UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

MINI GUÍA DE SEGURIDAD EN INTERNET

¡TODO LO QUE TIENES QUE SABER!

EL INTERNET
ES UNA HERRAMIENTA MUY ÚTIL...

SI LA SABES MANEJAR
ADECUADAMENTE

Navegar en Internet, hacer uso de las redes sociales y comunicarnos usando la tecnología es una experiencia gratificante y positiva. Sin embargo, el uso de las tecnologías de información y comunicación, como computadoras o teléfonos celulares pueden tener grandes riesgos para los niños, niñas y adolescentes; razón por la cual es necesario estar conscientes de los peligros y amenazas que existen en el Internet y cómo podemos protegernos.

LA MINI GUÍA DE SEGURIDAD EN INTERNET SE ENFOCA EN:

- *Dar a conocer las nuevas técnicas que una persona o grupo de personas están usando para causar daño a otras personas en el ciberespacio.*
- *Dar a conocer los peligros o riesgos a los cuales están expuestos los NNA (niños, niñas y adolescentes).*
- *Dar a conocer las prácticas de protección ante las amenazas.*
- *Dar recomendaciones para aprovechar las ventajas de la Web.*

¡Utiliza el Internet para tu beneficio!

Grooming

Seducción en línea

¿Te has hecho amigo(a) de alguna persona que conociste en las redes sociales, pero que no conoces en la vida real?

Se le llama Grooming a las acciones que realiza un adulto utilizando engaños y mentiras que buscan ganarse la confianza de niñas, niños y adolescentes, haciendo uso de las tecnologías de información y comunicación. El Grooming es utilizado como un medio para cometer los delitos de Violencia Sexual, Explotación y Trata de Personas.

La persona que hace Grooming suele utilizar las redes sociales, chats, juegos en línea y foros para contactar y hacer amistad con sus víctimas. Las atrae con un perfil atractivo para brindar confianza. En sus conversaciones expresa los mismos gustos y emociones, y utiliza las mismas expresiones, lenguaje, emoticones (figuritas) para simpatizar con sus víctimas. Se presenta como el amigo (a) o novio (a) perfecto (a).

Conoce las fases del Grooming

a. *Identifica y/o contacta a la víctima usando perfiles falsos, invitándole a ser su amigo (a).*

b. *Querrá asegurarse que el niño, niña y adolescente quiera hablar con él, te conversará sobre temas de su interés; le hablará de su situación familiar, relaciones sentimentales con el fin de crear un vínculo de amistad; hará preguntas sobre su edad y ubicación, e intentará conocer sus gustos para adaptarse a ellos. Su objetivo es ganarse su confianza.*

c. *Obtiene contenido íntimo que le permitirá ejercer presión sobre su víctima.*

Sexting
Mensajes sexuales

¿ Alguna vez has enviado o recibido imágenes o videos con poca o sin ropa a través de tus redes sociales, chat o correo electrónico?

El Sexting es el envío o recepción de contenido de tipo sexual (principalmente fotografías o videos), los cuales son producidos por quien los envía a través de las tecnologías de información y comunicación.

El Sexting se dá de forma voluntaria cuando:

a. *A través de engaños envías fotografías y/o videos con poca o sin ropa, a personas que han ganado tu confianza pero no conoces en la vida real.*

b. *En una relación sentimental o de amistad envías fotografías y/o videos con poca o sin ropa.*

¿SABÍAS QUÉ?

- *Durante una conversación a través de una cámara de computadora, esta puede capturar y/o grabar imágenes que pueden ser publicadas en Internet.*
- *Aunque utilices contraseñas y otros mecanismos de seguridad, tus fotografías y videos de tu celular o computadora pueden compartirse en internet por robo, error, broma o extravío.*
- *Quien te ama no te pide fotografías comprometedoras.*

La exposición de imágenes sexuales produce un daño irreparable a la privacidad e integridad de la persona y de sus familiares.

Las personas que hacen

SEXTING

con niños, niñas y adolescentes pueden incurrir en los delitos de:

Producción de pornografía de personas menores de edad. **Art. 194 del Código Penal.**

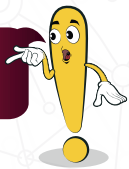
Comercialización o difusión de pornografía de personas menores de edad. **Art. 195 Bis del Código Penal.**

Posesión de material pornográfico de personas menores de edad. **Art. 195 Ter del Código Penal.**

Violación a la intimidad sexual. **Art. 190 del Código Penal.**

Ingreso a espectáculos y distribución de material pornográfico a personas menores de edad. **Art. 189 del Código Penal.**

Recuerda que una vez que envías imágenes o videos (incluyendo los que se hacen a través de cámara de computadora), pierdes el control de ellos.



Sextortion

Chantaje Sexual

¿ Te has sentido chantajeado (a) por alguien que te amenaza con difundir fotografías o videos tuyos con poca o sin ropa, si no haces lo que te dice?

El Sextortion es una forma de amenaza que sucede después que una persona ha logrado ganarse la confianza de alguien y obtiene imágenes o videos con contenido sexual. El chantaje se da cuando el agresor a cambio de no publicar las imágenes o videos, obliga a su víctima a realizar acciones que ponen en peligro su integridad, como relaciones sexuales involuntarias, producir pornografía, u otras acciones que pueden poner en peligro tu vida.

RECOMENDACIONES

- *Detén la conversación y/o relación y no accedas al chantaje bajo ninguna circunstancia, pide ayuda.*
- *Configura tus redes sociales para que sólo tus amigos (as) puedan ver tu perfil.*
- *Guarda todas las comunicaciones de tu computadora o teléfono para que puedas denunciarlo, no las borres.*

Las personas que cometen **SEXTORTION** pueden incurrir en el delito de:

Violación a la intimidad sexual. **Art. 190 del Código Penal.**

Cyberbullying

Ciberacoso

¿ Alguna vez te has sentido, acosado (a), discriminado (a), humillado (a), amenazado (a), molestado (a), o alguien te ha hecho comentarios hirientes a través de las redes sociales, correos electrónicos o chats?

El Cyberbulling engloba el uso de las tecnologías de información y comunicación, para causar daño psicológico, verbal o social de manera repetida, deliberada y violenta. Este abuso se comete entre grupos de niños, niñas y adolescentes.

¿QUÉ PUEDO HACER?

- *No contestes a las provocaciones o insultos.*
- *La mayoría de las redes sociales tienen mecanismos de seguridad "denuncia" y "bloqueo", actívalas cuando te sientas ofendido (a), acosado (a) o amenazado (a).*
- *Si te acosan, pide ayuda con urgencia a tus padres, maestros o un adulto de tu confianza.*
- *Compórtate con respeto hacia los demás en las redes sociales.*

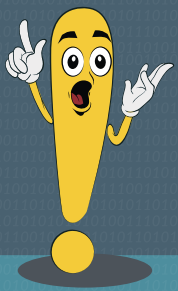
Malware

Programa malicioso

Es un programa malicioso diseñado para dañar un sistema, robar información y/o hacer modificaciones al sistema operativo y tomar control absoluto del equipo infectado. ¡Ten cuidado! Hay muchas clases de programas maliciosos que contienen virus como el caballo de Troya o troyano, los gusanos, keyloggers, los ackdoor o bot, el exploit, los software espía, el ransomware y muchos más.

¿Cómo se puede infectar tu equipo de cómputo o teléfono celular?

- *Mientras buscas contenido y bajas información.*
- *Al bajar aplicaciones de fuentes desconocidas en tu computadora o teléfono.*
- *Al conectar dispositivos de almacenamiento (USB, discos extraíbles) infectados en tu teléfono o computadora.*



¿Cómo puedo proteger mi equipo de cómputo o teléfono celular?

- *Manteniendo actualizado el software de seguridad (antivirus) y el sistema operativo.*
- *Analizando todo dispositivo de almacenamiento antes de conectarlo a tu computadora (USB, discos extraíbles, etc.).*
- *No descargando archivos sospechosos o de fuentes desconocidas.*

Phishing

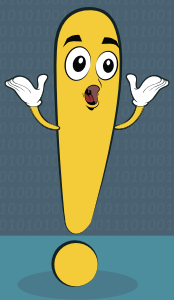
Robo de identidad

Es una técnica que consiste en engañar al usuario para robarle información confidencial, haciéndole creer que está en un sitio de total confianza.
Esto se realiza a través de correos electrónicos o mensajes que incluyen un enlace que llevan al usuario a un sitio web falso, el cual es una copia del original.

TIPO DE INFORMACIÓN ROBADA

- *Datos personales*
- *Información financiera*
- *Contraseñas*

RECOMENDACIONES



- *Nunca hagas clic en enlaces contenidos en mensajes sospechosos.*
- *Nunca descargues archivos de mensajes sospechosos, estos pueden contener un programa malicioso.*
- *Realiza copias de seguridad "backups" de tu información de manera periódica.*
- *Actualiza regularmente tu sistema operativo, antivirus y otros programas.*
- *Evita ingresar a sitios web de dudosa reputación o con contenido censurado.*
- *Utiliza contraseñas complejas y cámbialas periódicamente.*

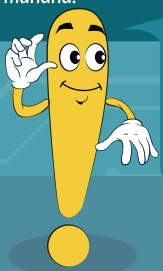
¡CUIDA TU REPUTACIÓN EN INTERNET!

Recuerda que la reputación se construye a lo largo de los años y es difícil de borrar o modificar.

Si no cuidas lo que compartes en Internet, puedes ser perjudicado (a), tu imagen e información personal difundida y tu familia afectada.

Tu reputación en Internet es la idea que los demás tienen sobre ti, esta se forma a partir de la información que subes o la que los demás comparten de ti. Se construye a través de las publicaciones, fotos y videos que pueden ser encontrados en Internet.

El Internet se ha convertido en la forma más común de conocer a una persona, cuando quieras conseguir trabajo tu entrevistador buscará información sobre ti en la Web, no subas hoy lo que no quieras que recuerden de ti mañana.



¡LO QUE SUBES A INTERNET, QUEDA AHÍ PARA SIEMPRE!

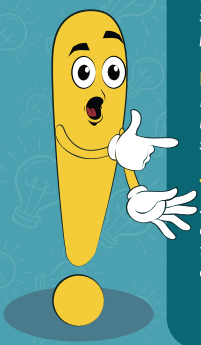
CONSEJOS
PARA NIÑOS, NIÑAS Y ADOLESCENTES

SE SELECTIVO(A):
Sólo añade o permite acceso a tu perfil en redes sociales a personas que conoces personalmente.

MARCA TU TERRITORIO:
Establece tu perfil en redes sociales como privado, con acceso restringido únicamente a las personas en las que confías.

SE DUEÑO(A) DE TU RUTINA:
Con información sencilla como el lugar donde estudias, y/o trabajas, vives y socializas, das las herramientas a un agresor para que pueda hacerte daño.

CUIDADO CON LO QUE DESCARGAS:
Recuerda que descargar o copiar juegos, canciones o software con derechos de autor es ilegal, además de que puede infectar tu computadora con un virus.



NO CAIGAS EN LA TRAMPA:
Hay quienes usan perfiles falsos en redes sociales y otros recursos en Internet para poner trampas, robar o simplemente acosar a los demás, ignóralos.

TÚ TIENES EL PODER DE HACER EL CAMBIO:
Si has pasado por una situación incómoda en Internet y quieres evitar que otros jóvenes se vean afectados, comparte tu experiencia con tus papás o adultos que les tengas confianza.

¿CÓMO CREAR UNA CONTRASEÑA SEGURA?

- *Al crear tu contraseña combina letras mayúsculas, minúsculas, números y símbolos, haz una contraseña larga.*
- *No uses la misma contraseña para todo.*
- *Procura cambiarla periódicamente.*
- *No la compartas con nadie.*

CONSEJOS PARA ADULTOS

1. *Aprende a utilizar la tecnología, no tengas miedo a saber cómo funciona el Internet.*
2. *Genera una comunicación de confianza con los niños, niñas y adolescentes e infórmales sobre los peligros de las Redes Sociales.*
3. *Enséñale a los niños, niñas y adolescentes que la diferencia entre lo que está bien y lo que está mal es la misma que en la vida real.*
4. *Utiliza controles parentales para restringir el acceso a páginas con contenido no apto para niños, niñas y adolescentes.*
5. *Monitorea el historial de búsqueda del navegador en Internet.*
6. *Establece límites de tiempo de uso de tecnología en niños, niñas y adolescentes.*
7. *Crea áreas libres de tecnología, por ejemplo: las habitaciones de los niños, niñas y adolescentes.*
8. *Insiste en que los niños, niñas y adolescentes nunca compartan su dirección, edad, número de teléfono u otra información personal, como la escuela a la que van, detalles de su rutina o dónde les gusta jugar.*
9. *Dile a los niños, niñas y adolescentes que no deben reunirse con amigos en línea que no conocen en persona sin la supervisión de un adulto, recuerda que las apariencias engañan.*

¿QUÉ HACER CUANDO ERES VÍCTIMA DE CIBERDELITO / DELITO INFORMÁTICO?

- *Detén cualquier comunicación con la persona que te esté chantajeando, acosando o que te haga sentir incómodo.*
- *No borres, destruyas o modifiques la información que poseas en la computadora o teléfono celular.*
- *Toma capturas de pantalla "pantallazos" o "Screen shots" de las conversaciones, horario, días y fechas.*
- *Nunca reenvíes los mensajes o correos electrónicos que tengan fotografías o videos de niños, niñas y adolescentes con poca o sin ropa.*
- *Copia toda la URL y guarda la información.*
- *Si eres víctima comunícale a tus padres, encargado o persona que le tengas confianza.*
- *No guardes silencio, presenta la denuncia ante la Policía Nacional Civil más cercana a tu domicilio (comisaría, subestación de tu barrio en cualquier lugar del país).*
- *Recuerda que tienen la obligación de tomar tu denuncia.*

RECUERDA QUE TAMBIÉN PUEDES PRESENTAR TU DENUNCIA EN LOS CENTROS DE LLAMADAS DE LA POLICÍA NACIONAL CIVIL SIGUIENTES:

110 Teléfono de emergencia de la Policía Nacional Civil

1510 Escuelas Seguras de la Policía Nacional Civil

1561 Cuéntaselo a Waldemar de la Policía Nacional Civil

¿EN QUÉ CONSISTEN ESTOS CENTROS DE LLAMADAS DE LA POLICÍA NACIONAL CIVIL?

Es un servicio gratuito brindado a toda la ciudadanía a nivel nacional, las 24 horas del día, para la recepción de denuncias sobre cualquier hecho delictivo, como trata de personas, violencia sexual, pornografía infantil, violencia contra la mujer, crimen organizado, extorsiones, tráfico de armas, etc.

Es un servicio que a diario salva la vida de muchas personas, cuando haces uso responsable de este servicio, ayudas a que la asistencia llegue de inmediato a quien lo necesita.

Recuerda usar los números de denuncia sólo con hechos reales, todas las llamadas que haces son registradas, y el mal uso es castigado por la Ley.

¡SÉ UN HÉROE ANÓNIMO, LLAMA ÚNICAMENTE POR UNA EMERGENCIA!

¡ESTO NO ES UN JUEGO!

ÚSALO DE UNA FORMA RESPONSABLE, PORQUE PUEDE SER QUE LA LLAMADA QUE NO ATIENDAN, SEA LA TUYA.

Glosario

Backups: *Copia de seguridad de uno o más archivos informáticos, que se hace generalmente, para prevenir posibles pérdidas de información.*

Comunidad virtual: *Personas unidas a través de Internet por valores o intereses comunes, como gustos, pasatiempos o profesiones.*

Delitos informáticos o Ciberdelitos: Toda actividad ilícita que: *(a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, (b) Tienen por objeto robo de información, robo de contraseñas, fraude a cuentas bancarias, entre otros.*

Explotación sexual: *Todo abuso cometido o amenaza de abuso en una situación de vulnerabilidad, de relación de fuerza desigual o de confianza, con propósitos sexuales.*

Internet: *Red global de redes de computadoras cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios.*

Netiqueta: *Conjunto de reglas que regulan el comportamiento de los usuarios para comunicarse en la red, es la etiqueta del ciberespacio.*

Pornografía Infantil: *Comprende toda representación real o simulada de un niño, niña y/o adolescente realizando actividades sexuales explícitas o sugerentes, de cualquier forma y a través de cualquier medio.*

Redes Sociales: *Se le denominan a las plataformas informáticas diseñadas para albergar comunidades virtuales de individuos interconectados que comparten contenido, información, archivos, fotos, audios, videos, entre otros.*

Sitios web: *Conjunto de páginas web desarrolladas en código html, relacionadas a un dominio de Internet el cual se puede visualizar en la World Wide Web (www), mediante los navegadores web o también llamados browser.*

Software: *Programas informáticos que hacen posible la realización de tareas específicas dentro de un Ordenador.*

Tecnologías de la Información y Comunicación –TIC´s–: *Son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego.*

Trata de Personas: *La captación, el transporte, traslado, retención, acogida o recepción de una o más personas con fines de explotación. También es conocido como una forma moderna de esclavitud humana.*

URL: *Es el Localizador Uniforme de Recursos o dirección Web, que al ser encontrada y visualizada por un navegador, muestra un recurso de información al usuario.*

Violencia sexual: *Todo acto sexual, la tentativa de consumar un acto sexual, los comentarios o insinuaciones sexuales no deseados, o las acciones para comercializar o utilizar de cualquier otro modo la sexualidad de una persona mediante coacción por otra persona, independientemente de la relación de esta con la víctima, en cualquier ámbito, incluidos el hogar y lugar de trabajo.*

Virus: *En el contexto de la informática, son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en el ordenador.*

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Canadá

GOBIERNO DE LA REPÚBLICA DE
GUATEMALA
MINISTERIO DE GOBERNACIÓN

SVET
Secretaría contra la Violencia Sexual, Explotación y Trata de Personas

CUENTASELO A WALDEMAR
Tel.: 1561

ESCUELAS SEGURAS DE LA POLICÍA NACIONAL CIVIL
Tel.: 1510

POLICIA NACIONALCIVIL,
GUATEMALA C.A.
Tel.: 110

Esta publicación fue impresa gracias al apoyo financiero generosamente provisto por el Gobierno de Canadá, a través del programa de Construcción de Capacidades Contra el Crimen.

Al escanear este código, podrás encontrar más información en el sitio Web de SVET.