Miniguía de SEGURIDAD en Internet

¡Todo lo que tienes que saber!

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

El Programa Global de Ciberdelito de la UNODC tiene como misión: proporcionar liderazgo global en la formulación de políticas y en la construcción de capacidades para combatir el delito cibernético y los delitos financieros. Para lograrlo, el Programa ha sido 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 Latinoamérica y el Caribe, África, Medio Oriente, el Sudeste de Asia y el Pacífico, con los siguientes objetivos:

- Generar mayor eficiencia y eficacia en la investigación, enjuiciamiento y sanción del delito cibernético, especialmente los vinculados a la explotación y abusos sexuales de niños, niñas y adolescentes; desde de 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 el 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 de esta herramienta.

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

Oficina de las Naciones Unidas contra la Droga y el Delito
Oficina Regional para Centroamérica y el Caribe en Panamá (ROPAN)

NOTA: este material ha sido elaborado de acuerdo con el compromiso de la UNODC de utilizar un lenguaje incluyente encaminado a consolidar la equidad e igualdad de género. No obstante, para facilitar la lectura, en algún pasaje concreto se ha utilizado la formulación masculina para aludir a ambos géneros.

¡EL INTERNET ES UNA HERRAMIENTA MUY ÚTIL!

si la sabes manejar adecuadamente...

- Las Tecnologías de la Información y Comunicación (TIC) han transformado el mundo entero y lo mejoran día a día. En esta nueva era digital es mucho más fácil resolver los problemas de la vida cotidiana.

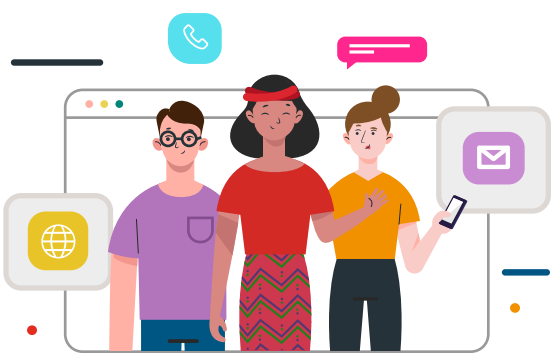
- El Internet es una herramienta versátil que te permite adquirir nuevos conocimientos y sirve como espacio para el entretenimiento.

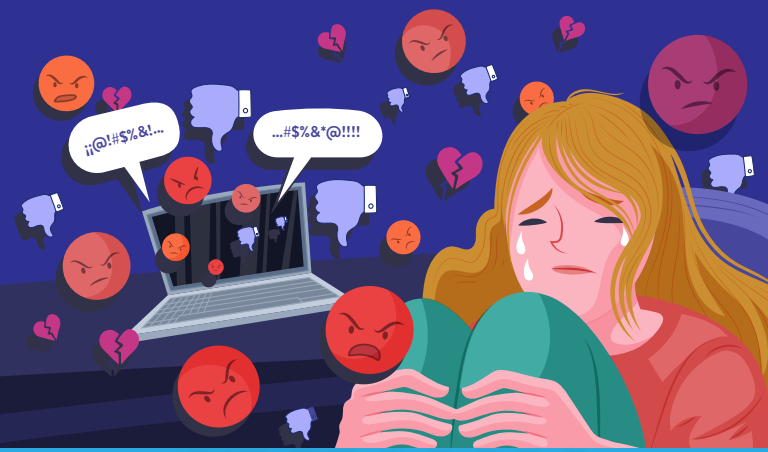
- Navegar en Internet, hacer uso de las redes sociales y comunicarnos usando la tecnología, es una experiencia gratificante y positiva.

- Cada vez resulta más fácil acceder a Internet usando distintos tipos de dispositivos.

- Las TIC ofrecen muchas oportunidades de comunicación y aprendizaje para las niñas, niños, adolescentes y adultos, pero se deben usar de manera correcta.

¡OCUPA EL INTERNET PARA TU BENEFICIO Y NO PARA TU PERJUICIO!





CIBERACOSO

CYBERBULLYING

¿Alguna vez has sentido acoso, discriminación, o alguien te ha hecho comentarios hirientes a través de las redes sociales, correo electrónico o mensajería instantánea?

¿Alguna vez alguien te ha atormentado, amenazado, hostigado, humillado o molestado a través de las redes sociales o por teléfonos celulares?

El *cyberbullying* engloba el uso de las TIC para causar daño de manera repetida, deliberada y hostil. Esto puede incluir, pero no limitarse, al uso del Internet, teléfonos celulares u otros dispositivos electrónicos para difundir o colocar textos o imágenes que dañan o avergüenzan a una persona.

¿Qué puedo hacer?

- La mayoría de las redes sociales tienen mecanismos de seguridad, denuncia y bloqueo. Actívalas cuando te ofendan, acosen o amenacen.
- Evita contestar a las provocaciones o insultos.
- Si te acosan, pide ayuda con urgencia a tus padres, maestros o a un adulto de tu confianza.
- Compórtate con respeto hacia los demás en la Red. No hagas a los demás lo que no te gustaría que te hagan a ti.

GROOMING

¿Has entablado una relación de amistad con alguna persona que conociste por la Red pero que desconoces en la vida real?

Se le llama *grooming* al conjunto de estrategias que una persona adulta realiza para ganarse la confianza de un niño, niña o adolescente, a través del uso de las TIC, con el propósito de abusar del niño, niña o adolescente o para explotarlo sexualmente.

¿Qué suele utilizar?

- Correos electrónicos.
- Videochats.
- Intercambio de imágenes o videos.
- Redes sociales.

Conoce las etapas del *grooming*

1. Identifica a la niña, niño o adolescente víctima, a través de redes sociales o chats. A veces utiliza perfiles falsos.
2. Se gana la confianza de niños, niñas y adolescentes.
3. Seduce a la potencial víctima a través de conversaciones.
4. Obtiene información y/o contenido íntimo de niños, niñas y adolescentes, que le permite ejercer presión sobre ellos o ellas.
5. Acosa, chantajea, amenaza y manipula para lograr sus objetivos: fotografías, videos o encuentros físicos de carácter sexual.

Seducción de niños, niñas y adolescentes por el uso de las Tecnologías de Información. Art. 190 Bis del Código Penal.

SEXTING

¿Alguna vez has enviado o recibido contenido sexual o erótico a través de tu celular, redes sociales o correo electrónico?

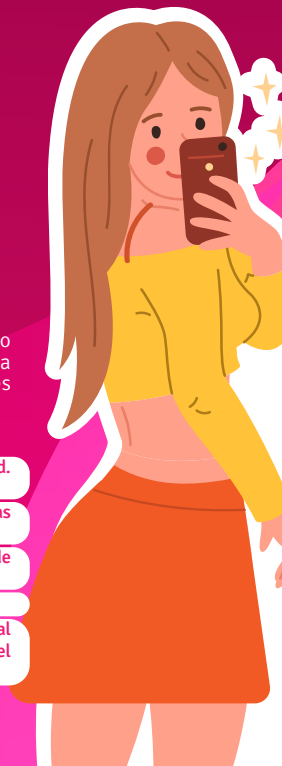
El *sexting* es la autoproducción, intercambio y transmisión de imágenes de desnudos o casi desnudos, sexualmente sugerentes, a través de las TIC.

Recuerda que una vez que envías imágenes o videos (incluyendo lo que envías en una videollamada o conversación por *webcam*), pierdes totalmente el control de estos.

Los peligros más comunes del *sexting*

- Daño a tu privacidad. La exposición indeseada de estas imágenes produce un daño irreparable a la privacidad e intimidad de la persona que comparte sus propias imágenes.

- Por más que se utilicen contraseñas y otros mecanismos de seguridad, tus datos pueden ser '*hackeados*' o robados, e incluso, difundidos en Internet sin tu consentimiento.



No olvides que, durante una conversación o videollamada con otra persona a través de una webcam, esta puede capturar y/o grabar imágenes que pueden ser publicadas en Internet.

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.

SEXTORSIÓN

¿Alguna vez te han chantajeado con difundir imágenes, videos o información tuyas si no haces lo que te dicen?

La 'sextorsión' es una forma de extorsión en la que se chantajea a una persona, por medio de una imagen o video de sí misma desnuda, que pudo haber compartido a través de Internet o de mensajes.

La víctima es coaccionada a ejecutar acciones de tipo sexual o pago de una cantidad de dinero, con la amenaza de que estas imágenes serán divulgadas si no lo hace.

Recomendaciones

1. Detén la conversación y/o la relación y no accedas NUNCA al chantaje bajo ninguna circunstancia.

2. Configura tus redes sociales para que solo tus amistades puedan ver tu perfil.

3. Guarda toda la comunicación para que puedas denunciarlo.

Chantaje a niños, niñas o adolescentes mediante el uso de las tecnologías. Art. 190 Ter del Código Penal.

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

Violencia de Género Digital

El espacio digital, debido a sus características, es un entorno que también reproduce formas variadas de violencia de género:

- **Ciberacoso.**
- **Ciberhostigamiento.**
- **Distribución no consensuada de imágenes íntimas y sexuales.**
- **Doxxing.**
- **Violencia sexual.**
- **Recepción de imágenes y videos sexuales sin consentimiento.**
- **Amenazas de violencia sexual.**

Como consecuencia de la violencia en línea, las mujeres y las niñas sufren graves daños psicológicos, físicos, sexuales, emocionales, económicos, laborales, familiares y sociales.

A tomar en cuenta:

- La violencia digital hacia las mujeres es un reflejo de la sociedad. Por ello es necesario prevenir y sancionar este tipo de violencia.

- Se debe dejar de normalizar la violencia en las plataformas digitales y conocer sus mecanismos de prevención y protección.

- Se requiere educación en ciudadanía digital y ciberseguridad en igualdad.

MALWARE

Es un *software* malicioso diseñado para dañar un sistema, robar información y/o hacer modificaciones al sistema operativo y tomar el control absoluto del dispositivo infectado. Hay muchas clases de *malware*: los virus, el Caballo de Troya o troyano, los gusanos, *keyloggers*, *backdoors* o *bots*, *exploit*, *software* espía, *ransomware*, entre otros.

¿Cómo te infectas?

- Mientras buscas contenido y bajas información.
- Al bajar aplicaciones de sitios no oficiales.
- Al conectar dispositivos infectados en tu celular o computadora.

¿Cómo los previenes?

- Mantén actualizado el *software* de seguridad (antivirus) y el sistema operativo del dispositivo.
- Analiza todo dispositivo de almacenamiento antes de conectarlo a tu computadora.
- No descargues archivos sospechosos ni visites páginas de dudosa reputación.

PHISHING

¿Cómo funciona?

Hay estafadores que envían mensajes, enlaces electrónicos o correos electrónicos falsos, imitando casi a la perfección la imagen de las entidades bancarias u otras compañías, para conseguir que personas desprevenidas revelen su información personal, contraseñas de perfiles o datos bancarios, para posteriormente, robar el dinero de sus cuentas.

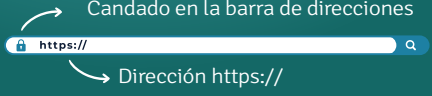
Tipo de información robada

1. **Datos personales.**
2. **Información financiera.**
3. **Contraseñas.**

Recomendaciones

- Nunca hagas clic en enlaces recibidos en mensajes sospechosos.
- Nunca descargues archivos adjuntos de mensajes sospechosos. Estos pueden contener *software* malicioso.
- Realiza copias de seguridad de tu información de manera periódica.
- Actualiza regularmente el sistema operativo, navegador, antivirus y otros programas de tus dispositivos electrónicos.
- Evita ingresar a sitios web de dudosa reputación o con contenido censurado.

Siempre verifica



JUEGOS ONLINE – GAMING

Cada vez hay más juegos *online* que se descargan en los teléfonos celulares, computadoras o se juegan en línea a través de videoconsolas, donde cientos de millones de usuarios de la comunidad *gaming* están conectados.

A veces, estos juegos obligan a entregar información sensible como números de tarjeta de crédito, datos personales, direcciones, etc.

Algunos delincuentes utilizan estas plataformas para acercarse con malas intenciones a niños, niñas y adolescentes, robar información y estafarte a ti o a tus padres.

Recomendaciones para *gamers*

- **Instala un antivirus.**
- **Mantén actualizados los programas.**
- **Utiliza contraseñas seguras y robustas.**
- **Compra exclusivamente en las tiendas *online* oficiales.**
- **Evita revelar información personal.**
- **No aceptes encontrarte con ningún jugador virtual en el mundo real sin el conocimiento de tus padres.**

¡Cuida tu REPUTACIÓN EN Internet!

Tu reputación en Internet es la idea que los demás tienen sobre ti, y está formada a partir de la información que compartes y la que comparten los demás sobre ti. Se constituye a través de las publicaciones, fotos y videos donde apareces y que pueden ser encontrados en Internet.

Recuerda que la reputación se construye a lo largo de los años y es difícil de borrar o modificar ya que en Internet no hay olvido. Lo que subes a Internet podría quedar ahí para siempre.

La reputación en Internet es importante

Internet se ha convertido en la forma más común y rápida de conocer a una persona. Cuando quieras conseguir una beca o un trabajo, tu entrevistador puede buscar información sobre ti en la web. Si no cuidas tu reputación en Internet, tu información privada puede ser difundida y tu imagen verse afectada.

Consejos para niños, niñas y adolescentes

Selecciona con criterio:

Solo añade o permite acceso a tu perfil en redes sociales, a quien conozcas personalmente.

Marca tu territorio:

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

Aduéñate de tu rutina:

Con información aparentemente sencilla como el lugar donde estudias, y/o trabajas, vives y socializas; das las herramientas a un agresor para que pueda hacerte daño.

Ten 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.

Evita caer en trampas o engaños:

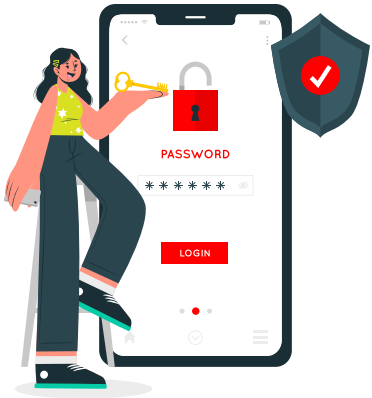
Hay quienes usan perfiles falsos en redes sociales y otros recursos en Internet para poner trampas, robar o simplemente acosar a los demás, ¡ignóralos!

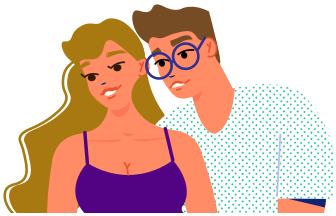
Tienes el poder de hacer el cambio:

Si has pasado por una situación incómoda en Internet y quieres evitar que otros jóvenes se vean afectados, comparte tu experiencia con tus padres o con los adultos a quienes tengas confianza.

¿Cómo crear una contraseña segura?

- Debe tener al menos 8 caracteres.
- No puede ser un dato fácil de adivinar (nombre, fecha de nacimiento, etc.).
- Tiene que incluir letras mayúsculas y minúsculas.
- Debe tener números y letras.
- No debe dejarse escrita ni guardada, sino introducirse cada vez que se use.
- Es un secreto que no debería compartirse con nadie ajeno a la familia.
- Debe ser cambiada de vez en cuando.
- Tiene que ser diferente para cada servicio, red social o app.





Consejos para **adultos**

- Aprende a utilizar la tecnología, no tengas miedo a saber cómo funciona el Internet.

- Genera una comunicación de confianza con los niños, niñas y adolescentes e infórmales sobre los peligros de las redes sociales.

- 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.

- Utiliza controles parentales para restringir el acceso a páginas con contenido no apto para niños, niñas y adolescentes.

- Monitorea el historial de búsqueda del navegador en Internet.

- Establece límites de tiempo de uso de tecnología en niños, niñas y adolescentes.

- Crea áreas libres de tecnología, por ejemplo: las habitaciones de los niños, niñas y adolescentes.

- 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.

- Dile a los niños, niñas y adolescentes que no deben reunirse en persona con amigos en línea que no conocen, 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 incomodidad.

- No borres, destruyas o modifiques la información que poseas en la computadora o teléfono celular.

- Toma capturas de pantalla 'pantallazos' o '*screenshots*' de las conversaciones, horario, días y fechas.

- Nunca reenvíes los mensajes o correos electrónicos que tengan fotografías o videos de niños, niñas y adolescentes que tengan poca o nada de ropa.

- Copia toda la URL y guarda la información.

- Si eres víctima, díselo a tus padres, encargados o persona a la que le tengas confianza.

- No guardes silencio, presenta la denuncia ante la Policía Nacional Civil (PNC) más cercana a tu domicilio (comisaría o subestación de tu barrio en cualquier lugar del país).

- Recuerda que la PNC tiene la obligación de tomar tu denuncia.

Recuerda que también puedes presentar tu denuncia en los centros de llamadas de la Policía Nacional Civil:

110 Teléfono de emergencia de la Policía Nacional Civil

1510 Escuelas Seguras de la Policía Nacional Civil

Denuncia en la Estación de Policía más cercana

Glosario

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 comete mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, y (b) Tiene por objeto el robo de información, robo de contraseñas y 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 de información entre todos sus usuarios.

***Malware*:** 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 archivos o datos almacenados en el ordenador.

Material de abuso sexual 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.

Netiqueta: Conjunto de reglas y prácticas que regulan y orientan el comportamiento de diferentes participantes en el ciberespacio. Es la etiqueta en el ciberespacio.

Redes sociales: Plataformas informáticas diseñadas para albergar comunidades virtuales de individuos interconectados que comparten contenido, información, archivos, fotos, audios y videos, entre otros.

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

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 una computadora.

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

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 o grupo mediante coacción por otra persona, independientemente de la relación de esta con la víctima, en cualquier ámbito, incluidos el hogar y el lugar de trabajo.


GOBIERNO de GUATEMALA
DR. ALEJANDRO GIAMMATTEI
MINISTERIO DE EDUCACIÓN


GOBIERNO de GUATEMALA
DR. ALEJANDRO GIAMMATTEI
MINISTERIO DE GOBERNACIÓN


GOBIERNO de GUATEMALA
VICEPRESIDENCIA
SVET


CYBERCRIME


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


Canadá