CIBERGUÍA

Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico

GOBIERNO DE MÉXICO | SEGURIDAD

SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA

CIBERGUÍA

ÍNDICE

Directorio 7
Introducción 9
1. Seguridad durante el teletrabajo 11
Teletrabajo y sus beneficios 12
Problemas asociados al teletrabajo 13
Medidas para evitar riesgos en el teletrabajo 13
2. Contraseñas seguras 14
¿Qué son las contraseñas seguras? 15
Riesgos de no usar contraseñas seguras 15
Recomendaciones para generar contraseñas seguras 16
¿Qué hemos aprendido del uso de las contraseñas seguras? 16
3. Malware y Ransomware 17
¿Qué son el Malware y el Ransomware? 18
¿Cómo actúa el Ransomware? 19
Recomendaciones para evitar ser víctima del Ransomware 20
¿Qué hemos aprendido del Malware y Ransomware? 21
4. Phishing: Estafas de suplantación de identidad 22
¿Qué es el Phishing? 23
Recomendaciones para evitar ser víctima de Phishing 24
5. Noticias falsas 26
¿Qué son las noticias falsas? 27
Problemas que desencadenan las noticias falsas 27
Recomendaciones para identificar las noticias falsas 28

ÍNDICE

6. Técnicas de Ingeniería Social 29
¿Qué son las Técnicas de Ingeniería Social? 30
Diversidad de ataques con el uso de las Técnicas de Ingeniería Social 30
Recomendaciones para proteger información ante terceros 32
7. Fraude electrónico 33
8. La reputación en el ciberespacio 36
Riesgos de identidad y la reputación en el ciberespacio 37
Recomendaciones para construir la reputación on line 39
9. Seguridad en dispositivos móviles 40
Consejos para mantener seguro el dispositivo móvil 41
10. Lineamientos para identificar y reportar páginas falsas 44
Identificación de páginas no autorizadas del Gobierno 46
Verificación de páginas en comercio digital 48
Denuncia 50
11. Ley Olimpia 51
¿Qué es la Ley Olimpia? 52
Violencia digital 53
Evolución de la Ley Olimpia 53
Conociendo la Ley Olimpia 54
Medidas de prevención VS. la violencia digital 54

ÍNDICE

12. Seguridad en redes sociales y comunidades virtuales 55
¿Qué son las redes sociales y comunidades virtuales? 56
Problemas de comunidades virtuales y redes sociales 57
Recomendaciones para aumentar tu seguridad en redes sociales y comunidades virtuales 58
Seguridad en videojuegos on line 59
¿Cuáles son los riesgos de los videojuegos on line? 59
Recomendaciones para aumentar tu seguridad en redes sociales y comunidades virtuales 61
13. Seguridad en el uso del correo electrónico 64
Recomendaciones básicas 65
En correo web 66
Uso de correo Outlook 67
En aplicaciones para dispositivos móviles 67
Decálogo de Ciberseguridad de la SSPC 68

DIRECTORIO

Licda. Rosa Icela Rodríguez Velázquez
Secretaria de Seguridad y Protección Ciudadana

Lic. Ricardo Mejía Berdeja
Subsecretario de Seguridad Pública

Lic. Miguel Ángel Urrutia Lozano
Jefe de Unidad de Información, Infraestructura Informática y Vinculación Tecnológica

Dr. Alejandro Canales Cruz
Director General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico

Mtro. Javier Ulises Miranda Nieto
Coordinación de Ciberseguridad, Administración y Análisis de Información de Seguridad Pública

Mtro. Eduardo Godínez Fernández
Director de Ciberseguridad y Sistemas Biométricos

INTRODUCCIÓN

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 y Protección Ciudadana, 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 SSPC 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

Teletrabajo y sus beneficios

TELETRABAJO: Es un recurso que se apoya de la tecnología digital para que las y los empleados realicen sus labores sin presentarse físicamente en sus centros de trabajo.

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

Beneficios del TELETRABAJO:

FLEXIBILIDAD DE HORARIO para compaginar la vida laboral y familiar.

INSERCIÓN LABORAL para las personas con dificultades de movilidad.

MENOR ESTRÉS

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.

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

Problemas asociados al teletrabajo

Trabajar remotamente sin seguir las pautas de seguridad genera un riesgo para las y 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.

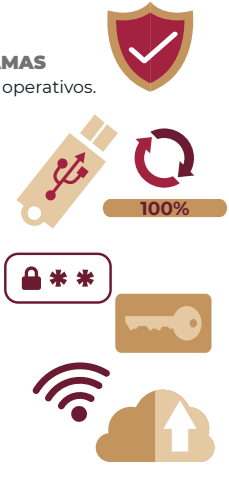
4 | **USAR CONTRASEÑAS SEGURAS** diferentes y para todos los dispositivos.

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.



2.
Contraseñas seguras

¿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 contraseñas seguras

Tips para generar contraseñas seguras:

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

   contraseñas seguras 4235

2. Utiliza mayúsculas y minúsculas.

   ContraseñA SeGUra 4235

3. Quita los espacios.

   ContraseñASeGUra4235

4. Convierte las vocales en números.

   C0ntr4s3ñ4S3GUr44235

5. Inserta caracteres especiales que fuercen a utilizar la tecla "SHIFT", como puede ser el símbolo asterisco (*), guión bajo (_), ampersand (&), porcentaje (%), etc.

   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

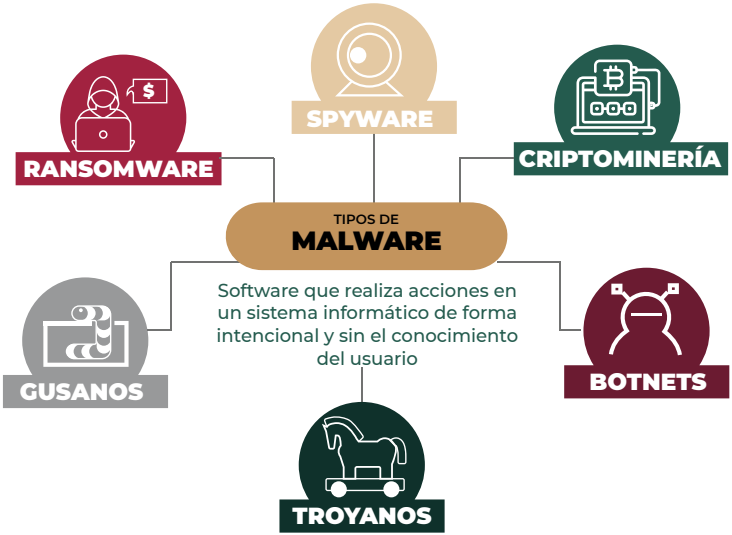
- CAMBIA LAS CONTRASEÑAS PERIÓDICAMENTE
- UTILIZA UN LLAVERO ELECTRÓNICO QUE PERMITA CREAR Y ENCRIPTAR DE FORMA FÁCIL Y SEGURA LISTAS DE USUARIOS Y CONTRASEÑAS

3.
Malware y Ransomware

¿Qué son el Malware y el Ransomware?

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":**



¿Cómo actúa el Ransomware?

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.

1

Un usuario recibe un correo spam con archivos adjuntos trampa, en formatos **PDF o Word.**

2

Al abrir los archivos, la o 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.

Lamentablemente, el pago NO GARANTIZA la liberación de la información o de los equipos.

Afortunadamente
PODEMOS PREVENIRLO

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.

Mantén los programas y el sistema operativo actualizados.

Haz copias de seguridad de tu información periódicamente.

Si recibes archivos, anuncios o enlaces no esperados, pregunta a la persona si los ha enviado. El sistema podría infectar y propagar el Malware.

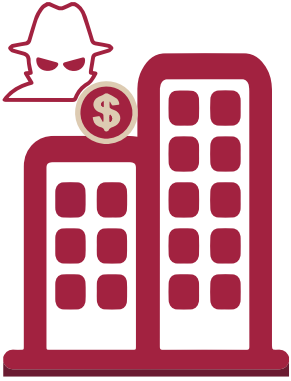
Instala un antivirus con capacidad proactiva de detección.

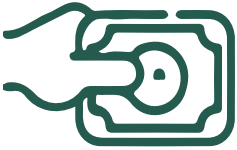
¿Qué hemos aprendido del Malware y Ransomware?

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.





4.
Phishing: Estafas de suplantación de identidad

¿Qué es el Phishing?

Es una práctica en la cual las víctimas literalmente **"MUERDEN EL ANZUELO"** que un ciberdelincuente les lanza.

Para cometer este acto, los criminales se apoyan de algunas técnicas conocidas como la **suplantación de identidad** y la **ingeniaría social.**

Se hacen pasar por una empresa o persona de confianza en una aparente comunicación oficial electrónica, convencen a sus posibles víctimas de facilitar datos confidenciales a cambio de hacer una verificación de alguna cuenta o servicio, e incluso ofrecen algún beneficio poco común. Con esto, los ciberdelincuentes obtienen información confidencial y cometen los siguientes delitos:

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 de 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.

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.

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.

Ante cualquier duda, no arriesgarse

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

5.
Noticias falsas

¿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.

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

Facilidad de difusión.

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

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

Recomendaciones para identificar las noticias falsas

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.

6.
Técnicas de Ingeniería Social

¿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

ATAQUE A NIVEL FÍSICO

POR TELÉFONO

El perpetrador llama a la víctima haciéndose pasar por un técnico de soporte o un empleado de la 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.

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).

ATAQUE VÍA SMS

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.

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.

EMPLEO EN EL MISMO LUGAR

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

LEER EL LENGUAJE CORPORAL

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

EXPLOTAR LA SEXUALIDAD

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

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.

7.
Fraude electrónico

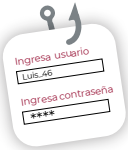
El fraude electrónico es un tipo de estafa que se realiza por medios digitales y en conjunto con distintas técnicas convencionales de la Ingeniería Social.

Las personas que hacen operaciones a través de medios electrónicos, como banca y comercio electrónico, son las principales víctimas, ya que en ocasiones 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.

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.

8.
La reputación en el ciberespacio

La reputación en Internet se basa en la opinión, consideración o prestigio que se tiene de algo o alguien; hay diferencias que la desmarcan **del concepto de reputación más clásico o si se prefiere, físico.**

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

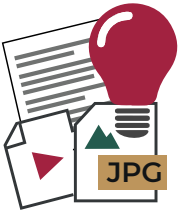
Normalmente publicamos una gran cantidad de información en la red, sin ser plenamente conscientes de que en el momento en que se difunde, perdemos el control sobre sus posibles usos y difusión.

3 Riesgos sobre la reputación on line

Son los que pueden afectar el prestigio u opinión que una persona ha adquirido en Internet. En comparación con el mundo físico, supone un riesgo mucho mayor porque en la web los contenidos se difunden con mayor rapidez.

4 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.



Recomendaciones para construir la reputación on line

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.

9.
Seguridad en dispositivos móviles

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 caracterízan por no usar cables e integan 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 men os desbloqueados.

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

4 **Deshabilitar la geolocalización** en aplicaciones que no sea necesario su uso.

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 identificar y reportar páginas falsas

En internet se puede encontrar información muy diversa publicada 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.

www.gob.mx/sspc

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.

Ya puedes tener la app COVID-19

La app fue lanzada para que las ayudas lleguen a los necesitados. Descárgala y recibe tus apoyos por COVID-19.

NotitasMéxico.com

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).

Información

Usamos **cookies propias y de terceros** para mejorar nuestros servicios.
Si continúa navegando, consideramos que acepta su uso.

Más información

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.

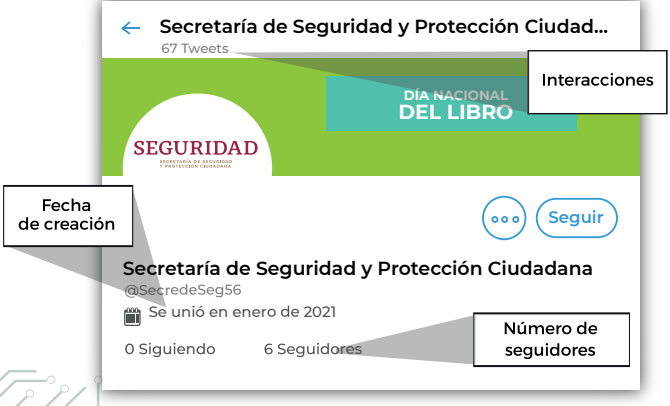
✓ Página real	✗ Página falsa
www.gob.mx/salud	www.salud.gob.mx

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.

✓ **Página real**

✗ **Página falsa**



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

✓ **Página real**

Información oficial y números de contacto

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.

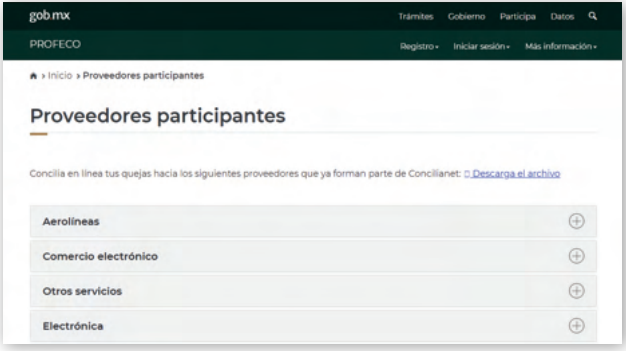
$$$$ | **www.comercio.com**

$$ | **www.barato.com**

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:

phishing@sspc.gob.mx

Si sospechas que el sitio web o cuenta de una red social sufrió una violación a la seguridad se debe reportar al:

088

Centro Nacional de Atención Ciudadana

11.
Ley Olimpia

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?

Modificaciones a disposiciones de carácter penal

- Protección a la intimidad personal y derechos sexuales
- Prevención de la violencia sexual en Internet
- Ciberacoso como delito
- Conciencia a través de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia
- Concientización sobre la violencia digital

Violencia digital

La Ley Olimpia la define como:

1. - Acoso
   - Hostigamiento
   - Amenazas
   - Vulneración de datos e información privada
2. Difusión de contenido sexual (fotos, video o audios) sin consentimiento a través de las redes sociales, que atente contra la integridad o vida privada.
3. Vulneración de algún derecho humano de las mujeres.

Evolución de la Ley Olimpia

2014

1. Surge a través de la propagación de un video íntimo de Olimpia Melo Cruz, expuesto por su expareja.

2018

2. Olimpia impulsó una iniciativa de Ley para reformar el Código Penal, logrando su aprobación en Puebla, Nuevo León y Yucatán.

2019

3. Se aprueba en Aguascalientes, BC-BCS, Chiapas, Coahuila, Durango, Guanajuato, Guerrero, Edo. de México, Oaxaca, Querétaro, Veracruz y Zacatecas.

2021

4. Legisladores de la Cámara de Diputados aprueban en lo general y en lo particular la Ley en el Código Penal Federal

Conociendo 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: cibervenganza, ciberporno y acoso sexual.

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.

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.

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

12.
Seguridad en redes sociales y comunidades virtuales

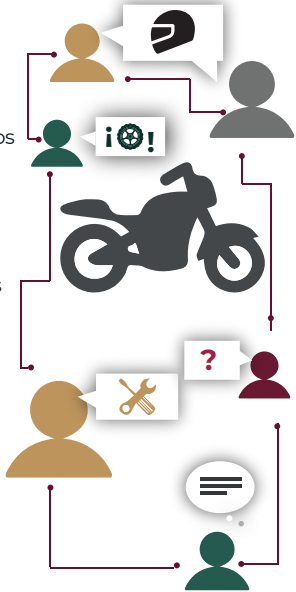
¿Qué son las redes sociales y comunidades virtuales?

COMUNIDAD VIRTUAL

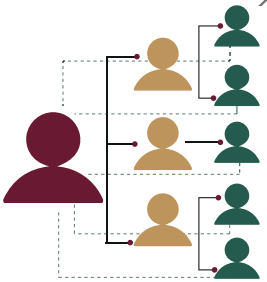
Es un foro, página o red social enfocada a **una idea en común,** donde todos los usuarios comparten y disfrutan alguna de las facetas que la componen.

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.



RED SOCIAL



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 SUPLANTACIÓN DE IDENTIDAD:
las personas no siempre son lo que dicen ser, buscan obtener beneficios con base en engaños, **¡no caigas!**

3 ROBO DE INFORMACIÓN:
a menudo las personas roban tu información y datos personales para la venta de las mismas, **¡cuidado con lo que publicas!**

4 CHANTAJE O EXTORSIÓN:
cuando una persona obtiene información, archivos sensibles o personales, tratará de chantajearte para obtener beneficios con base en tu temor.

Recomendaciones para aumentar tu 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 supervisión 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.
Actúa bajo las normas éticas y cívicas que te rigen.

7. **Protégete cambiando constantemente tus contraseñas para estar más seguro.**

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 competentes.

Seguridad en videojuegos online

VIDEOJUEGOS ONLINE (EN LÍNEA)

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.

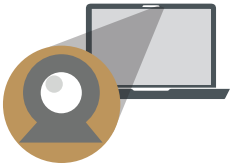
1 CIBERACOSO:
Existen distintas maneras, como "susurrar" directamente mensajes hirientes y dañinos a los jugadores o enviar spam con comentarios despectivos sobre sus víctimas a canales de chat mundiales.

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.

3 **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.

4 **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.



5 **CARGOS OCULTOS:**
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.

6 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.

Recomendaciones para aumentar tu seguridad en redes sociales y comunidades virtuales

1. **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.

2. **PROTEGER TUS DATOS:** nunca proporciones información personal y cuida que los nombres de usuario no revelen tuidentidad real, o que pudieran proporcionar tu ubicación o edad.

3. **ELIMINAR 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.

4. **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.

5. **SUPERVISIÓN DE UN ADULTO:** procura que los menores cuenten con el acompañamiento adecuado mientas interactúan.

6. **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.

7. **EVITAR DESCARGAR APLICACIONES Y JUEGOS FUERA DE LAS TIENDAS OFICIALES.**

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 088.

13.
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.

C0ntr4s3ñ4_S3G&r4_4235*

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).

Iniciar una navegación web privada en equipos compartidos.

Uso de correo Outlook:

Asegurar 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 de la información que se encuentre alojada en él.

En aplicaciones para dispositivos móviles:

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

App

Decálogo de Ciberseguridad de la **SSPC**

① PROTEGERÁS TU IDENTIDAD DIGITAL

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

② UTILIZARÁS MEDIDAS DE SEGURIDAD DURANTE EL TELETRABAJO

Protegerás las redes wifi y cambiarás 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

Utilizarás 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.

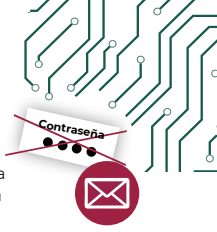
④ CUIDARÁS LOS DATOS PERSONALES QUE SE EXPONEN EN EL CIBERESPACIO

No expondrás datos personales en sitios públicos y los resguardarás con seguridad. 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.

⑤ NO COMPARTIRÁS NOTICIAS FALSAS

Validarás e identificarás 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 invitaciones en redes sociales de 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

Acudirás a instituciones que ayudan en la prevención de delitos cibernéticos, para orientación, capacitación o denunciar.

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

GOBIERNO DE
MÉXICO

SEGURIDAD

SECRETARÍA DE SEGURIDAD
Y PROTECCIÓN CIUDADANA

GOBIERNO DE
MÉXICO

SEGURIDAD

SECRETARÍA DE SEGURIDAD
Y PROTECCIÓN CIUDADANA