GTO Grandeza de México

Secretaría de Seguridad Pública

# CIBERSEGURIDAD

## CIBERGUIA

Hoy en día, el uso de las tecnologías de la información y comunicación son de suma importancia para el desarrollo de las actividades diarias de la sociedad en general.

A través de ellas se han facilitado muchos aspectos de la vida cotidiana. Sin embargo, esta facilidad que nos proporciona el ciberespacio, también trae consigo riesgos que, en muchas ocasiones, sin darnos cuenta pueden ocasionar daños, tanto en el trabajo como en la vida personal e incluso en la economía.

En ese sentido, la Secretaría de Seguridad Pública, refrenda el compromiso que tiene con la sociedad, y por ello presenta a través de esta Ciberguía, diferentes herramientas para facilitar la comprensión de conceptos relacionados a la ciberseguridad. De esta manera, ofrece orientación para evitar ser víctimas de los delincuentes y datos de contacto ciudadano para reportar incidentes cibernéticos.

Recuerda que la SSP trabaja constantemente para la protección y cuidado de la ciudadanía.

**¡POR UNA NAVEGACIÓN SEGURA, QUE LA SEGURIDAD Y PROTECCIÓN EN EL CIBERESPACIO SE VUELVA CULTURA!**

1. Seguridad durante el teletrabajo
2. Contraseñas seguras
3. Malware y Ransomware
4. Phishing: Estafas de suplantación de identidad
5. Noticias falsas
6. Técnicas de Ingeniería Social
7. Fraude electrónico
8. La reputación en el ciberespacio
9. Seguridad en dispositivos móviles.
10. Lineamientos para identificar y reportar páginas falsas
11. Ley Olimpia
12. Seguridad en redes sociales y comunidades virtuales
13. Seguridad en el uso del correo electrónico

**Decálogo de Ciberseguridad de la SSP**

## Teletrabajo y sus beneficios

**Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades de trabajo, utilizando como soporte las tecnologías de la información y comunicación (TIC), sin que se requiera la presencia física del trabajador en un lugar específico de trabajo.

El factor determinante y que ha impulsado la transformación digital de todos los sectores es el distanciamiento social, a causa del Coronavirus.

**FLEXIBILIDAD DE HORARIO**
para compaginar la vida laboral y familiar.

**INSERCIÓN LABORAL**
para las personas con dificultades de movilidad.

**MENOR ESTRÉS**

Sin embargo, el teletrabajo también tiene áreas de **OPORTUNIDAD** que dependen en gran parte de quien lo ejerce.

**AHORRO DE TIEMPO Y DINERO**
en traslados a los centros de trabajo. Reducción del uso de recursos en las instalaciones.

**REDUCCIÓN DEL TRÁFICO**
y descongestión en los servicios de transporte público.

## Problemas asociados al teletrabajo

Trabajar remotamente sin seguir las pautas de seguridad genera un riesgo para todos los empleados o servidores públicos, lo cual puede ser aprovechado por los ciberdelincuentes de la siguiente forma:

1. Infectan nuestros dispositivos por virus o malware
2. Roban, alteran o dañan la información que usamos
3. Roban nuestra identidad y pueden difamarnos
4. Defraudan
5. Espían

## Medidas para evitar riesgos en el teletrabajo

**1 |Usar Antivirus**

**2 |Mantener actualizados todos los programas**
considerando aplicaciones, navegadores web y sistemas operativos.

**3 |Respaldar los archivos**
en medios de almacenamiento externos o en la nube.

**4 |Usar contraseñas seguras**
diferentes y para todos los dispositivos.

**5 |Encriptar**
equipos y medios de almacenamiento utilizados.

**6 |Usar llaveros electrónicos**
para guardar usuarios y contraseñas.

**7 |Resguardar usuarios y contraseñas**
en los lugares de trabajo.

**8 |Cuidar dispositivos o medios de almacenamiento**
en lugares públicos.

## ¿Qué son las contraseñas seguras?

Una contraseña es un método de autenticación que utiliza información secreta para controlar, ya sea denegando o permitiendo el acceso hacia algún recurso que es considerado como restringido.
Las contraseñas son el recurso más común de la seguridad digital, que protege el acceso a:

**Servicios que se consumen en Internet**
(correo, redes sociales, servicios bancarios, servicios comerciales y educativos).

**Dispositivos electrónicos que utilizamos para realizar nuestras actividades**
(tabletas electrónicas, celulares, teléfonos inteligentes y computadoras).

**Archivos protegidos (de cualquier tipo)**
Una contraseña es segura cuando cumple con criterios de:

- **Longitud**
- **Complejidad**
- **Uso con responsabilidad**

## Riesgos de no usar contraseñas seguras

Actualmente, existen personas que buscan descifrar nuestras contraseñas para ingresar a los recursos tecnológicos que usamos y extraer de ellos información valiosa para obtener un beneficio de ello.

Como responsables de la información, podemos obstaculizar sus propósitos, ya que su éxito depende de lo bien que sepamos elaborar contraseñas seguras y las usemos de manera responsable.

## Recomendaciones para generar una contraseña segura

### Tips para generar una contraseña:

**1.** Piensa en una frase que tenga algún significado con un mínimo de 10 caracteres incluyendo números.

**contraseñas seguras 4235**

**2.** Utiliza mayúsculas y minúsculas.

**ContraseñA SeGUra 4235**

**3.** Quita los espacios.

**ContraseñASeGUra4235**

**4.** Convierte las vocales en números.

**0ntr4s3ñ4S3GUr44235**

**5.** Utiliza caracteres especiales (!¡*+-_$%&@).

**C0ntr4s3ñ4_S3G&r4_4235***

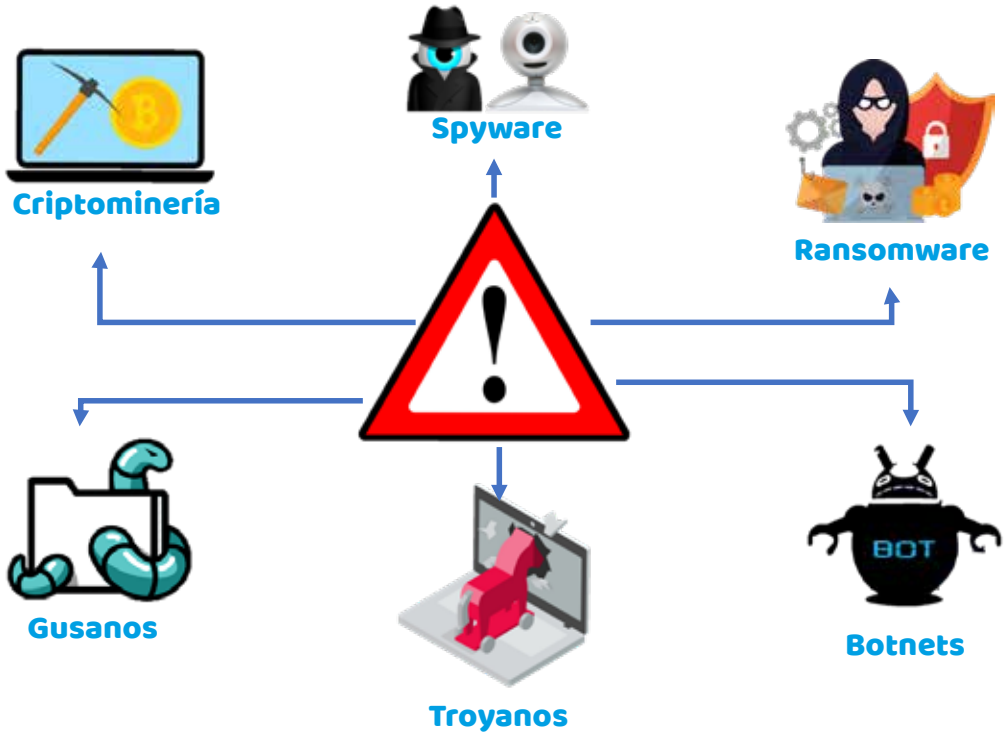
## ¿Qué hemos aprendido del uso de las contraseñas seguras?

- NO las compartas
- EVITA utilizar la misma para todos tus archivos, servicios y dispositivos.
- NO las escribas en libretas o papeles.
- NO las mantengas visibles en ningún lugar.
- Cambia las contraseñas periódicamente.
- Utiliza un llavero electrónico que te permita crear y encriptar de forma fácil y segura listas de usuarios y contraseñas.

Partamos de que el SOFTWARE es un programa informático que está presente en todos los dispositivos electrónicos. Permite que las personas puedan interactuar con éstos.

Existen distintos tipos de software y en particular hay uno que está diseñado para generar daño en ese entorno de funcionamiento habitual, y a ese se le denomina “MALWARE”:

Software que realiza acciones en un sistema informático de forma intencional y sin el conocimiento del usuario



Este tipo de ataque inicia con un análisis previo de los atacantes, quienes se encargan de reconocer a la empresa, la información que se maneja en  ella, e incluso, tienen datos sobre la interacción entre las personas (el tema de Ingeniería Social que veremos más adelante), el cual usan y disfrazan para lanzarlo como “gancho” y engañar a las posibles víctimas infectando sus equipos.

# 3. Proceso del Ransomware

1. Un usuario recibe un correo spam con archivos adjuntos trampa, en formatos PDF o Word.
2. Al abrir los archivos, el usuario es dirigido a un sitio desde donde se descarga e instala el software malicioso, propagándose dentro de la red de trabajo.
3. Una vez instalado, el software identifica los archivos más comunes y los cifra. En algunos casos todo el sistema operativo es cifrado.
4. La víctima recibe una solicitud de rescate con instrucciones de cómo realizar el pago, normalmente es en bitcoins.
5. La víctima compra bitcoins y las transfiere a la dirección Bitcoin del atacante. Envía el comprobante de la transferencia como prueba del pago.
6. Realizada la transacción, el cibercriminal debería enviar las instrucciones de decodificación a la víctima.

## Recomendaciones para evitar ser víctima del Ransomware

- Desactiva la reproducción automática de dispositivos de almacenamiento externo, como discos y USB.
- No confíes en correos con programas o archivos ejecutables adjuntos, presta atención a su extensión.
- Evita el software ilegal y pirata, ya que puede contener Malware.
- Usa cuentas de usuarios sin permisos de administrador.
- Si recibes archivos, anuncios o enlaces no esperados, pregunta a la persona si los ha enviado. El sistema podría infectar y propagar el Malware.
- Haz copias de seguridad de tu información periódicamente.
- Mantén los programas y el sistema operativo actualizados.
- Instala un antivirus con capacidad proactiva de detección.

## ¿Qué hemos aprendido del Malware y Ransoware?

Aunque el Ransomware en muchas ocasiones va dirigido a grandes empresas, nuestros equipos personales no están exentos de ser el objetivo de este tipo de ataques.

Como empleados y servidores públicos, tenemos una gran responsabilidad para prevenir un posible ataque, pues de otra manera, cerremos la brecha entre los ciberdelincuentes y las empresas o instituciones.

Es por ello que debemos hacer uso consciente de los recursos tecnológicos y tomar las precauciones adecuadas.

Principalmente, tenemos que revisar la información y recursos con los que estamos interactuando, ya sean correos electrónicos, sitios web o dispositivos de almacenamiento externos.

## ¿Qué es el Phishing?

Es una práctica que un ciberdelincuente les lanza a las víctimas para lograr obtener los datos de la persona(víctima) realizando algún tipo de envío de mensaje en el que solicitan la autenticación o el ingreso a una cuenta de apariencia oficial.

Particularmente, el acto de robar la identidad se usa de manera ilegal para abrir cuentas bancarias, contratar líneas telefónicas, seguros de vida, realizar compras e incluso, en algunos casos, para el cobro de seguros de salud, vida y pensiones.

## Recomendaciones para evitar ser víctima del Phishing

### Después de leer un correo no hacer clic en ningún enlace.

Realizar las verificaciones pertinentes en el espacio personal del cliente, acudiendo directamente desde la URL del navegador.



### Mejorar la Seguridad del dispositivo

Se deben tener las actualizaciones más recientes del sistema operativo y navegador web.

### Protección de dispositivos

Se debe tener un antivirus instalado y con una licencia vigente

## Recomendaciones para evitar ser víctima del Phishing

### Introducir los datos confidenciales sólo en sitios web seguros

Para que un sitio pueda ser considerado como seguro, su dirección web debe comenzar con **https://**, lo cual indica que sigue el protocolo de transferencia de hipertexto. También el navegador deberá mostrar el ícono de un candado verde cerrado.


### Ante cualquier duda, no arriesgarse

El mejor consejo ante el phishing es fomentar siempre la prudencia entre todas las personas.


### Revisar periódicamente las cuentas

Nunca está de más revisar facturas y cuentas bancarias con frecuencia para estar al tanto de cualquier irregularidad en las transacciones.

## ¿Qué son las noticias Falsas?

Siempre han existido las noticias engañosas o también conocidas como fake news, pero a partir de la proliferación de Internet y de las nuevas tecnologías de la información y comunicación, este tipo de información se ha viralizado con facilidad debido a:

La probabilidad de desestabilizar políticamente un país, trae beneficios para sectores opositores.


No existe un método automatizado para identificar este tipo de noticias, pues se requiere sentido común.

Facilidad de difusión.


En algunos casos, la difusión de este tipo de noticias significan ganancias económicas.

Las personas u organizaciones que las publican pueden ocultarse a través de perfiles falsos y por tanto no se hacen responsables de esa información.

## Problemas que desencadenan las noticias falsas

Las noticias falsas se emiten con la intención de:

1. Inducir el error
2. Manipular decisiones individuales
3. Desprestigiar o enaltecer a una institución, entidad o persona
4. Obtener ganancias económicas o rédito político

**1 | Los títulos no resumen con exactitud el contenido de la nota periodística**, por lo tanto, el consejo es no confiar en los titulares.

**2 | Identificar una URL falsa**, Examinar las URL asociadas a la nota.

**3 | La noticia pide creer en ella y no cita sus fuentes.**

**4 | Las fotografías utilizadas en este tipo de noticias suelen ser manipuladas.** Se debe verificar que las fotos sean auténticas.

**5 | Manifiesta opiniones en contra o a favor de alguna situación o persona.** El periodismo debe mostrar neutralidad de los hechos y debe permitir al lector formar su propia opinión.

**6 | Se recomienda consultar otras noticias**, pues si en ninguna otra fuente se informa sobre el tema, es posible que sea falsa.

**7 | El contenido se aprecia con lenguaje inapropiado, errores de ortografía y diseño.** Se debe mantener una actitud crítica cuando se lea una historia.

## ¿Qué son las Técnicas de Ingeniería Social?

Son técnicas utilizadas -en su conjunto o individualmente- para engañar a los usuarios incautos de servicios electrónicos o responsables de información electrónica privilegiada.

Consumidores de servicios digitales y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de protegerse ante este tipo de ataques, pues son muy diversos.

## Diversidad de ataques con el uso de las Técnicas de Ingeniería Social

Son técnicas utilizadas -en su conjunto o individualmente- para engañar a los usuarios incautos de servicios electrónicos o responsables de información electrónica privilegiada.

Consumidores de servicios digitales y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de protegerse ante este tipo de ataques, pues son muy diversos.

### Ataque a nivel físico

#### Por teléfono

El perpetrador llama a la víctima hacíendose pasar por un técnico de soporte o empleado de las misma organización.

### Ataque a nivel psicológico y social

#### "Exploit de familiaridad"

El atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por uno de ellos.

## Vía Internet


Por medio de correo electrónico, web o conversando en salas de chat, servicios de mensajería o foros.

## Ataque vía SMS


Se envía un mensaje SMS a la víctima haciéndole creer que es una promoción o servicio. Si lo responde, puede revelar información personal y ser víctima de robo.

## Dumpster Diving O Trashing

Busca información de la víctima en la basura como: agendas telefónicas de trabajo o unidades de almacenamiento (CD's, USB's, etc).

## Cara a Cara

Las personas susceptibles a este ataque son las más "ingenuas", (no es un reto para el atacante si elige bien a su víctima).
Para este ataque, el perpetrador requiere tener una gran habilidad social y extensos conocimientos.

## Situación Hostil

Crear una situación hostil donde hay vigilantes, esto provoca el suficiente estrés para no revisar al intruso o responder sus preguntas.

## Leer el lenguaje corporal

El lenguaje corporal puede generar una mejor conexión con la otra persona.

## Empleo en el mismo lugar

Obtener un empleo donde la víctima labora. Resulta más fácil si trabaja en una pequeña o mediana empresa

## Explotar la Sexualidad

El atacante juega con los deseos sexuales de la víctima haciendo que baje la percepción y sus defensas

# 6. Recomendaciones para proteger información ante terceros

**1 |** No divulgar datos sensibles con desconocidos o en lugares públicos (redes sociales, anuncios o páginas web).


**2 |** Si se sospecha que alguien intenta realizar un engaño, hay que exigir que se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del individuo.

**3 |** Implementar políticas de seguridad en las empresas y organizaciones y que éstas sean conocidas por los colaboradores.

**4 |** Realizar rutinariamente auditorías y pruebas de vulnerabilidades a través de la Ingeniería Social para detectar huecos de seguridad de esta naturaleza.

**5 |** Llevar a cabo programas de concientización sobre la seguridad de la información.

**El fraude electrónico** es un tipo de **estafa que se realiza por medios digitales** y en conjunto con distintas técnicas convencionales de la Ingeniería Social.

Las personas que hacen operaciones a través de medios electrónicos, como banca y comercio electrónico, son las principales víctimas, ya que en ocasiones su desconocimiento de los riesgos facilita a los delincuentes este tipo de prácticas.

Existen diversos tipos de fraudes, pero los más comunes son los **bancarios:**


## VISHING

**Se obtiene información de cuentas y tarjetas bancarias** para retirar dinero en cajeros o realizar movimientos entre cuentas bancarias.


## PHISHING Y SPOOFING

Gancho de información que envían los cibercriminales por correo electrónico y otros medios, como mensajes SMS y WhatsApp, para dirigir a las víctimas a un sitio falso en donde ingresan sus datos de inicio de sesión y son robados **(spoofing).**


## COMERCIO ELECTRÓNICO

Vendedores falsos que ofrecen productos y servicios, y al recibir el pago dejan de responder y el comprador no recibe respuesta sobre el estado de su pedido ni la devolución de su dinero.

## SCAM

Los cibercriminales ofrecen un gancho (una herencia ficticia o un supuesto billete de lotería premiado) por el que piden una pequeña cantidad de dinero como adelanto o varias cuotas antes de recibir un gran premio. Los Scams se basan más en engaños y técnicas de Ingeniería Social, que en las habilidades informáticas de los delincuentes.

Para evitar los fraudes por Internet o minimizar las situaciones de vulnerabilidad, te recomendamos lo siguiente:

1. **No confíes en precios sospechosamente bajos.**
2. **Duda de páginas que tengan muchas ofertas.**
3. **Verifica el registro e información de la empresa que oferta.**
4. **Consulta referencias y opiniones sobre la empresa.**
5. **Cuida la información personal bancaria: actualiza usuarios y contraseñas y usa distintos métodos de autenticación que ofrecen las plataformas de banca en línea.**
6. **Evita utilizar sistemas de giros de pagos o transferencias anónimas.**
7. **Utiliza contraseñas seguras y únicas para cada servicio.**

8. No entres al correo electrónico o banca en línea en lugares públicos.

9. Antes de entrar en una página web, asegúrate que no sea falsa.

10. Mantén el antivirus de tus dispositivos actualizado.

11. Si dudas de la identidad de las personas que solicitan información, pide que se identifiquen plenamente y comprueba los datos.

En ningún caso facilites claves de acceso; y si las otorgaste cámbialas inmediatamente.

Para evitar los fraudes por Internet o minimizar las situaciones de vulnerabilidad, te recomendamos lo siguiente:

La reputación en el ciberespacio es acumulativa en el tiempo. Internet no permite el olvido fácilmente, ya que siempre se deja un rastro o una huella difícil de borrar.

La reputación en el ámbito digital se genera a través de una gran cantidad de datos de carácter personal que pueden ser localizados con extrema facilidad, incluso sin que seamos conscientes de dicha situación.

Riesgos de Identidad y la Reputación en el Ciberespacio


**1 | Suplantación de nuestra identidad digital**

Sucede cuando alguien se apropia de nuestra identidad digital y actúa en nuestro nombre.

## 2 | Riesgos en la privacidad

Normalmente publicamos una gran cantidad de información en la red, sin ser plenamente conscientes de que en el momento en que la publicamos perdemos el control sobre sus posibles usos y difusión.


## 3 | Riesgos sobre la reputación On line

Normalmente publicamos una gran cantidad de información en la red, sin ser plenamente conscientes de que en el momento en que la publicamos perdemos el control sobre sus posibles usos y difusión.

## 3 |Vulneración de los derechos sobre propiedad intelectual

En muchas ocasiones, los cibernautas tienen la percepción de que todo lo que está en Internet se puede usar libremente, sin embargo, esto no es así. Las personas vulneran los derechos de otras al relacionarlos con contenidos de terceras personas, por ejemplo: imágenes, audios o cualquier tipo de contenido que haya sido registrado.

## ¿Qué hemos aprendido del Malware y Ransoware?

El contenido publicado en una página web o en las redes sociales es muy importante porque a través de éste comunicamos.


Hay que cuidar la información que se publica.

Se recomienda dedicar tiempo al diseño y creatividad de las redes sociales que nos representen, ya que esto determinará la percepción inicial de las personas.

Debemos ser coherentes, que nuestra personalidad y vida digital coincidan con la realidad.


Hay que evitar las reacciones inadecuadas ante las críticas o cualquier circunstancia.

La mejor manera de prevenir es contar con un sentido común desarrollado y ser conscientes de que la información que mostremos casi siempre será pública.

## Seguridad en dispositivos móviles

Un dispositivo móvil es todo aquel aparato electrónico que cuenta con autonomía propia, conectividad a redes de datos celulares y wifi. Se caracterizan por no usar cables e integran todos los periféricos de entrada y salida en un solo componente

Al permitir una amplia movilidad y por la gran cantidad de información que almacenan, estos dispositivos representan un serio problema de seguridad cuando no se toman las medidas básicas necesarias para proteger los datos que contienen.

### Consejos para mantener seguro el dispositivo móvil

**1 |** Activar la protección y bloqueo con una contraseña, validación biométrica o patrón de malla durante tiempos cortos de inactividad y utilizar aplicaciones que permitan el uso de los distintos factores de autenticación.

**2 |** No desatender los dispositivos en lugares públicos y menos desbloqueados.

**3 |** Activar la función de encriptar el dispositivo y unidades de almacenamiento si la opción está disponible.

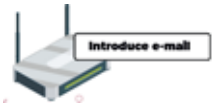
**4|** Activar la función de encriptar el dispositivo y unidades de almacenamiento si la opción está disponible.

**5 |** Mantener actualizado el sistema operativo hasta su versión más reciente.


**6 |** Apagar wifi, infrarrojo y Bluetooth cuando no se usen estas conexiones.

**7 |** Evitar conectar los dispositivos en centros de carga públicos o en equipos de cómputo de desconocidos.

**8 |** No establecer conexión a redes inalámbricas públicas o que te solicitan información personal.




**9 |** Reparaciones en sitios seguros siempre que sea posible. Antes de entregar un equipo a un servicio técnico procura eliminar o respaldar tu información o pide que el dispositivo sea reparado frente a ti y retira todas las unidades de almacenamiento antes de entregarlo.

**10 |** Utiliza el control parental cuando los dispositivos sean utilizados por niños.

**11 |** Procura que las cámaras de tus dispositivos estén cubiertas físicamente, principalmente en las laptops.

**12 |** Descarga y usa únicamente programas que estén disponibles en tiendas oficiales.

**13 |** Usa un antivirus profesional y con soporte.

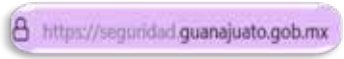
**14 |** Activa la función “Localizar y Recuperar Dispositivo” que ofrecen los fabricantes de los equipos, pues será de gran ayuda para encontrar el aparato cuando éste haya sido
extraviado e incluso sea posible restaurarlo a sus valores de fábrica cuando no se recupere.

# 10. Lineamientos para idénticar y reportar páginas falsas

En internet se puede encontrar información muy diversa publicad a en páginas web. Es conveniente identificar si estas páginas son legítimas para prevenir delitos como fraudes, estafas y extorsión. A continuación, te presentamos algunos criterios para identificarlas:

## Procedimiento

**1 |** Identifica en la barra del navegador (antes de la dirección electrónica) si se indica que la conexión es segura y verifica si existe un candado cerrado.




**2 |** Comprueba que la URL de la página contenga en el nombre la referencia a la institución, organización o marca a la cual dice pertenecer.

**3 |** Observa las imágenes que se exhiben en la página de inicio (si tienen baja calidad); secciones de carruseles o pestañas para identificar si corresponden con el sitio de interés. Observa si el texto tiene mala ortografía y/o redacción, lo cual confirmará la incoherencia de la información publicada.

**4 |** Al ingresar a un sitio web seguro, normalmente se debe presentar el Aviso de Privacidad, así como la autorización del uso de rastreadores o herramientas de recopilación de datos de los usuarios (cookies).


**5 |** Verifica en el pie de página los números telefónicos, dirección física, redes sociales o sellos de confianza que permitan generar certeza de la empresa o institución.


## Identificación de páginas no autorizadas del Gobierno

Actualmente, todas las páginas del Gobierno Federal inician con:
www.gob.mx, por lo que cada apartado de alguna secretaría, institución, Órgano Administrativo Desconcentrado, entre otras, deberá comenzar con el mismo dominio.

# 10. Lineamientos para idénticar y reportar páginas falsas

Las redes sociales institucionales mantienen la misma identidad gráfica, por lo que se recomienda verificar imágenes, colores, tipo de letra y textos que se exhiben para no seguir sitios engañosos o prevenir la divulgación de información falsa.

Asimismo, se debe poner atención en fechas de creación, número de seguidores, cantidad de interacciones, y en especial, en Twitter se coloca un signo de verificación (ícono de la paloma azul) en las cuentas oficiales.

Cada página institucional o cuenta en redes sociales presenta el sello oficial, los números de contacto, dirección o ubicación y políticas de privacidad.


## Verificación de páginas en comercio digital

Compara con otros sitios los precios de los productos, los cuales deben mantenerse dentro del rango; en caso contrario, si se presentan ofertas muy atractivas, probablemente se trate de un fraude.

# 10. Lineamientos para idénticar y reportar páginas falsas

Antes de realizar una compra en Internet, si desconoces la seguridad de la empresa se puede buscar en la página de la PROFECO, si el proveedor forma parte de CONCILIANET para que en caso que no se reciba el servicio o producto contratado y/o comprado, se pueda llegar a un acuerdo con el proveedor, posterior a la transacción.

Esta información se puede consultar en la sección “liga de interés” de la página oficial de la PROFECO o a través del siguiente enlace.

**https: //concilianet.profeco.gob.mx/Concilianet/ inicio.jsp**

Se puede buscar a los proveedores en la página de la PROFECO, en el apartado: **LIGAS DE INTERÉS-MONITOREO DE TIENDAS VIRTUALES.** Esta herramienta permite a los consumidores revisar si los sitios de los vendedores que realizan transacciones a través del comercio digital cumplen con la Ley Federal de Protección al Consumidor.

**https://www.profeco.gob.mx/tiendasvirtuales/index.html**


## Denuncias

En caso de identificar una página falsa puedes presentar la denuncia al correo electrónico: **seguridad@guanajuato.gob.mx**, si sospechas que el sitio web o cuenta de una red social sufrió una violación a la seguridad se debe reportar al:

**https://www.profeco.gob.mx/tiendasvirtuales/index.html**

089 DENUNCIA ANÓNIMA

911 EMERGENCIAS

**Ley Olimpia** se le denomina a un conjunto de reformas legislativas en varios estados de México encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como **CIBERVIOLENCIA.**

## ¿Qué es la Ley Olimpia?

## Violencia Digital:

Acoso, hostigamiento, amenaza, vulneración de datos e información privada, difusión de contenido sexual (fotos, videos o audios) sin consentimiento a través de las redes sociales, que atenta contra la integridad, vida privada y los derechos, principalmente de las mujeres.

## Reconoce:

La violencia digital: ciber venganza, ciberporno y acoso sexual.

## Castigará los actos de :

Elaboración de imágenes audios o videos simulados de contenido sexual íntimo sin el consentimiento de la persona implicada o mediante engaño.

## Contempla como delito:

Difusión, exhibición, divulgación, almacenamiento, tráfico de contenido sexual, de videos, fotos o audios, sin consentimiento, a través de medios digitales como las redes sociales, mensajería o sitios de Internet.

## Agravantes:

Cuando la víctima sea familiar hasta tercer grado en línea recta o cuando hubiese existido una relación sentimental, educativa o laboral entre el agresor y la víctima.

## Medidas de prevención vs. la violencia digital

**Alfabetización digital**

**Control de contenido**

**Educación sobre violencia de género**

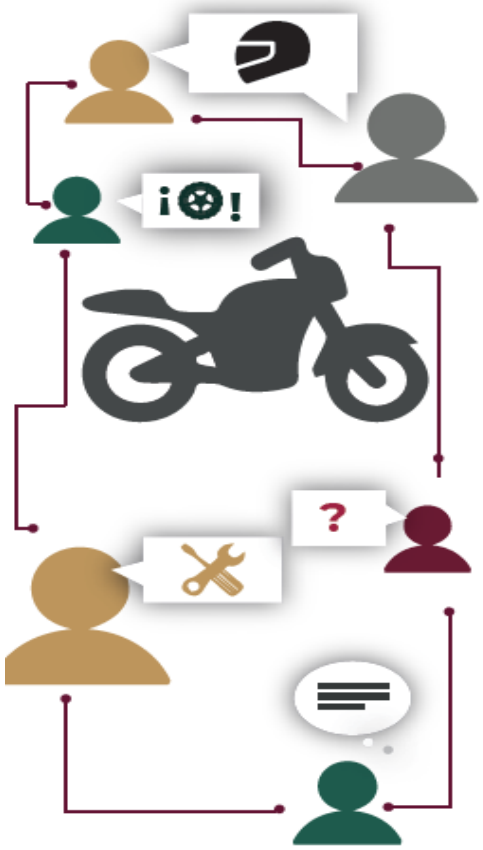

**Identificar el SEXTING y practicarlo con precaución**

## ¿Qué son las redes sociales y comunidades virtuales?


Es un foro, página o red social enfocada a una idea en común, donde todos los usuarios comparten y disfrutan alguna de las facetas que la componen.

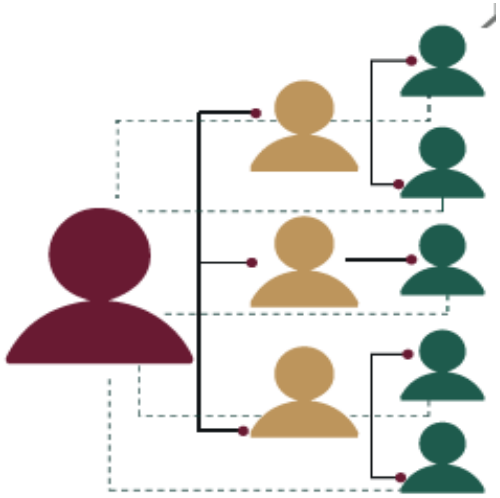
Un ejemplo es un grupo de aficionados en el que la temática son las motocicletas y se divide en foros sobre distintos tipos de motos.

Los usuarios activos aportan contenidos específicos, mientras que los roles pasivos obtienen esa información con diversas intenciones: adquirir uno de estos vehículos, saber si lo que les sucede mecánicamente es normal, encontrar repuestos, etc.



Es una red de relaciones que habitualmente se centra en uno mismo.

En el centro yo y luego los amigos de primer nivel, los amigos de mis amigos, etc., y todo ello conforma un sistema que usa páginas y aplicaciones.



## Problemas de comunidades virtuales y redes sociales

Al hacer uso de las comunidades virtuales como en las redes sociales corremos algunos riesgos que es mejor conocer para evitar ser víctimas:

1. **Desinformación:**
La información que circula en foros y en redes sociales no siempre es verídica, se debe confirmar en otra fuente.

2. **Robo de información:**
a menudo las personas roban tu información y datos personales para la venta de las mismas, ¡cuidado con lo que publicas!

3. **Suplantación de identidad:**
Las personas no siempre son lo que dicen ser, buscan obtener beneficios a base de engaños, ¡no caigas!

4. **Chantaje o extorsión:**
cuando una persona obtiene información, archivos sensibles o personales, tratarán de chantajearte para obtener beneficios con base en tu temor.

# 12. Seguridad en redes sociales y comunidades virtuales

**1 | Nunca subas fotos ni videos comprometedores a Internet.**
Pueden llegar a manos extrañas y utilizarlos para hacerte daño.

**2 | Evita brindar datos exactos en tus perfiles.**
Pueden terminar con desconocidos y ser utilizados para fines delictivos.

**3 | Configura tus perfiles para que solo lo vean tus amigos directos.**
Entre menos expuesto estés tendrás mayor seguridad.

**4 | No se recomienda el uso de redes sociales en menores de 14 años.**
A menos que tengan la super visión de los padres en todo momento.

**5 | Desconfía de los datos que te dan usuarios desconocidos.**
Pueden ser falsos, al igual que las imágenes.

**6 | Utiliza estos medios respetando a los demás.**
Todo lo que haces y difundes en Internet demuestra quién eres, tanto en la red como en la vida cotidiana.

**7 | Actúa bajo las normas éticas y cívicas que te rigen.**
Pueden terminar con desconocidos y ser utilizados para fines delictivos.

**8 | No compartas información financiera ni ubicaciones que vulneren tu integridad.**

**9 | Si eres víctima de** chantaje, extorsión, suplantación de identidad o algún otro delito cibernético, ¡no te calles!

**Repórtalo a las autoridades**

## Seguridad en videojuegos online


Son aquellos videojuegos que para jugarlos requieres de una conexión a Internet, independientemente de la plataforma. Puede tratarse de una sesión multijugador, en las que se interactúa con otras personas que se conectan desde una PC o una consola.

### ¿Cuáles son los riesgos de los videojuegos online?

Desde el ciberacoso hasta los depredadores online y los costos ocultos, hay muchas preocupaciones al hacer uso de los videojuegos online.

**1 | Ciberacoso:**

Existen distintas maneras, como "susurrar“ directamente mensajes hirientes y dañinos a los jugadores o enviar spam con comentarios despectivos sobre sus víctimas a canales de chat mundiales.

**2 | Problemas de privacidad:**

La naturaleza social de los juegos online permite a los cibercriminales manipular las conversaciones, te pueden elegir en un canal de chat general y luego empezar a enviar mensajes personales que piden información personal detallada.

Al juntar datos de los juegos y de otras fuentes, los hackers pueden crear cuentas a tu nombre o acceder a perfiles existentes.

**Información personal que se deja en consolas, computadoras o dispositivos móviles y portátiles:**
Los usuarios frecuentemente olvidan eliminar sus archivos e información personal de las consolas o dispositivos antes de venderlos, regalarlos o donarlos, lo que pone en riesgo su vida privada.

**Acciones relacionadas con las webcams:**
Los atacantes pueden controlar y utilizar cualquier dispositivo conectado, como una webcam o un equipo de audio para aprovecharse de ti, filtrando la información en distintos foros y páginas.

**Malware:**
Los troyanos pueden modificar una aplicación legítima y cargar la versión maliciosa, por ejemplo en Google Play, al descargarlo, el malware se ejecuta y toma el control del dispositivo Android de un usuario y puede convertirlo en parte de un "botnet" mayor.
El malware funciona con un temporizador de retardo, por lo que las víctimas no sospechan que su juego online es la fuente.

**Malware:**
Algunos juegos online utilizan el modelo "freemium", lo que significa que proporcionan algunos contenidos de forma gratuita, pero requieren de un pago para acceder a otras partes del juego o mejoras.
En la mayoría de los casos, se requiere una tarjeta de crédito para registrarse y jugar; el cargo se produce automáticamente si los usuarios deciden comprar nuevos artículos o servicios, lo que puede derivar en el robo de cuentas y datos.

## Recomendaciones para aumentar tu seguridad en redes sociales y comunidades virtuales

**Configurar mensajería de los videojuegos:**
La mayoría de los juegos permiten a los participantes "bloquear“ conversaciones y mensajes de otros usuarios; en algunos casos se realiza un reporte, por lo que para ello es bueno anotar o hacer una captura de pantalla de cualquier conversación ofensiva e informar de ella a los administradores del juego.

**Proteger tus datos:**
Nunca proporciones información personal y cuida que los nombres de usuario no revelen tu identidad real, o que pudieran proporcionar su ubicación o edad.

**Elimina información de tus dispositivos antes de deshacerte de ellos:**
Debes borrar todos los datos personales de las consolas de videojuegos, tablets y smartphones, así como realizar un restablecimiento de fábrica. Las herramientas o procedimientos pueden variar, según el tipo de dispositivo, por lo que es importante investigar cómo funcionan. Además, recuerda que algunos equipos podrían incluir zonas de almacenamiento que no se ven afectadas por las funciones de borrado. Revisa si el aparato incluye unidades de almacenamiento compatibles con computadoras (por ejemplo, tarjetas SD), conéctalas a tu PC y elimina los datos de forma segura.

**Webcams:**
Asegúrate que el ajuste predeterminado esté siempre en la opción de apagado, y si es posible, cúbrela con algo para evitar ser víctima de espionaje.

**Supervisión de un adulto:**
Procura que los menores cuenten con el acompañamiento adecuado mientas interactúan.

**No dejes tus datos de tarjetas bancarias expuestas:**
Evita guardar datos predeterminados de tus tarjetas de crédito; en la mayoría de los casos, si deseas comprar algo puedes hacerlo a través de las fichas de prepago para evitar que tus datos estén comprometidos.

**Evita descargar aplicaciones y juegos fuera de las tiendas oficiales.**

# 12. Decálogo para la ciberseguridad en videojuegos

**1 |** No jugar ni chatear con desconocidos.

**2 |** Establecer horarios de juego.

**3 |** No utilizar tu cuenta de correo electrónico personal sino generar una nueva para jugar.

**4 |** No proporcionar datos personales, telefónicos o bancarios.

**5 |** No usar micrófono ni cámara.

**6 |** No compartir ubicación.

**7 |** Reportar cuentas agresivas o sospechosas.

**8 |** Mantener la configuración de seguridad para los niños en los dispositivos (control parental).

**9 |** En el caso de los menores de edad, jugar bajo la supervisión de adultos.

**10 |** Si detectas conductas o algún tipo de acoso, violencia o amenaza en contra de tus hijos mientras juegan, repórtalo al 089 o al sistema de emergencias 911.

## Seguridad en el uso del correo electrónico

El correo electrónico se ha convertido en el medio de comunicación oficial de muchas organizaciones. Por este medio, diariamente se distribuye información diversa, pues no solo se envían mensajes en formato de texto, también se pueden adjuntar imágenes, videos, hojas de texto, presentaciones y casi cualquier formato soportado por las distintas plataformas.

Tal diversidad conlleva un riesgo cuando el emisor de un mensaje o el receptor no atienden las medidas básicas para mantener segura la información que está en sus buzones.

Existen varias opciones para hacer uso del correo electrónico: vía web, a través de un cliente instalado en nuestra computadora (Outlook de Office) y aplicaciones para dispositivos móviles.

### Recomendaciones básicas:

Mantener las computadoras o dispositivos actualizados, protegidos con contraseñas y bloqueados cuando no estén en uso.

Realizar un respaldo frecuente, tanto de la información como de las configuraciones de nuestro buzón de correo.

Depurar la información sensible, no mantenerla en nuestro buzón.

No compartir contraseñas de inicio de sesión ni permitir que otras personas hagan uso de nuestro buzón.



No abrir ni responder correos de dudosa procedencia.

**En correo web:**

Utilizar una contraseña segura para iniciar sesión en la cuenta.



Tomar las precauciones con el navegador desde donde se hará la consulta, que se encuentre actualizado y que la URL sea segura (inicia con HTTPS y corresponde al nombre de dominio de nuestra organización o proveedor del servicio).

Utilizar una contraseña segura para iniciar sesión en la cuenta.

## Uso de correo Outlook:

Asegurarse que la computadora o dispositivo donde está alojado nuestro correo es seguro: tiene un antivirus actualizado y no es de uso compartido.


Proteger con contraseña el archivo .PST que aloja nuestra información. Se recomienda respaldarlo periódicamente dependiendo de la importancia que se encuentre alojada en él.

## En aplicaciones para dispositivos móviles:

Instalar solo aplicaciones oficiales del proveedor del servicio o las que son las autorizadas por tu centro de trabajo.

## 1 | Protegerás tu identidad digital

Verificarás la privacidad de los sitios donde navegas, tendrás precaución en el contenido de las fotos y videos que publicarás, cuidarás la información en tiempo real que compartirás en redes sociales y configurarás las opciones de privacidad de los perfiles utilizados.

## 2 | Utilizarás medidas de seguridad durante el teletrabajo

Se deberán proteger las redes wifi y cambiar constantemente las contraseñas; mantendrás actualizado el software, con los parches de seguridad y utilizarás las redes privadas virtuales proporcionadas por la institución.

## 3 | Usarás contraseñas seguras

Deberás utilizar caracteres especiales, números, letras mayúsculas y minúsculas para garantizar su complejidad e incrementar su longitud, no guardarás las contraseñas de manera automática en los sitios web, cambiarás periódicamente tus contraseñas y tendrás que hacer uso responsable de ellas.

## 4 | Cuidarás los datos personales que se exponen en el ciberespacio

El robo de identidad se usa para abrir cuentas de crédito, contratar líneas telefónicas y/o seguros de vida, realizar compras y cobro de seguros de salud, vida y pensiones, es por ello, que no expondrás datos personales en sitios públicos y los resguardarás con seguridad.

### 5 | No compartirás noticias falsas

Deberás validar e identificar las fuentes de información; observarás las imágenes que se exhiben, detectando si la noticia emite un juicio de opinión y/o el uso de lenguaje inapropiado.


### 6 | Pondrás más atención cuando compartas datos personales

No difundirás información personal, contraseñas y/o datos bancarios a través de correos electrónicos que desconozcas su origen para evitar la vulnerabilidad de tu seguridad, a través de la ingeniería social.


### 7 | Verificarás ofertas y proveedores cuando se trate de comercio digital

No caerás en ofertas que no hayas solicitado y/o en productos que estén muy por debajo del costo en el mercado, sin antes verificar la información; no ingresarás a enlaces que provengan de fuentes desconocidas, si se desconoce el origen del proveedor evitarás revelar datos personales o realizar pagos por adelantado.

### 8 | Protegerás todos los equipos informáticos

Realizarás copias de seguridad constantemente y emplearás almacenamiento en la nube, que incluya cifrado de alto nivel y autentificación multifactorial, para prevenir el malware y ransomware.

### 9 | Evitarás el ciberacoso

No aceptarás en redes sociales a personas que no conozcas o cuya información no identifiques, no exhibirás imágenes privadas o íntimas si el receptor no es de tu entera confianza, no compartirás información personal, económica o laboral con desconocidos.


### 10 | Denunciarás

Existen instituciones que ayudan en la prevención de delitos cibernéticos, a las cuales podrás acudir para orientación, capacitación o denuncia.


**No te calles, ¡Denuncia cualquier tipo de conducta inapropiada!**