



COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

GUÍA DE CIBERSEGURIDAD

dirigido a niñas, niños y adolescentes
para utilizar internet, los dispositivos
de telecomunicaciones y las tecnologías
digitales de forma segura y responsable



Introducción

Hoy en día conectarte a Internet se ha convertido en una acción cotidiana que simplifica en muchas maneras tu día a día.

Internet es una herramienta poderosa para tu desarrollo porque te permite acceder a nuevos conocimientos, comunicarte con familiares y amigos, así como con personas que están a miles de kilómetros de distancia, en todo el mundo. Asimismo, Internet te permite crear y compartir contenidos como imágenes, texto, audios, videos, entre muchos otros.

Internet ofrece una lista interminable de beneficios, pero su uso intensivo también te expone a muchos riesgos y amenazas, como pueden ser el uso indebido de tu información personal o privada (robo o publicación de ésta sin tu consentimiento), sufrir acoso o abuso por parte de personas desconocidas, robo o suplantación de tu identidad, entre otros riesgos que pueden hacer que tu experiencia en internet sea desagradable, incómoda e insegura.

Por eso es muy importante que, como usuario de Internet, puedas identificar y comprender los riesgos y amenazas más comunes a los que te enfrentas al navegar en Internet, y que cuentes con los conocimientos adecuados para hacer un uso seguro y responsable de esta herramienta.

Es decir, es muy importante que desarrolles habilidades y capacidades en ciberseguridad e higiene digital para que aproveches todo el potencial que te ofrece Internet y que, al utilizarlo, tengas una experiencia positiva, que aporte a tu desarrollo y el de tu comunidad.

¿Conoces cuáles son los riesgos más comunes a los que se enfrentan niñas, niños y adolescentes al utilizar dispositivos electrónicos e Internet?

A continuación, encontrarás una descripción sencilla de los riesgos y amenazas más comunes que puedes enfrentar por el simple hecho de navegar en Internet, utilizar tu celular, tableta o computadora, éstos son:

- Ataques a través de códigos maliciosos o malware

- Ataques por medio de técnicas de ingeniería social, particularmente, el Phishing
- Ciberacoso
- Establecer contacto con depredadores en línea

Además, en esta sección encontrarás recomendaciones sencillas que puedes poner en práctica para mantenerte seguro en el mundo digital.

Códigos maliciosos o malware

¿Qué son?

Son programas que están diseñados para introducirse en tu computadora, teléfono celular, tableta y en la red de internet (red Wi-Fi) sin que te des cuenta cuando los instalas o descargas. Entre los códigos maliciosos más comunes se encuentran los malware y virus.

Cuando un código malicioso se encuentra dentro de tu computadora, celular, tableta o red de Internet, puede:

- Acceder a toda tu información, incluyendo tu ubicación en tiempo real y tus listas de contactos
- Acceder a tus fotos y archivos y publicarlos en Internet, redes sociales o chats.
- Adivinar tus contraseñas de correo electrónico, redes sociales y aplicaciones que utilizas y utilizarlas con fines malintencionados.



Algunas señales de que has descargado códigos maliciosos en tu computadora, tableta o teléfono celular son:

- Tu dispositivo está raro o lento
- Las aplicaciones que utilizas se comportan de manera extraña (se abren o cierran sin que tu tengas control de esto)
- Tienes registros de llamadas o mensajes SMS o WhatsApp de desconocidos
- Consumo muy rápido de tus datos
- Se acaba muy rápido la batería
- Aparecen anuncios todo el tiempo o ventanas nuevas
- Tienes aplicaciones desconocidas

En estos casos debes estar alerta al comportamiento de tus equipos y adoptar las siguientes medidas de protección:

- Instala un programa antivirus en tus equipos y actualiza tu suscripción de manera frecuente.
- Actualiza el sistema operativo y las aplicaciones de manera frecuente
- Instala programas y aplicaciones únicamente de fuentes o fabricantes conocidos.
- No descargues programas de páginas web “pirata”
- Utiliza contraseñas seguras en tu red Wi-Fi, tus equipos y tus cuentas en Internet, que incluyan números, letras en mayúsculas y minúsculas, así como símbolos o caracteres especiales.
- Evita conectarte a redes Wi-Fi gratuitas.
- No divulgues tus contraseñas.
- Mantente alerta a los correos o comunicaciones de personas desconocidas, que recibes correo electrónico, chats, WhatsApp, redes sociales, en las que te piden realizar alguna acción con urgencia.

- No descargues archivos tampoco accedas a ligas electrónicas que recibas por medio de comunicaciones que recibas de personas desconocidas.

Técnicas de Ingeniería Social

¿Qué son las técnicas de ingeniería social?

Se le llama ingeniería social a las diferentes técnicas de manipulación, engaño o estafa que usan los ciberdelincuentes para obtener información personal y privada de las personas.

Los ciberdelincuentes engañan a sus víctimas haciéndose pasar por una persona de confianza, para convencerlas de visitar páginas de internet desconocidas, descargar archivos o rellenar alguna encuesta o formulario, con el objetivo de que:

- Facilites datos personales
- Abras enlaces a sitios de internet maliciosos
- Descargues o abras archivos que parecen ser inofensivos, pero que en realidad contienen algún código malicioso.

Las tres técnicas más usuales por medio de las cuales puedes ser víctima de un ataque de ingeniería social son:

- El Phishing: Cuando recibes un correo electrónico de personas desconocidas en los que te piden descargar algún archivo adjunto, hacer click en una liga electrónica, llenar algún formulario o proporcionar información privada, personal o familiar, así como tus contraseñas.
- El Smishing: Cuando recibes un mensaje de texto corto (SMS) de personas desconocidas en los que te solicitan llamar a algún teléfono, ir a un sitio web o descargar información desde un enlace desconocido.
- El Vishing: Cuando recibes una llamada telefónica o mensaje de voz de personas desconocidas, quienes se hacen pasar por personas de confianza, para solicitarte datos personales, de tus familiares y amigos o solicitarte que llesves a cabo alguna acción como visitar un sitio en internet (generalmente malicioso).



Este tipo de técnicas comparten la característica de establecer alguna comunicación contigo por medio de mensajes o frases que llamen poderosamente tu atención para que realices alguna acción de manera inesperada y urgente.

Puedes identificar las técnicas de ingeniería social a partir de mensajes que incluyen:

- Haberte ganado un premio (viajes, dinero, celulares, autos u objetos de gran valor económico)
- Haber sido seleccionado para obtener grandes descuentos, promociones u ofertas
- Mensajes relacionados con la cancelación de alguna de tus cuentas, la falta de espacio en tu dispositivo o cuenta de correo.
- Mensajes relacionados con supuestas infecciones por algún virus
- Mensajes relacionados con la invitación a descargar alguna aplicación, función o programa para avanzar o ganar puntos en algún juego en línea.

¿Qué puedes hacer para protegerte de los ataques con técnicas de ingeniería social?

- Mantente alerta ante correos electrónicos, mensajes de WhatsApp, mensajes SMS, mensajes por redes sociales y llamadas de desconocidos.
- Antes de abrir cualquier enlace o archivo de direcciones de correo desconocidas debes preguntarte: ¿Espero esa información?; ¿reconozco a la persona que envía esa comunicación?; y ¿solicitan que haga algo con urgencia?
- No abras archivos adjuntos o enlaces que provienen de cuentas de correo electrónico de desconocidos.
- No respondas a solicitudes de información personal o familiar por correo electrónico, mensajes de texto o llamadas telefónicas.
- No introduzcas ninguna de tus contraseñas después de hacer clic en un enlace sospechoso.

- Si recibes correos, mensajes o llamadas de personas desconocidas, que te parezcan sospechosos, denúncialos inmediatamente. Existen funciones en tu correo electrónico y redes sociales para hacer estas denuncias.
- Si recibes correos o mensajes de personas desconocidas, que te parezcan sospechosos, procura eliminarlos de tus bandejas de mensajes.

Ciberacoso o Cyberbullying

¿Qué es?

Es una conducta de acoso o intimidación que ocurre utilizando Internet y las tecnologías digitales como medio de ataque, como puede ser:

- A través de mensajes SMS, WhatsApp o cualquier servicio de mensajería instantánea
- En las redes sociales como Facebook, Instagram, Tik Tok y los servicios de mensajería instantánea de estas plataformas las plataformas
- Al utilizar juegos en línea
- En grupos de chats
- Por medio de llamadas y mensajes cortos a los teléfonos celulares, entre muchos otros medios.

El Ciberacoso es un comportamiento que busca atemorizar, enfadar, agredir o humillar a otras personas, algunos ejemplos de esta conducta nociva son:

- Difundir información privada, falsa o vergonzosa de una persona, como pueden ser fotografías o videos privados de alguien en las redes sociales.
- Enviar mensajes, imágenes o videos hirientes, abusivos o amenazantes a través de plataformas de mensajería
- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

Una persona que sufre ciberacoso puede sentirte inseguro, avergonzado, nervioso, ansioso y



tener dudas sobre lo que la gente dice o piensa. Esto puede llevarle a aislarse de sus amigos y familiares, a tener pensamientos negativos y a sentir culpa por cosas que ha hecho o por aquellas que ha dejado de hacer.

Las víctimas de ciberacoso sufren daños importantes en su salud física y psicoemocional:

Su estado físico puede afectarse luego de sufrir estrés, dolores de cabeza, náuseas, dolores de estómago frecuentes, insomnio, falta de apetito o apetito desmedido, abuso de sustancias como el alcohol, el tabaco, entre otras.

Además, el ciberacoso causa daños a la salud emocional y psicológica de las niñas, niños y adolescentes que lo sufren, como consecuencia, las víctimas suelen perder la motivación para llevar a cabo actividades que normalmente disfrutaban y sentirse aislados de las demás personas o perder la confianza en éstas y la autoestima.

También es habitual que quienes sufren ciberacoso se sientan solos, abrumados y desconfiados para pedir ayuda, lo que podría perpetuar los sentimientos y pensamientos negativos que llegan a formar parte de un círculo vicioso.



Es importante tener la sensibilidad y comprender que las personas con discapacidad, las minorías y aquellas que son percibidas como diferentes, se encuentran en un mayor riesgo de sufrir ciberacoso y discriminación en línea.

¿Cómo puedes prevenir ser víctima de ciberacoso?

- Poniendo en práctica las siguientes reglas de comportamiento en línea:
- Practica la “regla de oro”: Actuar con empatía, compasión y amabilidad en cada interacción en línea, y tratar a todos en línea con dignidad y respeto.
- Respetar las diferencias: Apreciar las diferencias culturales, sociales, económicas, físicas y las diferentes formas de pensar y expresarse de los demás, esto significa comportarse de manera reflexiva y evitar los insultos y los ataques personales.
- Haz una pausa antes de actuar en Internet: Detente a analizar y pensar antes de comentar, responder, publicar o enviar información que pueda lastimar a otra persona, dañar su reputación o amenazar su seguridad.
- Piensa antes de publicar o compartir información tuya en plataformas digitales porque puede permanecer en línea para siempre y ser utilizado más adelante para hacerte daño.



- Defiéndete y defiende a demás:
 - Si ves que alguien que conoces sufre ciberacoso, procura ofrecerle tu apoyo tratando de encontrar a un adulto de confianza que pueda ayudarle a afrontar la situación.
 - Reporta cualquier actividad que consideras puede dañar tu seguridad y la de otras personas y conserva pruebas de conductas inapropiadas o peligrosas.
 - No hagas nada que pueda llevar a una persona a pensar que todos están en su contra o que a nadie le importa. Tus palabras pueden marcar la diferencia.
 - Aprende sobre los ajustes de privacidad de tus aplicaciones favoritas para las redes sociales. Algunas de las acciones que puedes realizar son las siguientes:
 - Puedes decidir quién puede ver tu perfil, enviarte mensajes directos o comentar tus publicaciones ajustando la configuración de privacidad de tu cuenta.
 - Puedes informar sobre comentarios, mensajes, fotografías y videos hirientes y pedir que los eliminen.
 - Además de “dejar de ser amigo(a)”, puedes bloquear completamente a alguien para que no pueda volver a ver tu perfil ni contactarte.
 - También puedes elegir que los comentarios de ciertas personas solo las puedan ver ellas mismas, pero sin bloquearlas por completo.
 - Puedes borrar publicaciones en tu perfil o esconderlas de determinadas personas.
 - La mayoría de tus redes sociales favoritas no avisan a quienes tú bloqueas, restringes o denuncias.
- familiares cercanos, un profesor o un amigo y le cuentes lo que te está ocurriendo para que, en conjunto puedan discutir la problemática e identificar las soluciones.
- En la escuela puedes hablar con un consejero, el entrenador deportivo o tu maestro(a) favorito(a), ya sea en línea o en persona.
 - Si no te sientes cómodo(a) hablando con alguien que conoces, comunícate con una línea telefónica de ayuda de la policía cibernética para recibir apoyo profesional o bien, hacer una denuncia:
 - 55 5242 5100 ext. 5086 o al correo electrónico policia.cibernetica@ssc.cdmx.gob.mx.
 - Es conveniente que reúnas pruebas –mensajes de texto y capturas de pantalla de las publicaciones en las redes sociales– para mostrar lo que está ocurriendo.
 - Si el acoso ocurre en una plataforma social, no respondas a los mensajes o comunicaciones que recibes de un acosador, piensa en la posibilidad de bloquearlo e informar sobre su comportamiento en la propia plataforma.
 - Utiliza las opciones de bloquear, silenciar o restringir la cuenta de alguien que te esté acosando, esa cuenta no recibirá ninguna notificación.

Depredadores en línea

Internet es un espacio que facilita la comunicación con familiares y amigos, pero también puede ser un espacio para contactar con una gran diversidad de personas que no conoces y que pueden tener intenciones maliciosas como acosar o abusar de niñas, niños, adolescentes y jóvenes, a través de conductas como el Grooming.

Grooming

¿Qué es el Grooming?

Este tipo de conducta consiste en que una persona mayor de edad establece una comunicación permanente y agradable con niñas, niños y adolescentes, buscando ganarse su amistad y confianza, para convencerlos posteriormente, de realizar actividades como las siguientes:

¿Qué hacer si eres víctima de ciberacoso?

- Es muy importante que te dirijas a alguien de confianza –ya sea tus padres, hermanos,



- Enviar fotos o videos en los que aparezcan desnudos o con poca ropa
- Acudir a una cita secreta para conocerse

Es muy común que este tipo de acosadores lleguen a amenazar a las niñas, niños y adolescentes de la siguiente forma:

- Publicar aquellas fotos o videos que enviaron y avergonzarlos frente a padres, familiares, amigos u otras personas.
- Hacerle daño a sus familiares y amigos si los menores dejan de enviar este tipo de contenidos o hablan con sus familiares.

El grooming puede tener muchas consecuencias negativas en la salud mental y desarrollo de niñas, niños y adolescentes quienes pueden sentir estrés, vergüenza, culpa, ansiedad, depresión y miedo.

¿Qué puedes hacer para prevenir ser víctima de un depredador en línea? Es importante que adoptes las siguientes recomendaciones:

- No compartas información confidencial o de tipo personal (nombre completo, fecha de nacimiento, dirección, número de teléfono) con personas desconocidas.
- Utiliza un alias/nombre alternativo o apodo como nombre de usuario si interactuar con otros en línea.
- No interactúes con extraños a través de Internet ni aceptes solicitudes de amistad de personas que no conoces.
- No publiques en redes todas tus actividades cotidianas ni las de tus familiares o amigos.
- No envíes fotografías ni videos personales a desconocidos, especialmente si estos son con poca o nula ropa. Tampoco las compartas por redes sociales, aplicaciones (apps) o chats.
- No abras ni respondas correos electrónicos ni archivos adjuntos de desconocidos.
- No respondas a mensajes de desconocidos ni visites páginas web que soliciten información personal.

- No organices encuentros con desconocidos ni accedas a hacerlo si algún extraño te lo pide.
- Informa inmediatamente a un adulto, amigo o persona de confianza si algún extraño te pide el envío de fotos o videos íntimos con poca o nula ropa o bien si te pide que se vean en algún sitio.

El Sexting

¿Qué es el sexting?

Es la conducta por medio de la cual cualquier persona de forma voluntaria produce y envía a otra persona, textos, fotos o videos de sí mismo, de carácter sexual, mediante el uso de un dispositivo como teléfono, computadora o tableta. Aunque hacerlo es una decisión muy personal, es importante pensar muy bien antes de llevar a cabo este tipo de actividades y estar consciente de que es una práctica riesgosa.

El riesgo de practicar el sexting radica en que, una vez que se envían estos contenidos a otra persona, éstos permanecen en Internet por tiempo indefinido y pueden ser utilizados de forma dañina por más personas.

¿Qué tipo de acciones debes realizar al practicar el sexting, para evitar incidentes negativos?

- Asegúrate de que la persona con la que compartes textos, imágenes o videos tuyos, es digna de tu confianza y que existe un mutuo acuerdo de cuidar la privacidad e intimidad de ambos.
- Confirma que la otra persona desea recibir este tipo de contenidos ya que puede ser que no lo desee o no sea de su agrado y lo sienta como un ataque o intimidación.
- Si Compartes textos, fotografías o fotografías de ti mismo, con contenido sexual, borra o excluye cualquier detalle o información que pueda identificarte, dejando fuera rostro, cicatrices, tatuajes o marcas características tuyas.
- Si recibes contenido de carácter sexual de otra persona, con o sin el consentimiento de esa persona, es importante que lo reportes a las autoridades, no lo compartas por ningún medio electrónico y lo elimines de tus equipos.





Poner en práctica permanente las recomendaciones y medidas de ciberseguridad que se presentan en esta Guía, fortalece la adopción de buenos hábitos para identificar riesgos y amenazas de ciberseguridad y prevenir ser víctimas de los ciberdelincuentes.

Además, al poner en práctica esta Guía, aportas tu granito de arena para crear una cultura de valores en torno al aprendizaje y uso de Internet y las tecnologías digitales, de manera positiva y constructiva, en beneficio de tu entorno y tu comunidad.

Lo que nos lleva a discutir brevemente el concepto de Civismo Digital y su importancia...

¿Qué es el Civismo Digital?

El Civismo Digital tiene como objetivo que cada persona se convierta en ciudadana o ciudadano digital capaz de conocer y ejercer sus derechos y responsabilidades en el uso de Internet y las tecnologías digitales. Los ciudadanos digitales asumen un conjunto de acuerdos de convivencia para contar con una experiencia agradable en el uso de Internet y las tecnologías, así como aprovechar todo su potencial, con base en el respeto mutuo.

Los acuerdos de convivencia del ciudadano digital son:

- Utilizar un lenguaje amable en redes y dirigirse a los demás con respeto.

- Respetar las opiniones y expresiones de los demás.
- Pedir permiso a las personas antes de publicar información, fotos o videos de éstas.
- Comunicar a otras personas lo que pueden publicar y lo que no, sobre tu persona.
- Saber que NO representa un problema rechazar o ignorar solicitudes de amistad, invitaciones a eventos, grupos o comunidades en línea.
- Si surge un problema, buscar solucionarlo de manera personal y directa y no a través de redes sociales o medios digitales.
- Tratar de reaccionar de manera calmada y no violenta ante algo que te moleste.

Al practicar recomendaciones básicas de ciberseguridad, así como al adoptar una ciudadanía digital responsable, estarás aportando tu granito de arena para hacer del mundo digital un mundo más seguro, incluyente, productivo, ameno, respetuoso de la privacidad y de los derechos de las niñas, niños, adolescentes y jóvenes.



