Dirección de Cooperación y Gestión
Programa de Acceso Comunitario a la Justicia

Módulo: Riesgos en la Red

Programa de Acceso Comunitario a la Justicia

CONTENIDO

INTRODUCCIÓN 2
NORMATIVA 3
QUE ES LA HUELLA DIGITAL? 4
Datos personales y privacidad 4
Qué es la viralización 4
CIBERDELITOS 5
CIBERBULLYING ¿Qué es? 5
Consecuencias del ciberbullying: 5
GROOMING ¿Qué es? 6
Componentes y fases del Grooming 6
Qué hacer en casos de Grooming 7
Lo Sabías? 7
El Grooming puede derivar en otros graves delitos 7
SEXTING ¿Qué es? 8
Consecuencias del sexting 8
PHISHING ¿Qué es? 9
¿Cómo prevenirlo?: 9
¿Dónde denunciar un delito informático? 10

INTRODUCCIÓN

Las TIC (Tecnologías de la Información y la Comunicación) inspiran a explorar, a ser creativos, a comunicarse y a aprender, pero es importante que se cuente también con información y estrategias de protección ante los posibles riesgos que pueden surgir en los espacios digitales.

Estas tecnologías son el lugar donde mayor información personal se genera y se comparte, fuente de recursos para identificar a una persona. Los datos que residen en la web y se asocian a la identidad de una persona constituyen la manera que otros usuarios tienen de conocerla.

NORMATIVA

LEGISLACIÓN NACIONAL

• **Ley n° 25.326** (2000) **"Protección de datos personales"**: tiene por objeto proteger la información personal de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables, y explicita la confidencialidad del responsable del tratamiento de los mismos (incluyendo la protección de la privacidad e intimidad en internet).

- Código Penal:

  - Art 128 consiste en la producción, distribución, facilitación, comercialización, divulgación y/o tenencia de material de explotación sexual infantil.
  - Art. 131 "*Grooming*" o ciberacoso sexual infantil.
  - Art. 153 bis Acceso sin autorización a un sistema o dato informático de acceso restringido.
  - Art. 183: Daño Informático. Se produce cuando se altera, destruye o inutiliza datos, documentos, programas, o sistemas informáticos.
  - Art. 184, inc. 5º y 6º: Daño Informático agravado. Cuando el daño es producido a datos, documentos, programas, o sistemas informáticos públicos o bien, cuando se ejecutara en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, medios de transporte, etc.

LEGISLACIÓN DE LA CIUDAD DE BUENOS AIRES

- **Ley 863 de Protección de Menores en establecimientos comerciales que brindan acceso a Internet** (2002).

• **Código Contravencional**

- Art. 64: Suministro de material pornográfico a menores de edad a través de medios informáticos.
- Art. 71 bis : Difusión no autorizada de imágenes o grabaciones íntimas. La víctima pudo haber consentido la obtención de dichas imágenes en un espacio privado, pero NO su distribución masiva.
- Art. 71 quinquiés: Suplantación digital de identidad. Son los casos en los que el ciberagresor crea un perfil digital falso haciéndose pasar por la víctima y, a través de aquel, comete otros delitos en nombre ajeno.

QUE ES LA HUELLA DIGITAL?

La huella digital incluye las publicaciones que un usuario realiza, aquellas en las que sea etiquetado o mencionado, las fotos o videos personales o subidos por otros, las páginas web donde se cite su nombre, las cuentas de usuario en redes sociales que estén asociadas a su nombre real, las noticias referidas a su persona, y la participación como usuario en foros, salas de juegos, de chat u otros.

Como se construye la huella digital: Puede ser de tres maneras:

→ ACCIÓN PROPIA: Publicaciones que hace un usuario en redes sociales, blogs, sitios web como diarios o foros, dando su identidad.

→ OMISIÓN: No tener cuentas en redes sociales o participación web es de por sí un dato que se incluye en nuestra identidad digital cuando alguien busca información sobre nosotros.

→ ACCIONES DE OTROS: Publicaciones en donde el usuario es citado o nombrado por otro.

Datos personales y privacidad

Los datos personales son información de cualquier tipo que puede ser usada para identificar, contactar o localizar a una persona. Entre ellos se encuentran número de documento, nacionalidad, sexo, estado civil, número de teléfono y/o celular, huellas digitales, dirección de correo electrónico, actividades, etcétera.

Qué es la viralización

La dinámica de internet y las redes sociales permite que algunos contenidos comiencen a ser compartidos rápidamente por distintos usuarios. A este proceso se lo llama viralización.

Un contenido puede popularizarse por ser gracioso, polémico, atractivo, de denuncia o por otras razones. En la mayoría de los casos es difícil prever su viralización y alcance, pudiendo llegar a cientos, miles o hasta millones de personas.

LO SABÍAS?

EN INTERNET NO HAY DERECHO AL OLVIDO

Cuando subimos algún dato o imagen a la web, es difícil de borrar. Aunque se borre una publicación, no se elimina la totalidad de esa referencia.

CIBERDELITOS

Son conductas ilegales realizadas por ciberdelincuentes que actúan en grupos o trabajan solos a través de dispositivos electrónicos y redes informáticas. Son estafas, robo de datos personales, de información comercial estratégica, robo de identidad, fraudes informáticos cometidos por ciberdelincuentes que actúan en grupos o trabajan solos

- Ciberacoso o ciberbullying
- Sexting
- Grooming
- Phishing
- Pornografìa infantil

CIBERBULLYING ¿Qué es?

Se trata del acoso durante repetidas y sostenidas veces (insultos, chantaje, coacción, humillación, injurias, calumnias vejaciones) entre iguales, mediante el uso de las nuevas tecnologías (telefonía móvil, internet -foros, chats, correo electrónico videojuegos online). Puede ser anónimo o existir contacto o relación previa

Consecuencias del ciberbullying:

- Deterioro físico y psicológico
- Aislamiento, insomnio, fatiga, stress
- Depresión, bajo rendimiento, desorden alimenticio
- Alteraciones de nuestros hábitos, hasta el suicidio

El ciberbullying se puede prevenir

- Configurar adecuadamente el grado de privacidad de los perfiles sociales
- **No compartir fotos ni videos con todos.**
- **No aceptar contactos de desconocidos..**
- Cortar la cadena de mensajes.

GROOMING ¿Qué es?

Es el acoso sexual de una persona adulta a un niño, niña o adolescente por medio de Internet. Las personas que realizan grooming se llaman groomers o acosadores..

Componentes y fases del Grooming

Acercamiento, compartir gustos y preferencias.

Ganar confianza, generar charla íntimas, pedir fotos, videos de índole sexual.

Acoso y chantaje para obtener mayor material o lograr un encuentro personal

Qué hacer en casos de Grooming

PEDIR AYUDA. No aislarse. Hablar con padres o adulto de confianza.

MANTENER NUESTRA PRIVACIDAD. NO enviar imágenes o información personal

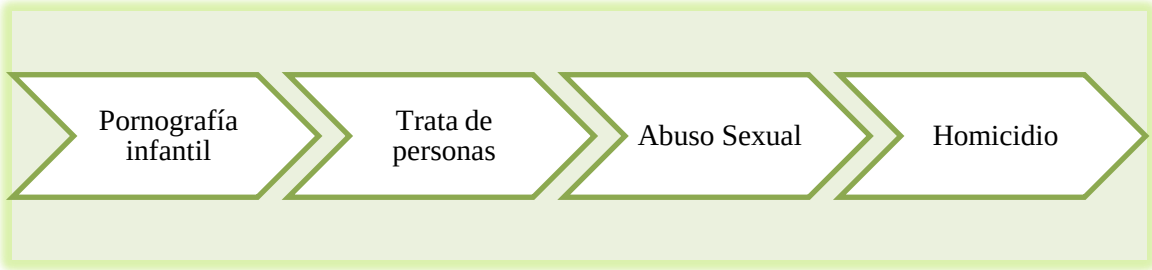
NO CEDER AL CHANTAJE.

GUARDAR LAS PRUEBAS. No borres los mensajes o todo aquello que pueda servir de prueba

Es un delito penado por la **ley n° 26. 904 DEL CODIGO PENAL** que incluye prisión de 6 meses a 4 años a quien por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier tecnología de transmisión de datos, contacte a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Lo Sabías?

El Grooming puede derivar en otros graves delitos



SEXTING ¿Qué es?

Consiste en el envío de imágenes, videos y/o mensajes de contenidos eróticos-pornográficos **sin consentimiento** a través de la TIC (tecnología e informática de la comunicación

n

Consecuencias del sexting

Quien envía las fotos o videos de contenido sexual lo hace de forma voluntaria y dentro de una situación íntima. Sin embargo, cuando esa imagen o video circula en internet, pueden surgir situaciones no deseadas.

1

- **Descontextualización de la situación:** la imagen o video consentida y apropiada en el momento de intimidad se viraliza

2

- **Exposición:** las imágenes viralizadas son recibidas por personas que no son los destinatarios originales. Cuantas más personas vean la imagen o video, más expuestos estarán los protagonistas

3

- **Sextorsión:** Es una forma de chantaje en la que se amenaza a una persona con divulgar y hacer pública imágenes y videos de su intimidad sexual. Las imágenes o videos pueden ser viralizados por venganza luego de terminar una relación amorosa.

PHISHING ¿Qué es?

La palabra **phishing** quiere decir suplantación de identidad.
Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esa persona.
Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para "pescar" contraseñas y datos personales valiosos.
.

¿Cómo prevenirlo?:

- **No contestar formularios en línea** enviados por destinatarios desconocidos.
- **No responder a ningún correo electrónico, teléfono o fax, que solicite divulgar información personal.**
- **No enviar ni compartir ningún código de seguridad**
- **Desconfiar de los archivos adjuntos:** pueden causar la descarga de la clave de registro o software "spyware" en su computadora.
- **Utilizar un antivirus** actualizado.
- **Actualizar el sistema operativo.**

LO SABÍAS?

En la Web circulan los datos personales que compartimos en las redes sociales, en los sitios que frecuentamos, en formularios digitales, en sitios de juegos y de compras, pero también circulan otros datos nuestros que muchas veces desconocemos.

¿Dónde denunciar un delito informático?

Línea gratuita 137

• Programa Las víctimas contra las violencias: línea 137. Es un servicio telefónico gratuito del Ministerio de Justicia y Derechos Humanos. Funciona las 24 horas, los 365 días del año, en la Ciudad Autónoma de Buenos Aires.

MINISTERIO PÚBLICO FISCAL DE LA CIUDAD DE BUENOS AIRES: Unidad Fiscal Especializada en delitos y contravenciones informática:

0800 33347225 FISCAL que atiende las 24hs, y también se puede denunciar

Enviando un mail a denuncias@fiscalias.gob.ar

Desde la APP “DENUNCIAS MPF”.

Denuncia presencial de lunes a viernes de 9 a 20hs.

Denuncias Online en www.mpfciudad.gob.ar

POLICÍA METROPOLITANA - Área de Cibercrimen: Ecuador 261, CABA

Tel. 4309-9700 internos 4008 O 4009

cibercrimen@buenosaires.gob.ar

DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES. Para denuncia de delitos relacionados con la privacidad o la protección de datos personales.

Av. Pte. Gral. Julio A. Roca 710 | Ciudad Autónoma de Buenos Aires

(54-11) 2821-0047

datospersonales@aaip.gob.ar

https://www.argentina.gob.ar/aaip/datospersonales

EQUIPO NIÑ@S CONTRA LA EXPLOTACIÓN SEXUAL Y GROOMING:. Es un servicio telefónico gratuito del Ministerio de Justicia y Derechos Humanos de laNación. Funciona las 24 horas, los 365 días del año, en todo el país. Se puede

0800-222-1717

equiponinas@jus.gov.ar
