportunidad para su pleno desarrollo y para la participación en la sociedad, pero al mismo tiempo, presenta retos y desafíos que demandan trabajar en la educación y la protección de los más jóvenes. Resulta imprescindible brindar herramientas que promuevan la autoprotección, facilitando el acceso oportuno a la información que permita detectar los factores de riesgo presentes en las distintas modalidades del ciberdelito, así como sus consecuencias, esto implica concienciar sobre los riesgos y proporcionar información clara relacionada a quienes acudir y los canales legales disponibles para la investigación y sanción de estos hechos. De la misma manera, es necesario apelar a una escucha activa y respetuosa por parte de los referentes adultos hacia las víctimas de un ciberdelito, validando su relato y desplegando todas las estrategias a su alcance para garantizar la atención y reparación de sus derechos vulnerados.

Esta guía se estructura en torno a diez temáticas principales. La ciberseguridad y privacidad están relacionadas entre sí y son factores de protección necesarios: no hay privacidad sin ciberseguridad ni ciberseguridad con la privacidad comprometida. Se trata además de cuestiones colectivas donde unas personas influimos en las demás sin apenas darnos cuenta. El sexting, por su parte, no es un daño en sí, sino que es una práctica de riesgo de la cual, por acciones de terceros, pueden producirse graves consecuencias. El apartado dedicado al grooming trata las claves del ciberabuso y ciberacoso hacia menores de edad. En el caso del ciberbullying están los más jóvenes a ambos lados del ciberacoso entre iguales que afecta el clima escolar de manera creciente e importante. Asimismo, la conectividad constante genera la repetición de estas conductas fuera del ámbito escolar, 24/7. La sextorsión tiene varias manifestaciones en función del objetivo perseguido, siempre basadas en la coacción mediante amenaza de hacer público contenido íntimo. Adicionalmente se han incluido temas vinculados a la ciudadanía digital como son conocer las consecuencias de la desinformación y malinformación así como la huella digital. Además, se reflexiona acerca de las consecuencias negativas del consumo de pornografía y la ciberviolencia de género que se ejerce en Internet.

La Fiscalía General de la Nación, a través de sus equipos fiscales, es la encargada de dirigir la investigación de delitos (con la asistencia de la policía), a fin de llevar a los posibles responsables ante un Juez para que les imponga las penas previstas en la legislación de Uruguay. Además, cumple el cometido de brindar protección y asistencia a las víctimas y testigos de delitos, mientras se realiza la investigación y se lleva a cabo el proceso penal.

68

Sexualidad y consumo de pornografía en Internet

Introducción
Para tener muy en cuenta
Definición y características
Fuentes, acceso y consumo de contenidos pornográficos
Ficción con apariencia y efectos reales
Violencia hacia las mujeres
Relaciones de dominio-sumisión y cosificación de las mujeres
Efectos psicológicos y relacionales adversos
Relaciones sexuales sin afectos
Prácticas de riesgo
Consumo problemático

Estrategias frente a la pornografía
Sensibilización de la población
Educación afectivo-sexual adecuada a las nuevas realidades
Limitación del acceso
Promoción de un posicionamiento social crítico

Diez pautas para mitigar influencias nocivas del consumo de pornografía

76

Desinformación y malinformación en Internet

Introducción
Claves para tener muy en cuenta
Definición, conceptos y características
Desinformación y malinforamción
Alfabetización mediática e informacional
El pensamiento crítico, aptitud y actitud
Vida digital adolescente y pensamiento crítico
Sesgos, emociones y su importancia en la desinformación
Filtro burbuja y cámaras de eco

Qué hacer para prevenir y actuar contra la desinformación
Pausar y considerar la opción de no compartir
Tomar conciencia de los efectos y la responsabilidad propia
Estimular el pensamiento crítico en un sentido amplio
Conocer, para evitar, los efectos de sesgos y emociones
Conocer sus estrategias: para qué y cómo se desinforma
Conocer y usar herramientas para contrastar informaciones

Decálogo para luchar contra la desinformación
Procedencia
Contenido
Intencionalidad

Ciberseguridad

Introducción

Este capítulo aborda algunas de las amenazas a la seguridad en relación a los dispositivos y procesos relacionados con Internet.

El tema de la ciberseguridad es tan amplio y avanza con tanta rapidez que hace complicado abarcarlo en una guía de estas características más allá de sus aspectos básicos. No obstante, el propio Internet nos brinda amplia y detallada información en lo relativo a aspectos más técnicos que pueden ser explorados junto con los escolares.

La ciberdelincuencia es un lucrativo negocio en auge que evoluciona cada día por lo que contar con la información precisa y desarrollar los hábitos preventivos básicos desde edades tempranas resulta imprescindible. No se debe olvidar que de la seguridad de los dispositivos depende la seguridad personal.

¿Por qué es importante la seguridad en internet?

En un mundo conectado estamos al alcance de ciberdelincuentes y otras personas que buscan la manera de aprovechar descuidos o prácticas erróneas.

El software malicioso (malware) inunda Internet y puede ocasionar molestias leves o ser causante de graves problemas personales.

Puede colarse en nuestros equipos conectados, en caso de ataques, o puede que seamos nosotros, sin darnos cuenta, quienes lo introduzcamos.

La ciberdelincuencia también utiliza el engaño y busca sacar provecho de nuestros errores: entrega de información sensible en el lugar equivocado o dar por buena una información fraudulenta.

Otras veces, por ejemplo, al no utilizar una contraseña robusta permite que sea fácilmente robada para que otras personas tomen el control de nuestros dispositivos y aplicaciones, y por tanto de nuestra vida e información digital.

¿Qué peligros nos acechan?

Cuando existen vulnerabilidades de seguridad o se sufre un ataque las consecuencias pueden ser muy variadas:

- **Utilización del equipo para finalidades ajenas.** Se hace uso del dispositivo de la víctima de forma impersonal para acciones como la recopilación de información de navegación, la muestra de publicidad, o la integración en una botnet (red de bots o “zombies”) utilizada para cometer otros ciberdelitos. La infección pretende pasar desapercibida y es habitual que quien la sufre no sea consciente.

- **Secuestro del dispositivo mediante ransomware.** Tipo de malware que cifra o bloquea el acceso a los archivos o a todo el sistema del dispositivo.

- **Acceso a datos sensibles o información personal.** El robo de información personal (claves, fotografías, datos bancarios, documentos de identificación, etc.) puede tener las más variadas finalidades y suele exigir una intervención complementaria

de quien ataca. Entre las consecuencias más dañinas está la sextorsión o la suplantación de identidad, pasando por el ciberacoso o el espionaje mediante la activación de la cámara o el micrófono.

- **Estafas y fraudes.** Tras el engaño, la víctima se ve expuesta al robo de dinero u otros bienes digitales o incluso implicada en la comisión de ciberdelitos.

Para tener muy en cuenta

- El celular, la tableta o una computadora son dispositivos que cuando se conectan a Internet se convierten en objetivos vulnerables.
- Existen muchos tipos de amenazas informáticas, de malware, que pueden llegar por los distintos canales de la Red y cuyos efectos negativos son muy variados.
- Cuando tus dispositivos son infectados o atacados, incluso aunque no te estés dando cuenta de ello, eres tú quien puede sufrir graves consecuencias personales.
- Cuidar tu propia ciberseguridad es una labor personal cotidiana que debe irse adaptando a nuevas circunstancias y aplicaciones.
- Es muy importante que también prestes atención y apoyo a las demás personas. Si ellas están protegidas aumenta tu seguridad porque vivimos en conexión.
- Para mantenerte a salvo, es imprescindible que cuentes con un programa de seguridad o antivirus en todos tus dispositivos (celulares, tabletas o computadoras) y que tengas contraseñas robustas para el acceso a tus servicios, perfiles y aplicaciones online.

Malware

Concepto

Como definición genérica, llamamos malware al código informático o software que se introduce en nuestros dispositivos y sistemas informáticos de formas muy diversas pudiendo producir efectos molestos, nocivos e incluso destructivos o irreparables.

Aunque en su origen este código malicioso tenía el claro propósito de causar más o menos daño en los dispositivos (borrar información, sacar una molesta pantalla de broma, demostrar fallas en la programación, entre otras), hoy en día su presencia es deliberadamente sigilosa y en muchas ocasiones suele estar relacionado con actos delictivos con fines lucrativos, pudiendo convivir con las personas afectadas y sus dispositivos en absoluta, discreta y aparente armonía.

Conocido genéricamente como “virus informático”, actualmente resultan más correctas denominaciones como: programa malicioso, badware, software malicioso o código maligno derivados del inglés malicious software.

Características generales

Básicamente, y de ahí su nombre originariamente generalizado como “virus”, es comparable con un virus en el ámbito de la biología: infecta a otros organismos, se

propaga de muchas y diferentes maneras, varía su apariencia y composición, se manifiesta con diversos síntomas y no todos provocan enfermedades.

Las formas como el código malicioso se introduce en nuestros dispositivos pueden ser diversas. Algunos necesitan de la intervención o algún tipo de acción del usuario como puede ser hacer clic en un "falso" enlace, descargar, abrir, instalar un archivo o app en el que está incluido el código, etc. Otros tipos de malware son "inyectados" por terceras personas gracias a la inacción, el descuido o la desinformación del usuario. Aprovechan, por ejemplo, que no haya cambiado las claves que vienen por defecto en los dispositivos para colarse en ellos, que utilice una contraseña fácil de descubrir, etc.

Los sistemas operativos y el software que instalamos en nuestros dispositivos, en tanto que son código informático, pueden contener errores de programación (bugs) y dejar, también, la puerta abierta para que terceras personas entren en los mismos.

Los medios de propagación empleados son variados e incluyen, entre otros, unidades de USB, mensajes de correo electrónico con archivos adjuntos, descargas de Internet, transferencia de archivos a través de FTP (protocolo de transferencia de archivos), redes de intercambio de archivos entre pares (P2P), etc.

Dado que el malware es también programado informáticamente, puede afectar a todo tipo de dispositivos en los que se ejecute (computadoras de sobremesa, laptops, tabletas, celulares, routers, etc.), por lo que es recomendable tener en cuenta todos ellos a la hora de adoptar medidas de seguridad.

No se debe olvidar que tras la creación y distribución de estos códigos maliciosos existen personas y, por lo tanto, es difícil establecer los objetivos que persiguen. Un determinado malware, un troyano por ejemplo, puede haber sido programado por un grupo de estudiantes como una broma o experimento sin intención de ocasionar graves daños, o bien como forma de demostrar las vulnerabilidades en el software o los dispositivos de compañías legalmente establecidas. Pero no hay duda de que, hoy en día, se ha generado un gran negocio en torno a ello, y existen personas, en solitario u organizadas como equipo que, con intención de obtener beneficios económicos, no dudan en actuar de manera delictiva.

Son nuestros datos, datos de terceras personas, datos del lugar donde estudiamos o trabajamos que utilizamos y guardamos en nuestro día a día, aquellos que pueden aportar información valiosa que, en caso de caer en manos inadecuadas, pueden ser utilizadas en nuestra contra (robo, suplantación de identidad, venta a terceros de información sensible, etc.) o que, en caso de ser destruida o inutilizada, pueden ocasionarnos graves perjuicios (cifrado y consiguiente imposibilidad de acceso a determinada información, por ejemplo).

Las amenazas más peligrosas y sofisticadas actualmente son híbridas, que combinan características y funcionalidades entre sí y que emplean técnicas de reinstalación tras la limpieza y re-arranque del dispositivo con objeto de dificultar su análisis por parte del software de protección (llamado habitualmente antivirus).

Tipos de malware

Existen múltiples tipos de programas maliciosos y su clasificación suele basarse en la forma en que se propagan aunque también, de manera alternativa, se categorizan en base a la amenaza que suponen. Citamos en este caso aquellos cuyas características de propagación son más habituales o genéricas.

Virus y gusanos (malware infeccioso)

- Infectan a otros archivos y programas modificándolos para crear copias de sí mismos en el dispositivo infectado.
- Pueden además estar programados para realizar otras acciones, como eliminar archivos o mostrar publicidad
- Los virus necesitan de la intervención del usuario para propagarse.
- Los gusanos se reproducen automáticamente propagándose de máquina en máquina.

Troyanos (malware oculto)

- Disfrazado de “benigno” invita al usuario a que lo ejecute, creando entonces una puerta de entrada a otros programas nocivos.
- Es incapaz de auto-replicarse, no puede propagarse por sí solo, por lo que necesita de la intervención del usuario.
- Realiza su labor de forma imperceptible.
- Recaba información o controla remotamente el dispositivo anfitrión comprometiendo la confidencialidad y seguridad del usuario o dificultando su trabajo.

Spyware (malware para obtener información)

- Recopila información del equipo en el que se encuentra y se lo transmite a quien lo ha introducido.
- Puede espiar el comportamiento del usuario en Internet, datos, contactos, hábitos de uso, páginas visitadas, apps ejecutadas, datos de la conexión, inventario de las aplicaciones instaladas en el dispositivo, etc.
- Sus consecuencias finales pueden ser graves porque posibilita desde robos bancarios hasta suplantaciones de identidad.

Otros tipos de malware destacado son:

Rogue software (software bandido o fraudulento): suele descargarse e instalarse de manera desapercibida desde Internet y, haciendo creer al usuario que su dispositivo está infectado, ofrece la instalación gratuita de una versión de prueba de un antimalware y una versión de pago para la eliminación de la supuesta infección.

Ransomware (criptovirus, secuestradores): son programas que cifran (encriptan o codifican) los archivos importantes para el usuario haciéndolos inaccesibles para luego solicitar el pago de cuantiosos “rescates” para poder recibir la contraseña que permita recuperar el acceso a esa información “bloqueada” o “encriptada”.

Pautas de prevención generales

Al igual que promovemos medidas básicas de seguridad para evitar algunos peligros

que acechan a los más jóvenes hoy en día, deberíamos promover entre nuestros niños, niñas y adolescentes la protección de sus dispositivos, teniendo en cuenta que portamos infinidad de información sensible y datos, no solo propia sino también de terceras personas. A continuación se describen algunas recomendaciones generales para niños, niñas y adolescentes:

- Ante todo, precaución, espíritu crítico y sentido común frente a cualquier comunicación e interacción a través de Internet especialmente en relación a mensajes o correos inesperados de amistades, personas desconocidas o entidades.

- Se debe tener en cuenta que la descarga de software desde sitios web no confiables o compartir archivos P2P (Peer-to-Peer, de computadora a computadora) resulta arriesgado, por lo que es recomendable utilizar los servicios de descarga de empresas legalmente establecidas y de reputación confiable. Ante la duda, siempre es preferible no abrir o ejecutar archivos y confirmar por otros medios la veracidad o fiabilidad de aquello que se va a descargar, abrir o ejecutar.

- Conocer los dispositivos propios, saber cómo se comportan y funcionan de manera “normal” puede ayudar a detectar la presencia de código malicioso. Un funcionamiento irregular o anómalo podría estar indicando una infección y es conveniente prestar especial atención si recientemente se ha instalado algún programa nuevo o navegado por páginas web de dudosa reputación.

- Tener siempre instalado un “antivirus” en todos los dispositivos que sirva de protección en tiempo real de posibles ataques es imprescindible, cualquiera sea el sistema operativo utilizado. Además de detectar amenazas derivadas de la interacción en Internet en cada momento, podría descubrirlas en memorias tipo USB, discos duros externos u otro tipo de hardware que se conecte al propio equipo. Al mismo tiempo, no se debe olvidar realizar un escaneo profundo de los equipos periódicamente recordando que los antivirus tienen sus limitaciones y no son infalibles, por lo que no se debe confiar toda la protección únicamente en ellos.

- Mantener actualizado el software (sistema operativo, navegadores, apps, etc.) es igualmente importante, ya que los errores detectados en la programación de los mismos suelen ser subsanados con esas actualizaciones y evitan que terceras personas puedan acceder a nuestros dispositivos a través de estas fallas o vulnerabilidades.

- Configurar, tanto los dispositivos como los sistemas operativos, programas, apps y servicios de la forma más “cerrada” o restrictiva posible, antes incluso de empezar a utilizarlos, es una estrategia recomendable para intentar evitar cualquier intrusión en ellos. Funcionalidades tales como el bluetooth o el servicio de ubicación, que dejan expuestos los dispositivos y a quien los usa, deberían activarse únicamente en el momento de necesidad y mantenerse desactivadas por defecto.

- Es algo muy común utilizar contraseñas o patrones de acceso, a dispositivos, redes y otros servicios, fáciles y que resultan sencillas de descifrar o descubrir.

La importancia del uso de contraseñas difíciles o robustas es tanta como el tipo de cerradura que se utiliza en el hogar. Crearlas con pautas ya conocidas (combinar letras, números y símbolos o que sean de longitud mayor o igual a 8 caracteres es recomendable) o bien utilizar servicios de creación de contraseñas ayudará a componer una clave que, si bien puede llegar a ser descifrada, al menos complicará su descubrimiento a terceras personas. Reglas nemotécnicas o el uso de un archivo único protegido por contraseña o cifrado que contenga todas aquellas claves que se utilizan pueden ayudar a su recuerdo sin problemas. En cualquier caso, casi todos los servicios que se usan hoy en día proporcionan una sencilla opción de recuperación de contraseñas en caso de olvido.

- Por último, pocas veces se toma en consideración la gran importancia de realizar copias de seguridad periódicamente de los archivos (especialmente de aquellos cuya pérdida suponga un gran daño). Así, en caso de quedar inutilizados nuestros archivos o dispositivos por cualquier causa, se minimizarán las consecuencias de su pérdida.

Casi tan importante como la prevención es la detección temprana de una amenaza que ha conseguido vencer las medidas preventivas y la posterior actuación reparadora.

Detección y actuación

Además de aplicar medidas preventivas, los más pequeños deben tomar conciencia de la necesidad de poder identificar posibles problemas de ciberseguridad así como conocer, al menos de forma elemental, qué hacer en esos casos.

Una vez que se ha introducido el código malicioso, no siempre es fácilmente detectable. Sin embargo, se puede estar teniendo problemas si observamos alguno de estos síntomas en nuestros dispositivos:

- Se calienta en exceso.
- Se percibe un consumo excesivo de batería.
- Aparecen ventanas emergentes, sin aparente razón, durante la navegación en Internet.
- El navegador redirecciona a sitios web que no son solicitados.
- Desaparecen archivos y programas o se vuelven inactivos sin motivo aparente y sin que hayamos realizado ninguna acción fuera de lo común.

Dependiendo de la gravedad de la infección y de si se tienen conocimientos suficientes, pueden tomarse algunas acciones:

- Realizar un escaneo profundo y limpieza con antivirus/antimalware. Si no se dispone de un antivirus instalado, varias compañías ofrecen herramientas gratuitas para realizar un escaneo rápido online de nuestros dispositivos o bien versiones de prueba o más ligeras, instalables para realizar una búsqueda más profunda. En caso de que no se detecte nada en un primer momento, puede ser conveniente realizar otros escaneos con distintos antivirus dado que utilizan diferentes herramientas de detección.

- Efectuar una limpieza en el navegador de Internet utilizado (cookies, complementos que se hayan podido instalar…)
- Desinstalar programas, complementos o apps, especialmente si ha sido tras su instalación cuando hemos detectado el inicio de problemas en el dispositivo.
- Buscar ayuda de profesionales especializados.
- Formatear el dispositivo (previa copia de seguridad de los datos, configuraciones e informaciones de interés ya que se pierde todo el contenido del dispositivo en esta acción).

Dependiendo de las características del hecho perpetrado, esta conducta podría será sancionada por los artículos 297 BIS, 297 QUATER, 358 QUATER y 358 QUINQUIES, del Código Penal

En cuanto al Phishing, recuerda que dependiendo de las etapas ejecutadas por el o los delincuentes, al momento de descubrirse la maniobra, podrían resultar aplicables los artículos 347 BIS y 347 TER, del Código Penal.

Conexiones no seguras

Cada vez es más común navegar en internet con celulares y tablets. Ello hace que en muchas ocasiones, especialmente en edades tempranas, se busque una red, por lo general Wifi, para establecer una conexión. Conviene alertar a niños, niñas y adolescentes de que este punto de conexión puede representar una amenaza también.

Al conectarse a Internet desde cualquier lugar por cable, por medio de ondas Wifi, de radio, etc., se accede y se pasa a formar parte de una red de millones de dispositivos interconectados entre sí. Estos dispositivos, por lo general, tienen medidas de seguridad implementadas al igual que los propios para poder acceder, navegando, solo a aquellos contenidos "abiertos". Sin embargo, estas medidas de seguridad pueden estar deficientemente configuradas, ni siquiera establecidas o resultar lo suficientemente atractivas para ingresar sin autorización y terceras personas podrían, además de interceptar nuestras comunicaciones, acceder por medio de la conexión a nuestros dispositivos con los peligros que ello conlleva. Igualmente, las redes de dispositivos incluso desprovistas de conexión a Internet comparten características y riesgos parecidos.

Se debe recordar que, así como podemos controlar la configuración de nuestros propios dispositivos y conexiones en nuestro hogar o centro educativo, desconocemos en general las medidas de seguridad adoptadas en aquellos lugares públicos o privados que permiten a los usuarios el acceso a sus redes con y sin conexión a Internet.

Es habitual que muchas personas, especialmente las más jóvenes, para ahorrar en el consumo de datos que sus proveedores de Internet limitadamente les proporcionan, instalan software para buscar conexiones Wifi abiertas con contraseñas fáciles de crackear, pensando que están "robando" Wifi. Al hacerlo no son conscientes de los riesgos que esto implica, quedando expuestos a caer en la trampa de otras personas que "abren" la conexión para poder establecer la intercomunicación entre dispositivos y acceder, así, a los de aquellas que se encuentran conectadas.

Del mismo modo, conexiones gratuitas o abiertas, podrían esconder intenciones fraudulentas. El principal comportamiento a evitar es conectarse a una red Wifi pública y abierta (sin clave) porque, sencillamente, puede ser una trampa donde la Red gratuita es proporcionada por el ciberdelincuente ofreciéndola por proximidad y con un nombre que induzca a pensar que es la que se estaba buscando.

Enlaces fraudulentos

Una amenaza habitual que permite de forma recurrente muchos engaños es la provisión de enlaces fraudulentos que, bajo inocente y en ocasiones tosca apariencia, llevan a quien los sigue a situaciones de engaño que se materializan comenzando con proporcionar datos sensibles. Hay que pensar que, aunque los menores de edad no suelen ser objetivo de ciberdelitos con fines económicos puesto que no cuentan con solvencia o liquidez, es importante que conozcan estas técnicas puesto que son extensibles a sistemas de pago próximos a sus actividades como pueden ser las compras o los videojuegos online.

¿Cómo actúan?

Llegan por comunicación directa (email, WhatsApp, foros, redes) o indirecta (banners, anuncios, descargas de código malicioso de manera oculta, etc.) y redirigen cuando son activados, por lo general, a páginas web muy similares a las reales en las que el usuario debe rellenar un formulario. Si el usuario completa dicho formulario proporcionando los datos solicitados, estos datos acabarán siendo controlados por ciberdelincuentes. Algunos de estos mensajes apelan a la caridad (imposibilidad de cobrar una herencia por estar en un país remoto), a la curiosidad ("entérate quién te ha borrado de su círculo de amigos"), a la "ingenuidad" ("has resultado ganador de un coche") o a la amenaza ("confirmación de datos indispensable por actualizaciones en el sistema") consiguiendo, de entre los millones de mensajes que envían automáticamente, engañar a muchísimas personas. Una técnica de estafa de las que más beneficios aporta a los ciberdelincuentes se denomina phishing, cuyo modus operandi se resume así:

- Suplanta la imagen de una entidad (por ejemplo bancaria) para conseguir el número de cuenta, claves y otro tipo de información sensible.
- Las páginas a las que redirigen los enlaces fraudulentos que se envían mediante correo, SMS o Redes Sociales, no comienzan, en general, con "https" y su apariencia gráfica, logo y lenguaje simulan la imagen real de la institución.
- También es posible que se solicite la descarga de archivos desconocidos con el objetivo de infectar los dispositivos con malware. La página a la que redirigen se asemeja mucho a la página original de la entidad suplantada.

Medidas preventivas

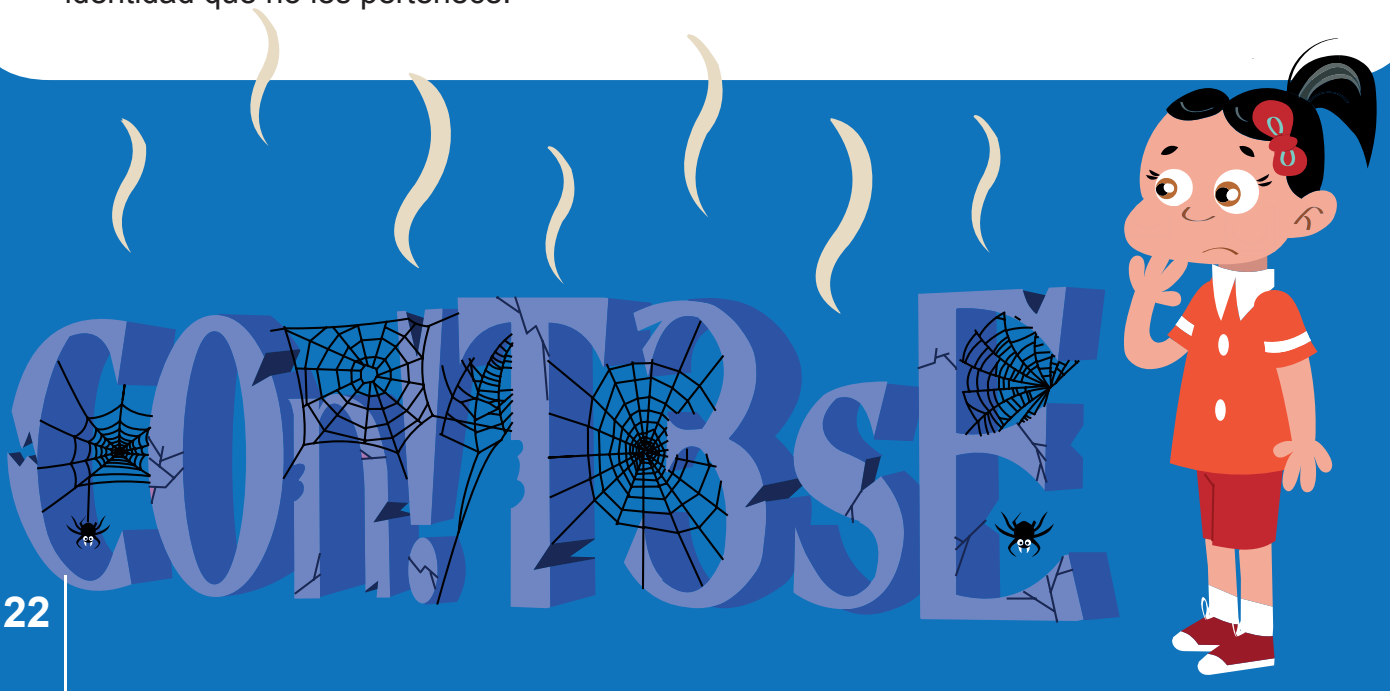
Para limitar las probabilidades de acceder a un enlace fraudulento se recomienda:

- Escribir la URL o dirección de la página web en el navegador en vez de acceder haciendo clic en enlaces aportados en emails, mensajes, websites.
- Evita hacer clic en enlaces recibidos por correo, SMS o redes sociales, ya que pueden dirigirte a sitios fraudulentos que suplantan la identidad de una institución para generar tu confianza. Nunca ingreses datos sensibles en sitios HTTP:// (sin la 's'); siempre busque el protocolo HTTPS:// y el icono del candado para asegurar que la comunicación esté protegida. A pesar de ello, es fundamental inspeccionar la dirección URL en busca de errores ortográficos o nombres extraños, dado que el cifrado no es una garantía de la legitimidad del sitio
- No abras ni descargues archivos desconocidos, ya que podrían infectar tu dispositivo con malware.
- Tener presente que una entidad bancaria o empresa nunca pedirá datos personales por correo electrónico.
- Evitar introducir datos confidenciales ante cualquier duda que surja y contactar con la entidad directamente.
- Usar el sentido común que dice que es muy difícil que alguien regale algo a cambio de nada.

Acceso no deseado a los dispositivos

El celular es un elemento portable de uso permanente y, como tal, puede ser olvidado, extraviado o incluso sustraído. También puede estar en manos ajenas poco deseables en un momento determinado en el que se ha perdido de vista. Es importante provocar esta reflexión entre nuestras niñas, niños y adolescentes y que la tomen en cuenta también desde el punto de vista de la privacidad. En este supuesto, se les puede sugerir diversas medidas preventivas ente las que se encuentran las siguientes:

- Configurar contraseña, patrón de desbloqueo, PIN y/o huella de acceso al dispositivo para que únicamente su propietario pueda utilizar aquello que guarda en el mismo.
- No permitir a las aplicaciones, navegadores y programas que almacenen las contraseñas en la memoria del dispositivo de modo que, si terceras personas se apoderan del mismo, no puedan acceder a ellas ni, como puede ser el caso, realizar acciones bajo una identidad que no les pertenece.
- Anotar y guardar el IMEI (International Mobile System Equipment Identity) del teléfono celular. Éste es un número exclusivo que sirve para identificar el dispositivo y, en caso de robo o pérdida, denunciarlo. Se podrá, por ejemplo, bloquear las llamadas que pudieran realizarse desde el mismo. De manera genérica, para obtener dicho número, se puede teclear desde la app que utilizamos para las llamadas de teléfono los siguientes caracteres: *#06# (asterisco, numeral, seis, cero, seis, numeral).
- Existen apps, programas y servicios de localización y rastreo de dispositivos, celulares y laptops, que si son instaladas antes de cualquier robo o pérdida, permitirán dar con ellos.
- Otras apps pueden ayudar también, por ejemplo, a inhabilitar la información contenida en el dispositivo de forma remota (resetearlo a sus opciones de fábrica), a descubrir a la persona que lo posee (tomando una fotografía de quien lo enciende, identificando el número sim de la tarjeta insertada…), etc.



Contraseñas robustas

Las contraseñas son la primera protección del acceso a datos (conversaciones, imágenes, contactos, etc.) y servicios personales que pueden ser utilizados para causarnos daño. Son la primera barrera de ciberseguridad, la puerta de entrada a nuestra vida digital y, como tales, deben ser robustas. Su elección es una decisión importante que se debe tomar con frecuencia.

Las contraseñas son sinónimo de privacidad dado que abren la puerta a informaciones personales pero cabe también relacionarlas con la seguridad de quien las creó puesto que el acceso a determinados datos puede ser utilizado para causar daño de diversas maneras como, por ejemplo, mediante suplantación de identidad o chantaje. En síntesis, las contraseñas son la puerta de entrada de la vida digital por lo que, para protegerlas mejor, las mismas deben ser robustas. Es necesario que niñas, niños y adolescentes sepan cómo construir estas barreras de manera sólida.

Ocho claves para una contraseña robusta

1. Debe tener al menos 8 caracteres que contengan números, letras (en mayúsculas y minúsculas) y caracteres especiales. Puedes elegir una frase fácil de recordar y sustituir algunas letras por símbolos, números y caracteres especiales.
2. No puede ser un dato fácil de adivinar (nombre, fecha de nacimiento, etc.).
3. No debe dejarse escrita ni guardada sino introducirse cada vez que se use.
4. Es un secreto que no debería compartirse con nadie.
5. Debe ser cambiada regularmente o cuando hay evidencia o sospecha de que ha sido vulnerada.
6. Tiene que ser diferente para cada servicio, red social o app.
7. Doble Factor: Actívalo siempre, es una capa de seguridad esencial que evita el acceso no autorizado aunque roben tu contraseña.
8. Gestor de Contraseñas: Utiliza un gestor; que requiere memorizar solo una clave (almacena de forma segura y facilita claves únicas).

Pautas para protegerte de las amenazas a tu ciberseguridad

Son muchos los aspectos de ciberseguridad que, como se ha visto, deben ser tomados en cuenta tanto por niñas, niños y adolescentes como por las personas adultas. No obstante, se podrían tratar de sintetizar en estas ocho recomendaciones que podemos llevar a cabo con facilidad:

- Usa un antivirus en los dispositivos (computadora, celular o tableta) con los que te conectes a Internet. Los hay gratuitos y para todos los sistemas operativos.
- Mantén tu sistema operativo y aplicaciones actualizadas porque incluyen refuerzos de seguridad.
- Cuando descargues apps, hazlo desde las tiendas autorizadas. Desconfía

del software de dudosa legalidad o procedencia porque puede incluir malware.

- Evita acceder a enlaces o archivos inesperados o de personas desconocidas. No los descargues de forma automática.
- Presta especial atención a dónde introduces tus contraseñas y quién te las pide. Que la dirección de una página web comience por “https” es una de las señales que indica que la misma puede ser segura y confiable.
- Conectarse a redes Wifi públicas y abiertas es arriesgado. Procura no realizar nada crítico porque tus comunicaciones podrían ser espiadas.
- Activa los servicios para compartir información de tu celular, como el bluetooth, únicamente cuando vayas a usarlos.
- Mantente alerta y contrasta las informaciones, las personas con las que te relacionas y los servicios que usas. Buscar datos o referencias online para comparar puede ayudar a descubrir fraudes y engaños.

Privacidad

Acceso no deseado a los dispositivos

Se habla mucho sobre privacidad, es algo recurrente y apenas podemos destacar sobre ella dos certezas. Por un lado, que como concepto está cambiando y, por otro, que existe cada vez más la sensación de que preservarla es una misión muy complicada, cuando no imposible.

¿Por qué es importante la privacidad?

Existen dos razones fundamentales:

- Es un f**actor de protección** de primer orden. Los datos sobre quién eres, qué aspecto tienes, quiénes son tus amistades y familiares, dónde estás, qué te gusta, qué haces… son la mejor fuente de información para alguien que quiera hacerte daño.
- **Afecta a la imagen**, identidad y huella digital. Puede que ahora no sea importante para ti. Puede que pienses que lo que publicas o cuentan de ti solamente importa aquí, ahora y a quienes te imaginas. Sin embargo, el rastro que deja lo que se sabe de ti en la Red puede afectarte de forma negativa en un futuro no tan lejano, y ese rastro es profundo, amplio y casi imposible de borrar.

¿Qué consecuencias negativas puede haber?

Cuando no realizas un cuidado adecuado de tu privacidad, seleccionando y gestionando lo que deseas publicar y quien puede llegar a conocerlo, puedes correr riesgos:

- Eres más vulnerable frente a peligros muy variados: ciberdepredadores sexuales, ciberbullying, sextorsión, suplantación de identidad, etc.
- Tu identidad y tu reputación digital son más diversas y complicadas de gestionar o cambiar.
- Puedes molestar e incluso poner en riesgo a otras personas cuando publicas momentos de tu vida compartidos con ellas.

Para tener muy en cuenta

- Si alguien te quiere hacer daño lo podrá conseguir de formas más diversas y de manera más sencilla cuanto más sepa sobre ti.
- La privacidad y la ciberseguridad van de la mano. Si los dispositivos son vulnerables o las contraseñas inseguras tu información privada estará en riesgo.
- Lo que se sepa de ti depende también de las demás personas a la vez que tú también eres responsable de la privacidad de ellas.
- Para cuidar tu privacidad, la clave es ser proactivo. Habla con tus conocidos y diles claramente qué pueden compartir sobre ti y qué no.
- Tienes el derecho a decidir sobre el uso de tus datos personales, entre ellos tu imagen.
- Las aplicaciones y los servicios online que utilizas son otra fuente de divulgación de tu vida personal, incluso cuando no eres consciente de ello.

La privacidad como derecho y factor de protección

Más allá de una opción, la importancia de la privacidad es de tal relevancia que se configura como una de las cuestiones clave en Internet. De hecho, supone un constante campo de batalla entre las grandes empresas de la Red y las instituciones que velan por su ciudadanía. También es motivo de disputa entre particulares puesto que en Internet estamos permanentemente invitados, inducidos podría decirse, a compartir información, incluso ajena. La privacidad se nos escapa como granos de arena entre los dedos.

Privacidad como derecho

A finales de 2013, la Asamblea General de la ONU adoptó una resolución en la que defiende el derecho a la privacidad y llama a los Estados miembros a poner fin a las actividades que violen este “principio de la sociedad democrática”. En el texto se recogió la solicitud a la Alta Comisionada de la ONU para los Derechos Humanos para que elaborara un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia nacional y extraterritorial. Ya el artículo 12 de la Declaración Universal de los Derechos Humanos establece que el derecho a la vida privada es un derecho humano. También se hace referencia al derecho a la autoprotección en la era digital cuando menciona que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

Por otro lado, las sociedades actuales establecen como individuos sujetos a medidas de especial protección a los menores de edad y las personas incapaces

por su situación de especial vulnerabilidad. Por último, atendiendo a la Convención de los Derechos del Niño (CDN) se debe citar el “interés superior del niño” que actúa como un derecho, un principio y una norma de procedimiento y que, en síntesis, insta a priorizar el bienestar de niñas, niños y adolescentes cuando su garantía entre en conflicto con otros intereses.

Así pues, la privacidad de las personas menores de edad en Internet es una cuestión capital, un derecho que debe ser objeto de especial atención. En la Unión Europa, el RGPD (Reglamento General de Protección de Datos), en vigor desde el 25 de mayo de 2018, supone importantes restricciones en este sentido elevando a 16 años, salvo indicación expresa de cada país en contrario y nunca por debajo de los 13 años, la edad en la que una persona puede tener plena autonomía para consentir el tratamiento de sus datos personas en los servicios de la sociedad de la información (como, por ejemplo, las redes sociales).

No hay una regulación o convención con alcance mundial en protección de datos personales, sino que este derecho se aborda principalmente a través de legislaciones y regulaciones de cada país o comunidades políticas. En Uruguay, se encuentra específicamente regulado en la Ley Nº 18.331 promulgada el 11 de agosto de 2008, siendo la Unidad Reguladora y de Control de Datos Personales (URCDP), el Órgano encargado de garantizar este derecho.

Privacidad como factor de protección

Sin duda, una persona es tanto más vulnerable cuanta más información se conoce de ella. Esto, llevado al contexto digital donde infligir daño a alguien es demasiado sencillo, inmediato y a menudo queda impune, se vuelve un aspecto crítico. Esa asimetría de poder que ya se da entre víctimas y victimarios en Internet se ve acentuada por la balanza de la privacidad que, casi siempre, se inclina en favor de quien causa daño. Así, mientras quien agrede puede recurrir al anonimato, la suplantación o la impostura para esconder su identidad, la víctima necesita vivir su vida en línea con su propio nombre y, desafortunadamente, sin un control total sobre lo que se sabe de ella.

Causar daño a una persona online es demasiado sencillo (mensajes amenazantes, calumnias e injurias, mentiras, difamaciones…) y ese daño puede ser más intenso cuanta más información se conozca de la víctima. Así pues, el trabajo por una Internet más segura pasa también por reducir las posibilidades de victimización y la intensidad del daño y esto, necesariamente, va ligado a una gestión efectiva y consciente de la privacidad y los datos personales.

Educar en la cultura de la privacidad

La pérdida de privacidad de la ciudadanía puede analizarse desde muy distintos aspectos. Siendo un tema amplio que va desde el control, la fusión y el intercambio de información entre administraciones públicas o grandes empresas hasta el Internet de las cosas, es preferible centrarse en el día a día.

Privacidad en peligro de extinción

¿Por qué ha sufrido tanta pérdida significativa nuestra privacidad? Simplificando, podemos decir que depende de la información personal que sea creada, conservada, enriquecida (ganando así un valor añadido y una mayor trascendencia) y transmitida o publicada.

- Más información creada: la generación de información personal es permanente y en demasiadas ocasiones inconsciente. Se puede pensar tanto en una imagen personal posteada y etiquetada como en la geolocalización que de forma incesante pudiera estar capturando nuestro celular, pasando por la compra electrónica de un producto o servicio. Es significativo que todos llevemos encima, integrada en el celular, una cámara de fotografía y vídeo.

- Más información conservada: el almacenamiento de información digital ha sufrido una revolución permanente con la reducción del precio de la unidad de almacenamiento y la amplia diversidad de tecnologías y dispositivos cada vez más versátiles. En pocos años se ha pasado de llevar una fotografía de papel de algún familiar en la cartera a llevar en el celular decenas de imágenes y vídeos de personas conocidas o incluso desconocidas.

- Más información enriquecida: en gestión de información, los datos interrelacionados multiplican su valor. Las tecnologías actuales permiten realizar una explotación de la información que, mediante nexos, evidencias o supuestos, logra obtener nueva información derivada de alto valor añadido muy superior a la simple suma de datos agregados.

- Más información transmitida/publicada: al margen de lo que las grandes corporaciones o los servicios públicos pudieran realizar (limitados por la legislación y las prácticas de autorregulación) es evidente que somos las personas quienes en muchas ocasiones compartimos la información. Cada vez es más fácil, cómodo, inmediato y barato hacerlo, y se hace en exceso, atendiendo en demasía a intereses comerciales que nos invitan a “compartir la vida”.

¿Está la privacidad en peligro de extinción? Desde luego, ya no es la misma privacidad que antes de la proliferación de celulares, ni ésta última comparable a la existente antes de la llegada de Internet a los hogares. Las redes sociales por su lado, colocando a los usuarios como creadores y consumidores de información personal, marcaron un punto de inflexión que se ha acentuado con la normalización de los celulares que facilitan, pero sobre todo digitalizan, nuestra vida y, literalmente, nuestros pasos.

Educación tradicional para la privacidad en Internet

Ha venido siendo habitual en la concienciación de la población, especialmente en el caso del público adolescente, la realización de campañas donde la sensibilización sobre la protección de los datos personales se centraba en dos aspectos. Por un lado, la configuración de privacidad de las redes sociales y, por otro, la identidad y la reputación digital. En ambos casos la intención se focaliza en limitar la difusión personal de información y reflexionar sobre el efecto de la misma a largo plazo. También, más recientemente, se habla de proteger el celular con contraseña y atender lo que se publica de otras personas cuando les puede hacer daño. De alguna manera parece que el peso de la privacidad recae sobre uno mismo y que es ese su único marco de actuación.

Coprivacidad

La frecuente alusión a la privacidad como cuestión personal queda algo distante de nuestro día a día actual. Vivimos en una sociedad interconectada con personas hiperconectadas donde la actitud por defecto, el impulso, es compartir. Niños, niñas y adolescentes simplemente lo conciben como un juego de imitación, una travesura o un pasatiempo. Las y los adolescentes, pero cada vez más las personas jóvenes y adultas, lo hacen de manera irreflexiva, insistente y compulsiva. Es lo que en ocasiones se ha ligado con términos como “extimidad” (exposición de la intimidad), “oversharing” (compartir en exceso) o “sharenting” (cuando la familia comparte datos de sus hijos/menores en línea). Sin embargo, muy frecuentemente lo que es compartido afecta a la privacidad de terceras personas. Compartir la vida fuera de la Red significa hoy, necesariamente, compartirla también online y a partir de aquí la privacidad es un reto delicado. Es por ello que la privacidad deja de pertenecernos, de estar bajo nuestro dominio y pasa a ser un patrimonio de gestión colectiva; hablamos de coprivacidad. El fomento del valor y la cultura de la privacidad y la intimidad deben hacerse desde esta concepción de coprivacidad fundamentalmente, como un ejercicio consensuado, consciente y responsable de la privacidad propia, de la ajena, y de la compartida y no tanto como un ejercicio individual. Por supuesto que es importante saber qué se publica sobre uno mismo, cómo se hace y dónde se hace, pero sin duda lo fundamental está fuera de nuestra esfera de decisión, en las demás personas. Así, la privacidad se convierte en un ejercicio de derechos y deberes para la ciudadanía digital.

Ciberseguridad y privacidad

Reforzando el planteamiento de la privacidad como una cuestión colectiva se puede entender y asociar con la ciberseguridad. Por un lado, privacidad y ciberseguridad son conceptos relacionados puesto que no existe información con garantías de mantenerse en privado si no existe certeza de que está a salvo, segura. Por otro lado, la ciberseguridad es un asunto a gestionar e impulsar de manera comunitaria porque un entorno es tanto más seguro cuanto más lo son cada una de sus partes o componentes. Si vivimos en conexión, no podemos tener un buen nivel de ciberseguridad existiendo eslabones que no observan los principios básicos de la misma.

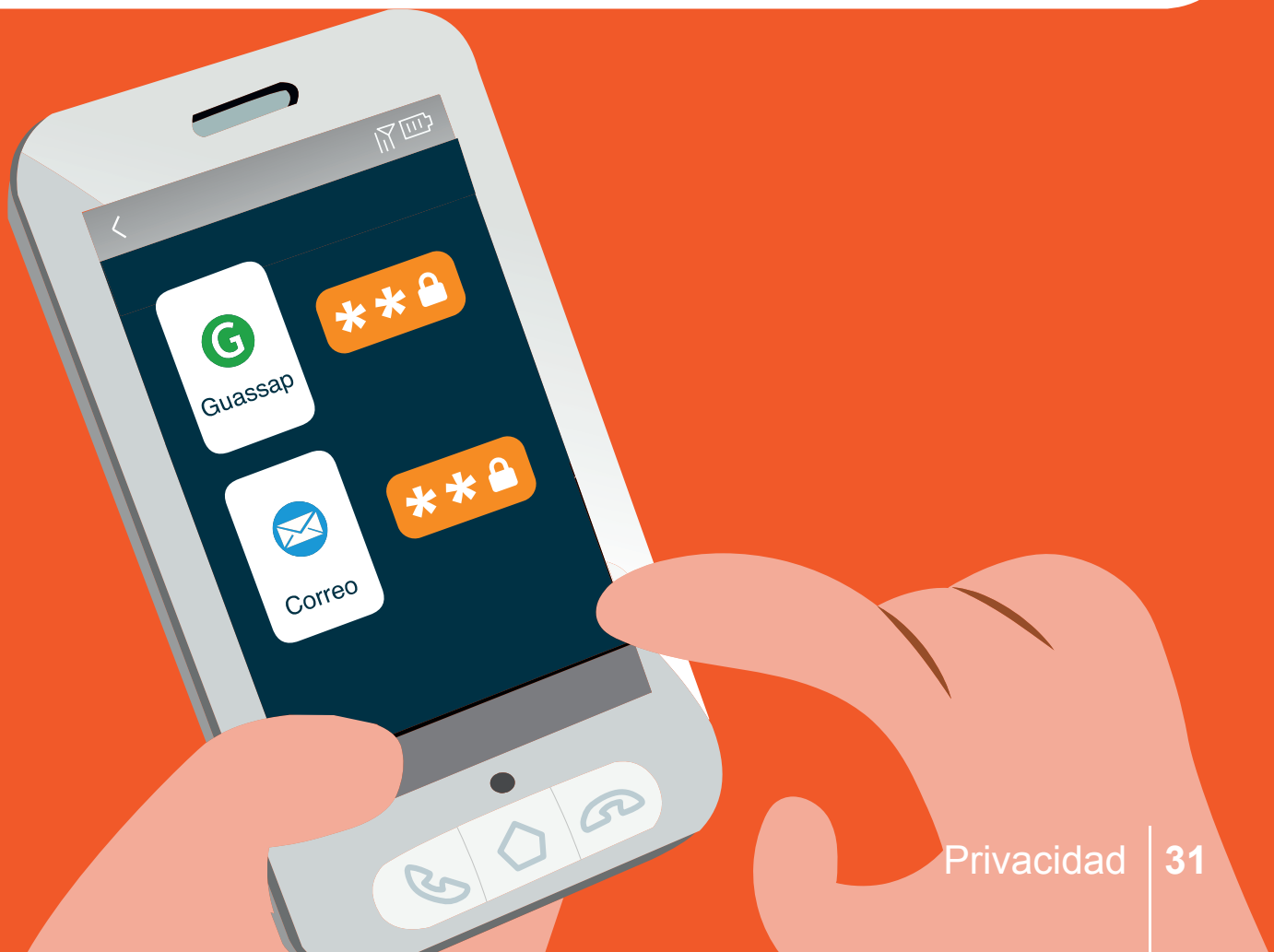
Identidad y huella digital

Tanto la identidad como la huella digital son dos aspectos íntimamente relacionados con la privacidad y que tienen una gran relevancia puesto que pueden condicionar la socialización de nuestros niños, niñas y adolescentes tanto en el presente como en el futuro.

Se puede decir que nuestra identidad digital es lo que Internet (concretado con frecuencia y sobre todo en Google y en menor medida otros gigantes de Internet como Meta o X Corp) induce a pensar que somos. Se compone de lo que decimos (escribimos) y hacemos, de lo que otras personas dicen (reflejan, muestran o escriben) de nosotros y sus interacciones y de cómo esas informaciones son mostradas a terceros por las diferentes aplicaciones o servicios de Internet. Tanto es así que incluso las ausencias significativas, como por ejemplo puede ser para un adolescente no contar con cuenta de Instagram, también configuran nuestra identidad digital.

La huella digital es el rastro online dejado por cada cual, ligado a la identidad digital, pero especialmente a las acciones que han tenido reflejo significativo en Internet a lo largo de su vida.

Es necesario que nuestros niños, niñas y adolescentes tomen conciencia de la importancia de estos dos conceptos y de cómo les afectan. Aunque no sea siempre ni del todo justo, cada vez es más relevante la parte digital de su identidad. Una inapropiada reputación online o la evidencia de una acción incorrecta realizada tiempo atrás pueden tener consecuencias negativas sin que ni siquiera se den cuenta o puedan remediarlo.



Redes sociales, etiquetado y geolocalización

Al margen de cambios sociales o culturales, dos han sido los elementos clave que han marcado el desmantelamiento de la privacidad: las redes sociales que socializan la información y los celulares que registran muchos datos de manera automática, entre ellos la geolocalización. Nuestros niños, niñas y adolescentes, desde edades tempranas, deben tomar conciencia de ello para actuar de manera crítica, responsable y proactiva ante este reto.

Gestión de la privacidad en redes sociales

Determinando, a modo de ejemplo, el fenómeno de la gestión de la privacidad al ámbito de las redes sociales, consideramos que la propia privacidad depende de tres factores fundamentalmente:

- De lo que publicamos de nosotros mismos y cómo lo hacemos (restringido, público…),
- De la manera en que la plataforma en la que publicamos trata esa información, y de las demás personas, especialmente.

Un ejemplo muy ilustrativo es el de las etiquetas en las fotografías de redes sociales. Con independencia de quién haya publicado la imagen, si alguien pone etiquetas, vinculando cada persona que aparece en la imagen con una identidad en la red social, el efecto es multiplicador porque la propia plataforma social se encarga de comunicar a la comunidad que existe una imagen en la que aparecen determinados usuarios (y toda la información que en la misma va incluida de forma más o menos explícita). Así pues, de los tres factores que modulan la privacidad (qué y cómo se publica, cómo es tratada esa información y el resto de las personas) se aprecia que los más relevantes son aquellos que no podemos gestionar. Cabría pensar que tenemos la capacidad de elegir en qué plataforma publicamos y que además podemos conocer con certeza cómo gestiona a diferentes niveles, micro y macro, esa información pero la realidad es que no, no en la práctica. Ni podemos elegir ni podemos asegurar de forma cierta y continuada que conocemos los efectos de las cambiantes normas de privacidad de las redes sociales. Las etiquetas en las imágenes de las redes sociales son un claro ejemplo y se debe hacer hincapié sobre esta cuestión tan común entre los niños, niñas y adolescentes.

Etiquetas en las fotografías

Cada vez es más sencillo y común subir imágenes a Internet. En el contexto de las redes sociales existe además la posibilidad de poner etiquetas, esto es, relacionar a personas con esas fotografías. ¿Se han parado nuestros niños, niñas y adolescentes a pensar qué implicaciones puede tener esta función? Les tenemos que ayudar a descubrirlo.

Las etiquetas en las redes sociales son un atentado directo y claro contra la privacidad en tanto que la plataforma debería solicitar permiso expreso y previo a la persona que está siendo etiquetada antes de exponer la imagen y anunciar su existencia. ¿Con qué derecho alguien te identifica en una imagen y lo que supone de contexto y datos adicionales- asignando un conjunto de puntos de luz o pixeles de la misma con tu identidad? y ¿Cuál es la ética por la que la red social lo permite, promueve y divulga?

Publicar una imagen en una red social es una acción casi cotidiana para los y las adolescentes y, en muchas ocasiones, esas fotografías se completan con etiquetas. Si subir una foto a Internet puede ser en ciertas ocasiones un atentado contra la privacidad de personas implicadas en esa instantánea ¿qué efectos puede causar el empleo de etiquetas? Veámoslo, a grandes rasgos, dejando de lado las diferencias de funcionamiento y de configuración de privacidad entre las distintas redes sociales. De manera sencilla, se puede decir que una etiqueta en una fotografía es una marca o señal que relaciona esa imagen, y en particular un área rectangular de la misma, con una determinada persona. La marca se asocia, por lo general, a la zona de la fotografía donde aparece esa persona. ¿Qué ocurre cuando te etiquetan? Son dos los efectos:

- Efecto de asociación: Si te etiquetan, te están relacionando con esa fotografía y, en particular, con un área de esa fotografía que por lo general es la zona en la que apareces.No obstante, no hay manera de asegurar esta correspondencia ya que la red social permite marcar una zona gráfica, un conjunto de pixels, que no es capaz de interpretar.
- Efecto de difusión: Si te etiquetan, los “amigos” de tu red social serán avisados de que has sido etiquetado en una nueva fotografía y que para verla les basta un simple clic. Tan fuerte es el efecto llamada y difusor de esta funcionalidad ligada a las imágenes que ofrecen las redes sociales que incluso los usuarios la usan para otros fines, a modo de aviso, sin atender a su original misión que es identificar a una personas en una imagen.

En definitiva, ello supone que otras personas van a tener un aviso de que tú estás relacionado con una imagen y podrían verla incluso antes de que tú supieras que esa imagen está publicada. Si tienes suerte, sabes que esa foto existe y que estás implicado en la misma e incluso puedes presuponer que alguien la puede haber subido online, sea esto o no de tu agrado. Sin embargo, la etiqueta es una llamada de atención, un altavoz para la labor de pregonero de tu vida que realizan los demás y las redes sociales. De pronto, muchos “amigos” tuyos saben que pueden ver un fotograma de la película de tu vida y en muchas ocasiones compartirlo con terceros.

En el plano más pragmático, al margen de lo relacionado con la legislación de datos personales, podemos identificar situaciones concretas donde las etiquetas causan problemas de privacidad que, en muchas ocasiones, son origen y/o consecuencia de una mala convivencia digital. Estos problemas pueden ser causados de manera accidental o bien de forma intencionada:

- Etiquetado en un contexto inoportuno por la actitud, el lugar, el momento, la compañía.
- Etiquetado revelando el aspecto físico de

alguien representado en la red social sin imagen o mediante un avatar.

- Insultos, ofensas públicas y amenazas, por ejemplo, relacionando a la persona etiquetada con una foto lesiva de su imagen o amenazante.

- Engaño para que la imagen implicada, que puede ser hiriente o desagradable, sea vista por la persona etiquetada, atendiendo a la notificación de que una etiqueta le afecta.

Geolocalización

Gracias a la posibilidad de geolocalización o georreferenciación que tienen los celulares, esto es, de identificar el lugar en el que se encuentran, son capaces de aportarnos más ventajas. Además de servir de mapa y brújula, ofrecen datos más relevantes como qué personas pueden encontrase cerca o qué información nos puede resultar de mayor utilidad en ese lugar y momento determinado.

Es un gran valor añadido que, sin embargo, tiene su contraprestación en términos de privacidad.

Con los permisos configurados de forma permisiva, cualquier acción realizada con el celular y sus apps puede tener como información anexa, en forma de metadato no perceptible a primera vista o de manera más explícita, la ubicación desde la que se hace y, por lo tanto, dónde se encuentra la persona que usa el dispositivo en ese momento. No siempre es sencillo de gestionar y puede resultar que esos datos sean una amenaza para la seguridad porque pueden revelar el paradero exacto, con las coordenadas geográficas, de una persona o el lugar donde se ha tomado una fotografía. Hay que tomar conciencia de esto porque de forma natural las aplicaciones instaladas y el propio software del teléfono nos invitarán, siempre y a la menor ocasión, a que permitamos acceso al dato de la ubicación del dispositivo. Debemos insistir en esta cuestión con niños, niñas y adolescentes que pueden, incluso, llegar a exponerse a peligros tan serios como el rapto sin tan siquiera saberlo.

Protección de la privacidad en los dispositivos móviles electrónicos

Tu celular contiene gran cantidad de informaciones y datos personales. Tus contactos, el acceso a las aplicaciones que sueles usar como Instagram o WhatsApp, las fotografías… están en tu celular donde también se pueden encontrar datos de los que ni siquiera eres consciente: redes Wifi a las que te conectas o los lugares donde has estado.

Es necesario, por lo tanto, que los escolares tengan bien presente esta cuestión y pongan en práctica las medidas a su alcance para que el uso del celular no suponga un riesgo en este sentido. A continuación, se plantean diez recomendaciones que habría que tratar que conozcan, comprendan y asuman.

Decálogo para proteger la privacidad de tu celular

1. Instala en tu celular un software de seguridad (antivirus) para combatir el malware.
2. Mantén actualizado el sistema operativo del celular para mejorar su seguridad.
3. Bloquea el dispositivo con una buena contraseña (números y letras) o un patrón.
4. Evita dejar guardada la clave en las apps que sean más importantes para ti.
5. Pon en marcha el servicio de localización del teléfono por si lo extravías.
6. Aprende a bloquear y eliminar remotamente los datos de tu celular en caso de pérdida o robo.
7. Activa la geolocalización y su uso por apps solo cuando lo necesites y sepas las consecuencias.
8. Verifica los permisos solicitados por cada app al instalarla y asegúrate de que no abusa.
9. Instala aplicaciones desde las tiendas oficiales para evitar malware.
10. Ten especial cuidado antes de acceder a enlaces, archivos o redes Wifi desconocidas.

Claves para mantener tus datos y vida privada a salvo

Cuando se habla de privacidad, se habla de ciberseguridad y, en consecuencia, se aborda la salud y el bienestar de alumnos y alumnas, de niñas, niños y adolescentes. Es clave tratar de hacerles a ellos mismos agentes competentes, conscientes y críticos al respecto y trasladarles las siguientes pautas fundamentales:

- Cuida la seguridad de tus dispositivos y conexiones a Internet.
- Utiliza contraseñas robustas.
- Tapa la cámara de tu computadora cuando no la utilices.

- Recuerda que todo lo que aparece en una pantalla puede ser capturado: conversaciones, imágenes, vídeos… A partir de ese momento pierdes su control para siempre.

- Toma en cuenta los metadatos (datos complementarios y ocultos), como por ejemplo la geolocalización. Pueden decir muchas cosas sobre ti sin que te des cuenta.

- Presta especial atención a la configuración de privacidad en tus dispositivos, aplicaciones y redes sociales:

  - Aprende dónde están las opciones relacionadas.

  - Asegúrate de entender su significado y consecuencias.

  - Actívalas según tus preferencias y necesidades.

  - Mantente alerta de los cambios que puedan sufrir.

- Ten cautela con las personas que manejan su privacidad de manera deficiente o no guardan medidas de ciberseguridad mínimas porque puede tener consecuencias negativas para ti. Ayudándoles te ayudarás.

- Evita el etiquetado en las fotografías de las redes sociales porque una imagen aporta gran cantidad de información.


Ciberbullying

Introducción

El ciberacoso entre iguales, llamado generalmente ciberbullying por su similitud con el término bullying aplicado al acoso en el ámbito escolar, es sin duda un grave problema en nuestras aulas y hogares. Se trata de una forma específica de violencia digital entre adolescentes, incluso niñas y niños, que no deja de aumentar y que trasciende el espacio escolar.

El sufrimiento de la persona acosada es muy intenso y se manifiesta en tristeza, aislamiento, pérdida de confianza y autoestima, trastornos con el sueño y la alimentación, aparición de dolencias psicosomáticas, etc. Deja una marca profunda y duradera en quienes lo padecen.

Para tener muy en cuenta

- El ciberbullying es el reto más relevante al que se enfrentan las personas menores de edad en Internet: causa graves daños, se da con cierta frecuencia y resulta muy complicado de prevenir y frenar.
- Es importante tomar conciencia de que la no existencia de agresiones físicas no significa ausencia de victimización o que se produzca un daño menor.
- Dado que Internet es una herramienta muy potente, cuando se utiliza para hacer daño, sus efectos pueden ser devastadores. Hay un gran desequilibrio de poder entre víctimas y victimarios.
- Esta forma de violencia digital entre iguales resulta favorecida por tres características: es sencilla de realizar, tiene consecuencias inmediatas y está siempre al alcance.
- Las personas que sufren ciberbullying tienden a aislarse, en ocasiones se sienten culpables de su situación y es poco común que pidan ayuda de forma temprana.

Definición y caracterización del ciberbullying

El ciberbullying es el hostigamiento realizado en o por medio de Internet (redes sociales, videojuegos, mensajería instantánea, páginas web…) intencionado, reiterado y mantenido en el tiempo por parte de una o varias personas hacia una víctima, de edad similar y con vinculación en el contexto escolar, sobre la que se posee o establece una posición de superioridad, ya sea por impunidad o por el ejercicio de dominio. Es frecuente que acoso y ciberacoso escolar vayan de la mano, pero no siempre es así.

Se concreta de muy diversas formas: la publicación de un rumor falso, de una imagen burlona o que pone en ridículo, exclusión de un grupo de mensajería, robo de la contraseña en una red social para insultar a otros en su nombre, etc.

La reiteración de las agresiones no siempre es realizada por la misma persona, sino que son muchas y diversas las que pueden participar con un simple "me gusta" o compartiendo información hiriente.

¿Cómo se manifiesta?

La realidad es que la manera de hacer daño a niñas, niños y adolescentes usando Internet es tan variada como amplia es la imaginación. El hecho de que la Red sea tanto un entorno de socialización como un elemento transversal al resto de contextos permite una diversidad mayor. Las manifestaciones más habituales del ciberbullying suelen ser:

- Flaming: envío de mensajes ofensivos a un foro sin ningún propósito constructivo.

- Denuncias premeditadas a los administradores de servicios online tales como Facebook. Las redes sociales tienen unas condiciones de uso que son aceptadas durante el proceso de alta y que impiden determinados comportamientos como pueden ser insultos o la publicación de imágenes íntimas. Al mismo tiempo, piden ayuda a la comunidad de usuarios para que denuncien estas infracciones usando un canal o formulario. Así, unos usuarios pueden denunciar a otros, simulando o provocando una situación de forma fraudulenta, por infracción de los términos y condiciones de uso, pudiendo conseguir incluso la expulsión o cierre del perfil denunciado.

- Acecho y persecución con mensajes ofensivos e insultantes que pueden ser dejados, por ejemplo, en grupos de WhatsApp o en aplicaciones, tipo ThisCrush (sitio de Internet donde se puede comentar los pensamientos o sentimientos hacia una persona con el nombre real o de forma anónima) que promueven el anonimato de quienes las usan.

- Robo de contraseñas, impidiendo el uso o suplantando la identidad para actuar de forma ofensiva o comprometedora frente a terceros.

- Acoso con matices sexuales con la mera intención de desagradar mediante, por ejemplo, el envío de imágenes pornográficas.

- Intimidación con amenazas, que pueden adoptar la forma de palabras, memes, o un simple enlace a un vídeo donde se da una agresión física.

- Denigración, creación de páginas de burla o puesta en circulación de informaciones o noticias falsas que hacen creer a una persona o grupos de personas que algo falso es real y que dañen su reputación y amistades.

- Revelación de información sensible o privada, como ocurre con frecuencia con víctimas homosexuales que no deseaban revelar su orientación sexual.

- Exclusión deliberada de actividades online como, por ejemplo, la no inclusión en el grupo de mensajería instantánea

(por ejemplo WhatsApp) del alumnado de la clase.

Es necesario conocer la forma en que este problema puede ponerse de manifiesto en el niño, niña y adolescente en el entorno escolar:

- Falta de asistencia a clase, por ejemplo, con ausencias pobremente justificadas.
- Disminución de la capacidad de concentración.
- Cambios de humor repentinos.
- Momentos de tristeza, apatía o indiferencia.
- Explosiones momentáneas de agresividad.
- Ausencia de amistades o de relaciones sociales.
- Poca comunicación o aislamiento en la clase.

Diferencias entre bullying y ciberbullying

Para el personal docente, es importante conocer las diferencias entre las distintas formas de victimización entre iguales de cara a poder identificar de manera eficiente los primeros síntomas y los factores de riesgo.

A pesar de que el sufrimiento de la víctima es el resultado final común, hay características diferenciales muy importantes entre el ciberacoso entre iguales con respecto al bullying tradicional:

- La víctima siempre está al alcance de las agresiones, en cualquier momento y en cualquier lugar. Incluso aunque no esté conectada, sus perfiles en redes sociales pueden estar recibiendo mensajes insultantes, por ejemplo, al tiempo que puede estar siendo dañada su identidad o reputación digital mediante comentarios negativos en foros, grupos de mensajería o imágenes de redes sociales.
- El liderazgo del acoso está más disperso y suelen participar más personas. Internet permite sumarse a la agresión a cualquiera que lo desee, incluso perteneciendo a otro centro escolar y, como casi todo en la Red, se puede hacer de forma colaborativa y compartida.
- Las agresiones son percibidas por más público y son más duraderas, a pesar de que son menos visibles para las familias y la comunidad educativa. Por ejemplo, la creación y compartición de un perfil falso en Facebook simulando ser el alumno o la alumna acosada y que publica fotografías hirientes, desagradables o amenazantes supone poco esfuerzo y tiene un enorme impacto.
- La percepción del daño causado es menor puesto que muchas veces no se ve directamente el sufrimiento de la persona acosada. El desarrollo de la empatía cuando median las pantallas y la distancia, e incluso el tiempo, no es sencillo. Una amenaza escrita como una broma puede parecer a quien la recibe, en un momento y contexto determinado, la más acusada condena.
- Los perfiles de agresores y víctimas son muy diversos, y no existen unos patrones claros. Cualquiera tiene la capacidad de hacer daño, y es común encontrar personas que han sufrido el ciberacoso pero que también lo han ejecutado e incluso liderado.

Esta distinta caracterización se debe a los factores diferenciales que ofrece Internet como canal y contexto de socialización entre nuestro alumnado.

Elementos que favorecen el ciberacoso entre iguales

Internet y la vida digital presentan determinadas características que facilitan el ejercicio de la violencia entre el alumnado a resultas de las cuales es más sencilla de realizar y difícil de frenar, adquiere formas más diversas y tiene más posibilidades de impunidad. Se pueden identificar los siguientes factores catalizadores:

- El anonimato (no identificarse), la suplantación (hacerse pasar por otra persona) y la impostura (adoptar una identidad ficticia) que permite Internet da mayor posibilidad y sensación de impunidad.

- El desconocimiento de que las normativas legales tienen la misma validez dentro y fuera de la red conduce a que se cometan, en el entorno digital, delitos graves impunemente.

- La inmediatez, calidad, potencia y precio del acceso y producción de contenidos online, junto con la disponibilidad y bajo coste de los dispositivos, pone al alcance de acosadores un arsenal valioso para el ataque. Desde una computadora o en el celular, en cualquier lugar es posible editar y comenzar a circular un meme.

- La muy positiva valoración de la destreza tecnológica en el grupo de iguales puede inducir a algunos alumnos a llamar la atención demostrando sus habilidades mientras acosa a algún compañero.

- La continua aparición de aplicaciones y servicios, que provocan nuevas posibilidades de acecho y un esfuerzo preventivo adicional. Una nueva forma de acoso puede nacer con la aparición de una nueva app social.

- La dificultad de prueba porque adquiere formas cambiantes y diversas muy difíciles de perseguir. En un entorno tan cambiante es complicado establecer protocolos duraderos y estándar para identificar a quienes acosan y obtener las pruebas de su acción.

- La apuesta de los videojuegos online por la creación de comunidades virtuales sin mayor cuidado en preservar la privacidad y el clima de convivencia. Se trata de entornos lúdicos que, en algunos casos, parecen carentes de responsabilidades y regulación al respecto.

- La no necesidad de coincidir físicamente con la víctima (ni siquiera en ocasiones es persona conocida) ni de ser más fuerte mental o físicamente. Esto hace que las combinaciones posibles de perfiles de personas acosadas y acosadoras aumente cada vez más en el tiempo.

- La fácil “agrupación” de acosadores. En la Red no es complicado encontrar personas dispuestas a defender una causa real o ficticia, propia o ajena o simplemente a formar parte de un grupo de acosadores.

- El no conocimiento de las consecuencias de las diferentes acciones. Quizás empieza como una broma o es fruto de un enfado, pero puede que esa foto donde la víctima es ridiculizada se acabe expandiendo más de lo deseado. Puede además que coincida con un momento

delicado (otros asuntos personales, baja autoestima…) en el estado de ánimo de la víctima. Así, alguien puede hacer mucho más daño del pretendido o del que se imagina.

- Las "excusas" del tipo "todo el mundo lo hace", "no era en serio" o "no era yo únicamente". Se trata de formas sencillas de tratar de eludir la responsabilidad.

- La adopción de un rol al que responsabilizan de su acción. Cuando alguien asume y se muestra en Internet como otra persona diferente, puede considerar que su responsabilidad y conciencia son diferentes a cada lado de la pantalla.

- La importancia creciente de la vida online, que implica mayor incidencia y menos alternativas de escape. Si antes estar conectado a Internet era algo circunstancial, cada vez más lo anecdótico será estar desconectado. Estando conectado las posibilidades de sufrir y sentir el acoso son mayores.

En definitiva, y por desgracia, es fácil, es barato, está siempre a mano y queda muchas veces impune.

La relevancia de las habilidades para la vida

En 1993 la División de Salud Mental de la Organización Mundial de la Salud (OMS) lanzó una iniciativa internacional para la Educación en habilidades para la vida en las escuelas (Life Skills Education in Schools). El propósito era difundir a escala mundial la formación en un conjunto de destrezas consideradas relevantes en la promoción de la competencia psicosocial de niñas, niños y adolescentes: habilidades sociales, cognitivas y de gestión de las emociones. La educación con enfoque en habilidades para la vida se centra en la formación en destrezas útiles para afrontar las exigencias y desafíos de la vida diaria. La educación en habilidades para la vida persigue mejorar la capacidad para vivir una vida más sana y feliz, intervenir sobre los determinantes de la salud y el bienestar, y participar de manera activa en la construcción de sociedades más justas, solidarias y equitativas.

Aunque hay diversas formas de clasificarlas, la propuesta de la OMS cuenta con un gran reconocimiento por su gran flexibilidad y aplicabilidad. Así, podemos identificar las diez principales habilidades para la vida:

- Autoconocimiento
- Empatía
- Comunicación asertiva
- Relaciones interpersonales
- Toma de decisiones
- Manejo de problemas y conflictos
- Pensamiento creativo
- Pensamiento crítico
- Gestión de emociones y sentimientos
- Manejo de tensiones y estrés

Todas ellas son necesarias aunque intervienen en diferente medida en las distintas situaciones y, por otro lado, toman diferente relevancia cuando de la vida digital se trata. Podemos por lo tanto potenciar en las aulas, y en el caso del ciberbullying, el desarrollo de algunas de ellas que nos servirán como antídoto.

Algunas habilidades clave para la ciberconvivencia

El ciberbullying presenta grandes retos para cada uno de los roles principales que intervienen: victima, victimario y testigo/ espectador. Sin duda, las habilidades para la vida ayudarían, dependiendo del momento y del rol, tanto para prevenir como para afrontar esta forma de hostigamiento. Entre ellas, las más destacadas pueden ser:

- Empatía: Resulta fundamental cuando se trata de las relaciones interpersonales. Si no sentimos que padece, no podemos compadecernos. Las pantallas y las distancias dificultan la percepción del daño.

- Autoestima: La baja autoestima suele caracterizar a quienes acosan, aunque no lo parezca, y suele desarrollarse también en quien padece el acoso.

- Pensamiento crítico: Además de otras habilidades y valores que deben entrar en juego posteriormente, el primer paso es no aceptar el acoso como algo “normal”. Es vital la desnormalización para movilizar a los espectadores.

- Asertividad: Los testigos deben ser capaces, cuando menos, de no participar en aquello con lo que no se sienten cómodos, aun cuando sea una postura a contracorriente.

La ciberconvivencia como reto consciente, permanente y colectivo

Las características de Internet facilitan el ejercicio de la victimización de manera sencilla y cómoda, tanto fuera como dentro de las aulas. Por ello, el buen clima de convivencia se debe construir día a día, entre todas las personas que habitamos la Red. Es preciso adquirir conciencia de ello unido, como no podía ser de otra manera, al concepto de ciudadanía digital responsable. Tomar en consideración siempre a las demás personas de la Red intentando incluso prevenir confrontaciones que puedan derivar en acoso es una práctica preventiva que se debe promover. A continuación, se citan diez consejos necesarios para ello que el personal docente puede fomentar entre sus alumnos y alumnas para mejorar el clima de ciberconvivencia, y con ello el bienestar digital de su alumnado.

Decálogo para la convivencia digital positiva

1. **Disfruta con ética y educación la Red, usa la netiqueta.**

   Netiquétate! La netiqueta es comunicarse de forma respetuosa, educada y responsable en internet, son los buenos modales aplicados al mundo digital. Respetarlas facilita la convivencia en Internet.

2. **Evita usar de manera pública expresiones que puedan ofender a otras personas.**

Lo que se dice en Internet tiene muchas veces una difusión inesperada y puede que sea molesto o incómodo para alguien.

3. **Si sufres acoso o te sientes incómodo/a, pide ayuda y rompe el silencio:**

   Comparte inmediatamente la situación con un adulto de confianza para que puedan asistirte y, en su caso, ayudarte a denunciar.

4. **Ten presente que estar de este lado de la pantalla no te sirve de protección.**

   Enfrentar situaciones pensando que se pueden evitar solo desconectándote no es inteligente. Internet tiene un alcance muy grande.

5. **Cuida tus datos personales y tu privacidad para aumentar tu nivel de protección.**

   Cuanta más información se tiene de una persona, más posibilidades hay de hacerle un daño.

6. **No hagas en Internet lo que no harías frente a frente.**

   En ocasiones, quien está al otro lado de la pantalla es alguien que está más cerca de lo que se puede pensar. Idioma, edad, intereses y cultura ayudan a ello.

7. **Rehúye de la gente incómoda o agresiva, y ten cuidado con los nuevos contactos.**

   En Internet algunas personas buscan la provocación y hacer daño. Evitarlas es importante, en especial dentro de tus redes sociales.

8. **Evita suposiciones porque puedes equivocarte.**

   Una ofensa a veces es una acción involuntaria, mal interpretada o dirigida a otra persona. También puede esconder un engaño premeditado.

9. **Ignora las provocaciones. Cuenta hasta diez y piensa en otra cosa.**

   Contestar una ofensa no ayuda a evitar el conflicto y puede derivar en ciberacoso. Alguien con mala intención e Internet puede causarte graves daños.

10. **Pide ayuda al administrador de la página o del servicio cuando te molesten online.**

    Muchos servicios online, como las redes sociales y los juegos, tienen políticas de uso que prohíben conductas molestas para sus usuarios.

La labor de prevención

El ciberacoso escolar es fundamentalmente una cuestión de valores. No obstante es posible condicionar esos valores o, en todo caso, la intensidad con la que se pudiera manifestar la ausencia de los mismos. Hay varias líneas de actuación que, de forma complementaria al desarrollo de habilidades para la vida, contribuyen a la disminución del ciberacoso.

Fomento de la privacidad y la ciberseguridad

Privacidad y ciberseguridad van de la mano y, con ellas, la seguridad de las personas. Un niño, niña y adolescente tendrá menos probabilidades de sufrir ciberacoso o de que éste sea menos intenso o con menores consecuencias si desarrolla buenas prácticas de seguridad y privacidad.

Divulgación de los límites y responsabilidades legales

Dar a conocer qué está al margen de la Ley y las consecuencias que puede suponer para quien realiza este tipo de acciones es muy importante. Amenazas, ofensas, revelación de secretos, suplantación de identidad son acciones que pueden tomar parte del ciberbullying y ser susceptibles de ser castigadas por la Ley. Un adolescente, consciente de esta situación, puede que decida no involucrarse en un acoso o, si ya comenzó, desistir en su actitud o moderarla. Por su parte, quien sufre la victimización es consciente de que la Ley está de su lado, guardar las pruebas de los delitos y, en su caso, actuar legalmente.

Impulso del concepto de ciudadanía digital y de netiqueta

Es necesario trasladar a niños, niñas y adolescentes que Internet no es algo que se usa, sino un lugar donde vivimos y convivimos. Por esa razón, debemos ser partes proactivas de ese nuevo contexto, ciudadanos y ciudadanas digitales, con un ejercicio activo de derechos y deberes que nos permita disfrutar del gran entorno de socialización. Internet es lo que hacemos de ella y por esa razón hay que impulsar la corresponsabilidad. En esta línea se puede incluir el concepto de netiqueta como conjunto de reglas establecidas por un determinado grupo para mejorar las condiciones de disfrute y convivencia de un determinado contexto digital. De igual forma, la creación de dinámicas donde el alumnado de mayor edad toma la responsabilidad de orientar a alumnado más joven sobre el uso saludable y la convivencia positiva online, producen un efecto magnífico en el clima escolar. El programa Cibermanagers de Pantallas Amigas fue la experiencia pionera en este sentido y desde 2010 se realiza con éxito.

Llamada a la acción de los diferentes tipos de espectadores

Dentro de los que se denominan generalmente espectadores o testigos del acoso o ciberacoso hay diferentes tipos, pero para con todos ellos hay una posibilidad para hacerles parte de la solución: sacarles de su pasividad, que en cierta manera supone una forma de complicidad con quienes acosan. Como ejemplo, proponerles evitar ser espectadores es el primer paso, que muestren apoyo a la víctima en privado sería el segundo y el tercer grado de implicación sería posicionarse activa y públicamente contra la situación del acoso online.

Puesta en valor del buen ambiente en los espacios de relación digital

Existe tanta violencia online que es preciso contrarrestarla para que no sea normalizada e interiorizada como habitual. Se debe hacer notar la diferencia y para ello nada mejor que hacer valer, mediante la toma de conciencia, lo positivo del buen clima online entre iguales, de valores tan básicos como el respeto y la tolerancia a la diversidad en todas sus formas. La percepción en positivo del buen clima de convivencia sin duda repercute en un mayor compromiso con el mismo y al rechazo de las acciones que lo destruyen.

La labor de prevención

La actuación en caso de tener constancia o indicios de que se da una situación de ciberbullying tiene muchos condicionantes (contexto escolar y social, intensidad y duración del acoso, perfil de víctimas y victimarios…). Aunque las autoridades educativas o el centro escolar tengan un protocolo específico, siempre cabe insistir en la prudencia y la discreción así como en la toma informada de decisiones. Se trata de un terreno resbaladizo donde la constatación de la situación es tan difícil como fundamental. Conviene tener presente también que quien acosa suele ser alguien necesitado de ayuda y que, en todo caso, sus derechos deben ser respetados (privacidad, presunción de inocencia…).

Decálogo para una víctima de ciberbullying

Cada minuto que pasa la víctima está a un clic de sus acosadores. Intervenir de inmediato y hacerlo de forma adecuada es clave. En ocasiones la iniciativa, para ganar tiempo o porque no encuentra o no desea pedir ayuda, debe ser de la propia víctima y, en todo caso, es precisa su colaboración. Por ello, aunque los maestros y maestras deben tratar de prestar su ayuda directa, es también necesario que sean capaces de hacer a la víctima competente para que se ayude a sí misma llegado el caso. Estas serían las pautas a seguir, en forma de decálogo, que deben trasladar a sus escolares para que puedan limitar o frenar el daño:

1. **Pide ayuda.** Recurre a tu padre o tu madre o, en su defecto, a una persona adulta de confianza. Asegúrate de que esa persona conoce y entiende estas pautas para que ambos puedan remar en el mismo sentido y para que, en su ánimo de protección, no haga cosas que acaben siendo perjudiciales.

2. **Nunca respondas a las provocaciones o insultos.** Hacerlo no te ayuda en nada y, sin embargo, es un estímulo y una ventaja para quienes te acosan. Mantén la calma y no actúes de forma exagerada o impulsiva en ningún caso.

3. **No hagas presunciones.** Puede que ni las circunstancias ni las personas que parecen implicadas sean como aparentan. Mantén un margen para la duda razonable porque actuar sobre bases equivocadas puede agravar los problemas y crear otros nuevos.

4. **Trata de evitar aquellos lugares en los que te acosan** en la medida de lo posible hasta que la situación se vaya clarificando. Si se trata de redes sociales o comunidades online no te será difícil.

5. **Cuanto más se sepa de ti, más vulnerable eres y más variado e intenso es el daño que pueden causarte.** ¿Imaginas una mentira ridiculizándote construida sobre datos privados reales escrita en un lugar visible? ¿qué pasaría si alguien, haciéndose pasar por ti, insulta a tus amistades? Es momento, por lo tanto, de cerrar las puertas de tu vida online a personas que no son de plena confianza. Puedes hacerlo así:

   a. **Evita intrusos.** Para ello debes realizar, en orden, estos dos pasos:

      a.1. Realiza un chequeo a fondo de tus dispositivos para asegurarte de que no tienes software malicioso (troyanos, malware…) que puede dar ventajas a quien te acosa. Es importante.

      a.2. Cambia las claves de acceso a los servicios online que usas, pero nunca antes de haber realizado el paso anterior. Recuerda que deben ser complejas de adivinar y llevar combinados números y letras.

   b. **Depura la lista de contactos.** Revisa y reduce la lista de contactos que tienes agregados en las redes sociales o en otros entornos sociales online.

   c. **Reconfigura** las opciones de privacidad de las redes sociales o similares en las que participes y hazlas más estrictas. Asegúrate de que sabes bien cómo funcionan estas opciones y sus implicaciones.

   d. **Comprueba qué cuentan de ti en las redes sociales.** Busca la información sobre ti publicada por otras personas y trata de eliminarla si crees que puede ser utilizada para hacerte daño.

   e. **Repasa la información que publicas** y quién puede acceder a ella y quién puede compartirla con terceros.

   f. **Comunica a tus contactos** que no deseas que hagan circular informaciones o fotografías tuyas en entornos colectivos.

   g. **Ejerce tu derecho sobre la protección de datos personales.** Tú decides el uso que se puede hacer de ellos, incluyendo tu fotografía.

6. **Guarda las pruebas del acoso** durante todo el tiempo, sea cual fuere la forma en que éste se manifieste, porque pueden serte de gran ayuda. Trata también de conocer o asegurar la identidad de los autores pero, en todo caso, sin lesionar los derechos de ninguna persona.

7. **Comunica a quienes te acosan que lo que están haciendo te molesta** y pídeles, sin agresividad ni amenazas, que dejen de hacerlo. Recuerda que no debes presuponer hechos o personas en tu comunicación, por lo que debes medir muy bien cómo lo haces, sin señalar a nadie en público, pero a la vez tratando de asegurarte de que se entera la persona o personas implicadas.

8. **Trata de hacerles saber que lo que están haciendo es perseguible por la Ley** en el caso de que el acoso persista. Les puedes sugerir que visiten online una noticia de un caso o condena para que lo comprueben por sí mismos.

9. **Deja constancia de que estás en disposición de presentar una denuncia** si a pesar del paso anterior continúa el acecho. Manifiesta que cuentas con pruebas suficientes recopiladas desde el inicio y que sabes cómo y dónde presentarlas. Debes indicar que, si el ciberacoso persiste, te verás obligado a acudir a la policía.

10. **Toma medidas legales** si la situación de acoso, llegado este punto, aún continúa.

Para la puesta en práctica de estas recomendaciones es importante tener en cuenta las siguientes notas:

- Aunque son, en su mayoría, pautas de aplicación también para víctimas adultas y fuera del contexto escolar, cuando se deseen transmitir a niños, niñas y adolescentes, se precisa una modulación en la forma de comunicar el mensaje.

- Cada caso y persona es diferente. Por ello, estas indicaciones pretenden ser de ayuda, de forma completa o parcial, en los sucesos más comunes.

- El orden en que se toman las medidas es importante. No obstante, la gravedad de los hechos en algunos casos puede requerir acelerar la ejecución de determinados pasos, reducir el intervalo entre ellos o directamente obviarlos.

- En casos extremos, la solicitud de ayuda a la policía debe ser inmediata.

Por último, para el entorno de la víctima, hay tres principios básicos que adoptar:

1. **Proteger y arropar a la víctima.** Es lo más importante. Debe sentirse consolada, comprendida, acompañada.

2. **Renunciar** a las presunciones porque es precisamente el engaño una de las armas comunes de quien acosa y, en Internet, la suplantación suele ser común en estos casos.

3. **Actuar de manera comedida**, pausada, colaborando con el resto de los agentes intervinientes. Elevar la intensidad de la violencia ya existente o extenderla no ayudan a una pronta solución.

Recuerda que las conductas aquí referidas podrían encontrarse sancionadas en los arts. 288 BIS, 149 BIS, 149 TER, del Código Penal


Grooming

Introducción

El acoso sexual a menores de edad es un delito, que no para de crecer en Internet, tipificado en el art. 277 bis del Código Penal de Uruguay. La aparición de Internet ha supuesto un aumento de este tipo de riesgo para niñas, niños y adolescentes por varias razones, entre ellas las siguientes:

- Los pedófilos y pederastas ya no son personas aisladas que se ocultan sino que, además de comunicarse con personas de su misma condición online, pueden encontrar en la Red contenidos que promueven, impunemente, el "amor con los niños". Esto los fortalece porque reduce su posible sentimiento de culpabilidad y además les proporciona respaldo al encontrar una comunidad afín.

- Las imágenes de explotación y abuso sexual de menores de edad, inadecuadamente llamada pornografía infantil, son el objeto de un negocio clandestino potenciado por Internet y, como tal, mueve importantes sumas de dinero.

- La Dark Web es un medio que ayuda a este tipo de ciberdelitos porque los hace casi indetectables. Según un estudio de la Universidad de Porstmouth, el 80% del tráfico generado en ese contexto está relacionado con la difusión de imágenes íntimas y abuso sexual de menores de edad.

- La asimetría de poder entre víctimas y victimarios se acentúa en este caso. Depredadores pueden alcanzar a un mayor número de víctimas, de cualquier edad, y en cualquier país, incluso simultáneamente, por lo que la posibilidad de prevención y persecución de este delito se ve limitada.

Así pues, es un gran reto el que afrontamos en la sociedad de hoy en día en el que los y las docentes tienen la oportunidad de contribuir de forma efectiva. Si bien el ciberbullying llega a provocar suicidios, este tipo de violencia contra menores de edad es la que más se ha incrementado y la que, sin llegar a esas situaciones extremas, sí puede estar vinculada a la violencia sexual, explotación y trata de personas y, en todo caso, deja igualmente una profunda marca en las víctimas.

Para tener muy en cuenta

- El grooming supone una grave amenaza para la salud e integridad sexual de niñas, niños y adolescentes. Su vida digital conectada desde edades cada vez más tempranas los sitúa al alcance de depredadores sexuales de todo el mundo con quienes tienen claras desventajas: edad, experiencia y competencias tecnológicas.
- Afecta en mucha mayor medida a las niñas que a los niños. En casos extremos puede desembocar en encuentros físicos con el agresor, secuestro, violación, explotación sexual o trata de personas.

- Los canales y contextos que permiten una comunicación permanente, fluida, privada y sin controles severos de identidad son los más propicios para este acecho: redes sociales, apps de mensajería instantánea, juegos online multijugador…
- El gran reto para combatir el ciberacoso sexual infantil, al margen de la prevención y la difícil detección temprana, es sin duda que las víctimas pidan ayuda. Familias, sociedad e instituciones deben trabajar de la mano para lograrlo.

Internet grooming: qué es y cómo se produce

El grooming es una estrategia de ciberacoso sexual por parte de una persona adulta hacia una menor de edad. El depredador sexual, tras ganarse la confianza de la víctima mediante empatía, atención o adulación busca luego, generalmente con amenazas y chantajes, obtener concesiones de índole sexual (imágenes, vídeos o hasta un encuentro personal). También recibe los nombres de “child grooming”, “Internet grooming” o ciberacoso sexual de menores de edad.

La persona que hace grooming suele utilizar redes sociales, chats, juegos en línea o foros para contactar y hacer amistad con sus víctimas. Capta su interés con un perfil atractivo que le brinda confianza, expresa en sus conversaciones los mismos gustos y emociones y utiliza las mismas expresiones, lenguaje y emoticonos para ganar la simpatía con sus víctimas. Se presenta como el amigo, amiga, novio o novia ideal.

Se da no obstante un manejo diverso y algo confuso de los términos ya que, por similitud en objetivos y consecuencias, existe un tipo de ciberacoso sexual que no se aproxima a los menores de edad de forma amistosa sino directamente por la fuerza y que también es referido como grooming. De igual manera ocurre con la sextorsión, que suele ser una de las etapas finales del grooming, y por ello es habitual también utilizar aquel nombre sustituyendo a éste.

¿Quién puede ser víctima de grooming?

Cualquier persona menor de edad puede resultar atrapada en las garras del ciberacoso y ciberabuso sexual. No obstante, las niñas y adolescentes lo sufren mucho más que ellos. Los ciberdepredadores tienen desarrollada su técnica, perfeccionada con cada nuevo acoso, siendo el primer paso el estudio de su “presa” y los factores de vulnerabilidad. A partir de entonces, el grado de dificultad o resistencia que presente la víctima, así como el umbral de riesgo que desee alcanzar el acosador sexual, determinarán que la estrategia de grooming llegue o no a su término. Por desgracia, las distancias juegan a favor del criminal dado que el abuso sexual de menores puede realizarse desde un país o continente diferente, lo que supone una dificultad para activar los mecanismos legales para su persecución.

Condiciones necesarias para el grooming

Hay dos aspectos o momentos clave en el grooming:

- La toma de control por parte del depredador mediante la obtención de un elemento para doblegar, con chantaje, la voluntad de la víctima: la posesión

de una imagen íntima, el secuestro de su perfil en una red social, la obtención de un secreto inconfesable… En unas ocasiones la persona menor de edad entrega este elemento de control pero, en otras, simplemente se obtiene por la fuerza o mediante engaño, sin que se pueda hacer nada para evitarlo.

- La ausencia de búsqueda de ayuda y apoyo por parte de la víctima suele responder a dos factores. En primer lugar, la fuerte presión que el abusador ejerce, mediante manipulación y amenazas. En segundo lugar, la sensación que padece la víctima de haber hecho algo inadecuado o inconfesable.

Si no se dieran alguna de estas dos situaciones la victimización no se produciría.

Un elemento que tradicionalmente ha facilitado el grooming ha sido la cámara web de la computadora o celular. Si bien está claro que hay muchos otros medios de producir y enviar una imagen a otra persona, la disponibilidad, la facilidad y la inmediatez con la que se puede hacer usando la cámara es un factor determinante. De esta forma, el depredador tratará que su víctima le muestre, en una pretendida intimidad, una imagen comprometedora que él podrá capturar para dar luego lugar al chantaje mediante la estrategia de sextorsión.

Factores de riesgo a evitar

Conociendo como se desarrolla esta forma creciente de victimización, es posible identificar cuatro circunstancias específicas que pueden elevar el riesgo de grooming:

- La baja autoestima hace que aprecien más los halagos y las nuevas amistades, que busquen mayor aprobación, que no quieran fallar a las expectativas o solicitudes de esa persona.

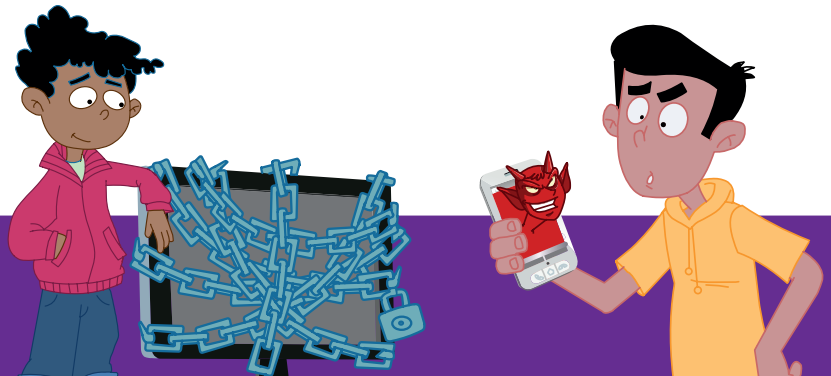
- El excesivo tiempo de conexión puede llevar a explorar personas o lugares inadecuados.

- La adopción de conductas de riesgo o “inconfesables” que puedan servir de elemento de chantaje a terceros.

- La falta de cohesión y confianza en la familia supone, a menudo, ausencia de supervisión adecuada y una dificultad añadida para que la víctima busque ayuda.

¿Cómo afrontar un caso de grooming?

Cuando se detecta entre el alumnado un caso posible de grooming, lo principal es impedir que el abuso o sus consecuencias continúen y apoyar a la víctima. Las situaciones de acecho sexual rara vez terminan por sí mismas, siendo habitual la reincidencia en el acoso incluso en momentos muy distantes en el tiempo. La familia debe estar informada desde el primer momento para que tomen medidas con las



autoridades competentes, como es la policía, para detener la situación. Es preciso no bajar la guardia y tratar de llegar hasta el final. Es por ello que si se identifica alguna alumna o alumno que pueda estar siendo víctima de grooming se informe a la familia y se le den los siguientes consejos:

1. Analizar en qué ilegalidades ha incurrido el acosador y cuáles pueden ser probadas. Puede ser inviable probar que el depredador dispone de ciertas imágenes o información que ha hecho públicas. También puede ocurrir que no se pueda demostrar que esas imágenes fueron obtenidas por la fuerza o mediante engaño o incluso que se han recibido amenazas. Por todo ello conviene saber en qué ilícitos ha incurrido o incurre el depredador porque ello habilita la vía legal.

2. Buscar y recopilar las pruebas de la actividad delictiva: capturas de pantalla, conversaciones, mensajes, etc., todo aquello que pueda demostrar las acciones del depredador o dar pistas sobre su paradero o modo de actuar será de gran utilidad tanto a efectos de investigación como probatorios. Se debe tener presente no vulnerar la Ley en este recorrido.

3. Formular una denuncia. Con un adecuado análisis de la situación y elementos de prueba que ayuden a la investigación el hecho ha de ser puesto en conocimiento de la policía con independencia de que el acecho hubiera o no remitido. Se debe tener presente que, por lo general, estos ciberdelincuentes suelen tener decenas de presas de forma simultánea y que debe acabar siendo investigado y juzgado para que no continúe con su deleznable actividad.

Cada caso es diferente y la manera de abordarlo también. En determinadas circunstancias, incluso puede ser recomendable seguir con prudencia la corriente del acosador para tratar de identificarle u obtener pruebas. En otras, la denuncia inmediata a la policía es la opción más razonable. No obstante, las anteriores son orientaciones que pueden funcionar bien en la mayoría de los casos y mientras la policía ofrece su asistencia.

Diez consejos para luchar contra el grooming

A continuación, se plantea una decena de recomendaciones preventivas frente al ciberacoso sexual que equipo docente y familia pueden transmitir a nuestros niños, niñas y adolescentes:

1. **No te fíes de las apariencias.**

   Es fácil dejarse llevar por impresiones. Simular ser otra persona o tener amistades en común es un engaño frecuente.

2. **Contrasta la identidad de los nuevos contactos**.

   Si vas a incluir a alguien como nuevo contacto, antes ocúpate de de tratar de comprobar su identidad.

3. **Guarda tu información íntima y tus secretos.**

   Tus cosas íntimas, tus secretos, lo que no te gustaría que supiera nadie, es un tesoro que hay que proteger.

4. **Si te hacen sentir mal, corta el contacto.**

   Cuando alguien te haga sentir incomodidad, te ofenda o te presione, corta el contacto.

5. **Pide ayuda si te amenazan o te hacen chantaje.**

   Si te amenazan o tratan de chantajearte, pide ayuda a una persona adulta de confianza.

6. **Cuida tu ciberseguridad.**

   Tu seguridad personal depende de la seguridad de tus dispositivos conectados (celular, tableta, computadora…).

7. **Protege tu privacidad.**

   Cuanto más se sepa de ti, más daño se te puede causar. Cuídate aumentando tu privacidad.

8. **Desconfía de las buenas palabras de las malas personas.**

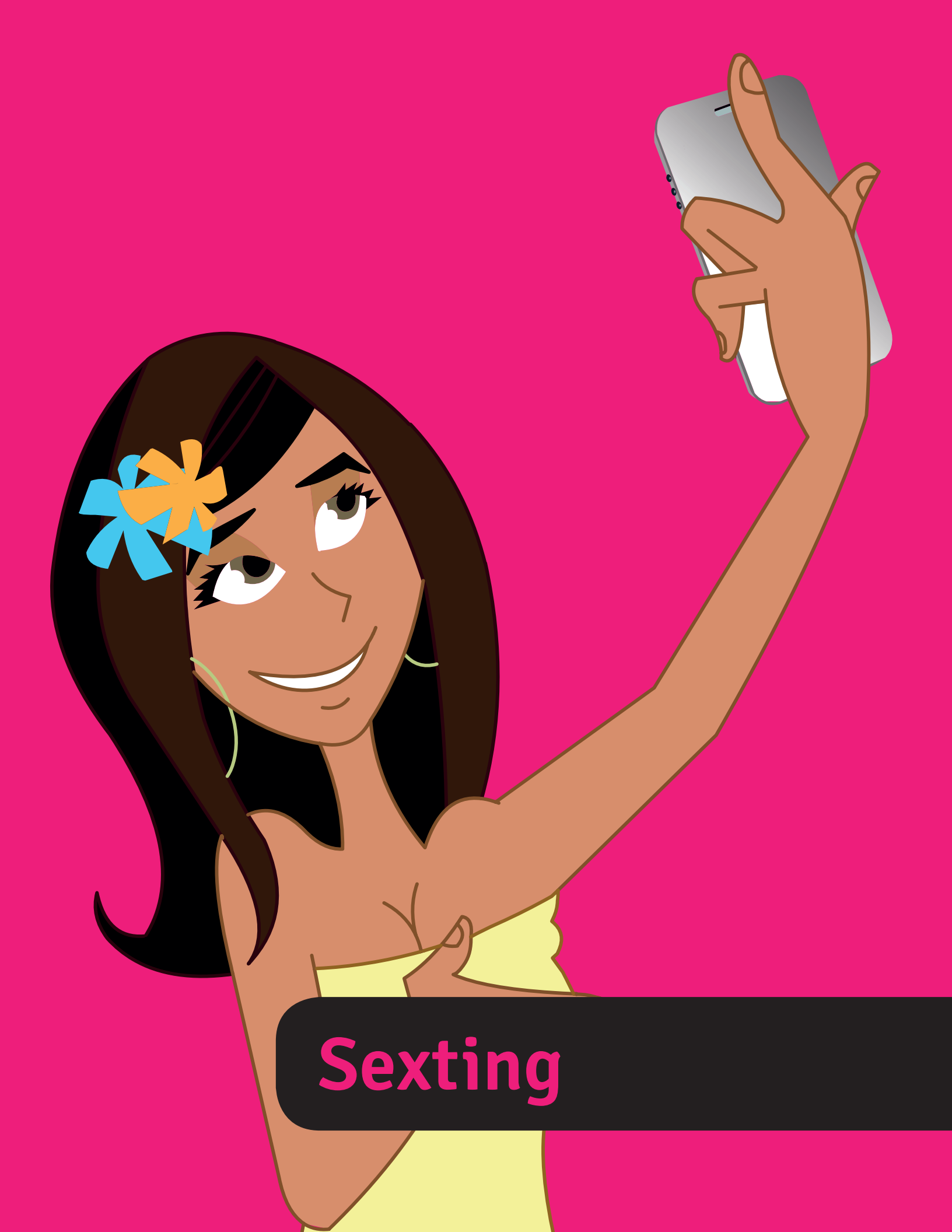
   Si alguien ha intentado hacerte daño no merece tu confianza. No valen las promesas ni los tratos.

9. **Recuerda que tú no tienes la culpa.**

   Aunque te sientas mal o hayas hecho algo que no debías, no te ocultes y pide ayuda.

10. **Nunca acudas sin la compañía de una persona adulta a una cita.**

    Si te citas con alguien que has conocido en Internet, hazlo siempre en un lugar público y acude en compañía de una persona adulta.


Sexting

Introducción

La práctica del sexting con imágenes íntimas tiene más de una década. Diez años en los que ha pasado de ser una cuestión residual a constituir una práctica relativamente habitual realizada de muy diversas maneras. Es necesario decir que, al margen de cuestiones de tipo ético o legal que se quieran plantear en cuanto afecte a menores de edad, el sexting no implica en sí mismo un daño. Se trata de una acción que en ocasiones por error o, la mayoría de las veces, por la mala intención de otras personas, puede causar graves problemas. Estamos por lo tanto ante una práctica de riesgo que se da también entre escolares y que se debe abordar en el aula.

¿Qué es el sexting?

El sexting es una práctica que consiste en enviar, de forma voluntaria, imágenes propias (fotografías o vídeos) íntimas de alto contenido erótico o sexual a otra persona, usando el celular o computadora.

Desde el punto de vista de los riesgos, es equivalente a mostrarse por medio de la cámara de la computadora o en un directo desde el celular. La diferencia en estos casos con respecto al sexting es que, para que exista riesgo, esa imagen efímera debe ser capturada por quien la recibe.

Suele estar enmarcado en la relación de pareja, pero también es realizado con personas cuya atención se quiere reclamar o incluso con desconocidas.

Existe cierta confusión con este término ya que en algunos países se usa incluso cuando una persona adulta envía imágenes íntimas a una menor de edad. En ese caso, los niños no están participando en una práctica de riesgo, sino que podrían ser víctimas de un delito. También en algunos casos se ha usado ese término para referirse al tipo penal que regula ciertos usos indebidos de imágenes íntimas.

¿Qué riesgos puede haber para quien practica sexting?

Se trata de una práctica de riesgo porque la existencia de esas imágenes íntimas puede convertirse en un problema para quienes las protagonizan. Pueden dejar de ser privadas si quien las recibe hace mal uso de ellas, compartiéndolas o publicándolas sin permiso, o bien cuando son extraviadas, robadas o enviadas por error. Si son compartidas, además de verse dañado el derecho a la propia imagen y la intimidad, se puede ser víctima de ciberbullying. También es posible convertirse en víctima de sextorsión si quien posee las imágenes pide dinero u otras

exigencias a cambio de no hacerlas públicas.

En todo caso deben tomarse en consideración las leyes relativas a la producción, la posesión, la distribución y comercialización de contenido sexual de niños, niñas y adolescentes.

Se puede citar de forma específica el "revenge porn", también llamado "porno venganza" o "porno vengativo". Es cada vez más frecuente, constituye también una modalidad de vulneración de la privacidad e intimidad, y es una forma de ciberviolencia de género. Consiste en "castigar", supuestamente por venganza o despecho, a tu pareja o expareja con la publicación de imágenes de alto contenido sexual protagonizadas por ella.

Cuando la situación de ciberacoso a la víctima protagonista de las imágenes no es realizada por un entorno acotado y cercano sino que es masivo aunque de menor intensidad en vez de ciberbullying podríamos denominarlo "linchamiento digital".

Es importante no cargar la culpa del daño derivado del sexting en quien lo practicó sino sobre quien realizó una acción indebida con las imágenes privadas ajenas.

A continuación, se presentan unas ideas clave para trasladar a los y las estudiantes.

Para tener muy en cuenta

- El sexting es una práctica de riesgo. Si lo practicas puedes sufrir mucho daño por mala acción de otras personas o incluso por casualidad o descuido.
- Frente al sexting debes tomar una decisión meditada, sin presión de ningún tipo y con información sobre el daño que puedes llegar a sufrir o provocar.
- Cualquier imagen o escena de video que es vista en una pantalla puede ser capturada y compartida para siempre.
- En ningún caso existe derecho a compartir una imagen íntima, aunque su grabación haya sido consentida.
- Si llegan a tus manos imágenes íntimas de otras personas, respeta y bórralas. Si las compartes, además de causar daño, puedes estar cometiendo un delito grave.

Prevención del sexting desinformado, precipitado o bajo presión

Dado que del sexting se pueden derivar consecuencias negativas, es preciso que quien decida sextear lo haga desde una posición libre, sin atender a presiones grupales, sociales o de pareja. Además, debe ser una decisión informada, que cuente con conocimiento suficiente sobre los riesgos potenciales que asume. Por último, y por ser una cuestión importante, debe afrontarse de forma meditada, no precipitada. La invitación a reflexionar sobre las razones para no sextear es un contrapeso necesario que se

ha de exponer de manera clara y explícita. En ningún caso se trata de una imposición ni de una prohibición.

Pensar antes de sextear

10 razones para no hacer sexting ¡Tú decides!

1. **Existe otra persona implicada de la que ahora dependes.**

   Ya no es algo que depende de ti. Alguien más puede tomar decisiones que te afecten.

2. **Las personas y las relaciones pueden cambiar.**

   Cierta circunstancias de la vida cambian nuestros sentimientos, y a veces grandes amistades se vuelven los mayores enemigos.

3. **La protección de la información digital es complicada.**

   Es muy complejo garantizar una seguridad total.

4. **La distribución de información digital es incontrolable.**

   Toda imagen que aparece en una pantalla es irrecuperable para siempre.

5. **Una imagen puede aportar mucha información.**

   Adornos, tatuajes, piercings… el número de celular vinculado a la imagen o quien tiene tu foto pueden revelar tu identidad.

6. **Existen leyes que penalizan acciones ligadas al sexting.**

   Ten especial cuidado cuando las imágenes sean de alguien menor de 18 años.

7. **Se produce sextorsión si la imagen de sexting cae en manos de chantajistas.**

   Una imagen de sexting en manos inadecuadas supone un riesgo de sextorsión.

8. **Internet es rápido y potente.**

   Las imágenes de sexting pueden llegar a Internet, el canal de difusión más potente nunca conocido.

9. **Las redes sociales facilitan la información a las personas cercanas.**

   Internet y las redes sociales ayudan a que te encuentres con las personas con las que puedes tener cosas en común.

10. **Existe grave riesgo de ciberbullying si la imagen de sexting se hace pública en Internet.**

    Hay personas que parecen disfrutar haciendo daño. Para ellas serás culpable y te convertirán en su víctima.

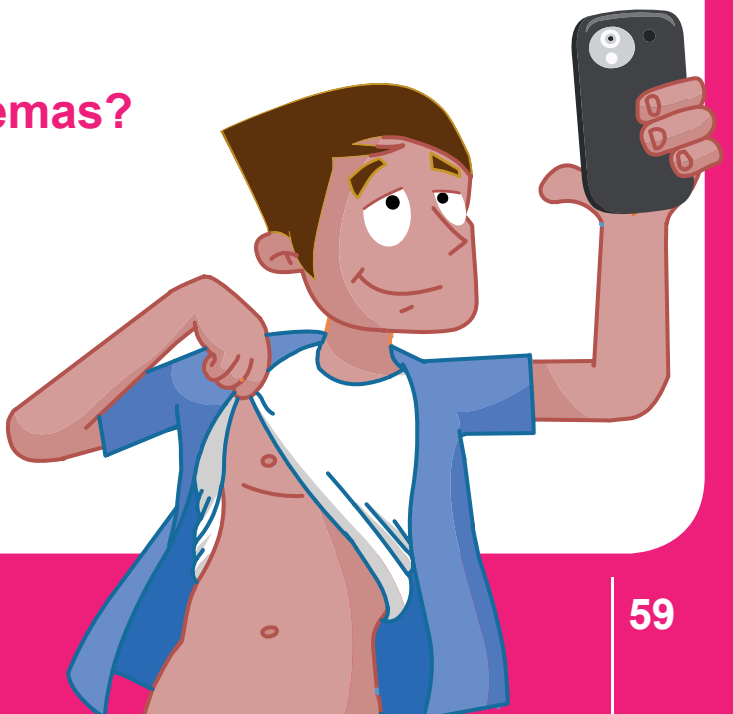
Decálogo para sextear con menos riesgos

Hay personas que deciden practicar sexting por lo que, desde el punto de vista preventivo, es necesario poner de manifiesto las medidas que ayudan a reducir los riesgos asociados, es decir, lo que se puede hacer si se desea que las probabilidades de victimización sean menores. Se expone a continuación un decálogo de sugerencias que se pueden compartir con el alumnado y las familias siempre y cuando **se enfatice la recomendación de no asumir el riesgo de sextear:**

1. Asegúrate de que conoces los riesgos asociados al sexting, que tu decisión ha sido tomada sin presiones o amenazas y que lo haces sin precipitación.
2. Valora hasta qué punto la persona destinataria merece tu confianza y está preparada para proteger tu privacidad e intimidad.
3. Confirma que quien recibiría tu mensaje desea tenerlo y cuenta con aviso previo para que no resulte incómodo o problemático.
4. Revisa que tu celular no tenga malware y pide a la persona destinataria que también lo haga.
5. Decide con calma qué tipo de imagen o vídeo quieres enviar.
6. Excluye de la imagen o vídeo partes que puedan ayudar a conocer tu identidad (rostro, marcas corporales, objetos o entorno) y metadatos como la geolocalización.
7. Selecciona el medio o aplicación que mejor se adapte a tu propósito con las mayores garantías. Existen apps específicas para ello y también sistemas de encriptación.
8. Evita el uso de redes Wifi públicas durante el envío y solicita a quien se la envías que haga lo mismo.
9. Centra tu atención en lo que haces. Verifica bien qué y a quién envías antes de pulsar. No hay opción a arreglar un error.
10. Elimina del celular (y de la nube si es el caso) las imágenes íntimas, las usadas o las pruebas. Solicita a quien se las envías que haga lo mismo.

¿Qué hacer en caso de problemas?

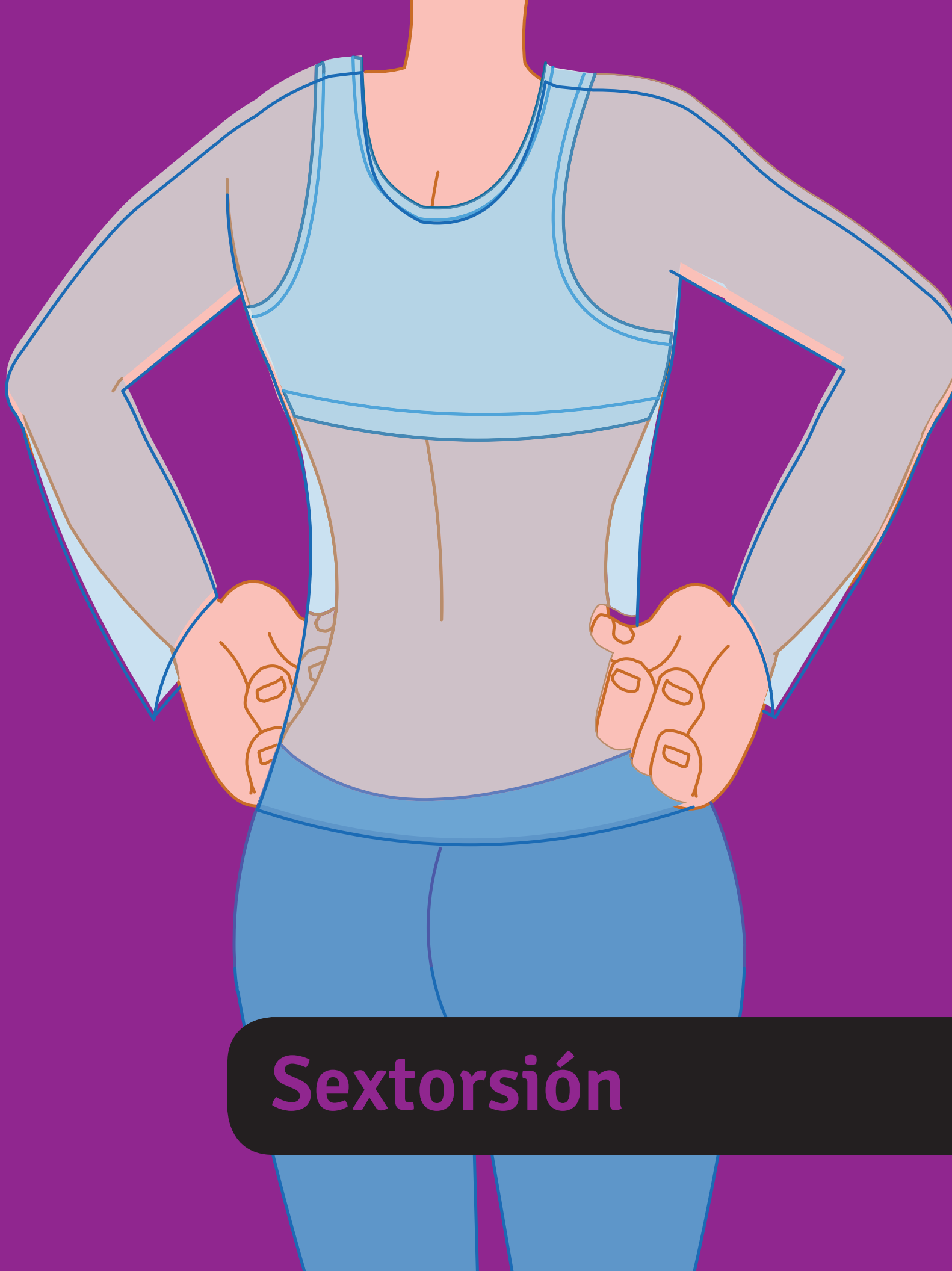
A pesar de las medidas que se puedan tomar, puede suceder lo menos deseado: que las imágenes estén al alcance de personas a las que no iban destinadas inicialmente, lo que constituiría, según el caso y la modalidad, delitos previstos en el Código Penal Uruguayo. Las formas y causas por las que esto puede llegar a



ocurrir son múltiples y diversas, pero una vez ha ocurrido, la situación viene a ser equivalente en todos los casos. Es habitual que estos sucesos se den entre el alumnado y como docentes es importante poder aportar un camino a seguir ante esta circunstancia tan complicada y asesorar al alumno o alumna y a su familia sobre cómo proceder. En estas situaciones se pueden recomendar cuatro acciones teniendo en todo caso en cuenta que se debe mantener en la medida de lo posible la discreción necesaria para la víctima:

1. Intentar conocer quién y cómo sacó esas imágenes de la esfera privada.
2. Tratar de bloquear o retirar las imágenes. Es un esfuerzo que merece la pena hacer aunque se debe tener presente que los resultados son limitados.
3. Difundir en los contextos implicados, como puede ser el centro escolar, la gravedad legal que supone poseer o distribuir mediante reenvíos esas imágenes, especialmente si son de menores de edad.
4. Reunir las pruebas y formular la correspondiente denuncia.

Recuerda que las conductas aquí referidas podrían encontrarse sancionadas en el artículo 92 y 93 de la Ley N.º 19.580 -Ley de Violencia hacia las Mujeres Basada en Género- y en los artículos 1 a 4 de la Ley N.º 17.815 -Violencia Sexual contra Niños, Adolescentes o Incapaces-.



Sextorsión

Introducción

La sextorsión es uno de los ciberdelitos en auge y esto se debe a la coincidencia de varias cuestiones. Por un lado, y por distintas razones, hay una mayor proliferación de producción de imágenes íntimas. Por otro lado, la posibilidad de obtenerlas mediante la fuerza (malware) o el engaño es creciente. Y, por último, la amenaza es tan grave, sencilla de realizar e imparable si se ejecuta, que permite a quien la utiliza, solicitar de la víctima prácticamente cualquier acción o suma de dinero.

¿Qué es la sextorsión?

La sextorsión supone el chantaje por parte de un ciberdelincuente para que la víctima realice una determinada acción o entregue una cantidad de dinero bajo la amenaza de publicar o compartir imágenes íntimas que de ella tiene. La casuística es muy variada siendo muy diversas las víctimas, las motivaciones y los daños finales que pueden llegar a provocarse.

¿Qué consecuencias puede tener?

La víctima puede sufrir varias consecuencias:

- El caso más favorable se da cuando no se acepta el chantaje y el ciberdelincuente no ejecuta su amenaza.

- El peor de los casos ocurre cuando el chantajista da cumplimiento a su amenaza. Para la víctima supone una vulneración de su intimidad; su derecho al honor y a su propia imagen. Además, se deben afrontar los efectos colaterales de que esas imágenes puedan afectar otras cuestiones personales.

Cabe mencionar que las consecuencias pueden ser amplias y variadas dependiendo de la forma, frecuencia y periodicidad en la que se realice la sextorsión. Ésta es muchas veces parte de una estrategia, cuya finalidad última es el grooming o ciberabuso sexual de personas menores de edad. También es una forma de ciberviolencia de género.

Para tener muy en cuenta

- La sextorsión es uno de los ciberdelitos más comunes y en mayor crecimiento.
- El aumento del sexting y de otras prácticas sexuales online, la normalización de la grabación de algunas actividades íntimas, las crecientes posibilidades tecnológicas para grabar y difundir imágenes, y las vulnerabilidades de ciberseguridad de los dispositivos favorecen la sextorsión.
- Las consecuencias de la sextorsión para las víctimas pueden ser muy graves en lo emocional y también pueden tener efectos económicos. Aun cuando quien extorsiona haya cesado en su chantaje, sus efectos pueden perdurar. Tampoco se podrá tener la certeza de que no lo volverá a hacer, pues nunca se le puede desarmar.
- Todos tenemos una gran oportunidad de contribuir a acabar con la distribución no consentida de imágenes íntimas y sus efectos negativos. Proteger la intimidad ajena y no mirar ni circular imágenes privadas es nuestra responsabilidad.

Prevención de la sextorsión

Para prevenir la sextorsión y sus efectos negativos se pueden considerar tres líneas de actuación a distintos niveles. La primera se focaliza en la protección de las imágenes, la segunda trata de plantear cuáles son las motivaciones finales de quien extorsiona y la tercera pone el foco en la educación y la concienciación social.

Evitar que la imagen íntima llegue a manos equivocadas

La imagen puede ser más o menos explícita o comprometedora (independientemente de si es una fotografía o un video) y su origen muy diverso:

- Entregadas de forma voluntaria por quien la protagoniza.
- Recibidas de terceras personas o encontradas de forma casual.
- Extraídas de un dispositivo perdido o que se ha llevado a reparar.
- Hackeadas o robadas por una intrusión en el sistema.
- Grabadas de forma consentida u oculta.
- Tomadas por la activación remota de la cámara web de la computadora.

En ocasiones no es una imagen real sino que se usa una falsificada, de gran credibilidad que puede ser un fotomontaje o incluso un vídeo (“deepfake”).

Aunque no son útiles para todas las tipologías descritas, las medidas de privacidad y ciberseguridad son fundamentales en este sentido.

Conocer cuáles son las motivaciones para ejercerla

Los tres fines habituales de la sextorsión son:

- La satisfacción o dominio sexual:

  - Grooming, cuando el abuso consiste en solicitar la provisión de más imágenes o un encuentro sexual.

  - Ciberviolencia sexual de género, para vulnerar la libertad sexual de su pareja o expareja.

- El lucro, si la víctima debe aportar dinero u otro tipo de bien o servicio.

- El condicionamiento de conductas, donde la exigencia es hacer o dejar de hacer algo.

Si se conoce bajo qué circunstancias y con qué objetivo las imágenes íntimas son utilizadas para la sextorsión se podrán reconocer de manera más temprana prácticas o situaciones de riesgo.

Prevención personal y social

Para reducir los riesgos de ser víctima de la sextorsión existen acciones preventivas individuales y colectivas a poner en práctica:

- Proteger, no compartir ni reproducir imágenes íntimas propias ni de otras personas.

- Promover la educación en el respeto de la intimidad ajena. Nada íntimo deja de serlo si no es mirado ni es compartido.

Se debe tomar conciencia de que una imagen no se distribuye ni se hace viral sin personas que participen de manera activa o que revictimicen a quien la protagoniza dando importancia a su existencia o realizando negativos juicios de valor.

Recuerda que estos comportamientos son sancionados por los artículos 273 BIS, 277 BIS y 277 TER lit A), del Código Penal.

Decálogo para una víctima de sextorsión

El mayor problema que surge ante la sextorsión es que la presión es enorme para la víctima puesto que, además de la persona que amenaza, existe una sensación de culpa o de vergüenza que no permite pedir ayuda. A ojos de las personas menores de edad, que el caso llegue a conocimiento de sus sus padres, madres y/o adulto responsable, es el peor de los escenarios. Por ello es especialmente importante proporcionar herramientas, pautas a las víctimas para que si deciden tratar de afrontarlo en solitario puedan, al menos, reducir el daño potencial e incluso terminar con la sextorsión. Ahí es donde el personal docente puede tratar de ayudar, como figuras de referencia, cercanas y de apoyo. A continuación, se proponen diez pasos a modo de recomendación de autoayuda para las víctimas, que puede dar al alumnado destacando que deben ser tomados en el orden planteado.

1. **Pide ayuda.**

   Solicita el apoyo de una persona adulta de confianza.

   Es importante contar con la compañía de alguien que tenga experiencia vital y que ayude a analizar con calma la situación, poniendo un punto de contraste a lo que, desde la angustia y el estrés, pueda pensarse.

2. **No cedas al chantaje.**

   No accedas a las peticiones del chantajista. Al hacerlo, solo lo estás fortaleciendo.

   El chantaje se hará más intenso y doloroso si se cede y son entregadas nuevas opciones de control. Si el chantaje se realiza porque está en posesión de una imagen delicada, entregando más, la situación empeorará.

3. **No des información adicional.**

   Cualquier dato o información puede ser usado por quien te acosa.

   Los datos que posee quien realiza la extorsión son siempre un arma potencial. Cuanto más se sepa de alguien, más vulnerable es. Se debe evitar proporcionar información adicional aunque parezcan irrelevantes.

4. **Guarda las pruebas.**

   Cuando te amenace, te muestre cosas delicadas… captura la pantalla y anota el día, la hora, y la URL.

   Tanto para revisar lo que está ocurriendo de forma más calmada como para consultarlo con otras personas es importante guardar la prueba o el rastro de las amenazas anotando día y hora en que se producen.

5. **Retira información sensible.**

   Borra o guarda en un lugar seguro informaciones o imágenes privadas y tapa la cámara de tu computadora.

   Quien chantajea pueda tratar de conseguir imágenes o datos comprometedores que le den más poder. Es importante impedirlo eliminándolos incluso del disco duro. Se debe revisar con quién se comparte vida y confidencias en redes sociales.

6. **Elimina malware**.

   Asegúrate de que no tienes software malicioso -troyanos, spyware…- en tu equipo.

   El malware es un aliado del enemigo en territorio propio y hay que evitarlo. No es fácil librarse de él y hay que mantener una postura proactiva y persistente al respecto. La seguridad del equipo garantiza la seguridad de quien lo utiliza.

7. **Cambia las claves personales.**

   Puede que esté espiando tus comunicaciones en las redes sociales.

   Después de haber comprobado la ausencia de malware es fundamental cambiar las claves de acceso a nuestros servicios de correo, redes sociales… para dificultar las posibles labores de espionaje.

8. **Comprueba, si te es posible y sin asumir riesgo alguno, si podría llevar a cabo sus amenazas.**

   Muchas amenazas son falsas, imposibles de cumplir.

   Quizás la amenaza no pueda ser llevada a cabo porque el extorsionador no dispone realmente de la imagen íntima o, en ella, no es posible identificar a su protagonista.

9. **Avisa a quien te acosa que comete un delito grave.**

   Debe saber que la Ley le puede perseguir y que tú lo sabes.

   Puede que quien chantajea no haya reflexionado sobre los delitos que está cometiendo o en los que incurriría en caso de cumplir con su amenaza. Debe conocerlos y también saber que su víctima sabe las penas a las que se enfrenta.

10. **Formula una denuncia ya que según el caso y la modalidad, esta conducta constituiría delitos previstos en el Código Penal de Uruguay.**

    La Ley persigue con dureza este tipo de delitos, sobre todo si eres menor de edad.

    Las amenazas, realizar grabaciones o publicarlas sin consentimiento, usar malware para manipular un equipo ajeno o extraer claves privadas son acciones ilegales. La denuncia debe hacerse si peligra la intimidad, el honor o la integridad física o psicológica.

Sexualidad y consumo de pornografía en Internet

Introducción

Entre los contenidos considerados nocivos para edades tempranas y, por ejemplo, prohibidos en ciertos horarios de televisión considerados de horario infantil están los de violencia extrema y los sexualmente explícitos. Esto es así porque se considera que la exposición a los mismos de personas menores resulta nociva al no reunir a tan temprana edad condiciones de desarrollo y capacidad adecuada para afrontarlos.

Sin embargo, de la limitación de contenidos en la televisión en los horarios de protección infantil se ha pasado en muy pocos años a la presencia incontrolable, muchas veces abundante, no mediada e incluso accidental de estos contenidos audiovisuales en celulares, tabletas y computadoras de niñas, niños y adolescentes.

Existe el agravante de que en la industria porno los contenidos son cada vez más abundantes, baratos y extremos. Cualquier persona conectada a Internet puede acceder ahora de forma gratuita a imágenes que hace unos pocos años se monetizaban online exigiendo un pago.

En definitiva, el porno se puede consumir ahora sin límite de edad ni cantidad, a cualquier hora, de forma gratuita, desde cualquier lugar y, lo que no es menos importante, desde el mayor de los anonimatos. La industria del porno, por su parte, hace lo posible para "colocar" su producto en el mercado aunque inicialmente no pida pago alguno, y la presión de su publicidad es importante. En definitiva, se puede decir que la cultura del porno está en el aire ("porn is in the air") y, como tal, se respira en ocasiones sin pretenderlo e incluso sin darnos cuenta… y ese aire lo respiran incluso las personas que, por edad, no son capaces de filtrar con éxito sus toxinas.

Para tener muy en cuenta

- La sociedad digital, globalizada y conectada que nos ha tocado ejerce, sin que seamos conscientes, una presión constante hacia la erotización temprana y la hipersexualización en niños, niñas y adolescentes que debe ser contrarrestada de forma permanente y activa.

- Las manifestaciones de machismo y patriarcado, que en ocasiones se pueden limitar fuera de la Red, se multiplican y circulan sin límite, fuera de todo control, en Internet. En consecuencia, hay que despertar en las personas más jóvenes una aproximación crítica a lo que, quieran o no, se van a encontrar online.

- La pornografía es accedida de forma accidental o puntual, incluso consumida regularmente, por muchos preadolescentes, provocándoles un impacto negativo psicológico y emocional, así como una visión distorsionada de la afectividad, la sexualidad y las relaciones sexuales.

- La industria pornográfica se ha convertido en la primera fuente de educación sexual para niños y adolescentes.
- La pornografía promueve y perpetúa normas de masculinidad tóxica, estereotipos racistas y violencia sexual.
- Las y los jóvenes que ven pornografía aprenden que un hombre real no respeta un NO, que la violencia es vista como fuerza y poderío masculino. Mujeres jóvenes se condicionan a pensar que la violencia sexual es lo esperado en los encuentros sexuales. La pornografía no es educación sexual.
- Algunas investigaciones demuestran que las escenas de pornografía contienen un 10% de comportamientos positivos como besos, abrazos y sonrisas y el resto de las escenas son actos agresivos.
- Los contenidos pornográficos, con independencia de su adecuación al nivel de desarrollo evolutivo de quien los consume, trasladan en la mayoría de las ocasiones valores machistas visibilizando incluso acciones contrarias a la Ley y el respeto por los derechos humanos.
- Siendo fundamental la promoción de la salud sexual y reproductiva, es preciso también poner el foco en una educación afectivo-sexual que limite la influencia de un entorno hipersexualizado y desbordado por la pornografía de amplia difusión que consumen muchos adolescentes.
- Es vital evitar que la pornografía sustituya a la educación sexual que familias y escuelas deben proporcionar a las y los menores de manera gradual y adecuada a su edad.

Para tener muy en cuenta

Para dimensionar el problema de la exposición a o del consumo de pornografía por parte de niñas, niñas y adolescentes se deben analizar las variables y los agentes intervinientes.

Fuentes, acceso y consumo de contenidos pornográficos

El origen del contenido de alta carga sexual, y más en concreto el pornográfico que llega a nuestras pantallas, puede ser muy diverso y, en consecuencia, también resulta muy complicado limitar el acceso al mismo. Las formas más comunes son, según este orden:

- Sitios web de pornografía mainstream de grandes corporaciones.
- Otras fuentes web proveedoras de pornografía, de contenido y uso menos selecto y marginal.
- Envíos privados por WhatsApp, a modo de distribución viral o en cadena.
- Producciones distribuidas en directo, bien en abierto o con público objetivo acotado.

No obstante no son las únicas fuentes de acceso al porno y hay otras que en determinadas circunstancias, falseando datos y habilitando métodos de pago, pueden llegar a ser usadas por menores de edad.

- Servicios entre particulares más o menos sofisticados donde una persona accede a las imágenes que la otra, previo cobro, le ofrece. Un ejemplo es el popular OnlyFans, que nació para evitar la censura en las habituales redes sociales y que ahora tiene esta utilidad de "porno bajo demanda" como una de las más populares.

- Videollamadas sexuales en vivo, también llamadas videollamadas porno.

La casuística no termina ahí pero sirve de ejemplo para esbozar el amplio abanico de posibilidades y, por tanto, la presencia del porno online y la dificultad de acotar su llegada y acceso a niños, niñas y adolescentes.

Por otro lado, y aunque no hay estadísticas homogéneas para un país ni entre países, se puede decir que el primer contacto con el porno, accidental o movido por la curiosidad infantil, se produce antes de los 10 años de forma general. Se puede apuntar también que a partir de los 12 años es consumido por una parte significativa de los adolescentes con cierta regularidad, y claramente más por ellos que por ellas. También cabe destacar que existe una dificultad importante en controlar el acceso a estos contenidos, con conexiones cada vez más baratas y potentes en dispositivos autónomos y portátiles, por lo que se concluye que hay que tomar medidas urgentes al respecto. Cabe decir que para acceder a pornografía gratuita basta con afirmar que se tiene la edad adecuada en el país desde el que se accede, eximiendo así de responsabilidad alguna a quien proporciona el contenido que, por otro lado, no pone mayores medidas para evitarlo.

Ficción con apariencia y efectos reales

Una de las características del porno que potencia las influencias negativas que puede tener para personas jóvenes es que es utilizado como fuente de información o inspiración debido a dos razones: la falta de implicación e influencia de otras fuentes o factores protectores (familia, escuela…) y el grado de realidad que se le atribuyen, olvidando que se trata de ficción. Esta sensación de presenciar escenas pornográficas que pudieran tomarse por reales se produce por varias razones, entre ellas:

- Existen vídeos protagonizados por actores y actrices amateurs.

- Aparecen actores y actrices profesionales simulando ser personas ajenas a la industria pornográfica, personas de a pie.

- Se ofrecen vídeos reales (robados de un dispositivos o grabados de manera furtiva al aire libre) entre las imágenes profesionales.

Así pues, si lo que se consume diluye la percepción de la diferencia entre realidad y ficción, quizás de forma intencionada por suponer un hipotético incremento de la excitación producida, se infiere que lo que allí sucede puede sucederle a cualquiera. En consecuencia, también podremos imitar los comportamientos y actitudes que forman parte de esas escenas y que nos llegan de manera casi subliminal por no ser parte nuclear de lo buscado durante el consumo.

Violencia hacia las mujeres

Muchas escenas del porno mainstream incluyen violencia física hacia las mujeres. En ocasiones forma parte, más o menos forzada, del guion. Otras veces es de lo más gratuita, como un fin en sí misma. Se usa la fuerza, en ocasiones la violencia y los golpes, para obligar a las mujeres a soportar o realizar determinados actos sexuales. Son violadas, a veces incluso por un grupo de personas. También se pueden ver imágenes de agresiones sobre mujeres que son violadas aprovechando su debilidad al encontrarse bajo los efectos de alcohol o drogas. Todo parece justificado, nada se cuestiona, el guion parece fluir y este tipo de actitudes parecen querer adquirir, a fuerza de repetición, cierto grado de normalización y legitimación.

Relaciones de dominio-sumisión y cosificación de las mujeres

Al margen de la violencia que de por sí justifica y habilita el dominio de los hombres sobre las mujeres, éstas aparecen siempre como objetos que tienen como única finalidad ser usados para satisfacer el deseo sexual masculino. Sus necesidades, impulsos, inquietudes o placeres no figuran en las escenas.

Efectos psicológicos y relacionales adversos

El consumo abundante de pornografía sin una visión crítica puede provocar efectos muy nocivos en la salud y la autoestima de las personas y sus parejas sexuales. El mundo que presentan como idílico, de cuerpos hermosos, genitales sobredimensionados y encuentros sexuales maratonianos llenos de placer se presenta como el estándar a seguir, algo a imitar. La realidad, sin embargo, es muy diferente a esa ficción. El tamaño promedio del pene real equivale a medio pene en las escenas pornográficas. La relación media dura… lo normal, y no lo que la industria porno vende rodando sus escenas durante horas e incluso días. Los integrantes de la pareja sexual no son tan atractivos y aquello que se supone que tendrían que hacer o dejarse hacer, en ocasiones, no les gusta ni siquiera les agrada. Todo esto puede suponer posteriormente, confusión, baja autoestima, frustración, complejos y relaciones disfuncionales.

Relaciones sexuales sin afectos

Cuando se utiliza la pornografía para identificar modelos a seguir en nuestro comportamiento y vida sexual se anulan de la misma todo componente afectivo. No hay diálogos, no hay generosidad, no hay cuidado de la otra persona, y sentimientos y afectos son invisibles. El encuentro sexual se reduce al componente impulsivo o pasional, egocéntrico, y se traduce, por imitación, en una coreografía gimnástica realizada por un robot. Las relaciones sexuales, que son en esencia afectivo-sexuales, se convierten en atlético-sexuales, en la más básica genitalidad.

Prácticas de riesgo

Las medias anticonceptivas y de prevención de las infecciones de transmisión sexual (ITS) no tienen cabida en las escenas pornográficas. Da igual una relación entre dos o más personas, da igual si presuntamente es esporádica o regular. El riesgo de embarazo o de infección no se consideran, se omiten, es sexo sin protección que se eleva, muchas veces a la

categoría de práctica de alto riesgo en tanto que las parejas pueden ser, en la misma escena, aleatorias, diversas y abundantes. Se normaliza así el sexo sin protección.

Consumo problemático

Como toda actividad que resulta placentera, el consumo de pornografía desata la liberación de dopamina y pone en marcha el circuito de recompensa. Aunque la adicción a la pornografía online, llamada también “ciberpornografía” para identificar su forma de consumo, no está reconocida como un trastorno adictivo científicamente, la realidad es que el abuso de la misma es un problema de difícil reversión en muchos casos. Aumento de la tolerancia, interferencias graves en las actividades cotidianas y su uso como modulador de estados de disforia lo asemejan mucho a una adicción comportamental como puedan ser las ludopatías. Así, como en el resto de trastornos adictivos no químicos, personas con problemas preexistentes pueden desarrollar esta forma de “enganche” a una fuente de satisfacción que es barata, cómoda, anónima. accesible y no tiene fin.

Estrategias frente a la pornografía

La intervención sobre este problema requiere cuatro líneas de acción:

- Sensibilización de la población.
- Educación afectivo-sexual adecuada a las nuevas realidades.
- Limitación del acceso.
- Promoción de un posicionamiento social crítico frente a la industria.

Algunas de estas intervenciones están más en el ámbito familiar y escolar y es más fácil tomar partido de manera directa pero en todas ellas la voluntad ciudadana que impulse cambios legislativos y modelos más éticos de negocio tiene un papel fundamental.

Sensibilización de la población

Por diversas cuestiones de tipo cultural o social, en algunos lugares o comunidades, abordar la cuestión del sexo es tabú o cuando menos muy incómodo. De igual manera, la existencia de pornografía al alcance de menores de edad es algo de lo que se habla poco y, cuando salta a primera plana de los medios, es común que la gente se perturbe y sorprenda a partes iguales. Sentir pudor, obviar el problema o escandalizarse por él no sirve de nada. Muchas personas adultas saben, por supuesto, que hay porno en la Red pero desconocen lo fácilmente que se accede al mismo y su naturaleza diversa y extrema. Padres y madres manifiestan que el acceso a contenidos inadecuados es una de sus

preocupaciones principales en relación al uso de Internet por parte de sus hijas e hijos. Desconocen la crudeza del porno actual y, por supuesto, todos los posibles efectos perniciosos, más allá de la explicitud sexual, que pueden derivarse de su consumo por parte de niñas, niños y adolescentes. Es necesario sensibilizar a las familias para que no menosprecien las consecuencias de la omnipresencia online de este poderoso adversario.

Educación afectivo-sexual adecuada a las nuevas realidades

La educación afectivo-sexual es el antídoto frente a las influencias de erotización temprana, hipersexualización, y machismo existentes en la sociedad y dominantes en la pornografía. Es preciso que la familia y la escuela sean los referentes al respecto de las primeras inquietudes sexuales de las y los adolescentes para que no tomen las páginas web porno como su Wikipedia sexual de consulta. Sin embargo, aunque las bases de dicha educación son las mismas, quizás el contenido o la planificación (edades, agentes, métodos…) deba evolucionar para adaptarse a una nueva realidad imperante y persistente y presentar nuevos modelos de masculinidad. El porno está ahí, nos podemos tropezar con él o consumirlo. El porno de hoy es un tipo de porno diferente al que podemos imaginarnos como disponible hace tan solo una década. Una respuesta educativa contundente y adaptada a los nuevos tiempos se hace imprescindible. La familia juega un papel fundamental como referente básico en cualquier aspecto de la educación de niños y niñas. Es preciso que no delegue esta responsabilidad en la escuela y adopte un papel activo y protagonista, que genere normalidad y confianza en torno al tema, de forma que sirva así de guía, de recurso, también en este aspecto muchas veces delicado por lo personal e íntimo.

Limitación del acceso

Se ha mencionado anteriormente que la forma en la que el porno puede llegar a las pantallas digitales es variada, pero la más común, cómoda y accesible es por acceso a páginas web pornográficas. Existen muchas soluciones de control parental que ayudan en la labor de evitar, limitar, controlar o supervisar el acceso a contenidos no deseados. Se trata de un tipo de herramienta que se debe evaluar, adecuar y configurar para cada situación (plataforma, dispositivo, autonomía de uso…) y edad pero que en ningún caso debe considerarse definitiva. Pueden ser una gran ayuda, sin duda, especialmente en las edades más tempranas en las que, por otro lado, habría que comenzar por plantearse si se debe tener un dispositivo digital autónomo conectado a Internet. Otra estrategia para limitar el acceso a contenidos potencialmente nocivos como es determinado tipo de pornografía podría llegar a ser también la visibilización de alternativas específicas que puedan sustituir los consumos más tóxicos. Así, en los últimos años han surgido muchas propuestas de pornografía bajo las etiquetas de ético, feminista o educativo que proponen un modelo de industria diferente. Si la eliminación falla, la reducción o sustitución puede ser un mal menor.

Promoción de un posicionamiento social crítico

El acceso libre a contenido pornográfico por parte de niños, niñas y adolescentes está teniendo importantes consecuencias que exigen una compleja respuesta. Como a toda

industria, y esta es en muchas ocasiones muy lucrativa, se le debe exigir más allá que el cumplimiento de la Ley. Se le debe pedir que implemente medidas que limiten sus efectos nocivos allá donde se produzcan aplicando criterios éticos que mejoren sus estándares de responsabilidad social. Crear una conciencia colectiva que cuestione y visibilice prácticas irresponsables es preciso para ejercer la presión necesaria capaz de incomodar a las empresas de esta industria. Esta conciencia también servirá para pedir ajustes legislativos más estrictos y, en consecuencia, mayores restricciones en el difícil entorno global que es Internet en el que no hay que renunciar a exigir la atención del principio del interés superior del niño o niña.

Diez pautas para mitigar influencias nocivas del consumo de pornografía

Dado que el acceso a la pornografía, accidental o voluntario, no puede controlarse, es preciso formular recomendaciones para limitar los efectos nocivos en quienes tengan contacto con ella. A continuación se proporcionan diez pautas de forma sintética:

- Ten presente que el porno es ficción. Escenas y protagonistas tienen mucho truco/trampa.
- Considera el porno como una fantasía. Puede estimular la imaginación pero no ser tomado como fuente primaria de información.
- Descubre ritmos, emociones, necesidades y preferencias propias y de tu pareja. Evita imitar un guión y presta atención a los afectos.
- Recuerda que el consentimiento es necesario siempre, antes y durante. Debe ser claro y puede ser revocado.
- En el sexo comparte, escucha, habla, cuida con empatía, de igual a igual. La otra persona no es algo para ser usado por ti.
- Evita toda forma de violencia porque nunca es una opción. El respeto es obligado y una parte fundamental.
- Analiza qué tipo de escenas tienes delante porque al verlas estás dando tu respaldo. Si consumes porno, hazlo de forma crítica y responsable.
- Utiliza protección en las relaciones. Aunque en pantalla no se aprecie o no lo hagan, siempre es necesario.
- Desarrolla tu vida sexual sin presiones. El sexo no es una competencia y pertenece a la esfera privada de cada cual.
- Toma conciencia de tus pautas de consumo. Si el porno condiciona aspectos importantes de tu vida o te causa problemas, pide ayuda.

Desinformación y malinformación en Internet

Introducción

La Declaración Universal de los Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas, enuncia en su artículo 19: “Todo individuo tiene derecho a la libertad de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”. Esto implica que todas las personas deben ser educadas de manera que desarrollen de forma suficiente la capacidad de acceder, analizar y evaluar la información (imágenes, mensajes…) que aparecen en los medios de comunicación tradicionales (prensa, televisión, radio…) y en los nuevos medios y dispositivos digitales conectados, así como de producirlas.

En este contexto toma un papel central la Alfabetización Mediática e Informacional (AMI) que se puede definir como un proceso de formación de conocimientos y competencias (habilidades y actitudes) que faculta a las personas para comprender las funciones de los medios de comunicación y otros proveedores de información, para evaluar críticamente los contenidos de los medios y para tomar decisiones informadas como usuarias y productoras de información y conocimiento. En la sociedad actual donde Internet ocupa un papel central cabe incluir la alfabetización digital en la AMI.

El empoderamiento de las personas a través de la AMI es uno de los requisitos más importantes para fomentar el acceso equitativo a la información y al conocimiento y para promover medios de comunicación y sistemas de información libres, independientes y plurales.

La facilidad con la que se producen contenidos y la velocidad a la que se replican y viralizan en una sociedad digital, global, frenética e interconectada han hecho que los llamados trastornos de información (desinformación y malinformación) sean objeto de preocupación por las graves consecuencias que pueden desencadenar.

En definitiva, se puede decir que identificar, desenmascarar y, en general, combatir los contenidos e información erróneas, producidas intencionadamente o no, se convierte en un reto personal y en una necesidad colectiva.

En una sociedad donde el acceso, la creación o compartir información y desinformación es tan cómodo y fácil como apresurado y eficiente, es necesario, desde el punto de vista educativo, recordar las palabras de Noam Chomsky: “El aprendizaje verdadero tiene que ver con descubrir la verdad y no con la imposición de la verdad oficial, pues esta última opción no conduce al desarrollo de un pensamiento crítico e independiente”.

Claves para tener muy en cuenta

Vivimos en una época de sobreinformación creciente, desordenada y llena de intereses que desconocemos. La creación de desinformación incluso se ha democratizado y automatizado, como muestra la existencia de sitios web cuyo servicio, gratuito incluso, consiste en la posibilidad de crear una pieza ficticia de contenido con apariencia de

realidad. En este contexto, la ciberciudadanía responsable se debe ejercer desde una participación impulsada y basada en información veraz y exige una postura combativa contra la difusión de la desinformación.

Desde el punto de vista de la ética ciudadana es importante tomar en cuenta los siguientes efectos que puede tener la desinformación:

- Creación de desconcierto y confusión, dificultando el discernimiento y el posicionamiento.
- Manipulación de decisiones personales, de forma directa o indirecta.
- Reputación o desprestigio de personas, entidades o instituciones por medio de la manipulación de la percepción y la opinión sobre las mismas.
- Generación de beneficios económicos.
- Condicionamiento de la opinión pública para crear un estado de opinión que puede beneficiar a una determinada ideología o grupo de interés.

Desde el punto de vista personal, quien está al alcance de la desinformación:

- Pierde su tiempo y distrae su atención sin ningún beneficio.
- Puede sufrir manipulación y en consecuencia no obrar u opinar libremente o hacerlo de forma equivocada.
- Puede convertirse sin saberlo en parte de la cadena de difusión.
- Puede padecer consecuencias, incluso de tipo legal, derivadas de haber participado en la difusión de desinformación que ha afectado negativamente a terceras partes.

La lucha contra la desinformación tiene mucho de capacidad, pero sobre todo es una cuestión de actitud. Se trata de saber, pero sobre todo de dudar. Es más una labor de observar y escuchar, que de ver y oír.

Definición, conceptos y características

Desinformación y malinformación

El informe del Consejo de Europa “Information Disorder: Toward an Interdisciplinary framework for research and policymaking” (2017) establece estas definiciones, asumidas por el Programa de Naciones Unidas para el Desarrollo (UNDP) en su nota informativa de mayo de 2020 con motivo del COVID-19:

- Desinformación (dis-information en inglés). Información que es falsa y que ha sido creada deliberadamente para dañar a una persona, un grupo social, una organización o un país.
- Malinformación (mis-information en inglés). Información que es falsa, pero que no ha sido creada con la intención de causar daño.
- Adicionalmente, se puede hablar de la utilización malintencionada de la información al referirse a aquella información que tiene cierta base en la

realidad, pero que es utilizada para causar daño a una persona, una organización o un grupo.

Realizamos aquí, no obstante, algunas puntualizaciones que ayudan a completar y comprender el alcance y significado de las definiciones anteriores:

- La desinformación muchas veces es planificada, orquestada y dotada de medios para conseguir su propósito dañino.
- En el caso de la malinformación, además de no tener intencionalidad dañina, quienes la difunden no saben, por lo general, que se trata de información errónea.
- La utilización de la información de forma maliciosa se caracteriza por su utilización poco ética.

Por último, mencionar que el uso del término noticias falsas o fake news para referirse a informaciones falsas queda totalmente desaconsejado porque atribuye la categoría de notica a algo que no lo es.

Según la UNESCO, el concepto de desinformación se utiliza para referirse a intentos deliberados, con frecuencia planificados y coordinados, de confundir o manipular a las personas haciéndoles llegar información deshonesta. Se considera especialmente peligrosa porque con frecuencia está organizada, se provee con los recursos necesarios y aplica técnicas y tecnologías avanzadas que aumentan su efectividad y alcance. Existen muchos recursos y estrategias que pueden provocar una determinada forma de desinformación:

- La sátira y la parodia.
- Los titulares diseñados como cebos para ganar clics (clickbait headlines, en inglés).
- El uso engañoso de subtítulos, recursos visuales o estadísticas.
- El contenido genuino que se comparte fuera de contexto.
- El contenido de autoría impostada (cuando se usa un nombre de periodistas o el logo de medios cuando no hay relación con ellos).
- El contenido manipulado y fabricado.

Alfabetización mediática e informacional

Instituciones internacionales relacionadas con la educación como la UNESCO y la OCDE han estado durante años llamando la atención sobre la necesidad de educar desde edades tempranas para una interacción crítica e inteligente con los medios (alfabetización mediática).

Por su lado, la UNESCO establece como requisito para una educación inclusiva y basada en el conocimiento el desarrollo entre la ciudadanía, desde las edades más tempranas, de las competencias y capacidades que configuran la Alfabetización Mediática e Informacional (incluyendo la Digital, específica para los medios digitales).

Esta alfabetización proporciona autonomía y capacidad a las personas para desenvolverse de manera eficaz en los entornos tecnológicos, digitales y de comunicación y, en consecuencia, los habilita para el ejercicio libre y pleno de la ciudadanía.

La Alfabetización Mediática e Informacional

se centran en cinco posibles competencias básicas que son referidas como las «5Ces: comprensión, pensamiento crítico, creatividad, consciencia intercultural y ciudadanía». Así, asumiendo el criterio de la UNESCO, la competencia de pensar críticamente para recibir y elaborar productos mediáticos se incluye dentro de la AMI y, en consecuencia, impulsa la capacidad de combatir el consumo, la creación y la distribución de contenidos no veraces o manipulados que puedan generan confusión, desinformación e incluso daño.

El pensamiento crítico, aptitud y actitud

El pensamiento crítico es una de las Habilidades para la Vida definidas por la OMS en 1993 como "aquellas aptitudes necesarias para tener un comportamiento adecuado y positivo que nos permita enfrentar eficazente las exigencias y retos para la vida diaria".

La palabra "crítica" viene del griego y su significado es similar a separar, distinguir, enjuiciar. El pensamiento crítico ayuda a distinguir lo bueno de lo malo, lo justo de lo injusto, lo cierto de lo falso. El pensamiento crítico se desarrolla ejerciéndolo en primer lugar con uno mismo. Es fundamental desmontar, mediante la argumentación lógica y la interrogación, prejuicios, ideas preconcebidas y sesgos cognitivos.

Atendiendo al trabajo de investigación de Peter A. Facione "Critical Thinking: What It Is and Why It Counts" (Pensamiento Crítico: Qué es y Por Qué Cuenta") el pensamiento crítico incluye:

- Curiosidad sobre una amplia gama de temas.
- Preocupación por convertirse en y mantenerse como una persona bien informada.
- Estado de alerta sobre las oportunidades para usar el pensamiento crítico.
- Confianza en los procesos de cuestionamiento razonado.
- Autoconfianza en la propia capacidad para razonar.
- Mente abierta con respecto a visiones mundiales divergentes.
- Flexibilidad al considerar alternativas y opiniones.
- Comprensión de las opiniones de otras personas.
- Imparcialidad al evaluar.
- Reconocimiento y afrontamiento honesto de la propia parcialidad, prejuicio, estereotipo o tendencia egocéntrica.
- Prudencia al suspender, hacer o alterar juicios.
- Disposición a reconsiderar y revisar puntos de vista cuando la eflexión honesta sugiere que el cambio está justificado.

Planteado desde el punto de vista de los procesos, el pensamiento crítico implica al menos cinco acciones clave:

- Interpretación de la información para clarificar su significado.

- Validación de la credibilidad de la información en función de su origen, coherencia e intencionalidad o efectos posibles así como de los propios conocimientos previos.
- Cuestionamiento de los datos y la información tanto explícitas como implícitas y contraste mediante la definición de alternativas.
- Profundización mediante la obtención de más datos pero también identificando incógnitas.
- Autoevaluación por medio de una revisión del propio proceso mental seguido con la información para cuestionar, confirmar o revisar el razonamiento y los resultados finales obtenidos.

Cabe preguntarse ahora hasta qué punto el resultado del desempeño de esas acciones tiene que ver con la capacidad intelectual. Se puede decir que existe una correlación lógica entre inteligencia (en términos de la que es susceptible de ser medida mediante tests del tipo que miden el cociente o coeficiente Intelectual, CI) y pensamiento crítico. Parece obvia la relación porque valorar correctamente una información requiere captarla, tratarla y comprenderla y porque las personas con mayor CI resisten mejor la influencia de los sesgos cognitivos. Sin embargo, el pensamiento crítico depende además de otras capacidades cognitivas no medidas por los tests de inteligencia y de determinados rasgos de la personalidad.

Por otro lado, hay investigaciones que han identificado tres características de las personas que promueven el pensamiento crítico:

- La curiosidad o apertura, que invita a explorar de forma abierta.
- El deseo de encontrar la verdad, que actúa como motivación para implicarse en el esfuerzo.
- La humildad intelectual, que es vital ya que pensar de forma crítica implica dudar de las demás personas pero sobre todo de uno mismo. El pensamiento crítico es una actitud que comienza presumiendo la falta de conocimiento.

Por último, merece la pena mencionar que desarrollar el pensamiento crítico supone estimular capacidades de razonamiento de alto nivel que, según estudios e investigaciones, proporcionan ventajas en otras facetas de la vida:

- Favorece decisiones más acertadas.
- Reduce la frecuencia de acontecimientos negativos.
- Mejora el rendimiento académico.
- Aumenta la eficiencia en ocupaciones que requieren habilidades analíticas.

En conclusión, desarrollar y activar el pensamiento crítico no es solo una necesidad impuesta por la desinformación y la malinformación sino que se convierte así en una oportunidad para mejorar la vida personal y profesional, lo cual explica su inclusión en la lista de Habilidades para la Vida de la OMS.

Vida digital adolescente y pensamiento crítico

El pensamiento crítico en la adolescencia es fundamental, especialmente en la parte digital de su vida. Internet es un entorno con unas características que lo hacen adecuado para el engaño dado que, además de ser muy permeable a las falsedades, se trata de un lugar donde muchas veces prima la cantidad y la velocidad frente a la calidad o la precisión.

Usar el pensamiento crítico en las edades tempranas, más allá de una cuestión de responsabilidad ciudadana, es una herramienta para la seguridad y el bienestar. Niños, niñas y adolescentes afrontan riesgos, por ejemplo, cuando se consume desinformación o malinformación relacionada con la salud (trastornos alimentarios, dietas milagro…). Corren también peligro cuando a una persona recientemente conocida que inspira confianza le otorgan trato o privilegios que se deben reservar a las personas realmente cercanas. Pueden estar ante un problema cuando acceden o consumen nuevos servicios online que no han sido validados o contrastados. Por otro lado, gestionarán mejor sus consumos digitales, sin caer en el uso abusivo, cuando se cuestionen qué hacen, por qué lo hacen y quién sale ganando más realmente con ello.

Es preciso generar en las personas menores de edad una actitud crítica frente al mundo digital cuestionando informaciones, personas y servicios pero también el propio ecosistema y sus agentes, comenzando por la autoevaluación de su conducta personal, muchas veces cargada de uso abusivo y compulsivo. Además de con esa motivación para activar el pensamiento crítico será necesario capacitarles para ello con conocimientos, procedimientos e incluso herramientas.

Sesgos, emociones y su importancia en la desinformación

La desinformación puede adquirir muchas formas y, aunque no todas ellas tengan el mismo objetivo, sí pueden compartir estrategias para ganar efectividad. A este lado de la pantalla estamos las personas y el que la desinformación tenga más o menos éxito depende de cómo sea nuestra reacción frente a ella.

La reacción frente a algo pasa por nuestro cerebro y por nuestro corazón, se tamiza por el raciocinio y las emociones. Este raciocinio, esa interpretación razonada de la información en ocasiones se produce de manera inconsciente y afectada por los sesgos cognitivos.

Un sesgo cognitivo es una interpretación errónea sistemática de la información disponible que ejerce una influencia en la manera de procesar los pensamientos, emitir juicios y tomar decisiones. Los sesgos cognitivos tienen un origen muy variado: cuestiones culturales, influencias sociales, motivaciones emocionales o éticas, simplificación del procesamiento de la información, distorsiones al recuperar recuerdos o memoria, etc.

Los sesgos vienen a suponer atajos que nuestro cerebro ha desarrollado para simplificar los problemas y facilitar las decisiones y son resultado de la necesidad evolutiva de realizar un filtrado selectivo de los estímulos, aliviando al cerebro de parte de las tareas de análisis de la información. Sin embargo, habitualmente son un obstáculo para identificar la desinformación.

Veamos algunos de los sesgos más comunes:

- El mayor sesgo es el llamado del punto ciego que precisamente hace que, a pesar de que conozcamos los sesgos, nos sea complicado identificar los propios sesgos aunque sí los veamos en las demás personas.

- El sesgo de confirmación es el que nos induce a valorar en exceso la información que encaja con nuestras propias creencias (valores, ideologías, prejuicios) o, en su defecto, las creencias predominantes y, sin embargo, obviar inconscientemente la que no coincide con nuestras opiniones.

- El sesgo o efecto contraproducente de familiaridad implica que cuanto mayor sea la frecuencia con la que estamos expuestos a una determinada información, con independencia de su veracidad, mayor probabilidad hay de que la consideremos cierta.

- El sesgo de validación de interacción social nos conduce a hacer lo que otras personas hacen, reforzando así algo tan primario como el sentimiento de pertenencia al grupo.

- El efecto de superioridad visual viene dado porque nuestro cerebro procesa una imagen hasta 60,000 veces más rápido que un texto. Por otro lado, recordamos el 80% de lo que vemos, el 20% de lo que leemos y el 10% de lo que oímos.

- Los contenidos que son acompañados por imágenes reciben un 84% más de visitas y son compartidos 40 veces más que los que no las tienen.

- El razonamiento motivado es un sesgo de tipo emocional y se refiere a la tendencia inconsciente a condicionar el procesamiento de información a conclusiones que se ajustan a algún fin u objetivo.

- El sesgo de disponibilidad supone una heurística cognitiva mediante la cual se juzga la probabilidad de un evento según sea la facilidad con la que nos vienen a la mente instancias del mismo. Esto puede llegar a hacer que las personas vean una afirmación incorrecta como verdadera simplemente porque pueden recordarla fácilmente.

Por su parte, las emociones tampoco ayudan a combatir la desinformación porque nuestro pensamiento es racional pero también emocional. Cuando una información nos provoca una emoción determinada es posible que esta condicione el análisis de aquella y luego se produzca una justificación racional.

Hay emociones que son especialmente difíciles de gestionar y nos producen descontrol como, por ejemplo, el enfado, la compasión, el morbo, la curiosidad, el miedo y la urgencia. La desinformación apela a ellas porque el componente emocional de nuestro pensamiento nos incitará a compartirla.

Filtro burbuja y cámaras de eco

El concepto de filtro burbuja, también conocido como la burbuja de filtros, hace referencia al hecho de que la información que los diferentes servicios que usamos en Internet (buscadores, redes sociales, proveedores de entretenimiento, tiendas online…) nos ofrecen, está limitada por nuestras propias características. La tecnología hace posible la personalización de la información de forma que nos las presenta en función de la relevancia o importancia que presuntamente tendría para cada uno de nosotros . Eli Pariser en su libro "El filtro burbuja, cómo la Red decide cómo pensamos y lo que leemos" vuelve en 2017 a profundizar sobre esta cuestión que ya evidenció en una obra anterior 6 años antes.

Para combatir la desinformación debemos ser conscientes de esto porque el pensamiento crítico debe llegar no solo a lo evidente y alcanzable sino a lo que puede no aparecer ante nosotros. Este tipo de filtros burbuja, entre otras cosas, limitan nuestra capacidad de descubrir y el resultado de nuestra curiosidad, así como la oportunidad de cuestionar o profundizar. Son un obstáculo para el pensamiento crítico y, en consecuencia, aliados de la desinformación.

Respecto al consumo de medios, existe la teoría de las cámaras de eco según la cual si las personas tienen una preferencia por las personas e informaciones afines, se formarán cámaras de eco, esto es, espacios vacíos donde rebotan nuestras propias ideas. Esta teoría supondría que las tecnologías digitales no aportan una ampliación de nuestras opciones sino una limitación de nuestras posibilidades. Quizás esto pueda ser así cuando no tenemos consciencia de ello y no activamos mecanismos para enriquecer nuestras fuentes incluso con influencias e ideas que, a priori, son contrarias.

En definitiva, creemos estar bien y es más fácil así, más cómodo, más rápido, pero dejamos de participar en la construcción colectiva desde el pensamiento crítico y la aportación individual. Reflexionemos si somos tan libres como creemos en el mundo físico como digital.

Definición, conceptos y características

Para educar una generación responsable, crítica y activa frente a la desinformación, hay varias líneas de intervención que se concretan a continuación.

Pausar y considerar la opción de no compartir

Compartir información parece la actitud por defecto, lo que hay que hacer salvo expresa indicación o motivación en sentido contrario. Es necesario reflexionar sobre ello y tomar conciencia de que compartir sin verificar no es un gesto de generosidad, sino algo insolidario en realidad. Nada habría de compartirse sin haber dedicado el tiempo necesario para su validación. Si no se dispone de ese tiempo, o de ganas de o capacidad de afrontar un contraste suficiente de la información, la única alternativa responsable es, simplemente, no compartir.

A continuación se plantean de forma sintética cinco razones para no compartir sin verificar.

- Si compartes información de manera

compulsiva o urgente hay más probabilidades de que no sea cierta. Si crees que es muy importante difundirla, también lo será el que te tomes el tiempo necesario para comprobarla.

- La desinformación suele provocar daños a otras personas o intereses. Si participas divulgándola eres también responsable de sus efectos.

- Participar, opinar, defender ideas, tratar de ayudar a otras personas… son derechos y obligaciones ciudadanas. Sin embargo, divulgar información no verificada es una imprudencia y una falta de ética.

- Cuando compartes sin saberlo una información falsa eres víctima, pero también cómplice involuntario de quien la creó. Además, con tu participación implicas y perjudicas a otras personas.

- La libertad de expresión o hacerse eco de lo que otras personas divulgan no te exime de la responsabilidad legal que puede derivarse, en ocasiones, de la difusión de informaciones erróneas.

Por último, conviene recordar que si se ha divulgado una información y se tiene luego constancia de su falsedad, existen acciones necesarias que deben emprenderse para desmentirla, dedicando tiempo a tratar de compensar la acción errónea.

Tomar conciencia de los efectos y la responsabilidad propia

La desinformación, y en ocasiones la malinformación, generan consecuencias negativas a terceras partes. Sepamos o no de qué tipo, cómo o a quién, se produce un daño. También, como se ha dicho, nos convertimos en víctimas más o menos leves de los efectos de estos trastornos de información. Sería útil para frenar la desinformación, por lo tanto, pensar en lo abstracto y lejano pero también en lo concreto y cercano. Visualizar, descubrir las consecuencias negativas y nuestra responsabilidad en ellas debe servir para frenar nuestra participación, consciente o no, en las cadenas de desinformación.

Con demasiada frecuencia se pone el foco en identificar y combatir las mentiras y la desinformación habilitando en las edades tempranas las capacidades para ello. Sin embargo, es más importante quizás poner énfasis en motivar, sensibilizar, dar razones para que pongan en marcha esa actitud crítica y responsable. No basta saber hacer, hay que querer hacer, tener motivación suficiente.

Estimular el pensamiento crítico en un sentido amplio

Además de desarrollar las capacidades para el análisis y evaluación de la información, la deducción y la conclusión, es importante proponer actividades que les ayuden a dudar de sí mismos, de sus propios planteamientos, de manera que aprendan a limitar la emisión precipitada y vehemente de sus opiniones o juicios de valor.

Suele ser útil para ello plantear una actividad de forma que se les solicite que defiendan, de forma racional, la postura contraria a la que tienen sobre una cuestión determinada. Esto les obligará a cuestionar sus propias impresiones, sin el componente de reto o confrontación personal, y profundizar en el conocimiento de la información a evaluar.

Conocer, para evitar, los efectos de sesgos y emociones

Combatir la desinformación supone una lucha consciente y constante frente a las limitaciones que sesgos y emociones nos imponen de forma inconsciente. Por lo tanto, la lucha contra la desinformación comienza por conocernos mejor, conocer qué sesgos tenemos y pueden entrar en juego a la hora de evaluarla y qué emociones sentimos frente a ella. Si tomamos conciencia de lo involuntario e inconsciente podremos dar pasos para limitar su influencia en el afrontamiento de una sociedad inundada de desinformación cada vez más camuflada y elaborada. Se pueden dar para ello los siguientes consejos:

1. Combatir nuestro propio sesgo.
2. Evitar considerar cierta información porque se repita muchas veces.
3. Cuestionar la información aunque provenga del entorno más cercano como familia o amistades.
4. Mantente alerta si hay imágenes porque atrapan nuestra atención y pueden estar truqueadas.
5. Contenerse, poner en cuarentena aquello que nos provoca emociones, especialmente si se trata de enfado, miedo, curiosidad, compasión, morbo o urgencia.

El sesgo de confirmación se combate cuestionando más aquella información que más coincide con lo que pensamos porque a pesar de estar dotados de inteligencia, estamos prediseñados para no cambiar de idea. Por esta razón tenemos que dudar especialmente de aquello que siendo poco creíble además coincida con lo que pensamos.

Conocer sus estrategias: para qué y cómo se desinforma

Conocer al adversario es siempre una ventaja para el combate. Por ejemplo, la desinformación vence la resistencia racional de las personas conociendo y activando estrategias para aprovechar las limitaciones referidas a sesgos y emociones. Saber esto es ya algo positivo y se podría avanzar más tratando de identificar cómo lo hace.

Por otro lado, es útil saber las motivaciones que pueden llevar a que se cree desinformación. En ocasiones es pura diversión, creada como un reto o para generar un cierto caos por simple entretenimiento. En otras, las más, se trata de objetivos económicos o finalidad ideológica. Es necesario tener la capacidad de analizar lo aparente desde la visión de una posible amenaza organizada. Si se sabe qué se pretende generalmente con la desinformación, analizando motivaciones y efectos finales, y qué estrategias se suelen utilizar, será más probable desenmascararla y más difícil que quien la produce logre su objetivo.

Conocer y usar herramientas para contrastar informaciones

Al final del proceso de validación de una determinada información siempre existen

datos concretos (incluyendo metadatos, informaciones textuales, en formato imagen, audio o vídeo) que deben ser contrastados. Esta tarea debe ser apoyada por una o varias de estas capacidades:

- Utilización de la búsqueda eficiente de información en las diferentes plataformas web o redes sociales.
- Acceso a fuentes de información confiables y pertinentes.
- Conocimiento y manejo de aplicaciones y servicios para la verificación rápida de imágenes y vídeos.
- Observación meticulosa de la información, sin obviar el uso de la lógica y la deducción.

Dependiendo de cada caso, se pueden activar procedimientos complementarios o alternativos. Por ejemplo, existen entidades como Maldita.es que se dedican a identificar desinformaciones de manera que es posible acceder a sus sistemas de información (bases de datos o páginas web) para comprobar si algo ya ha sido identificado como una mentira.

Decálogo para luchar contra la desinformación

La máxima principal es que si no se tiene la seguridad de que algo es cierto no se debe compartir. Por eso, antes de compartir una información es preciso tratar de realizar una validación para lo cual se presenta el siguiente decálogo de pasos a seguir:

Procedencia

1. Verifica la fuente de la información. Si no la conoces o no se identifica, ponte alerta y contrasta con fuentes de tu confianza.
2. Examina la apariencia: url truqueada, ortografía, calidad, diseños extraños o muy llamativos, fechas, etc. Cuidado también con las suplantaciones.
3. Sé prudente también cuando la información provenga de alguien de tu confianza, familia o amistades. Eso no es síntoma de calidad puesto que no asegura que haya sido verificada.

Contenido

4. Analiza toda la información, no solamente el titular. Cuidado con las citas o imágenes sacadas de contexto.
5. Presta atención a las imágenes o vídeos. Pueden falsearse con cierta facilidad o, simplemente, no corresponder al hecho o momento al que simulan asociarse.
6. Compara la información con otros medios o fuentes de confianza. Sospecha si no la encuentras. Si se trata de cuestiones relacionadas con la salud, alertas o emergencias recurre únicamente a fuentes oficiales.
7. Ten cuidado con las informaciones que mezclan datos falsos con otros verificados o verificables para camuflarse como plenamente ciertas.

Intencionalidad

8. Ponte alerta si la información te genera un sentimiento de enfado, preocupación o urgencia. Con frecuencia es una estrategia buscada por quienes crean desinformación.
9. Las noticias o informaciones excesivamente buenas o demasiado sorprendentes también suelen ser una forma de ocultar la desinformación. Mantén la objetividad en el análisis.
10. Identifica el humor y la sátira. Hay páginas web que se especializan en este tipo de noticias a modo de bromas y lo hacen de manera profesional, pero no siempre de forma desinteresada.

Ciberviolencias hacia las mujeres y niñas

Introducción

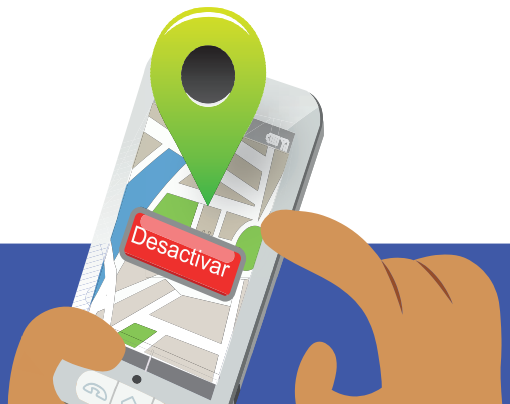
Las diversas formas de violencia hacia las mujeres son un problema estructural y global de primer nivel en todo el mundo. Las diversas manifestaciones de violencia machista y de violencia de género han encontrado en Internet un entorno propicio para difundirse debido a las singularidades del espacio digital. La victimización a niñas, adolescentes y mujeres adquiere múltiples formas, muchas de ellas derivadas de la falta de educación libre de prejuicios y estereotipos de género, que promueva la igualdad entre todas las personas.

La naturalización de la violencia machista hace que pase desapercibida, arropada y camuflada en una sociedad patriarcal. Desnaturalizar violencias y micro-violencias en la sociedad es necesario para lograr visibilizar y combatir la violencia en el espacio físico y digital. Es importante resaltar que la violencia que puede realizarse online puede darse de una manera inmediata, sencilla y sutil, al tiempo que grave.

Los mecanismos de prevención van de la mano de una sociedad más justa e igualitaria en la que la ciudadanía en general, especialmente los hombres, tome conciencia y parte de su responsabilidad en el combate contra estas formas de ciberviolencia. Se requiere también una legislación adecuada que brinde la colaboración necesaria de grandes plataformas y servicios de Internet donde estas violencias se manifiestan.

Claves para tener muy en cuenta

- La violencia digital hacia las mujeres es un reflejo de la sociedad que se ve incentivada por las características de Internet, aprovechadas para todo tipo de ciberdelitos.
- La ciberviolencia de género es violencia y, como tal, produce daño en la víctima.
- La normalización de ciertas conductas en una sociedad todavía machista, lo discreto de algunas formas de victimización y la aparente inocuidad de otras, son obstáculos a combatir para lograr una vida digital libre de violencia para niñas, adolescentes y mujeres.
- Junto con la educación para la igualdad y una legislación adecuada, es necesario el compromiso colectivo, especialmente por parte de los hombres para frenar la violencia digital machista.
- Es necesario aprovechar el potencial de la propia Red para la sensibilización, la denuncia, el empoderamiento de las mujeres y el activismo feminista frente a esta amenaza.
- El entorno vital digital en el que crecen niñas y adolescentes, donde se manifiestan y visibilizan diversos tipos de ciberviolencias que parecen quedar impunes, puede tener un efecto catalizador de este problema.



Definición y características

A continuación se presentan algunas manifestaciones de la ciberviolencia hacia las niñas, adolescentes y mujeres.

Grooming

Aunque no es una cuestión que afecte de manera exclusiva a niñas sí hay una mayor prevalencia y una casuística más abundante hacia ellas. Niñas y adolescentes son afectadas por agresores sexuales para perpetrar diversas formas de abuso y explotación sexual infantil. En cierta medida, la prevalencia y legitimación de las diversas formas de violencia hacia las mujeres está también en el origen de esta forma de abuso. Para profundizar sobre el grooming nos remitimos al capítulo completo disponible en esta misma guía.

Ciberacoso contra activistas feministas

El acoso en sus diversas formas (mensajes ofensivos, divulgación de mentiras, amenazas, suplantación de identidad…) se intensifica con frecuencia con mujeres que ejercen el ciberactivismo feminista utilizando el contexto online para exponer sus ideas, denunciar injusticias y luchar contra las desigualdades. Estas mujeres, por sus ideas y visibilidad, sufren todo tipo de acoso online que en ocasiones adopta la forma de linchamiento digital. Relacionado con este tipo de violencia, al menos en su origen, puede hablarse también del discurso de odio misógino, con una amplia presencia en las redes sociales.

Ciberacoso sexista o por razón de género

El ciberacoso supone la victimización (exclusión, amenazas, insultos, ridiculización, ofensas…) deliberada y reiterada de una persona. En ocasiones quien victimiza es una única persona y otras veces son varias, incluso una multitud, quienes con una simple acción (usando las opciones de “me gusta” o “compartir”, por ejemplo) reiteran la victimización y, por tanto, la convierten en acoso. La ciberviolencia hacia las mujeres adquiere la forma de ciberacoso sexista o por razón de género cuando el contenido del acoso tiene que ver con la presunta adecuación o no de la víctima a cánones estereotipados de conducta, estatus o apariencia asignados a las mujeres en una sociedad machista y patriarcal. Podemos encontrar ejemplos de esto en muchas facetas de la vida cotidiana online donde la mera presencia de las mujeres, por minoritaria o novedosa, se convierte en excusa para su acoso. Además, este tipo de violencia suele tener una connotación sexual o se relaciona con el ejercicio de la actividad sexual. Los estereotipos nocivos de masculinidad y feminidad se ven reforzados en numerosas aplicaciones y redes sociales donde ellas aparecen hipersexualizadas al tiempo que se censura el ejercicio de su propia sexualidad.

Ciberacoso sexual

Internet, las redes sociales y los diversos servicios y aplicaciones que permiten la comunicación entre las personas han facilitado el contacto entre ellas, incluso el no deseado por una de las partes. En este sentido, el ciberacoso sexual es toda conducta no deseada por quien la recibe de naturaleza o connotación sexual realizada por medio de Internet. Algunas de sus manifestaciones más comunes de acoso sexual online hacia las mujeres son comentarios subidos de tono, solicitud reiterada de atención o contacto personal con connotaciones sexuales, envío de imágenes o mensajes sexuales, solicitud de imágenes íntimas.

Ciberviolencia de control

Es posiblemente la forma de violencia más extendida y la que más se da en parejas adolescentes. Supone la utilización de las herramientas y el contexto digital para vigilar, condicionar y limitar la libertad de la pareja. Es algo que se ha hecho posible desde que las nuevas formas de relación se han volcado en los teléfonos celulares, las redes sociales y las aplicaciones de mensajería instantánea tipo WhatsApp. Exigir a la pareja la clave de la red social, que envíe su geolocalización o que retire de su perfil fotos donde parezca mostrarse atractiva o sugerente son algunas de las manifestaciones de este tipo de control.

Este tipo de violencia puede quedar invisibilizada por darse en el seno de una pareja y no ser fácilmente perceptible desde fuera de la misma. Sin embargo, es una de las formas más comunes de violencia que pudiera parecer de baja intensidad pero que igualmente limita la libertad, el desarrollo pleno y el bienestar de las mujeres que la sufren. Dado que este control se sustenta en el concepto de "posesión de la pareja" destilada del mito del amor romántico supone que no sean pocas las ocasiones en las que las mujeres la realizan sobre sus parejas masculinas. Esto dificulta la prevención de este tipo de victimización como violencia de género. Sin embargo, hay que entender que la violencia de género donde la mujer es victimizada es estructural y debe ser combatida de manera expresa. Nuestra sociedad mide de manera diferente las mismas conductas en función de si son realizadas por hombres o mujeres, y es por eso que esta ciberviolencia de control tiene una mayor capacidad de sometimiento sobre ellas que sobre ellos, bien porque ellas creen que deben actuar acorde a ese ideario socialmente establecido, cediendo ante la demanda de control de la pareja, o bien porque la consecuencia de no ceder ante dicha demanda puede tener efectos más perniciosos.

Ciberviolencia sexual

Esta categoría podría incluir el ciberacoso como forma de violencia pero se ha querido diferenciar aquí tanto por la intensidad como por la intencionalidad del daño. En ambos casos el agresor utiliza imágenes íntimas de la mujer (afectando por lo tanto a su derecho al honor, la intimidad personal y la propia imagen) para violentarla, ya sea mediante la divulgación no consentida de las mismas o mediante la amenaza de hacerlo.

La sextorsión supone la solicitud de una determinada acción a la víctima bajo la amenaza, caso de no atender la exigencia, de divulgar imágenes íntimas que de ella se dispone. Sobre este particular existe un capítulo específico.

La divulgación no consentida de imágenes íntimas es una forma de victimización en la que puede participar gran parte de la población. Visionar o compartir las imágenes de una actriz desnuda robadas en la intimidad de su hogar o dar a conocer el lugar donde poder verlas es algo que muchas personas han hecho. Subir imágenes íntimas de una pareja o expareja a una página web o compartirlas con otras personas es también algo demasiado común. Cuando la finalidad de esta acción es causar daño a la víctima suele recibir el nombre de "revenge-porn", pornovenganza o porno vengativo. Esta denominación, sin embargo, es muy inadecuada porque no fueron imágenes grabadas para ser consumidas por otras personas, como es el caso de la pornografía, ni se conoce afrenta previa que explique una supuesta venganza.

Es necesario considerar que ambas formas de violencia tienen especiales consecuencias para sus víctimas debido a la percepción machista de la sexualidad de las mujeres que critica el libre ejercicio de la misma, a diferencia de lo que ocurre en el caso de la actividad sexual de los hombres.

Qué hacer para prevenir y actuar

Educación en igualdad

En la raíz de toda actitud machista está una deficiente educación en igualdad que se manifiesta a diversos niveles: relacional, económico, simbólico, social… La violencia machista es una de las manifestaciones más graves de una sociedad no igualitaria por lo que toda forma de ciberviolencia digital se debe combatir, principalmente, mediante una educación desde, por y para la igualdad real y efectiva, entre mujeres y hombres.

Fomento de la empatía y visibilización de la violencia

En ocasiones, la dificultad de percibir el sufrimiento ajeno está en el origen de algunas formas de violencia. Esto es más común cuando no hay contacto directo ni sincrónico entre agresor y víctima o cuando se produce en un contexto tolerante con las prácticas violentas o abundante en las mismas. Estos dos factores pueden concurrir en el contexto digital y tiene como consecuencia que agresores inicien o se sumen al ejercicio de la violencia porque no son capaces, al menos en su medida real, de identificar el sufrimiento de quien la padece.

Otras veces la violencia no es perceptible por otras personas, sean las agresoras o no. Que se ejerza en el entorno digital y que adquiera tantas y tan variadas formas no ayuda. Por eso es importante la visibilización de la ciberviolencia hacia las mujeres, porque ayuda a identificarla, a reconocerla, a prevenirla y a combatirla.

Divulgación de las consecuencias legales

Aunque no es de tipo educativo, divulgar la Ley aplicable al efecto sí es una medida que puede evitar algunas acciones violentas. En muchos países, existe el agravante de violencia de género que supone, en la práctica, un aumento significativo del castigo legal asociado a un determinado delito. Que un potencial agresor conozca las consecuencias legales que puede llegar a afrontar puede hacer que desista de su intención. Por su parte, que una víctima sea consciente de que está siendo objeto de un delito puede ayudar a que tome medidas que reduzcan o frenen el daño o bien que ayuden a su persecución.

Promoción de la ciberseguridad y la privacidad

Ciberseguridad y privacidad son conceptos relacionados entre sí que se gestionan de forma individual pero también colectivamente. El foco siempre debe estar en que el violento no ejerza la violencia y no en limitar las libertades de las potenciales víctimas, pero no por ello debemos renunciar a un nivel de autoprotección razonable. Por otro lado, cada cual puede comprometer, incluso sin darse cuenta, a otras personas con las que se relaciona cuando, por ejemplo, sufre una suplantación de identidad o le roban información confidencial o íntima que no le pertenece. En resumen, es preciso cuidar la privacidad y la ciberseguridad no solamente por el propio interés sino por responsabilidad y respeto hacia aquellas personas con las que nos relacionamos, especialmente si son mujeres, por la especial cibervictimización que sufren.

Implicación colectiva

La violencia hacia las mujeres es un reto colectivo y es preciso que cada cual, especialmente los hombres, se implique en su erradicación. En muchas ocasiones somos testigos de actitudes violentas hacia mujeres en redes sociales, en nuestros grupos de mensajería instantánea, en foros o páginas web… Otras veces somos incluso cómplices cuando, por ejemplo, vemos o distribuimos un vídeo íntimo robado que alguien nos hizo llegar. Es necesario tomar conciencia de que nuestro papel debe ser más consciente, estando alerta, rechazando y ofreciendo resistencia frente a esas formas de cibervictimización machista.

Ciberactivismo

Más allá de la reacción ante la ciberviolencia machista está la participación proactiva para su eliminación. Así como la Red trajo nuevas formas de victimización, también ha traído nuevas opciones de lucha y participación, dando voz a quienes no suelen tener las mismas posibilidades de proyectarla. El ciberactivismo feminista, con el movimiento #MeToo de referencia, está obteniendo muchos logros y la participación o apoyo al mismo es, cómo no, una forma de frenar esta lacra fuera y dentro de la Red, de aprender y de enseñar sobre derechos de las mujeres e igualdad entre géneros.

Qué hacer para prevenir y actuar

La violencia de control ejercida hacia las mujeres tiene sus mayores aliados en el teléfono celular, los programas de mensajería instantánea y las redes sociales. Por ser una forma de violencia común y, hasta cierto punto, normalizada y confundida con una manifestación de complicidad, cuidado e incluso amor, se hace útil identificarla en acciones concretas de manera que sea más fácilmente reconocida. Es necesario identificarlo primero para evitarlo después porque no se puede prevenir ni combatir aquello que no se percibe como amenaza.

Diez manifestaciones de la ciberviolencia de control:

1. Acosar o controlar a tu pareja usando el celular o cualquier otro dispositivo.
2. Interferir en relaciones de tu pareja en internet con otras personas.
3. Espiar el celular o cualquier otro dispositivo de tu pareja.
4. Censurar fotos que tu pareja publica y comparte en redes sociales.
5. Controlar lo que hace tu pareja en las redes sociales.
6. Exigir a tu pareja que demuestre dónde está con su geolocalización.
7. Obligar a tu pareja a que te envíe imágenes íntimas.
8. Comprometer a tu pareja para que te facilite sus claves personales.
9. Obligar a tu pareja a que te muestre un chat con otra persona.
10. Mostrar enfado por no tener siempre una respuesta inmediata online.

Huella, reputación e identidad digital

Introducción

Tenemos una vida que se desarrolla, también, y cada vez con más presencia, en el entorno digital. En ocasiones es continuidad y reflejo, algo inseparable, de nuestra vida fuera de la Red. Sin embargo, en otros casos, ambas facetas de nuestra vida no parecen tener mucho que ver bien porque el propio medio no permite esa continuidad o bien porque Internet, con sus posibilidades, sus reglas y las personas que la habitamos, hace que nuestro comportamiento, nuestra vida, sea o parezca diferente a ambos lados de la pantalla. En todo caso, es nuestra vida, una única, que discurre por ambos escenarios. Por ello, y a pesar de su aparente independencia, lo que se hace en uno de ellos habitualmente tiene repercusión, reflejo, en el otro, aunque se rijan por parámetros bien distintos.

Es preciso tener muy en cuenta que Internet tiene unas características que, aunque obviamos en demasiadas ocasiones, afectan a lo que se sabe de cada cual y a cómo las otras personas nos perciben y se relacionan con nosotros. En Internet dejamos un rastro digital de lo que hacemos, podemos mostrar diferentes facetas de nuestra vida según sea el entorno o grupo de socialización concreto y las demás personas se hacen una imagen de nosotros incluso sin que ni ellas ni nosotros seamos conscientes.

Se trata de algo muy importante que puede marcar el futuro de una persona porque la información digital perdura en el tiempo, tiene un alcance ilimitado y viaja con la mayor celeridad. Sin embargo, muchas personas, especialmente las más jóvenes, no dan importancia al reflejo de su vida que dejan en la Red y esto puede ocasionarles inconvenientes más o menos graves en el corto, medio y largo plazo.

Claves para tener muy en cuenta

- Las personas muy jóvenes carecen de experiencia vital que les permita pensar en las consecuencias a mediano y largo plazo de sus acciones. Sienten, viven y comparten su vida online para una audiencia potencial concreta, conocida o indeterminada, en y para un momento puntual.
- Niñas, niños y adolescentes no tienen la capacidad de visualizar las consecuencias del rastro que dejan, o de la imagen que proyectan, en una realidad o sobre personas que no han tenido ocasión de conocer ni de imaginar. Es necesario ayudarles en esa tarea.

- Es preciso educar para un consumo saludable de la tecnología que permita desarrollar actitudes críticas frente a las presiones sociales (modas y costumbres) e intereses comerciales que incitan a compartir online nuestra vida de forma constante, exagerada e incluso compulsiva.

- La privacidad y la ciberseguridad son factores fundamentales también para determinar qué datos pasan a formar parte o no, voluntaria o involuntariamente, de la huella, la reputación y la identidad digital de cada cual.

- Huella, reputación e identidad digital se componen de muchos elementos que van más allá de lo que la propia persona publica. Dónde lo hace, con quién interactúa, qué comenta o incluso las cosas que no hace pueden ser datos relevantes.

Definición y características

Huella digital

Visitar páginas web, usar un servicio como Google, instalar una determinada app en el celular, subir una fotografía, consultar nuestra ubicación, realizar una videollamada, dar un “me gusta” o consultar una publicación en un blog es posible gracias a servicios, programas y plataformas digitales que interactúan con Internet y todo ello deja un rastro. Ese rastro, esa huella, puede quedar almacenada de forma duradera a pesar de que la acción o proceso que la genera pueda ocurrir en tan solo un instante y una única vez. Dejamos infinidad de huellas cada día que nos conectamos incluso por el mero hecho de hacerlo. Estas huellas son almacenadas de forma diferente por agentes diversos y pueden ser de acceso público o privado. No obstante, cada “pisada” puede ser combinada con otras, del mismo tipo a lo largo del tiempo o de diferente tipo en ese instante, de manera que aporte información mucho más significativa y relevante. Así, un conjunto de huellas describen un camino e incluso la forma de recorrerlo, del mismo modo que varios caminos pueden revelar nuestras preferencias de ruta. Combinar datos referidos a diferentes realidades, e incluso provenientes de diversas fuentes pero asignables a una misma persona, pueden generar información adicional de alto valor añadido.

En definitiva, nuestro paso por Internet deja una marca que las diferentes entidades y empresas implicadas pueden registrar de manera anonimizada o de forma nominativa, en cuyo caso se requiere un consentimiento expreso que, en ocasiones, es aceptado de manera casi inconsciente. Este rastro es guardado con diferentes propósitos entre los que se destacan tres: obtención de beneficios económicos, prestación condicionada del uso de Internet y mejora en la calidad y eficiencia del servicio o experiencia. Por esta razón, la huella digital puede condicionar, para bien o para mal, nuestro presente y nuestro futuro afectando a las oportunidades que se pueden encontrar en Internet pero también fuera de la Red.

Identidad digital

La identidad digital de una persona es, simplificando al límite, lo que Internet nos dice que esa persona es. Es decir, el conjunto de datos y características que pueden atribuírsele cuando se accede o se busca a esa persona en la Red. Esta identidad puede ser más o menos profunda o detallada, al igual que se puede conocer más o menos bien a una persona, dependiendo del tiempo que dediquemos a conocerla y de las informaciones que de ella podamos conocer. En ocasiones, también el conocimiento de una persona puede ser profundo pero parcial en tanto que tenemos acceso solamente a una parte sesgada o a una faceta concreta de su vida.

Los dos lugares de la Red donde se encuentra información de una persona de forma más frecuente son:

- Los buscadores, como Google, que realmente no contienen la información en sí misma pero que ayudan a encontrarla. Con ese objetivo hacen pequeñas copias temporales de parte de la misma para optimizar el proceso. Los buscadores catalogan, indexan, aquella información disponible en páginas web y en otros servicios y plataformas que así se lo permiten.

- Redes y plataformas sociales, que no son sino enormes bases de datos donde, por lo general, la información se asocia a un perfil concreto y es común referenciar a las personas mediante etiquetas o usando su nickname, apodo o nombre de usuario.

Así pues, la aproximación más sencilla a la identidad digital de una persona es el conjunto de información que nos devuelve los buscadores o las plataformas sociales. La identidad digital puede condicionar las relaciones con las demás personas y, en consecuencia, aspectos relevantes de nuestra vida, por lo que es importante cultivarla y cuidarla.

Elementos que componen la identidad digital

Es importante tomar en cuenta que la identidad digital va más allá de los datos (información de tipo texto, fotografías o vídeos principalmente) publicados sobre una persona identificable por ella misma o por otras. Eso conformaría la identidad digital más evidente o reconocible. La identidad digital más completa vendría dada también por otros elementos como por ejemplo:

- El nombre de usuario, la imagen del perfil y el texto breve con el que se define, presenta o anuncia su estado.

- Las personas con las que se relaciona.

- Los lugares o plataformas donde una persona dispone de perfil o participa, pero también en los que, siendo comunes, evita o no utiliza.

- Los comentarios y las interacciones (me gusta, reenviar…) que se puedan tener en plataformas cerradas o en plataformas abiertas en las que es identificable.

- Toda huella digital que sea accesible de forma abierta.

Identidad digital

Es importante conocer, además de la naturaleza de los elementos que la conforman, cuáles son sus características de forma que seamos conscientes de cómo se comporta y cómo influir sobre ella:

- **Con diferentes versiones.**

La identidad digital puede ser, como se ha dicho, más o menos detallada o profunda, en función de la cantidad, tipo y calidad de los datos analizados. También puede ser más completa o simplemente parcial, dependiendo de si atiende o no a fuentes limitadas y concretas de información.

- **Dinámica.**

La identidad digital es dinámica, se modifica con el tiempo. Es posible cambiarla interviniendo sobre los componentes que la conforman siendo, por lo general, más sencillo sumarle atributos o información que eliminarlas. También muta cuando se ve afectada por cambios ajenos a las personas que habitamos la Red, como puede ser modificaciones en las condiciones técnicas, de uso o indexación de las propias plataformas que afecten la forma de acceso a la información que la componen. Un ejemplo concreto de esto puede ser que una red social concreta decida en un momento determinado permitir o impedir indexar sus contenidos y bases de datos.

- **De complejidad creciente.**

La generalización del uso de las redes sociales que se produjo en torno al año 2010 provocó que la identidad digital de una persona se volviera más compleja, esto es, compuesta por más elementos, ya que las personas publican e interactúan en relación a otras de manera mucho más precisa, sencilla y constante.

- **Inferida, de gestión poco controlable.**

Las interacciones posibilitadas por las redes sociales provocaron también que la identidad digital fuera menos controlable por su titular, por la persona interesada, resultando más dependiente de lo que otras personas hicieran con respecto a ella, Dado que todas las interacciones en estas plataformas sociales están asociadas a perfiles específicos, son concretas e identificables. Como ejemplo de ello se puede decir que siempre que alguien etiqueta a otra persona en una red social está contribuyendo a su identidad digital de alguna manera, de forma positiva o no, al margen de que pueda estar afectando también a su privacidad.

Reputación digital

El concepto de reputación digital tiene que ver con la manera en que una persona es percibida por las demás en función de su trayectoria vital digital. Tiene que ver con la

identidad digital, en tanto que incluye lo que de una persona es perceptible online, pero va más allá porque incorpora una dimensión temporal más amplia y una valoración más o menos subjetiva. La reputación implica una valoración de los datos a lo largo del tiempo, no la mera localización o percepción de los mismos en un momento determinado.

La importancia de la reputación digital es que puede pesar más que la identidad digital en relación a nuestras relaciones y oportunidades, tanto fuera como dentro de Internet. Dicho de otra forma, puede tener más importancia cómo "dice" Internet que ha sido una persona que cómo refleja Internet que es en la actualidad y en un contexto determinado. Esto puede ser también así en la vida fuera de la Red pero la cuestión es que Internet tiene una capacidad inigualable para registrar, almacenar y, lo que es más importante, poner en primera plana de nuevo datos o acontecimientos puntuales de un pasado más o menos remoto de una persona, sin tener en cuenta para ello la necesidad u oportunidad de hacerlo.

Tomar conciencia desde edades tempranas de que nuestro paso por Internet va dejando un poso casi indeleble y que puede afectar a nuestra vida en un futuro es muy necesario en un mundo donde la celeridad y la inmediatez inhiben la reflexión y la proyección de las consecuencias sobre el mediano y largo plazo.

Qué hacer para prevenir y actuar

Tomando conciencia de los elementos intervinientes y sus relaciones

Muchas personas, más aún si son niñas, niños o adolescentes manifiestan que actúan, de buena fe y que, por esa razón, no tienen nada que esconder. En consecuencia dicen no tener que preocuparse por su huella, reputación o identidad digital.

Hay que recordar en este punto tres aspectos de contexto:

- La privacidad es un factor de protección. Cuanto más se sepa de una persona, más vulnerable es.
- La ciberseguridad es necesaria para garantizar la privacidad y en ocasiones la privacidad es una garantía de ciberseguridad.
- La privacidad y la ciberseguridad son cuestiones colectivas, de grupo. Lo que hagan las demás personas al respecto nos puede afectar y viceversa.

Se puede concluir también que la huella, la identidad y la reputación digital de cada persona están conformadas por la información y acciones que dejen algún tipo de rastro sobre ella en Internet y que, a su vez, dependen tanto de la propia persona, como de otras con las que se relaciona así como por las plataformas o servicios de Internet que utilice.

¿Cuáles pueden ser los problemas asociados a la huella digital?

La huella digital de una persona puede ser utilizada por quien posea una parte de ella para perfilar qué tipo de servicios o informaciones le son ofrecidos, de qué manera y en qué condiciones.

Esto puede ser una ventaja o, muy al contrario, un serio inconveniente. Tomando

en cuenta que, como se suele decir, la información es poder, que una empresa o persona con malas intenciones, por ejemplo, cuente con parte de nuestra información dejada en forma de huella digital puede proporcionarle un gran poder, una ventaja sobre la persona afectada (cliente o usuaria de la empresa) o posible víctima de algún ciberdelito. Si además pensamos que muchas veces no somos conscientes de la huella que dejamos, ni la recordamos, ni tenemos capacidad de conocerla, cambiarla o borrarla, nos damos cuenta de que se convierte en una hipoteca importantísima o una posible vulnerabilidad.

¿Cómo reducir la huella digital?

No es fácil identificar la huella que dejamos y mucho menos ser capaces de conseguir que nos pueda resultar favorable. Por eso, la única opción para evitar que nos pueda afectar negativamente es reducirla y para ello hay tres opciones:

- Disminuir las ocasiones en las que dejamos rastro, lo que se traduce en reducir el uso de dispositivos y servicios digitales conectados a Internet. Esto no siempre es posible pero sí hay oportunidades claras de hacerlo como, por ejemplo, prescindir de usar servicios digitales inteligentes y automatizados que no aportan excesivo valor añadido, como podría ser un altavoz inteligente o una determinada app.

- Restringir la captura de datos configurando los servicios, los dispositivos y las aplicaciones de la forma más restrictiva al respecto. Esto no es sencillo ni cómodo en muchas ocasiones. Inhabilitar la geolocalización podría ser una forma, por ejemplo.

- Dificultar la suma de datos a una determinada huella o impedir que los datos de la misma puedan combinarse generando información adicional de mayor valor. Esto se conseguiría, por ejemplo, usando diferentes cuentas de correo en diferentes ocasiones, para diferentes propósitos o en distintos dispositivos de referencia. El propósito es hacer más complicado que nos sigan la pista, es decir, que encuentren huellas identificables con el mismo zapato. Si se utiliza siempre el mismo dispositivo, con la misma cuenta de correo o perfil, por ejemplo el de Facebook, para autentificarse en los servicios o webs que se usan y que lo exigen, estaríamos facilitando una huella profunda y clara.

¿Cuáles pueden ser los problemas asociados a una reputación e identidad digital negativa?

Los retos que se abordan en el caso de la identidad y de la reputación digital tienen que ver con que una persona sea identificable de manera correcta y positiva allí donde resulte necesario y que la percepción de las demás personas con respecto a ella, su reputación, sea favorable. De no ser así, las oportunidades de una persona se ven reducidas porque o bien no es correctamente identificada en el lugar y momento adecuado o bien resulte descartada por su reputación.

¿Cómo fomentar una identidad y una reputación digital adecuadas?

Tener una identidad digital y mantener una reputación positiva no es una tarea sencilla porque supone un esfuerzo constante, a veces contracorriente, y depende de varios factores y otras personas. No obstante, es posible identificar catorce pautas que ayudan

a ello y que se presentan a continuación en tres categorías y en formato de recomendación directa:

En lo fundamental:

1. Ten un cuidado especial con la forma en que te presentas online. La foto de perfil, el nickname y la frase de presentación o estado deben siempre ser respetuosos y positivos.
2. Presta atención a las condiciones de privacidad y ciberseguridad de tus dispositivos, aplicaciones y redes sociales. A mayor restricción, mayor control.
3. Piensa dos veces antes de publicar algo, especialmente cuando estás inmerso en emociones como el enfado o la euforia excesiva.
4. Reflexiona, proyecta, imagina antes de publicar algo qué efecto tendría si pudiera ser visto públicamente o en cualquier momento futuro.
5. Participa de manera activa, ejerciendo la ciudadanía digital, de forma correcta, contextualizada e informada ya que quedará rastro de ello.
6. Recuerda que no es sencillo borrar un rastro digital porque puede ser capturado y reproducido por terceros o, simplemente, no estar a tu alcance.

En relación a las demás personas:

1. Sé insistente con el respeto de tu privacidad por parte de las demás personas. Es la mejor garantía para poder gestionar mínimamente tu reputación e identidad digital.
2. Evita sentir presión, inercia o necesidad por publicar lo que haces. Gestiona de forma inteligente qué compartes online de tu vida, cuándo, cómo y con quién.
3. Recuerda que la forma en que gestionen su privacidad y su ciberseguridad las personas y las plataformas con las que te relaciones también te afecta.
4. Sé especialmente cuidadoso con lo que publicas cuando afecta a otras personas, especialmente si aparecen identificadas.

En positivo, de manera proactiva:

1. Cultiva una reputación y una identidad digital positivas dejando rastro visible de aquellas cosas de las que, con seguridad presumirías, en un futuro.
2. Practica el egosurfing. Búscate en Internet (buscadores, redes sociales y plataformas diversas…) de forma periódica y variada para comprobar qué es lo que aparece sobre ti.
3. Crea un perfil en plataformas en las que participa gente como tú porque puede ser positivo para proteger tu identidad y dificultar que sufras una suplantación en las mismas.
4. Gestiona perfiles o identidades distintas para cosas específicas o temporales porque puede ser positivo ofrecer diferentes impresiones en lugares o momentos diferenciados.

Diez recomendaciones para una identidad y la reputación digital positivas

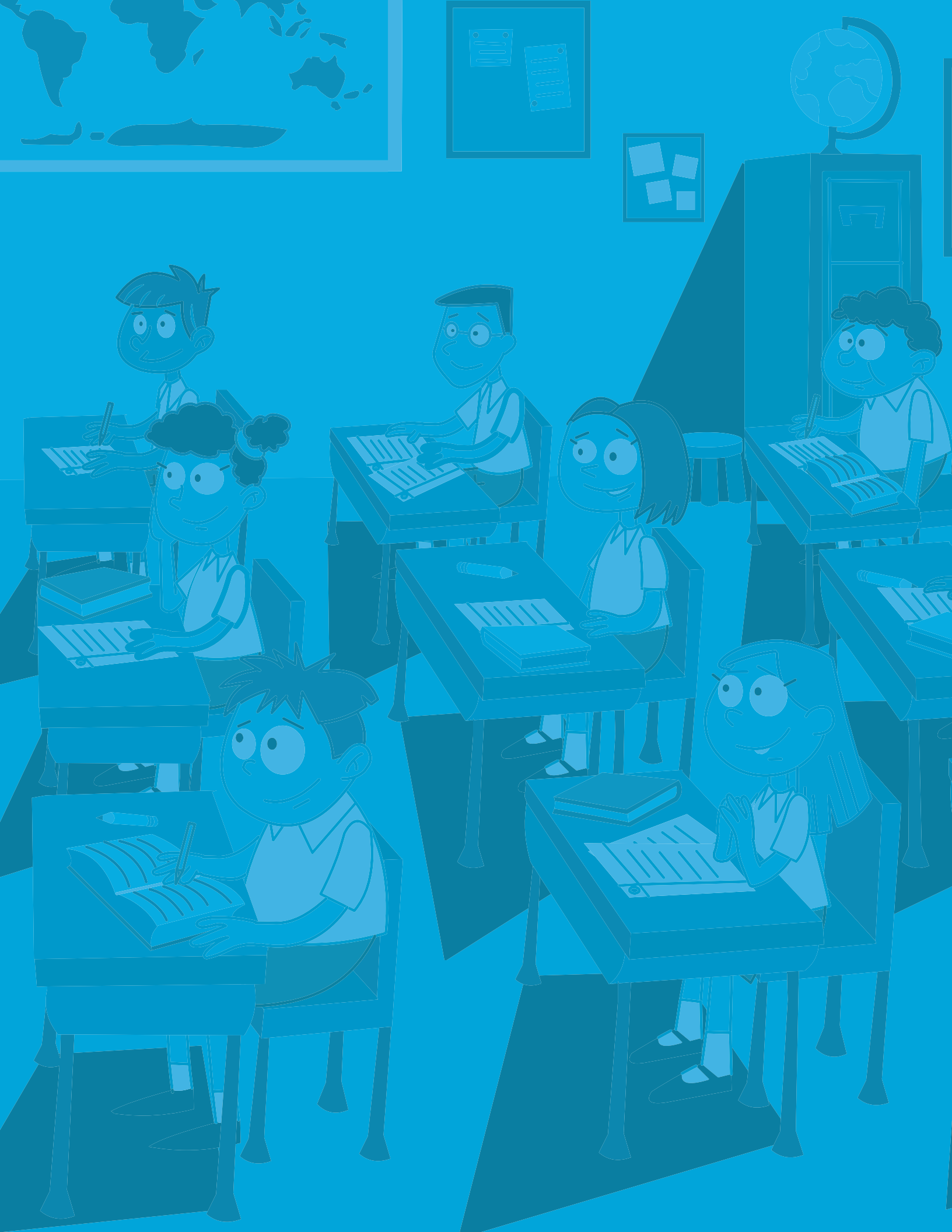
Cultivar de forma permanente la reputación y la identidad digital cuando su valor y relevancia no se perciben fácilmente en el momento en el que son generadas puede resultar difícil. Por esa razón es importante tener unas pautas claras, sencillas, para poder aplicar siempre que sea posible:

1. Selecciona y reduce lo que publicas.
2. Restringe el alcance de tus publicaciones a las personas necesarias eligiendo para ello las configuraciones y canales adecuados.
3. Piensa en una audiencia imaginaria global (cualquiera) y atemporal (siempre) antes de publicar nada.
4. Infórmate de cómo manejan tus datos las apps antes de descargarlas.
5. Presta atención y cuida la privacidad y la ciberseguridad propia y de las personas con las que te relacionas.
6. Mantén una actitud y un tono positivo. Es más saludable y te hace más aceptable.
7. Evita publicar cosas cuando estás inmerso en emociones o sentimientos intensos o negativos.
8. Huye de conflictos innecesarios porque no hay nada más fiel que un enemigo.
9. Genera diferentes perfiles para diferentes entornos y propósitos.
10. Búscate en plataformas sociales de vez en cuando para ver cómo te pueden ver.

Tu huella digital:

date una pausa y conéctate con responsabilidad

Proyecto educativo para la ciudadanía digital y la prevención del ciberdelito



Tu huella digital:

date una pausa y conéctate con responsabilidad

La presente guía es un recurso didáctico, interactivo y pedagógico destinado a docentes y familia y cualquier persona interesada en realizar acciones preventivas para abordar el fenómeno del ciberdelito y las amenazas en el ciberespacio entre niños, niñas y adolescentes para contribuir con la construcción de la ciudadanía digital entre las nuevas generaciones.

Presidencia Uruguay | agesic
ANEP Administración Nacional de Educación Pública
Centro de Estudios Judiciales del Uruguay
inau Instituto del Niño y Adolescente del Uruguay
Fiscalía General de la Nación
Presidencia Uruguay | Junta Nacional de Drogas
Ministerio del Interior
PantallasAmigas
Global Programme on Cybercrime
Naciones Unidas Oficina contra la Droga y el Delito