

# Miniguía de Seguridad en Internet en Uruguay



¡Todo lo que tienes que saber!







El Programa Global de Ciberdelito de 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 abuso sexual 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 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.



**Naciones Unidas**  
**Oficina contra**  
**la Droga y el Delito**

## **Oficina de las Naciones Unidas contra la Droga y el Delito**

La Oficina de las Naciones Unidas contra la Droga y el Delito ha adoptado todas las precauciones razonables para verificar la información que figura en la presente publicación, no obstante, el material publicado se distribuye sin garantía de ningún tipo, ni explícita ni implícita. El lector es responsable de la interpretación y el uso que haga de este material, y en ningún caso UNODC podrá ser considerada responsable de daño alguno causado por su utilización.

Se autoriza la reproducción total o parcial de los textos aquí publicados, siempre y cuando no sean alterados, se asignen los créditos correspondientes y no sean utilizados con fines comerciales.

# ¡INTERNET ES UNA HERRAMIENTA MUY ÚTIL!

si la sabes usar 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, puede ser 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.



# VIOLENCIA DE GÉNERO DIGITAL

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

- **Ciberacoso.**
- **Ciberhostigamiento.**
- **Distribución no consensuada de imágenes íntimas y sexuales.**
- **Doxxing** (publicar información privada o de identificación personal en internet con fines maliciosos).
- **Violencia sexual.**
- **Recepción de imágenes y videos sexuales sin consentimiento.**
- **Amenazas de violencia sexual.**

Aquellos que han experimentado violencia sexual en línea sufren graves daños psicológicos, físicos, sexuales, emocionales, económicos, laborales, familiares y sociales.



## ES IMPORTANTE TENER EN CUENTA:

- La violencia digital es un delito y se deben tomar medidas para prevenir y sancionar activamente este tipo de violencia.
- No normalizar la violencia en las plataformas digitales y conocer sus mecanismos de prevención y protección.
- Se requiere educación en ciudadanía digital y ciberseguridad al acceso de todos.



The background is a solid blue color with a complex network of white and light blue lines and shapes. These include circles of various sizes, some with a grid pattern like a globe, and others with a signal icon (three curved lines). There are also cloud shapes and starburst patterns. The overall theme is digital connectivity and technology.

# Ciberdelitos



## **MALTRATO CONTRA LAS PERSONAS MENORES DE EDAD**

### **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.

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



## Seducción en línea | Grooming

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

Grooming es el proceso mediante el cual un adulto busca establecer o construir una relación con niñas, niños o adolescentes, ya sea en persona o mediante el uso de internet u otras tecnologías digitales para facilitar el contacto sexual en línea o fuera de línea.

### ¿Qué medios suele utilizar?

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

### Conoce las etapas del grooming

1. Identificar a la niña, niño o adolescente víctima, a través de redes sociales o chats. En ocasiones se utilizan perfiles falsos para el primer acercamiento con víctimas potenciales.
2. Seducir a la potencial víctima a través de conversaciones.
3. Obtener información o contenido íntimo de niños, niñas y adolescentes, que le permite ejercer presión sobre ellos.
4. Ganar la confianza de niñas, niños o adolescentes.
5. Acosar, chantajear, amenazar y manipular para lograr sus objetivos: la recepción de fotografías o videos con contenido sexual o incluso, encuentros físicos con fines sexuales.

Recuerda que si eres víctima de este delito puedes denunciar en virtud del artículo 277 BIS, del Código Penal.

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

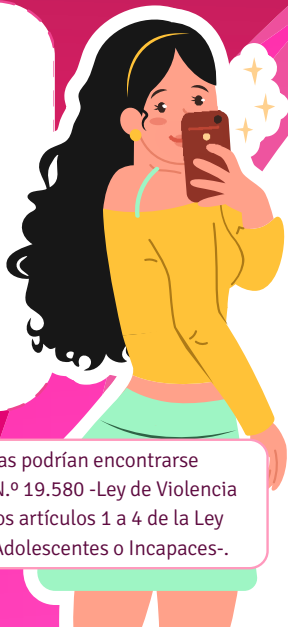
Sexting (mensajes sexuales en línea), es la autoproducción, intercambio y transmisión de mensajes sexuales, imágenes o vídeos de desnudos o casi desnudos, sexualmente sugerentes a través de teléfonos celulares y otros dispositivos tecnológicos.

Recuerda que una vez que envías una imagen, video o mensaje, incluso a través de una cámara web, pierdes el control sobre ese contenido. Otra persona puede capturar y/o grabar este contenido y publicarlo en Internet.

Lo mejor y más seguro es nunca compartir imágenes o mensajes personales a través de Internet, incluso con alguien de confianza.

## Los peligros más comunes del sexting son:

- 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.



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-.



## Chantaje en línea | Sextortion

¿Alguna vez te han chantajeado con difundir imágenes, videos o información tuyas si no haces lo que te dicen? La sextorsión ocurre cuando una persona chantajea a otra, amenazándola con compartir imágenes o videos íntimos, con el fin de obtener favores sexuales, dinero, más contenido u otros beneficios.

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 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 todas las comunicaciones para que puedas denunciar o reportar ante las autoridades.

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

The background is a solid blue color with a complex network of white and light blue lines and dots. Scattered throughout are various icons: a globe, a cloud, a Wi-Fi signal, and a starburst. The text "Otros Ciberdelitos" is centered in a bold, white, sans-serif font.

# Otros Ciberdelitos



## Malware

Es un software malicioso diseñado para dañar un sistema, robar información 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 se puede infectar tu dispositivo?

- Mientras buscas contenido y bajas información.
- Al bajar aplicaciones de sitios no oficiales.
- Al conectar dispositivos infectados con 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.
- No utilices softwares piratas.

Recuerda que dependiendo las características del hecho perpetrado esta conducta podría ser sancionada por los artículos 297 BIS, 297 QUATER, 358 QUATER y 358 QUINQUIES, del Código Penal.



# 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
4. Información confidencial.

### 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**



https://



→ Candado en la barra de direcciones

→ Dirección https://

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. Recuerda que tus datos personales se encuentran amparados por la Ley N° 18.331 de Protección de Datos Personales de Uruguay

The background is a solid blue color with a complex network of white and light blue lines and dots. Various icons are scattered throughout, including Wi-Fi symbols, clouds, and globes. The text is centered in a large, bold, white font.

# Consejos para un buen uso de internet



## 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.
- Para madres, padres y tutores: existen herramientas de control parental que permiten configurar la seguridad de los dispositivos y el tiempo de pantalla.

# ¡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 NIÑAS, NIÑOS 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, 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.

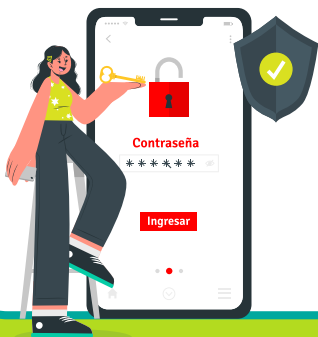
**Evita caer en trampas o engaños:** Hay quienes usan perfiles falsos en redes sociales y otros recursos en internet para poner trampas, robar o simplemente acosar a los demás, ¡ignóralos!

**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 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.
- No puede ser un dato fácil de adivinar (nombre, fecha de nacimiento, etc.).
- No debe dejarse escrita ni guardada sino introducirse cada vez que se use.
- Es un secreto que no debería compartirse con nadie.
- Debe ser cambiada regularmente o cuando hay evidencia o sospecha de que ha sido vulnerada.
- Tiene que ser diferente para cada servicio, red social o app.
- Doble Factor: Actívalo siempre, es una capa de seguridad esencial que evita el acceso no autorizado aunque roben tu contraseña.
- Gestor de Contraseñas: Utiliza un gestor; que requiere memorizar solo una clave (almacena de forma segura y facilita claves únicas).



# CONSEJOS PARA ADULTOS



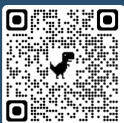
- Aprende a utilizar la tecnología, no tengas miedo a saber cómo funciona el internet.
- Genera una comunicación de confianza con niñas, niños y adolescentes e infórmalos sobre los peligros de las redes sociales.
- Enséñale a niñas, niños y adolescentes que la diferencia entre lo que está bien y lo que está mal es la misma que en la vida real.
- Utiliza controles parentales para restringir el acceso a páginas con contenido no apto para niñas, niños y adolescentes.
- Monitorea el historial de búsqueda del navegador en internet.
- Establece límites de tiempo de uso de tecnología en niñas, niños y adolescentes.
- Crea áreas libres de tecnología, por ejemplo: las habitaciones de las niñas, niños y adolescentes.
- Insiste en que las niñas, niños 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 niñas, niños 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, días y fechas.
- Nunca reenvíes los mensajes o correos electrónicos que tengan fotografías o videos de niñas, niños 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 delegación de la Policía Nacional más cercana a tu domicilio.
- Recuerda que la policía tiene la obligación de tomar tu denuncia.

**Recuerda que también puedes presentar tu denuncia a través de los siguientes canales:**

En cualquier comisaría cercana:



En cualquier sede fiscal del interior del país:



Llamando al 911 o bajando la aplicación "EMERGENCIA 9-1-1"



En Montevideo, en la Unidad de Cibercrimen sita en Carlos Quijano 1316 o en Fiscalía con sede en Carrito 431 (Ciudad Vieja).



# GLOSARIO

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

**Delitos informáticos o cibercrimes:** toda actividad ilícita que se comete mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, y 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:** son programas informáticos que tienen como objetivo alterar el funcionamiento de los dispositivos, 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 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, como computadoras, teléfonos celulares, 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.

[illegible]





Presidencia  
Uruguay

<>agesic

**ANEP** ADMINISTRACIÓN  
NACIONAL DE  
EDUCACIÓN PÚBLICA



**inau**

Instituto del Niño y  
Adolescente del Uruguay



Presidencia  
Uruguay

Junta Nacional  
de Drogas



Ministerio  
del Interior



GLOBAL PROGRAMME ON  
CYBERCRIME



Naciones Unidas  
Oficina contra  
la Droga y el Delito

