Recomendaciones

para mantener SEGURA TU PRIVACIDAD y DATOS PERSONALES en el entorno digital

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Directorio

© **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales**
Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco,
C.P. 04530, Delegación Coyoacán, Ciudad de México.

Edición • Marzo 2018

Contenido

Glosario

Antivirus: Software que tiene como propósito detectar y eliminar malware.

App/Aplicación: Software que puede ser instalado en dispositivos móviles, diseñado para facilitar al usuario la ejecución de una tarea.

Autenticación: Proceso mediante el cual un equipo de cómputo, dispositivo móvil, programa, aplicación o servicio, corrobora la identidad de un usuario.

Bluetooth: Tecnología de comunicaciones inalámbricas que permite la transmisión de datos entre dos equipos de cómputo o dispositivos móviles, generalmente en distancias cortas.

Borrado Seguro: Medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

Cifrado: Medida de seguridad para proteger la confidencialidad, la cual codifica la información a través de un algoritmo y una clave, para hacerla legible o ilegible.

Contraseña o clave: Medida de seguridad para controlar el acceso a un equipo de cómputo, dispositivo móvil, programa, aplicación o servicio, a través de una palabra, frase o un conjunto de caracteres alfanuméricos. Las contraseñas basadas sólo en números se conocen como PIN, mientras que las basadas en varias palabras o frases tienen el nombre de passphrase.

Cookies: Paquetes de información definidos por un sitio web, y almacenados por un navegador de forma automática en el dispositivo del usuario cuando éste visita dicho sitio.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información. Son ejemplos de datos personales, los siguientes: el nombre, los apellidos, la dirección postal, el número de teléfono o de celular, la dirección de correo electrónico, el número de pasaporte, la fotografía, la Clave Única de Registro de Población (CURP), el Registro Federal de Contribuyentes (RFC), los datos de salud, datos financieros, entre otros.

Derecho a la protección de datos personales: Derecho humano reconocido por los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, que ofrece amparo a los individuos contra la posible utilización de sus datos personales por parte de terceros, a través de la imposición de obligaciones a los responsables del tratamiento de los datos personales, y del otorgamiento de derechos a los titulares de los datos, a fin de garantizar el buen uso de la información personal y el derecho a la autodeterminación informativa de las personas.

Dispositivo móvil: Aparato pequeño que cuentan con tecnología de cómputo y acceso a Internet, es portable y se puede conectar a un equipo de cómputo para ver su contenido, por ejemplo, teléfonos inteligentes y tabletas[1] .

Dirección IP: Número con el que se identifica a los dispositivos electrónicos que están conectados en una red, la cual utiliza el protocolo IP (del inglés Internet Protocol).

Dispositivos periféricos: Dispositivos que se conectan por cualquier puerto a un equipo de cómputo o dispositivo móvil. Son todos los dispositivos de hardware a través de los cuales, la computadora se comunica con el exterior. Por ejemplo, teclados, monitores, cámaras, memorias USB o discos duros extraíbles.

Equipo de cómputo: Dispositivo electrónico para procesar y almacenar información, está compuesto por hardware, software y dispositivos periféricos.

Extensión del navegador o Plug-in: Programas que se instalan como complementos dentro de un navegador, incorporando nuevas funciones para personalizar la experiencia del usuario.

Filtro o control de contenido: Programa que permite limitar el acceso a contenido no deseado, al navegar en Internet. Por ejemplo, sitios web para adultos, publicitarios, o de descargas ilegales.

Firewall: Sistema o programa para proteger redes, equipos de cómputo y dispositivos móviles contra intrusiones provenientes de terceros (generalmente desde Internet).

GPS: Sistema de Posicionamiento Global (por sus siglas en inglés Global Positioning System), que permite determinar la posición de un objeto en la Tierra.

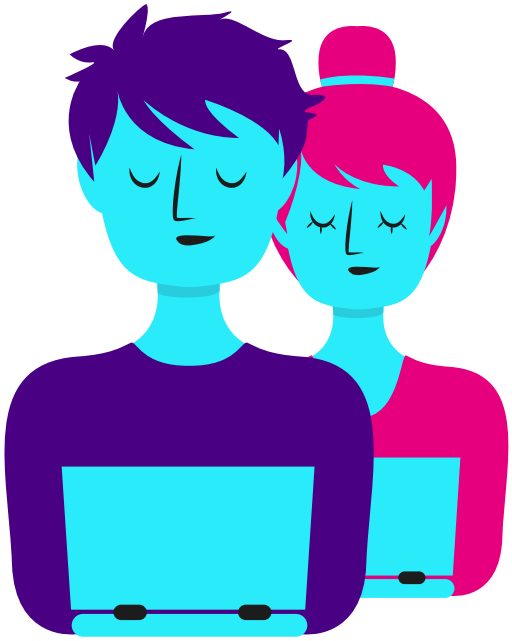
Hardware: Conjunto de elementos físicos y materiales que constituyen un equipo de cómputo o dispositivo móvil.

Malware o Software Malicioso: Término que engloba a todo tipo de programa o código malicioso cuyas funciones pueden variar desde extraer, borrar e incluso "secuestrar" la información en equipos de cómputo o generar malfuncionamiento en los sistemas. Algunos ejemplos de malware son: los virus, los troyanos, los gusanos y el ramsomware.

Mensajería instantánea: Comunicación en tiempo real mediante mensajes de texto, audio o video. Algunas de las aplicaciones de mensajería instantánea son Whatsapp, Facebook Messenger, Skype, Telegram, Line, Viber, Snapchat, WeChat.

[1] Véase: https://en.oxforddictionaries.com/definition/mobile_device

¿SABÍAS QUÉ?



USUARIOS *de* ***internet***

Al segundo trimestre de 2017

el **63.9 %** de la población de 6 años o más en México se declaró usuaria de Internet.[1]

Para el segundo trimestre de 2017

en México existían **71.3 millones de usuarios de Internet**, cuya actividad principal es obtener información, entretenimiento, comunicación, acceso a contenidos audiovisuales y acceso a redes sociales.[2]

Al 31 de diciembre de 2017

México ocupó el lugar número **9 del ranking** de usuarios de Internet a nivel mundial.[3]

El 73% de los usuarios

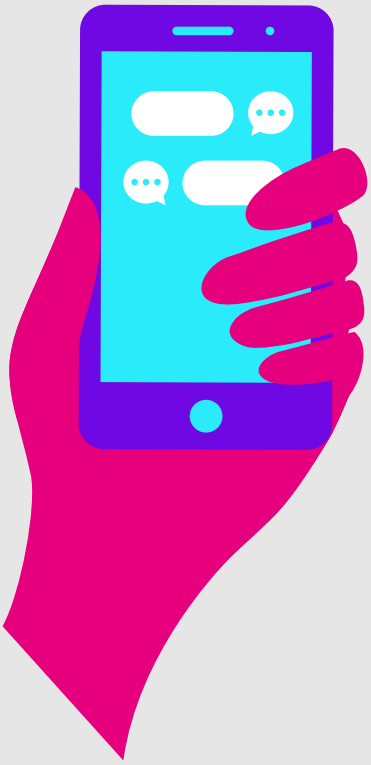
utiliza la red como una forma de **comunicación social**, convirtiéndose, por tanto, en una población vulnerable ante la delincuencia organizada, pues Internet facilita conocer datos personales y características de las víctimas potenciales.[4]

1 Consultable en: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf
2 Consultable en: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf
3 Consultable en: http://www.internetworldstats.com/top20.htm
4 Consultable en: https://www.gob.mx/cms/uploads/attachment/file/37682/Diagnostico_UNODC.pdf, (p. 121).

DISPOSITIVOS *móviles*

En 2017, el 72.2% de la población

de 6 años o más utiliza teléfono celular. **8 de cada 10 usuarios** disponen de un teléfono inteligente (*smartphone*).[1]



Al tercer trimestre de 2017

se reportaron **96.8 millones de teléfonos inteligentes en funcionamiento** en el país.[2]

Casi 9 de cada 10 internautas

poseen **computadoras de escritorio o portátiles, y *smartphone***. Disminuye el uso de la computadora de escritorio y crece el uso de tabletas.[3]

Android

es el sistema operativo móvil **más utilizado** en Latinoamérica.[4]

1 Para su consulta en: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf
2 Consultable en: https://www.theciu.com/publicaciones-2/2018/1/29/ecosistema-competitivo-del-mercado-de-smartphones-al-3t17?rq=smart
3 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid= (p.11).
4 Consultable en: https://www.imscorporate.com/news/Estudios-comScore/IMS-Mobile-Study-Septiembre2016.pdf (p.15).

REDES *sociales*

Cada usuario en México

tiene en promedio **5 redes sociales**.[1]

Las principales actividades

de los usuarios de Internet en 2017, fueron: obtener información **(96.9%)**, entretenimiento **(91.4%)**, comunicación **(90.0%)**, acceso a contenidos audiovisuales **(78.1%)** y acceso a redes sociales **(76.6%)**.[2]

Facebook

es la principal red social en México.[3]

1 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid= (p.18).
2 Consultable en: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf
3 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid= (p.18).

COMERCIO

electrónico y banca en línea

3 de cada 4 internautas mexicanos

realizaron una **compra** en 2017.[1]

Aproximadamente 7 de cada 10 mexicanos

que utilizan Internet reportaron haber utilizado **banca en línea** (2015).[2]

Los *millenials* [3]

acceden a la **banca en línea** a través de un **teléfono inteligente**.[4]

La mayoría de los usuarios

de banca en línea consideran que la **institución financiera** es principalmente **responsable de la seguridad** de las transacciones en línea.[5]

Los individuos mayores de 35 años

tomaron en promedio más **acciones encaminadas a la seguridad** en la banca en línea, que la generación del milenio.[6]

1 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Comercio-Electronico/Estudio-de-Comercio-Electronico-en-Mexico-2017/lang,es-es/?Itemid= (p.39)
2 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Banca-por-Internet/Estudio-Banca-Electronica-2016/lang,es-es/?Itemid= (p.16).
3 La Generación *Millennial* define a los nacidos entre 1981 y 1995, jóvenes entre 20 y 35 años que se hicieron adultos con el cambio de milenio.
4 Para su consulta en: https://www.asociaciondeinternet.mx/es/component/remository/Banca-por-Internet/Estudio-Banca-Electronica-2016/lang,es-es/?Itemid= (p.10).
5 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Banca-por-Internet/Estudio-Banca-Electronica-2016/lang,es-es/?Itemid= (p.13).
6 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Banca-por-Internet/Estudio-Banca-Electronica-2016/lang,es-es/?Itemid= (p.13).

ROBO *de identidad y fraudes*

México ocupa el 8° lugar

a nivel mundial en el **delito de robo de identidad**; en un 67% de los casos, el robo de identidad se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria.[1]

90% de las personas

tiene en su **cartera** información suficiente para ser **víctima de robo de identidad** (credencial de elector, tarjetas de crédito y débito, estados de cuenta, entre otros).[2]

Durante el 2016

en el **sector bancario**, se tuvo un total de 5 millones 297 mil 509 **reclamaciones por** posible **fraude**.[3]

En el tercer trimestre de 2017

los **fraudes cibernéticos crecieron** 102% respecto del mismo periodo de 2016 y representan cada año una mayor proporción (del 13% al 51%).[4]

1 Consultable en: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad
2 Consultable en: http://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf
3 Consultable en: https://www.gob.mx/cms/uploads/attachment/file/240481/FRAUDES_FINANCIEROS_web.pdf
4 Consultable en: http://www.condusef.gob.mx/gbmx/?p=estadisticas

RIESGOS *principales*

En México, 22.4 millones

(45%) de los consumidores fueron **afectados por el cibercrimen** en el año 2016.[1]

El correo electrónico

se ha convertido en el principal vector de propagación de malware.[5]

2 minutos:

el tiempo que tarda un dispositivo IoT[2] en ser atacado.[3]

En 2016,

1 de cada 131 correos electrónicos **contenían un malware**.[6]

México es el segundo país

con el mayor número de ataques **a dispositivos móviles** en América Latina.[4]

Más de tres cuartas partes (76%)

de los **sitios web** escaneados en 2016 **contenían vulnerabilidades**, 9% de las cuales eran críticas.[7]

1 Consultable en: https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf
2 Internet de los objetos: es un sistema de dispositivos de computo interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones, humano a humano o humano a computadora.
3 Consultable en: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (p.12).
4 Consultable en: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america
5 Consultable en: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (p.24).
6 Consultable en: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (p.24).
7 Consultable en: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (p.33).

Introducción

Las *Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital*, tienen por objeto explicar, de manera clara y sencilla, una serie de consejos prácticos sobre configuraciones de seguridad, aplicaciones móviles y software en general (gratuito o con costo), que se consideran útiles para que los usuarios o titulares de los datos personales mantengan segura su privacidad y sus datos personales en el entorno digital.

Este documento contiene **10 recomendaciones** para los titulares de los datos personales. Cada una de ellas explica por qué es importante seguir la recomendación y cuáles son los mecanismos o la mejor práctica a seguir para implementarla.

Es importante tener en cuenta que más allá del software, aplicaciones o configuraciones que se realicen, **no existe seguridad al 100%** y siempre será necesario implementar o actualizar medidas de seguridad continuamente, para reducir la posibilidad de cualquier daño.

Los 10 ejes principales de las Recomendaciones en el entorno digital incluyen:

1) El ***uso seguro de Internet***, que permita a los titulares navegar de forma protegida a través de configuraciones en los navegadores, buscadores o la instalación de herramientas adicionales que les ayude a protegerse de los diferentes tipos de riesgos existentes en el entorno digital.

2) El ***uso de las redes sociales*** de manera segura y responsable, para lo cual es fundamental establecer medidas de seguridad para que la información que se comparta sea vista sólo por aquellas personas autorizadas por el propietario de la cuenta.

3) La ***protección de cuentas***, a través del uso de ***contraseñas*** seguras u otros mecanismos para evitar que personas no autorizadas puedan acceder a información o a datos personales.

4) El uso seguro de ***dispositivos móviles***, para lo cual resulta indispensable contar con medios para su administración, que permitan en caso de pérdida, robo o extravío, tomar acciones como buscar, bloquear o borrar la información y datos personales del dispositivo, a fin de evitar que se haga un mal uso de esta información.

5) El ***uso de software y aplicaciones seguras*** mediante la descarga en sitios y tiendas oficiales.

6) La ***protección contra malware***, que consiste en el uso de herramientas para evitar y remediar infecciones, que pudiera provocar el daño o robo la información y/o datos personales de los titulares.

7) La instalación de ***actualizaciones*** en el software y aplicaciones, para reforzar su funcionalidad y sus elementos de seguridad.

8) Los ***respaldos de información*** como medio para garantizar que ante cualquier eventualidad se tendrá la información y los datos personales, en el momento que se necesite.

9) El ***cifrado de la información***, que consiste en un conjunto de técnicas que se aplican sobre los mensajes, para convertirlos en representaciones que carezcan de sentido para cualquiera que no esté autorizado a recibirlos o interpretarlos.

10) El cuidado en el ***entorno físico***, que también requiere atención, a la par del entorno digital, ya que sólo basta un descuido o error, para poner en riesgo la información personal, los dispositivos o medios digitales que la contienen.

Las recomendaciones incluyen un conjunto de herramientas, configuraciones y buenas prácticas, recopiladas de organismos e instituciones reconocidos en materia de seguridad y privacidad a nivel internacional.

Es importante señalar, que las herramientas o configuraciones presentadas pueden mostrar variaciones en el tiempo o surgir nuevas herramientas con mejores características y seguridad, razón por la cual estas recomendaciones podrían ser actualizadas.

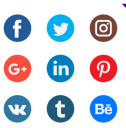
Al final de las recomendaciones se incluye una pequeña evaluación para que los usuarios puedan conocer su nivel de protección en el entorno digital.

Esperamos que te sean de utilidad las Recomendaciones.

10 RECOMENDACIONES

01 Navegar de forma segura

02 Configurar tu privacidad en redes sociales



03 Protege el acceso a tus dispositivos y cuentas

04 Administra tus dispositivos

05 Descarga software y aplicaciones de los sitios oficiales

06 Protégete del malware

07 Mantén actualizado tus software y aplicaciones

08 Respalda periódicamente tu información

09 Cifra tu información

10 Cuida tu entorno físico

RECOMENDACIÓN 1

Navega de forma segura

¿Por qué es importante la navegación segura para la protección de los datos personales?

En la actualidad, es parte de la rutina diaria navegar en Internet para realizar diferentes tipos de actividades, que van desde actualizar nuestras redes sociales hasta revisar estados de cuenta y hacer transferencias bancarias. Por ello, es de suma importancia que los usuarios utilicen *software* o aplicaciones como medidas de seguridad, para prevenir que su información personal se exponga, a las diferentes amenazas que existen en el entorno digital.

a) Navegadores:
Los navegadores *web* son programas que permiten el acceso a Internet. Actualmente existe una amplia variedad, las diferencias radican principalmente en la interfaz, opciones de configuración, rendimiento o recursos disponibles.

RECUERDA...

PROTEGER TU NAVEGACIÓN EN INTERNET TE EVITARÁ QUE PERSONAS NO AUTORIZADAS TENGAN ACCESO A TU INFORMACIÓN O DATOS PERSONALES

La mayoría de los navegadores *web* facilitan el uso seguro de Internet, ya que evitan el almacenamiento de información sobre los sitios visitados por el usuario, así como la instalación de rastreadores. Además, permiten bloquear publicidad no deseada e instalar *plug-ins* o extensiones, para mejorar la seguridad y experiencia del usuario.

Modo incógnito: Es una opción de navegación contenida en los navegadores *web*, su funcionalidad consiste en evitar que se guarde determinada información, por ejemplo, historial de navegación, cookies o al llenar un formulario. Sin embargo, se debe tomar en cuenta que este tipo de navegación no garantiza totalmente la privacidad, ya que la actividad seguirá siendo visible para los sitios *web* que sean visitados, para la empresa y para el proveedor de servicios de Internet.

Plug-ins, add ons y extensiones: Son las aplicaciones que funcionan como complementos dentro de los navegadores *web*, para equipos de cómputo, debido a que añaden o incrementan funcionalidades de uso a dichos navegadores.

Es importante señalar que instalar estos complementos implica otorgar permisos para acceder a información derivada de la navegación. Es recomendable que previo a dar el consentimiento, se verifiquen los permisos que se solicitan y en caso de ser necesario, cambiar la configuración antes de instalarlos, de este modo se reducirán los riesgos.

Para una navegación segura, se recomienda instalar complementos para navegadores *web* o aplicaciones móviles que limiten el rastreo de las actividades realizadas en Internet.

b) Buscadores:

Los buscadores o motores de búsqueda son sistemas que facilitan el acceso a los contenidos almacenados en Internet, enlistan resultados de sitios *web* basados en un parámetro de búsqueda.

Actualmente, existen diferentes buscadores que incluyen características para la seguridad en la navegación, no realizan recolección de ninguna clase de información sobre el usuario y cuentan con herramientas de privacidad para eliminar las búsquedas previas realizadas.

¿Cómo navegar de forma segura?

1. Utiliza siempre la última versión del navegador.
2. Comprueba que los *plug-ins* y extensiones están configurados para actualizarse automáticamente y que su actualización se realice desde fuentes confiables.
3. Revisa las opciones de seguridad y privacidad del navegador.
4. No almacenes contraseñas de forma predeterminada en el navegador.
5. Haz uso de extensiones o complementos adicionales que implementen funcionalidades, no consideradas en el navegador, por ejemplo, herramientas de privacidad y de bloqueo de publicidad.

A continuación, se presenta una lista de navegadores, buscadores y complementos (*plug-ins, add-ons* y extensiones), que podrán ser de utilidad para implementar esta recomendación de seguridad en el manejo de la información personal:

NOMENCLATURA

Win-Sistema Operativo *Microsoft Windows*

Mac OS- Sistema Operativo *Apple*

iOS- Sistema Operativo para móviles de *Apple*

An- Sistema Operativo para móviles de *Google*

ES- Idioma español

EN- Idioma inglés

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	Es	En
NAVEGADORES	*Tor Browser* Navegador que ofrece una protección en Internet mediante el uso de múltiples servidores anónimos, impide que alguien monitorice las páginas *web* visitadas.	x	x		x		x	x	x
	Kaspersky Safe Browser Navegador para brindar seguridad en Internet, filtra direcciones malintencionadas y contenido no deseado.			x			x		x
	Disconnect.me Navegador que realiza el cifrado de las búsquedas realizadas por el usuario, brinda protección anti-malware.	x	x	x	x	x	x		x
	Edge - Modo incógnito	x	x	x	x		x	x	x
	Chrome - Modo incógnito	x	x	x	x		x	x	x
	Firefox - Modo incógnito	x	x	x	x		x	x	x
	Opera - Modo incógnito	x	x	x	x		x	x	x

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	Es	En
COMPLEMENTOS	*Blur (DoNotTrackMe)* Complemento para el navegador *web* de privacidad, evita el seguimiento en línea y mejora la seguridad al navegar en Internet. Disponible en los navegadores *Chrome* y *Firefox*.	x	x	x	x	x	x		x
	NoScript Complemento que permite la ejecución de *JavaScript*, *Java* y otros plugins en los sitios *web* de confianza que el usuario seleccione. Disponible en navegador *Firefox*.	x	x				x	x	
	Orbot Proxy Sirve como base para otras aplicaciones para trabajar anónimamente a través de Internet.				x		x	x	
	Google Sharing Complemento para anonimizar el tráfico que *Google* ve del usuario. Disponible para el navegador *Firefox*.	x	x				x		x
	Ghostery Complemento para el navegador *web* que permite bloquear los rastreadores de las páginas *web*.	x	x				x		x
	KB SSL Enforcer Extensión para *Chrome* que fuerza una conexión segura a través de *SSL*.	x	x				x		x
	FoxyProxy Complemento para los navegadores *Firefox*, *Chrome o Internet Explorer* que facilita y agiliza la configuración de *proxies* y *VPN*.	x	x			x	x		x
BUSCADORES	*DuckDuckGo* Buscador que no recolecta o comparte información.	x	x	x	x		x	x	x

RECOMENDACIÓN 2

Configura tu privacidad en redes sociales

¿Por qué es importante configurar la privacidad en mis redes sociales?

Las redes sociales se han convertido en el medio de comunicación y pasatiempo favorito de los usuarios de Internet, debido a que son la forma de estar en contacto con otros usuarios, ver videos, fotografías y compartir distintos tipos de contenido.

Desafortunadamente, gracias a la popularidad que han adquirido se han convertido en una fuente de fácil acceso a información personal, para aquéllos que intentan hacer mal uso de la misma.

Por ello, los usuarios deben ser cuidadoso con la información que publican en estos medios y configurar la privacidad de cada una de las redes sociales que se utilicen, como una medida de seguridad indispensable para proteger los datos personales ante cualquier uso mal intencionado.

RECUERDA...

LAS 5 REDES SOCIALES MÁS UTILIZADAS EN MÉXICO SON:

- **FACEBOOK**
- **WHATSAPP**
- **TWITTER**
- **YOUTUBE**
- **INSTAGRAM**

Dos recomendaciones generales antes de configurar el nivel de privacidad, en cualquiera de las redes sociales son:

Pensar detenidamente antes de publicar

Previo a compartir cualquier contenido en una red social, se debe analizar la situación y preguntarse detenidamente si la información que será expuesta, se desea que esté disponible en Internet, pensar en quiénes podrán verla y por cuánto tiempo. Reflexionar sobre lo anterior, permitirá analizar, elegir y decidir de forma adecuada qué información personal se debe publicar y cuál mantenerse en privado.

Informarse sobre el uso de los datos personales proporcionados

Antes de utilizar cualquier red social, se sugiere leer su política de privacidad para conocer qué datos personales recopilan, cómo los utilizarán, si se compartirán y con quiénes, cómo se responde ante requerimientos legales, las condiciones del servicio a nivel global, entre otra información que pueda ser relevante para el usuario.

¿Cómo configuro la privacidad en mis redes?

Las redes sociales han simplificado sus controles de privacidad, lo cual facilita al usuario su configuración de una forma más sencilla.

A continuación, se presentan los pasos para configurar la privacidad de las **cinco redes sociales más utilizadas en México**.

1

Facebook

Es una red social que permite la interacción entre usuarios a través de publicaciones con contenido multimedia, directamente en el perfil de otro usuario o etiquetándolo en el propio perfil.

Configuración rápida de seguridad: Esta red social cuenta con una herramienta de verificación rápida de privacidad, misma que incluye un asistente digital, el cual ayuda a identificar tres aspectos básicos de privacidad en la red social.

Para realizar una comprobación rápida de privacidad realizar lo siguiente:

1) Verificar que se tenga la sesión de *Facebook* iniciada.

2) Ubicar el icono ayuda , al dar clic en éste, se desplegará un menú interactivo.

3) Dentro del menú interactivo, dar clic en la opción *Comprobación rápida de privacidad*, en este menú se pueden revisar:

   - Publicaciones: cuando se publique desde el perfil o desde la sección de noticias, se puede elegir quién puede ver la publicación que se va a postear. *Facebook* maneja diferentes filtros de privacidad en las publicaciones (para público en general, amigos en *Facebook* y configuraciones en específico), es importante seleccionar el filtro de privacidad que se desee para la publicación en específico, ya que el que se elija será aplicado como determinado por cada publicación que se realice.
   - Aplicaciones: en esta sección aparecerá un listado con las aplicaciones que se tienen vinculadas a la cuenta de *Facebook*, aquí se podrá editar la privacidad de las actividades que se realizan en cada aplicación vinculada, así como eliminar las que ya no se desea tener vinculadas, es importante recordar que cada aplicación que aparece en este listado, accede con las credenciales de *Facebook*.
   - Perfil: en esta sección se podrá definir qué información personal se tiene pública, los datos que se pueden gestionar en ésta son: correo electrónico, fecha de nacimiento, situación sentimental y ciudad en la que vives.

Figura 1. Menú de Comprobación rápida de privacidad

Configuración de Privacidad de la red social: Adicionalmente, se puede configurar a detalle la *Privacidad en la sección Privacidad de la red social*, en esta sección podrás configurar:

1) *Publicaciones realizadas*: en esta sección se puede limitar la visibilidad de las publicaciones, tomando como parámetro la fecha de las publicaciones que se han realizado desde que se dio de alta la cuenta de red social.

2) *Contacto:* en esta sección se puede administrar qué usuarios de la red social pueden establecer contacto, permitiendo tres opciones: cualquier usuario de la red social, amigos o amigos de amigos.

3) *Localizar mediante teléfono o correo electrónico:* en esta sección se puede habilitar o deshabilitar la búsqueda del perfil mediante el correo electrónico o número telefónico que se tiene dado de alta en la red social.

4) *Deseas que tu cuenta de Facebook sea accesible a través de motores de búsqueda:* esta opción es importante ya que permite desvincular que el perfil de la red social sea localizable desde cualquier motor de búsqueda como *Google*, lo cual haría que, solo pueda encontrarse el perfil a través de la red social.

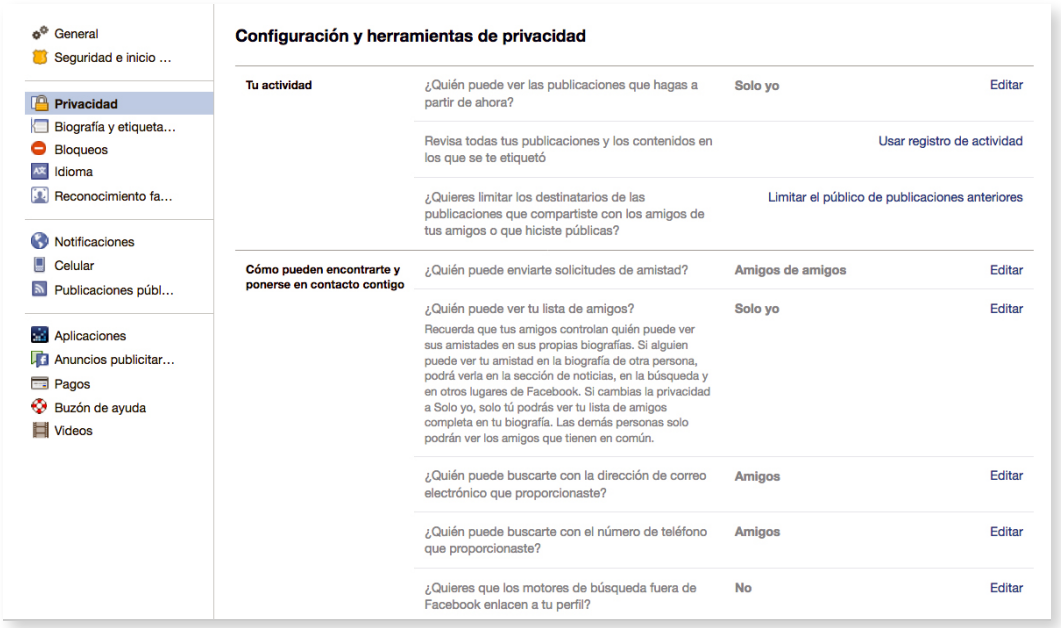


Figura 2. Menú de Configuración y herramientas de privacidad

Configuración de biografía y etiquetado: En cuanto a la privacidad de tu muro de publicaciones, en la sección *Biografía y etiquetado*, podrás configurar:

1) Quien puede publicar en su biografía: esta opción te permite seleccionar qué usuarios pueden publicar en tu perfil de red.

2) Revisión de las publicaciones en que se haya etiquetado: esta opción te notifica cuándo has sido etiquetado en alguna publicación, misma que puede incluir archivos multimedia como videos y fotografías, para que autorices o rechaces que aparezca dicha publicación en tu perfil y así ésta sea visible para tus contactos. Si no estás de acuerdo con ser etiquetado, la etiqueta se elimina, pero, esta publicación sigue siendo visible para los amigos del contacto que te etiquetó.

3) Quienes tienen acceso a tus publicaciones**:** esta opción te permite gestionar qué usuarios pueden ver lo que publicas.

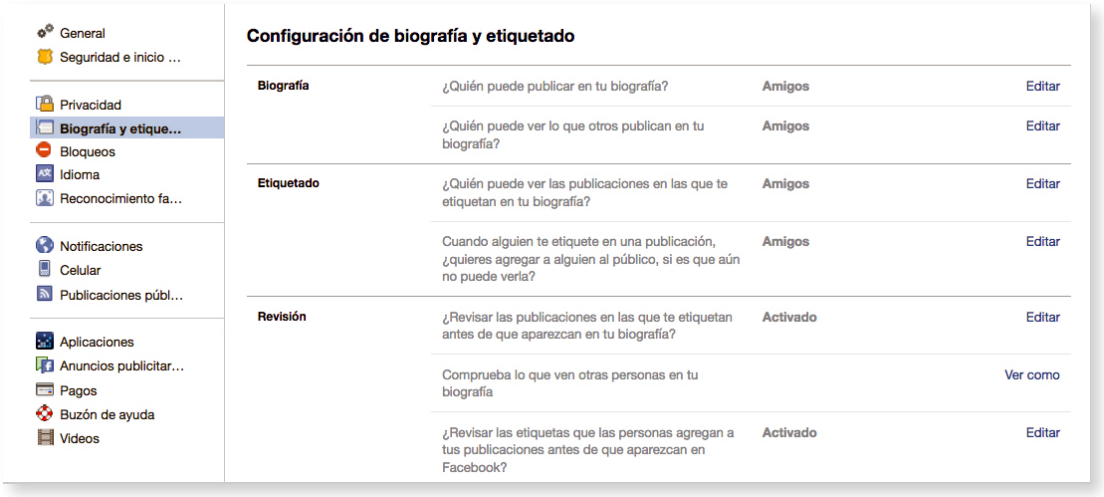


Figura 3. Menú de Configuración de biografía y etiquetado

Configuración de geolocalización: Se debe tomar en cuenta que la geolocalización se puede gestionar directamente desde el dispositivo donde se accede a la red social, o bien, al momento de realizar una publicación.

Antes de publicar, identificar el icono , dando clic en este se puede desactivar la opción que *Facebook* tiene predeterminada para identificar y añadir en cualquier publicación la ubicación.

Figura 4. Indicador de geolocalización

Configuración de alertas de inicio de sesión: *Facebook* cuenta con una opción que permite recibir alertas sobre inicios de sesión no reconocidos:

1) Ir a *Configuración de seguridad e inicio de sesión* haciendo clic en la esquina superior derecha de *Facebook* y, después, en Configuración.

2) Selecciona *Recibir alertas sobre inicios de sesión no* reconocidos y hacer clic en *Editar*.

3) Elegir en *dónde se quiere recibir las alertas*, como la cuenta de correo electrónico o una notificación de *Facebook* desde un dispositivo reconocido.

4) Haz clic en *Guardar cambios*.

5) A partir de este momento se comenzará a recibir alertas de inicio de sesión.

Configuración de autenticación en dos pasos: Para administrar la autenticación en dos pasos, realizar lo siguiente:

1) Ir a la configuración de la seguridad e inicio de sesión, dando clic en la esquina superior derecha de *Facebook* y, después, en *Configuración > Seguridad e inicio de sesión*.

2) Dirigirse a la opción *Usar autenticación en dos pasos* y hacer clic en *Editar*.

3) Elegir el método de autenticación que se quiera agregar (*mensaje de texto, correo electrónico, iconos de sesión,* etc.), dependiendo del método que se seleccione, se deberán seguir las instrucciones de configuración que aparecerán en pantalla.

4) Hacer clic en *Activar* cuando se haya seleccionado y activado un método de autenticación.

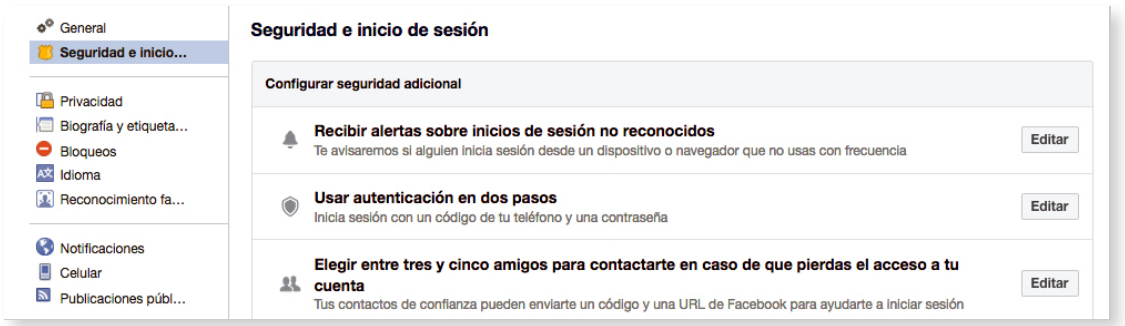


Figura 5. Menú de Seguridad e inicio de sesión

2

WhatsApp

Es una aplicación de mensajería instantánea que permite enviar mensajes y contenido multimedia a los usuarios de la misma, actualmente, la popularidad de esta aplicación ha aumentado en México, es por ello que se sugiere atender las siguientes recomendaciones para la protección de la privacidad.

Configurar la Privacidad: Esta opción permite configurar quiénes pueden ver del perfil la siguiente información:

- Ultima conexión
- Foto de perfil
- Información
- Estados

Adicionalmente, se puede bloquear contactos y activar o desactivar la confirmación de lectura de mensajes.

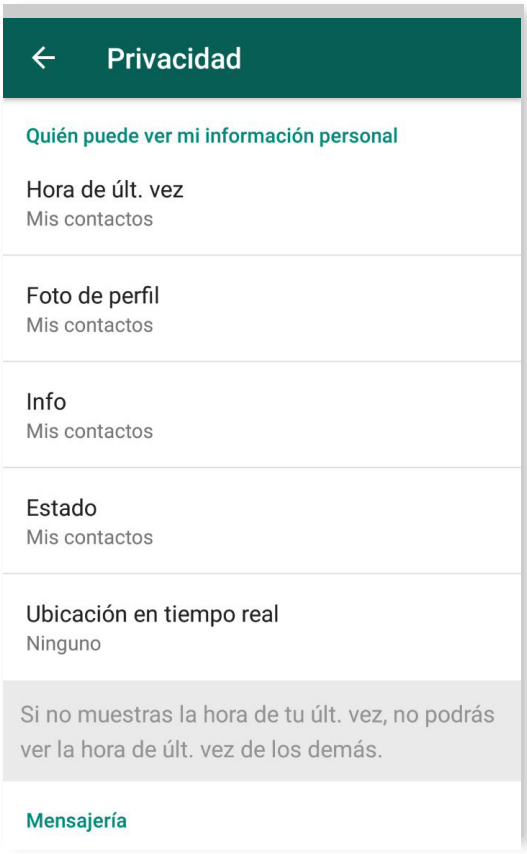


Figura 6. Privacidad en WhatsApp

Seguridad: Esta opción indica que existe un cifrado de extremo a extremo en las comunicaciones, esto quiere decir que los mensajes están seguros y que sólo el remitente y el receptor pueden leer el contenido. En esta opción se puede comprobar que los mensajes y llamadas son seguras al verificar en la pantalla las notificaciones de seguridad.

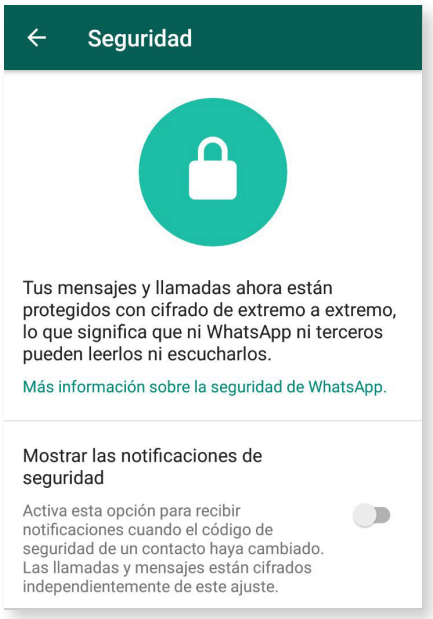


Figura 7. Cifrado en WhatsApp

Configurar la verificación de dos pasos: Para mayor seguridad, se puede activar la verificación de dos pasos, la cual solicitará un PIN que se debe definir, mismo que se utilizará como contraseña cada vez que se reinstale la aplicación.

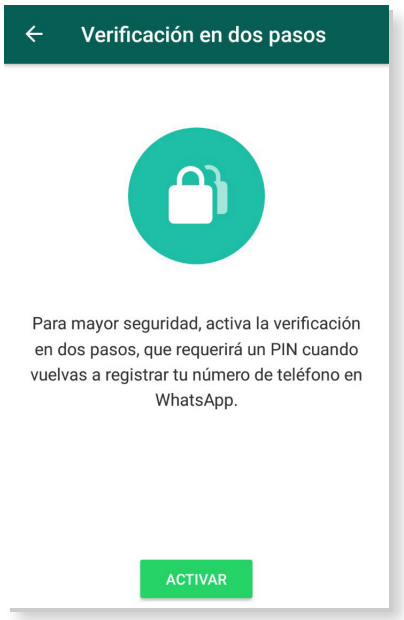


Figura 8. Verificación de dos WhatsApp

Revisar el uso de la versión web: La versión *web* es una novedad, es recomendable ser cuidadoso al usarla, ya que se puede dejar abierta la sesión en un navegador *web* y la aplicación no notifica que esto ha ocurrido, lo cual dejará expuestas las conversaciones.

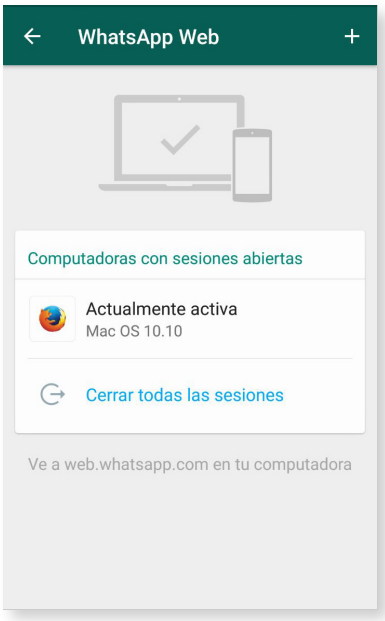


Figura 9. Versión web de WhatsApp

3

Twitter
Es una red social que permite que sus usuarios compartan contenidos con hasta 280 caracteres escritos, esta red social permite que los usuarios sigan diferentes cuentas y etiqueten a otros usuarios en sus publicaciones.

Configuración de Privacidad y Seguridad: Twitter cuenta con una sección dedicada a la configuración de privacidad y seguridad, para ingresar se debe dar clic en la imagen del usuario y buscar la opción *Configuración y privacidad*.

Figura 10. Menú de configuración y privacidad de Twitter

En esta sección se podrá configurar:

1) Privacidad de los Tweets, esta opción permitirá proteger las publicaciones para que solamente los contactos del usuario puedan verlas y, éstas no sean compartidas fuera del perfil.

2) Ubicación de Tweets, esta opción permite habilitar la detección automática y poner la ubicación de manera predeterminada en cualquier publicación que se realice.

3) Etiquetado de fotos, en esta opción se puede habilitar quiénes pueden etiquetar al usuario en fotografías.

4) Visibilidad, esta opción permite que los demás puedan encontrar al usuario a través de la cuenta de correo electrónico.

5) Personalización de datos, esta opción es muy importante, dado que permite gestionar el modo en que *Twitter* personaliza contenido y cómo recolecta y comparte ciertos datos.

6) Mensajes directos, en esta opción se configura si se admite que los usuarios que no son seguidores, puedan enviar mensajes directos.

7) Seguridad**,** esta opción gestiona el contenido que hay en *Twitter*, lo cual permite ocultar publicaciones que podrían ser sensibles, contenido multimedia que contenga imágenes con violencia implícita y eliminar las publicaciones en el muro del usuario de quienes han sido bloqueados.

Figura 11. Menú de configuración y privacidad de Twitter

Configuración de las notificaciones por correo: *Twitter* cuenta con una opción que permite recibir alertas sobre inicios de sesión no reconocidos a través del envío de un correo electrónico, cuando se detecte alguna de las opciones que trae pre configuradas en este menú. En particular, *Twitter* avisará cuando se trate de iniciar sesión con la cuenta en cualquier dispositivo, indicando el lugar aproximado en el que se realizó esta actividad y el navegador *web* o aplicación en donde fue utilizada.

Para habilitar esta opción, ir a la opción *Notificaciones por correo* y activar el correo electrónico, seleccionar las actividades por las cuales se desea recibir correos, por ejemplo, tendencias en la red, actualizaciones, entre otras.

Figura 12. Menú de configuración de Notificaciones por correo

Configuración de la autenticación en dos pasos: Cuando se requiera iniciar sesión, *Twitter* enviará un mensaje de texto con un código que se necesitará para acceder a la cuenta.

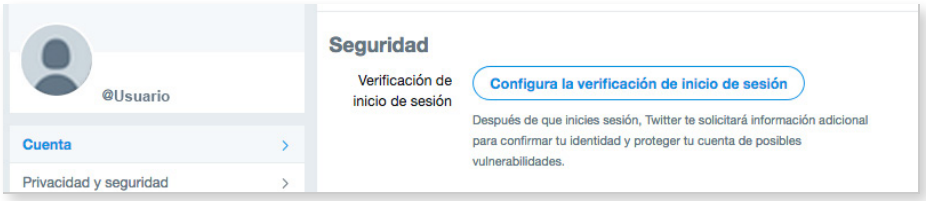


Figura 13. Menú de configuración de Seguridad

Controla las aplicaciones vinculadas a la cuenta de red social: Cuando se desee revisar qué aplicaciones se han vinculado con la cuenta de red social.

Figura 14. Menú de aplicaciones

4

YouTube

Es una aplicación para ver y compartir videos. Esta plataforma incluye una sección que permite la interacción con otros usuarios a través de comentarios en los videos y un indicador que permite señalar si el contenido gusta o no, además de que permite denunciarlo. Es importante considerar las configuraciones de privacidad del video antes de ponerlo en la red.

YouTube permite configurar la privacidad de los videos, y para ello cuenta con tres opciones disponibles:

- Público: El vídeo puede ser visto por todos
- Privado: Sólo los usuarios seleccionados pueden ver el vídeo
- Oculto: Sólo los usuarios con el enlace al vídeo pueden verlo

Si la cuenta es para videos personales, se recomienda ampliamente que los videos sean privados, de esta manera se podrán compartir con algunos amigos y no estarán disponibles para todos los usuarios de YouTube.

Figura 15. Panel de privacidad de video

5

Instagram

Esta red social permite compartir contenido multimedia a través de fotografías, videos y transmisiones en vivo, con la finalidad de interactuar con otros usuarios mediante mensajes directos, y comentarios en las publicaciones. Además, permite indicar si algún contenido es del agrado de los seguidores.

Volver la cuenta privada: Ir al menú *Opciones* y selecciona *Cuenta Privada*. Esto hará que quienes deseen acceder al contenido, deben previamente solicitar seguir al usuario, lo cual le da el control del círculo de amigos y seguidores.

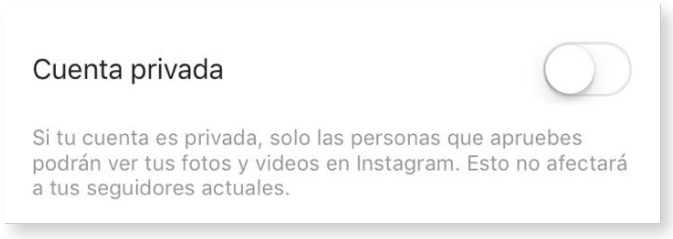


Figura 16. Habilitación de Cuenta privada

Verificar la geolocalización: Al realizar una publicación, se podrá ver que existe la posibilidad de agregar la ubicación, la cual puede mantenerse en privado.

Evitar la publicación simultanea: Esta opción, antes de publicar, permite incluir la publicación de manera simultánea en *Facebook* y *Twitter*, para lo cual se tendrán que ligar estas redes sociales. Es importante recordar que, si se publica un contenido, éste se someterá a la configuración de privacidad de la red social que se tenga vinculada.

Habilita el etiquetado: Al igual que *Facebook*, esta red social indica si el usuario ha sido etiquetado en algún contenido, y se podrá gestionar si quiere que éste aparezca en su perfil o no. Se debe recordar que, si no se acepta ser etiquetado, la fotografía seguirá en la red social accesible para los contactos de quien lo etiquetó.

Figura 17. Panel de verificación de geolocalización, publicación simultánea y etiquetado

RECOMENDACIÓN 3

Protege el acceso a tus dispositivos y cuentas

¿Por qué es importante tener el control del acceso a tus dispositivos y cuentas?

Tener el control personal para acceder a los dispositivos y cuentas, es una medida de seguridad básica para la protección de la información, y así evitar que personas mal intencionadas hagan uso de ellos sin autorización.

Para evitar esto, existen medidas como el uso de contraseñas, autenticación en dos pasos, uso de datos biométricos y aplicaciones o dispositivos para la verificación de la identidad del usuario.

El principal objetivo de estas medidas consiste en comprobar la identidad del propietario del dispositivo o cuenta, para permitir su acceso, de tal forma que los archivos, documentos, fotografías y/o datos personales queden protegidos de accesos no autorizados.

RECUERDA...

DEBES IMPLEMENTAR LAS MEDIDAS DE SEGURIDAD PARA EVITAR QUE ALGUIEN HAGA USO DE TU DISPOSITIVO O CUENTA.

LOS CONTROLES DE ACCESO TE PUEDEN AYUDAR CON ESTA TAREA.

Existen diferentes medidas para proteger los accesos a dispositivos y cuentas. A continuación, se presentarán las más recomendables.

a) Contraseñas e inicio de sesión:

Contar con una contraseña para acceder a los dispositivos y servicios es una práctica fundamental y necesaria, para controlar quién puede tener acceso a la información, gestionar el nivel de acceso y los privilegios que se otorgan a la misma.

Contraseñas: La mayoría de las personas están familiarizadas con el concepto de contraseña, que se refiere al uso de un código secreto para tener acceso a un equipo de cómputo, archivo o servicio.

Es recomendable que toda la información personal que se encuentre en un medio digital sea protegida a través de bloqueos por contraseña, para evitar accesos no autorizados y posibles eventos de robo o pérdida de información.

Para la creación de una contraseña robusta, se proporcionan los siguientes consejos:

1. Cuando el dispositivo o la aplicación lo permitan, utilizar frases como contraseñas (conocidas como *passphrase*). Entre más caracteres tiene una contraseña, más difícil resulta adivinarla o "romperla".
2. Si sólo se pueden utilizar contraseñas cortas, construirlas utilizando la combinación de mayúsculas, minúsculas, números y caracteres especiales.
3. Evitar el uso de contraseñas que hayan sido vulneradas, palabras de diccionario, caracteres repetitivos o secuenciales, palabras de un contexto específico como nombres de servicios, usuarios, nombre de marcas.
4. Para la recuperación de contraseñas, se recomienda hacer uso de preguntas abiertas en lugar de las sugeridas, que pueden ser fáciles de adivinar.
5. Las contraseñas deben cambiarse solamente si el suscriptor lo solicita o si existen indicios o evidencia de que ha sido comprometida.

Verificador de seguridad de contraseñas: es una herramienta que ayuda a corroborar qué tan segura es la contraseña proporcionada. Existen distintos tipos de verificadores gratuitos a los cuales se puede acceder para llevar a cabo esta revisión.

Es importante indicar que los servicios de verificación de contraseña cuentan con fórmulas matemáticas y algoritmos que calculan el tiempo que tardaría un *software* en descifrar la contraseña, estos servicios no almacenan datos y son gratuitos.

Administrador de contraseñas: es un *software*, aplicación o extensión del navegador, que almacena las contraseñas de cualquier cuenta y las cifra a través de una contraseña maestra, este tipo de herramienta, además, permite generar contraseñas seguras y verificar en un directorio las contraseñas que fueron asignadas a cada cuenta.

Control de inicio de sesión: se refiere a la correcta administración de los usuarios, contraseñas y privilegios de acceso (permisos para leer y modificar archivos). Cada sistema operativo permite tener un usuario administrador con todos los privilegios para gestionar los permisos y restricciones que tendrán el resto de los usuarios. Es recomendable hacer uso de cuentas diferentes a la de administrador, ya que en caso de comprometerse tendrá restricciones que le impedirán al atacante generar una mayor afectación.

b) Autenticación

La autenticación es la forma en la que cualquier dispositivo, *software* o aplicación corrobora la identidad del usuario para otorgar el acceso. Su funcionalidad consiste en garantizar que sólo el usuario autorizado pueda acceder a su cuenta o dispositivo.

Para una mayor seguridad, se han incorporado medidas adicionales para una autenticación más efectiva, esto a través del envío de un código a un dispositivo de confianza mediante un mensaje instantáneo, de texto o llamada de voz, o en su caso, la validación a través del uso de datos biométricos.

Autenticación en dos pasos: consiste en que, una vez ingresada la contraseña, se envía un código al dispositivo de confianza, que se haya configurado de forma previa, por ejemplo, al teléfono celular, el cual deberá ingresarse de forma complementaria a la contraseña para poder acceder a la cuenta. Esta medida de seguridad adicional es importante, ya que en caso de que alguien lograra conocer la contraseña, no podría acceder a la cuenta sin el código que fue enviado al dispositivo.

Uso de datos biométricos: consiste en permitir el acceso únicamente al usuario del dispositivo o cuenta, previo reconocimiento del dato biométrico configurado, por ejemplo, a través del reconocimiento facial, huella dactilar, voz o iris.

¿Qué puedo hacer para proteger mis dispositivos y cuentas?

1. Establece contraseñas robustas en dispositivos y cuentas.
2. No compartas contraseñas.
3. Ten diferentes contraseñas para cada equipo de cómputo y dispositivo móvil.
4. Para gestionar el acceso a programas, aplicaciones, y servicios, haz uso de administradores de contraseñas.
5. Utiliza autenticación en dos pasos, cuando sea posible.

A continuación, se presenta una lista de *software* y aplicaciones de utilidad para implementar esta recomendación y con ello proteger los accesos a cuentas y dispositivos:

NOMENCLATURA

Win- Sistema Operativo *Microsoft Windows*	iOS- Sistema Operativo para móviles de *Apple*	ES- Idioma español
Mac OS- Sistema Operativo *Apple*	An- Sistema Operativo para móviles de *Google*	EN- Idioma inglés

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
ADMINISTRADORES DE CONTRASEÑAS	Password Boss Gestor de contraseñas, implementa protección antirrobo con borrado remoto.	X		x	x		x		x
	KeeWeb Herramienta de gestor de contraseñas, disponible en versión de escritorio como aplicación web online, incluye generador de contraseñas.	X	x				x		x
	Dashlane Administrador de contraseñas que permite iniciar sesión automáticamente en cualquier sitio web y desde todos los dispositivos.	X	x	x	x		x		x
	LastPass Manager Gestor de contraseñas enfocado al almacenamiento de contraseñas de distintas páginas web.	X	x	x	x	x	x		x
	KeePass Password Safe Gestor de contraseñas que permite proteger de forma segura las contraseñas a través de una contraseña maestra.	X	x				x		x
	1Password Gestiona las contraseñas a través de una contraseña maestra.	X	x	x	x	x			x
VERIFICADOR SEGURIDAD	Asociación de Internautas https://goo.gl/Pe5Nfz						x	x	
	Kaspersky Lab https://password.kaspersky.com/mx/						x	x	
	How secure is my password? https://howsecureismypassword.net/						x		x
AUTENTICACIÓN DOS PASOS	iCloud	X	x	x			x	x	x
	Cuenta Google Gmail, Google drive, YouTube, G+	X	x	x	x		x	x	x
	Facebook	X	x	x	x		x	x	x
	Twitter	X	x	x	x		x	x	x
	Microsoft	X	x	x	x		x	x	x
	WhatsApp			x	x		x	x	x
	Google Authenticator			x	x		x	x	x

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
BIOMÉTRICOS	Touch ID			x			x	x	x
	Face ID			x			x	x	x
	Escáner de iris				x		x	x	x
	Lector de huella digital en Android				x		x	x	x
	Lector huella digital en Windows	x					x	x	x
CONTROL DE INICIO DE SESIÓN	Configuración de cuentas de usuarios para Windows	x					x	x	x
	Configuración de cuentas de usuarios para MacOS		x				x	x	x
	Sesión de invitado en Android				x		x	x	x

RECOMENDACIÓN 4

Administra tus dispositivos

¿Por qué es importante administrar tus dispositivos?

Los dispositivos guardan todo tipo de datos personales e información derivada de las actividades que se realizan, la cual se debe proteger para evitar que se extravíe o se conozca por personas no autorizadas. Ante esta posibilidad, es importante conocer las herramientas que permiten administrar los dispositivos, las cuales tienen funciones que permiten su búsqueda, bloqueo, realizar respaldos o eliminar, incluso de manera remota, cualquier información que contengan.

Actualmente *Google* y *Apple* cuentan con aplicaciones únicas para sus dispositivos, entre las que se encuentran la búsqueda o rastreo, borrado, bloqueo y respaldo de contenido para los dispositivos. Estas herramientas se encuentran asociadas a una cuenta única, y para hacer uso de ellas el usuario debe

RECUERDA...

TENER EL CONTROL DE TUS DISPOSITIVOS TE AYUDA A PROTEGER TU INFORMACIÓN PERSONAL

activarlas. De forma adicional, se pueden instalar aplicaciones que permiten realizar cualquiera de estas funciones, descargables desde la tienda oficial del dispositivo.

A continuación, se describen algunas funcionalidades que proporcionan las distintas herramientas para la administración de dispositivos:

Búsqueda o rastreo: para poder localizar el dispositivo es necesario configurar previamente el GPS, de tal forma que la herramienta de búsqueda o rastreo, pueda ubicarlo de forma aproximada en un mapa. Esta opción resulta efectiva para localizar un dispositivo en caso de robo o extravío.

Bloqueo: esta función está diseñada para evitar que personas no autorizadas utilicen el dispositivo en caso de robo o pérdida, la función se activa de manera remota y sólo puede desactivarse ingresando la contraseña de usuario configurada en el dispositivo. Esta función bloquea la pantalla, muestra un mensaje personalizado e impide que el dispositivo sea utilizado.

Respaldo: la información y los datos personales almacenados en teléfonos celulares o cualquier dispositivo, puede dañarse de manera parcial o total debido a fallas en los sistemas o aplicaciones, por errores de operación de las personas, o bien por variaciones inesperadas de energía eléctrica. Una forma de prevenir esto, consiste en realizar copias de seguridad de manera regular, o cuando se presenten cambios significativos en los datos que se almacenan. Para saber más sobre respaldos se puede consultar la recomendación *06 Respalda periódicamente tu información*.

Borrado: esta función permite eliminar de forma remota la información almacenada en el dispositivo, por ejemplo, contraseñas de acceso a aplicaciones, contenido multimedia, aplicaciones de pago, fotografías, videos. El borrado remoto del dispositivo se realizará cuando éste se conecte a Internet, se debe tomar en cuenta que después de borrar el contenido del dispositivo no se podrá recuperar la información que se haya eliminado.

Para mayor información sobre el **borrado seguro** se puede consultar la Guía para el Borrado Seguro de Datos Personales,[1] elaborada por el INAI.

¿Qué puedo hacer para administrar mis dispositivos?

1. Habilita la herramienta de administración remota con la que cuente tu dispositivo de fábrica.
2. Las herramientas de administración suelen requerir muchos permisos, revisa si son proporcionales o necesarios para el correcto funcionamiento de la herramienta.
3. Si instalas herramientas adicionales a las proporcionadas por el fabricante del dispositivo, verifica que los permisos de la aplicación no entren en conflicto con la herramienta incluida de fábrica.
4. Para utilizar las características de administración remota de los dispositivos, mantén habilitadas las configuraciones correspondientes como conexión a Internet y GPS.
5. Considera una contraseña para desbloqueo del equipo y de ser posible otra contraseña para las herramientas de administración de dispositivos.

[1] Consultable en: http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

A continuación, se presenta una lista de aplicaciones que pueden ser utilizadas para administrar los dispositivos y con ello proteger la información y datos personales almacenados:

NOMENCLATURA		
Win- Sistema Operativo *Microsoft Windows*	iOS- Sistema Operativo para móviles de *Apple*	ES- Idioma español
Mac OS- Sistema Operativo *Apple*	An- Sistema Operativo para móviles de *Google*	EN- Idioma inglés

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
	Prey Anti-Theft *Software* antirrobo para equipo de cómputo o dispositivos móviles permite localizar, bloquear y borrar de forma remota.	x	x	x	X	x	x		x
	Find my iPhone Aplicación que ayuda a encontrar cualquier dispositivo *Apple* a través de la localización en un mapa, permite al usuario el bloqueo, reproducción de sonido, mostrar mensaje en pantalla o borrar todos los datos.		x	x			x	x	x
	Avast Mobile Security & Antivirus Ofrece protección a los móviles frente a virus, permite la localización del dispositivo perdido o robado.	x	x	x	X		x	x	x
	Android Lost Aplicación que permite, la localización del dispositivo, borrado remoto, tomar foto remota para captar la imagen de la persona que lo tiene y bloqueo a través de una contraseña.				X		x		x

RECOMENDACIÓN 5

Descarga *software* y aplicaciones de los sitios oficiales

¿Por qué es importante descargar *software* y aplicaciones de los sitios oficiales?

Hoy en día, existe una gran cantidad de *software* y aplicaciones que se puede descargar de Internet, basta con buscar desde cualquier navegador *web* el nombre del programa o aplicación que se quiere instalar y abrir el primer resultado para encontrar un archivo en formato descargable.

Cuando se requiera instalar cualquier tipo de *software* o aplicación, se recomienda hacerlo directamente de la página o tiendas oficiales, ya que existen sitios *web* no confiables, generalmente con una gran cantidad de publicidad, que proporcionan versiones desactualizadas de *software* legítimo, o contaminadas por códigos maliciosos, lo cual representa un riesgo considerable para la información y datos personales que se almacenan en los dispositivos.

RECUERDA...

VERIFICA QUE EL SOFTWARE O APLICACIONES QUE DESCARGAS PROVENGAN DE SITIOS OFICIALES

Para el caso de los dispositivos móviles que sólo permiten la instalación de aplicaciones (apps), existen tiendas oficiales que son gestionadas por los desarrolladores del sistema operativo móvil, quienes revisan y validan todas las aplicaciones que se suben a las tiendas, con el objetivo de garantizar que las apps disponibles cumplan con los estándares de desarrollo y medidas de seguridad establecidas.

a) *Software*

Existen diferentes fuentes donde se puede descargar el *software*, de forma confiable como son:

Sitio web oficial del fabricante o desarrollado: generalmente cuenta con una sección de descargas, en dónde además del *software* se encuentran las instrucciones de instalación, datos sobre compatibilidad, versiones anteriores o programas adicionales.

Descarga de usuarios verificados: esto se refiere a obtener el *software* a través de un enlace de descarga directa proporcionado por una persona conocida, y generado por cualquier servicio de almacenamiento en la nube.

b) Aplicaciones

Para los móviles es recomendable utilizar sólo los canales oficiales para la instalación de aplicaciones móviles.

¿Qué puedo hacer para descargar *software* y aplicaciones de forma segura?

1. No modifiques la configuración de fábrica de los dispositivos.
2. Descarga *software* y aplicaciones de sitios *web* y tiendas oficiales.
3. Verifica los permisos y accesos requeridos por el *software* o aplicación antes de otorgarlos.

A continuación, se presenta información sobre las tiendas oficiales IOS de *Apple* y *Android* de *Google* para la descarga de aplicaciones para móviles:

Nombre	Logotipo	Sistema operativo	Descripción
App Store		*IOS*	Es la tienda oficial de *Apple* y solo es accesible mediante dispositivos con sistema operativo *IOS*. https://www.apple.com/mx/ios/app-store/
Android *Play Store*		*Android*	La tienda oficial de *Google*, lleva por nombre *Play Store* y solo es accesible mediante dispositivos con sistema operativo *Android*, el logotipo que la identifica se presenta a continuación. https://play.google.com/store/apps?hl=es

RECOMENDACIÓN 6

Protégete del *malware*

¿Por qué es importante protegerse del *malware*?

Existen diferentes tipos de *software* malicioso o malware como virus, troyanos, gusanos, programas espías, entre otros, que tienen como objetivo afectar la seguridad de los dispositivos, extraer información o datos personales de los usuarios, como contraseñas, números de cuenta bancaria, fotografías, videos, entre otros.

Por lo anterior, es importante instalar en los equipos de cómputo y dispositivos móviles *software* **antivirus**, así como herramientas complementarias que brinden una mayor protección contra el *malware*.

a) Antivirus

Los antivirus son programas que mediante un escaneo al equipo o dispositivo detectan, identifican y eliminan programas maliciosos. Para un resultado efectivo, es fundamental que el antivirus siempre esté actualizado. Lo

RECUERDA...

INSTALA EN TU DISPOSITIVO UN SOFTWARE ANTIVIRUS Y MANTENLO SIEMPRE ACTUALIZADO

anterior, debido a que éste realiza un escaneo para buscar *malware*, el cual se compara contra una base de datos que contiene las firmas del antivirus.

Actualmente, existe un mercado amplio de *software* antivirus para cualquier sistema operativo, algunas opciones son gratuitas, con características restringidas, otras requieren para su uso de una licencia cuyo costo debe cubrirse de forma anual.

Para equipo de cómputo: El *software* antivirus para equipos de cómputo es el más completo, dado que está diseñado para monitorear el tráfico de archivos, descargas y las conexiones de dispositivos periféricos al equipo de cómputo, generando alertas cuando detecta una amenaza potencial, de forma adicional, se pueden realizar escaneos al equipo en busca de *malware* en todo momento.

Para dispositivos móviles: El *software* antivirus para móviles tiene un funcionamiento limitado, dado que está diseñado para verificar los archivos y aplicaciones que se encuentran dentro de los dispositivos. Adicionalmente, incluye bloqueos de aplicaciones y monitoreo de tráfico *web*.

Existen en el mercado, paquetes de licencias antivirus para equipos de cómputo que incluyen la protección para dispositivos móviles.

b) Escáner antimalware

El escaneo antimalware es una medida de protección adicional al antivirus, este *software* se ejecuta directamente en el dispositivo donde está instalado y realiza una búsqueda de malware en sus archivos, para identificar y eliminar amenazas que pueden no ser identificadas por el antivirus.

¿Qué puedo hacer para proteger mis datos personales del malware?

1. Utiliza un *software* antivirus para el equipo de cómputo y los dispositivos móviles.
2. Actualiza frecuentemente el *software* antivirus instalado.
3. Realiza escaneos antimalware para identificar posibles amenazas que no hayan sido detectadas por el antivirus.
4. Revisa con el *software* antivirus todo dispositivo que se conecte al equipo de cómputo (usb, tarjeta sd, CD, DVD) previo a su uso.

A continuación, se presenta un listado de *software* antivirus y para el escaneo antimalware, que pueden ser de utilidad para implementar esta recomendación de seguridad en el manejo de la información personal:

NOMENCLATURA		
Win- Sistema Operativo *Microsoft Windows*	iOS- Sistema Operativo para móviles de *Apple*	ES- Idioma español
Mac OS- Sistema Operativo *Apple*	An- Sistema Operativo para móviles de *Google*	EN- Idioma inglés

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
EQUIPO DE CÓMPUTO	*Kaspersky Rescue Disk 10* Solución antivirus para eliminar malware sin necesidad de arrancar el sistema operativo infectado.	x					x		x
	Malwarebytes antirootkit Herramienta para detectar y eliminar infecciones por *malware*.	x				x	x		x
	Malware Bytes Anti-Malware Herramienta que incluye protección contra distintos tipos de infecciones por *malware*.	x				x	x		x
	Iobit Malware Fighter Herramienta que brinda protección contra distintos de *malware e intrusiones*.	x				x	x		x
	SpyBot Search & Destroy Herramienta que elimina *malware, spyware* y *adware*.	x					x		x
	Ad-Aware Free Antivirus Herramienta antivirus y *anti-espía*.	x					x		x
	Avira Free Antivirus Herramienta que realiza la detección de *malware* en tiempo real.	x	x	x	x		x	x	x
	Microsoft Security Essentials Herramienta antivirus de escritorio para sistemas operativos *Windows*.	x					x	x	x
	Sophos Anti-Virus for Mac OS X Herramienta antivirus para *Mac*, brinda protección contra virus, troyanos y gusanos.		x				x	x	x
	Avast! Free Herramienta antivirus realiza diferentes formas de escaneo en búsqueda de virus en el sistema.	x					x	x	x
	AVG Antivirus Herramienta antivirus de fácil uso que incluye de forma adicional un *firewall* para proteger las conexiones del equipo.	x	x				x	x	x

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
MÓVIL	*AppBrain Ad Detector* Aplicación para sistemas *Android*, para detectar publicidad que se muestren de otras aplicaciones descargadas.				x		x		x
	Avast Mobile Security & Antivirus Brinda protección a los dispositivos móviles frente a virus y ante robo del dispositivo.				x		x		x
	Norton Mobile Security Antivirus Brinda protección antivirus a dispositivos móviles como tabletas y teléfonos inteligentes Android e *iOS.*			x	x		x		x

RECOMENDACIÓN 7

Mantén actualizado tu *software* y aplicaciones

¿Por qué es importante actualizar el software y las aplicaciones?

El *software*, sistemas operativos, programas y aplicaciones, se encuentran constantemente en revisión de errores de seguridad y funcionalidad, buscando su mejora continua, cuando los desarrolladores identifican algún punto que requiere reforzarse, ponen a disposición de los usuarios actualizaciones que funcionan como "parches", con la finalidad de evitar que estos huecos sean identificados y aprovechados por atacantes.

Por esta razón, se debe mantener actualizado el *software* utilizado y tomar en cuenta lo siguiente:

- Las actualizaciones suceden principalmente por dos razones:
  - Por un hueco o falla que compromete la seguridad del

RECUERDA...

ACTUALIZAR TU SOFTWARE Y APLICACIONES REFUERZA TU SEGURIDAD

software y su información, ante este escenario se sugiere actualizar de inmediato, para proteger el software.
    - Cuando se presentan mejoras en la interfaz o se adicionan funciones al *software*, en este caso es conveniente esperar a que los desarrolladores tengan una versión estable.
- Los equipos de cómputo actuales, en su mayoría vienen pre configurados para actualizarse de manera periódica, se recomienda verificar que efectivamente esta funcionalidad se encuentre activada, de lo contrario, el usuario deberá fijar un periodo para buscar actualizaciones de forma manual.
- Las aplicaciones para dispositivos móviles adquiridas a través de las tiendas oficiales, tienen sus actualizaciones aseguradas por este medio, donde se proporciona información sobre la nueva versión y las características incluidas.

¿Cómo mantengo actualizado el *software* y las aplicaciones que utilizo?

1. Actualiza el sistema operativo, *software* y aplicaciones para contar siempre con las últimas versiones.
2. Configura las actualizaciones para que se realicen de forma automática.
3. Permite la instalación de las actualizaciones cuando éstas estén disponibles.

La siguiente información práctica, te puede resultar de utilidad para implementar esta recomendación:

a) Configuración de actualizaciones en *Windows*

Microsoft cuenta con un gestor de configuración de actualizaciones, el cual se llama *Windows Update*. Para su configuración se realiza los siguientes pasos:

1. Ingresar a *Configuración* desde la barra de inicio

2. Seleccionar el menú *Actualización y seguridad*

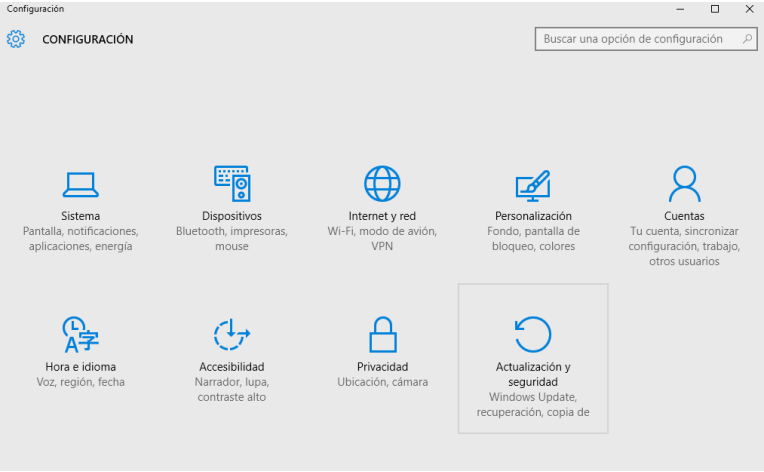


Figura 1. Panel de configuración

3. Dar clic en *Opciones avanzadas*

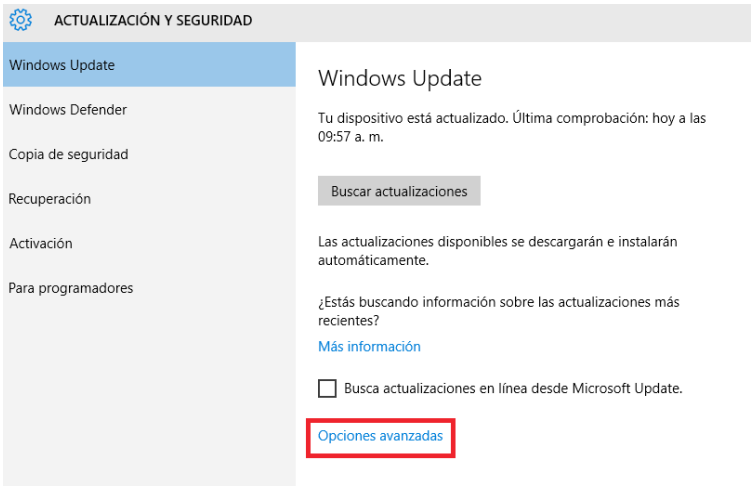


Figura 2. Panel de actualización y seguridad

4. Seleccionar la opción *Elige cómo quieres instalar las actualizaciones*, para esto, se recomienda dejar marcada la opción *Automático*, adicionalmente, seleccionar la opción de avisar sobre las actualizaciones de otros productos de *Microsoft* al actualizar *Windows*.

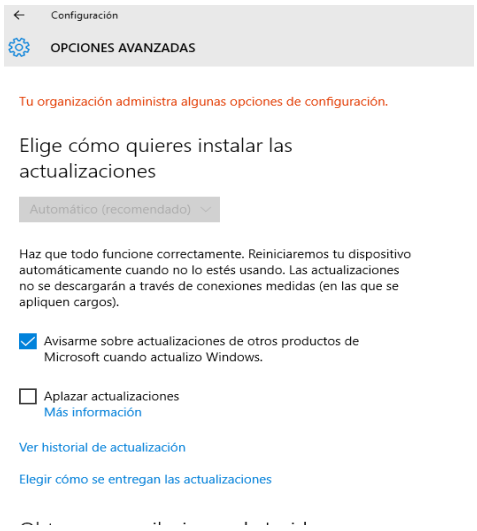


Figura 3. Panel de opciones avanzadas

b) Configuración de actualizaciones para Mac OS e iOS

Apple cuenta con un servicio integral para activar las descargas automáticas, este servicio actualiza todas las aplicaciones que se tengan instaladas tanto en dispositivos con *software* Mac OS como en dispositivos móviles con *software* iOS.

Se debe tener en cuenta que después de activar las descargas automáticas, todas las aplicaciones que se consigan mediante las tiendas oficiales, desde cualquier dispositivo *iPhone, iPad, iPod touch* o *Mac*, se actualizarán automáticamente en todos los dispositivos.

Configuración automática de actualizaciones desde un equipo de cómputo Mac OS

1. Abre *iTunes* desde la computadora.
2. Autoriza *iTunes* dando clic en la Tienda > *Dar autorización a este equipo*.
3. Ubica la barra de menús ubicada en la parte superior de la pantalla de la computadora, selecciona *iTunes > Preferencias*.
4. Haz clic en la pestaña *Descargas* y, selecciona el contenido que quieres que se descargue automáticamente.

Figura 4. Panel de configuración en Mac

Configuración de actualizaciones manualmente en Mac OS

Para comprobar si existen actualizaciones de *software* de Mac, realice lo siguiente:

1. Abre la *app Store* en la Mac
2. Da clic en *Actualizaciones* en la barra de herramientas.

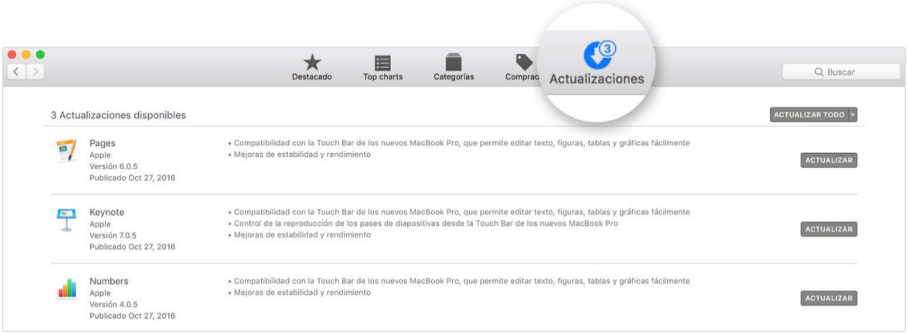


Figura 5. Panel de actualizaciones de Mac App Store

Nota: para el caso del sistema Mac OS, él mismo indica que existe una versión actualizada.

Configuración automática de actualizaciones desde un dispositivo móvil IOS

1. Ingresar en el dispositivo móvil a *Configuración > [nombre] > iTunes y App Store*.
2. Activar el contenido que se quiere descargar automáticamente.

Figura 6. Panel de actualizaciones de *iPhone*

Actualización manual del Sistema operativo para IOS

1. Ingresar a *Configuración > General > Actualización de software*.

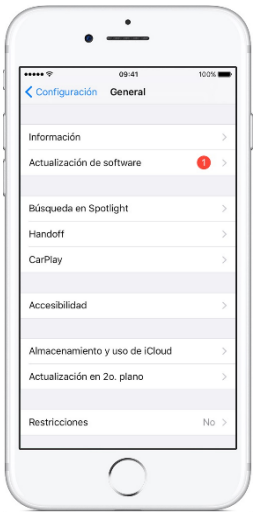


Figura 7. Pantalla de configuración

- Al ingresar a este menú se verá la versión de software que se tiene activa, en caso de que haya alguna aplicación, seleccionar Descargar e instalar. Si aparece un mensaje que indica que se debe eliminar aplicaciones debido a que iOS necesita más espacio para la actualización, dar clic en Continuar o Cancelar.

- Se puede actualizar de inmediato, seleccionando *Instalar*, también se puede instalar posteriormente, dando clic en *Más tarde* y seleccionando *Instalar esta noche o Recordar más tarde*. Si se indica *Instalar esta noche*, se debe conectar el dispositivo iOS a la corriente y el dispositivo se actualizará automáticamente por la noche.

Actualización manual de aplicaciones móviles en IOS

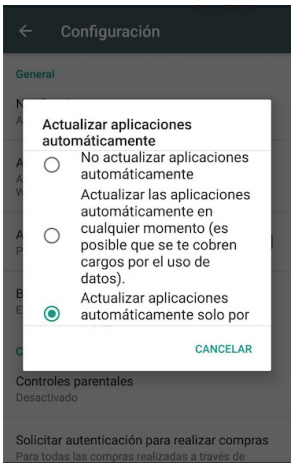
1. Abrir la aplicación App Store
2. Dar clic en Actualizaciones en la barra inferior de la pantalla

Figura 8. Panel de actualizaciones de App Store

c) Configuración de actualizaciones para *Android*

1. Desde el dispositivo móvil abrir la app de *Google Play Store*
2. Presionar el Menú ☰ > **Configuración**.
3. Seleccionar *Actualiza apps automáticamente*.

4. Indica alguna de las siguientes opciones:
   - *Actualizar aplicaciones automáticamente:* Actualiza las apps en cualquier momento, ya sea mediante una red Wi-Fi o de datos móviles.
   - *Actualizar aplicaciones automáticamente solo por Wi-Fi*: Actualiza las apps solo cuando te conectas a una red Wi-Fi.



RECOMENDACIÓN 8

Respalda periódicamente tu información

¿Por qué es importante respaldar mi información personal?

El respaldo, copia de seguridad o *backup* consiste en realizar un duplicado de documentos, archivos, carpetas o aplicaciones contenidas en un equipo de cómputo o dispositivo móvil, con la finalidad de recuperar la información en caso de que el dispositivo o equipo sufra algún daño, que impida tener acceso a la información y/o datos personales que se almacenan.

¿Cómo puedo respaldar mis datos personales?

Para realizar de forma adecuada un respaldo es importante considerar los siguientes pasos:

1. Identifica información a respaldar	Se debe identificar y clasificar la información, de tal forma que se respalde sólo aquella que por su nivel de importancia lo requiera, así como todo aquello que no pueda volver a obtenerse con facilidad.
2. Determina el tipo de respaldo	El tipo de respaldo a utilizar dependerá de las necesidades de cada usuario. Totales, si se desea copiar toda la información y si existen cambios significativos en la misma en poco tiempo. En caso de ser información que no varíaa significativamente, se recomienda sólo hacer respaldos parciales con aquélla que cambie.
3. Selecciona medio de almacenamiento	Se debe identificar y clasificar la información, de tal forma que se respalde sólo aquella que por su nivel de importancia lo requiera, así como todo aquello que no pueda volver a obtenerse con facilidad.
4. Decide la frecuencia en que se realizará	Es fundamental establecer la periodicidad con la que se realizará el respaldo de la información, eso debe decidirse con base en la frecuencia con que se modifica, elimina o crea la información.
5. Realiza pruebas a los respaldos	Es fundamental establecer la periodicidad con la que se realizará el respaldo de la información, eso debe decidirse con base en la frecuencia con que se modifica, elimina o crea la información.

Para incrementar la posibilidad de que datos perdidos o dañados puedan ser recuperados, el Equipo de Respuesta ante Emergencias Informáticas de Estados Unidos (por sus siglas en inglés US-CERT) recomienda seguir la regla 3-2-1 que consiste en:

03 Mantener **3** copias de cualquier archivo importante (1 primario y 2 copias de seguridad)

02 Mantener los archivos en **2** tipos de medios de almacenamiento diferentes para protegerlos contra diferentes tipos de peligros.

01 Almacenar **1** copia de seguridad fuera del sitio.

En las siguientes tablas se presentan los diferentes medios de almacenamiento comúnmente utilizados para los respaldos, donde se identifican sus ventajas, desventajas y elementos de seguridad que se recomienda tomar en cuenta.

Almacenamiento en la nube	
Ventajas	☐ Ayuda a proteger la información de alguno de los peores escenarios, como desastres naturales, fallas críticas o infecciones por *malware*. ☐ Acceso a la información en cualquier momento y lugar donde se tenga una conexión a Internet. ☐ La compra del servicio está basada en las necesidades del usuario.
Desventajas	☐ La nube depende de una conexión a Internet. ☐ No existen estándares, plataformas o lenguajes universales. ☐ La distribución física de los datos está en servidores geográficamente dispersos, con controles y regulación distinta. ☐ Por desconocimiento, los usuarios pueden ceder y otorgar control sobre sus datos. ☐ Los usuarios de la nube pueden tener poco o ningún control directo sobres sus datos.
Seguridad	☐ Los proveedores a menudo cifran los datos del usuario. ☐ Previo a confiar datos críticos a un proveedor de servicio en la nube, se debe revisar de forma cuidadosa, los elementos relacionados con el servicio. ☐ Para incrementar la seguridad, se recomienda buscar un proveedor que cifre los datos con algoritmos establecidos, los transfiera de forma segura, siga las prácticas recomendadas de seguridad de la red y proteja físicamente los dispositivos que almacenan, procesan y transmiten los datos. ☐ Hay que verificar que las condiciones del servicio garanticen que los datos no se filtren a otros usuarios o clientes.

Discos duros internos	
Ventajas	☐ Debido a su característica de regrabación, pueden ser utilizados para copias de seguridad progresivas (actualización automática y periódica de los archivos con las versiones más recientes). ☐ Actualización de los archivos de forma rápida dado que se encuentra en el mismo dispositivo.
Desventajas	☐ En caso de afectarse el disco duro, puede perderse la información principal y el respaldo. ☐ Si se realizan respaldos frecuentes sin control de los mismos, podría saturarse el almacenamiento del disco.
Seguridad	☐ Cuando se almacena el respaldo en el disco duro interno, éste se expone a las mismas amenazas que la información primaria. ☐ El disco duro interno es tan físicamente seguro, como el equipo de cómputo que lo contiene. ☐ Un disco duro se puede borrar o volverse inutilizable a través de la desmagnetización.

Medios de almacenamiento removibles (discos duros externos, tarjetas SD, USB, CD, DVD y Blu-ray)	
Ventajas	□ Son una alternativa flexible para el almacenamiento de datos dado que son portátiles y funcionan en la mayoría de los equipos de cómputo. □ Se tiene una amplia variedad de capacidades de almacenamiento y precios. □ La mayoría de los medios extraíbles son reutilizables. □ Son dispositivos portables que hacen cómodo y fácil su uso. □ Permiten controlar directamente los datos almacenados.
Desventajas	□ Dada su portabilidad, son más propensos a robos o extravíos. □ Las copias de seguridad pueden ser corrompidas o infectadas de malware si los archivos primarios se encuentran afectados.
Seguridad	□ El usuario es el responsable de proteger los datos almacenados en estos medios removibles. □ Es recomendable cifrar la información que se almacene en estos medios, por su propia exposición. □ También es recomendable conectar los dispositivos sólo a equipos confiables y utilizar un *software* antivirus para su revisión previo a que sean utilizados. □ Se sugiere asegurar el lugar donde se resguardan físicamente.

Asimismo, a continuación, se presenta una lista de herramientas que pueden ser utilizadas para el respaldo periódico y con ello proteger la información y datos personales:

NOMENCLATURA		
Win- Sistema Operativo *Microsoft Windows*	iOS- Sistema Operativo para móviles de *Apple*	ES- Idioma español
Mac OS- Sistema Operativo *Apple*	An- Sistema Operativo para móviles de *Google*	EN- Idioma inglés

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
NUBE	*Dropbox*	x	x	x	x	x	x	x	x
	iCloud		x	x		x	x	x	x
	Google Drive	x	x	x	x	x	x	x	x
	OneDrive	x	x	x	x	x	x	x	x
SOFTWARE / APLICACIONES	*Synkron* Herramienta que ayuda a mantener los archivos y carpetas siempre actualizados.	x	x			x	x		x
	SyncBack Herramienta para realizar respaldos sincronizados.	x				x	x		x
	PureSync Herramienta de sincronización y realización de respaldos de archivos y carpetas.	x				x	x		x
	Genie Timeline Herramienta para realizar respaldos mediante el apoyo de un asistente paso a paso, con opción de hacer copias de forma automática.	x				x	x		x
	Fbackup Herramienta para realizar respaldos con interfaz sencilla y mediante el apoyo de un asistente.	x					x		x
	Helium - App Sync and Backup Aplicación de sincronización de aplicaciones y respaldo para Android.				x		x		x
	Copia de Seguridad de Windows Creación de copias de seguridad de forma automática.	x					x	x	x
	Time machine Función de copia de seguridad integrada en *OS X*, realiza copias de seguridad automáticas de todo el contenido de la *Mac*.		x				x	x	x
	Avira Secure Backup Guarda de forma automática todos los archivos del equipo en un servidor remoto con acceso restringido.	x	x			x		x	x
	Recuva Es una herramienta que permite la recuperación de archivos eliminados.	x				x	x		x
	Cobian Backup Herramienta para realizar copias de seguridad de la información almacenada en el equipo, permite configurar qué se respalda, dónde se almacena y la frecuencia con la que se realiza.	x					x	x	x

RECOMENDACIÓN 9

Cifra tu información

¿Por qué es importante el cifrado de los datos personales?

El *cifrado* es un método que utiliza algoritmos matemáticos y una clave o contraseña para codificar la información, de modo que sólo los usuarios con acceso a esa clave puedan leer e interpretar la información. En la mayoría de los casos, el cifrado puede proporcionar una protección adecuada contra el tratamiento no autorizado o ilícito de datos personales.[2]

De esta forma, el cifrado es una medida de seguridad que puede proteger la confidencialidad de la información almacenada y en tránsito.

Con respecto al almacenamiento de información, el cifrado permite proteger el acceso a los datos que se encuentran en el

RECUERDA...

AL CIFRAR TU INFORMACIÓN TE PROTEGES CONTRA ACCESOS NO AUTORIZADOS QUE CONSTITUYEN UN RIESGO POTENCIAL PARA EL MAL USO DE LA MISMA

[2] Véase: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/

dispositivo, de manera que, aún si alguien no autorizado logra tener acceso a este medio, los datos que obtendrá serán incomprensibles, dado que no cuenta con la clave para tener acceso a la información.

En cuanto al tránsito de información, el cifrado permite la trasmisión segura de datos entre el remitente y el destinatario. De igual forma que en el almacenamiento, la información que transita se codifica, volviéndose ilegible, protegiéndola de tal modo que ningún tercero ajeno al intercambio de información podrá conocer el contenido del mensaje.

Es importante conocer que existen *software* y aplicaciones para cifrar información, actualmente, los modelos más recientes de equipos de cómputo cuentan con algún elemento en su configuración que permite cifrar su contenido, además existen herramientas de *software* para el cifrado de archivos, dispositivos periféricos de almacenamiento (como memorias USB) e incluso de la conexión a Internet (a través de las **Redes Privadas Virtuales** o VPN).

¿Qué puedo hacer para cifrar mis datos personales?

1. Clasifica adecuadamente la información para identificar cuál requiere ser cifrada.
2. Selecciona la herramienta de cifrado que mejor se adapte a las necesidades de protección.
3. No olvides la clave de cifrado.
4. En caso de que sea necesario compartir la clave de cifrado, selecciona un medio seguro para ello.

A continuación, se presenta una lista de *software* y aplicaciones de utilidad para cifrar tu información.

Antes, es importante señalar que las herramientas que a continuación se presentan se han dividido en dos grupos: 1) para el cifrado de almacenamiento y 2) para el cifrado de tránsito.

El cifrado de almacenamiento protege la información que se encuentra alojada en los dispositivos y que no requiere una conexión a Internet para acceder a dicha información:

a) Archivos: se refiere a la protección individual de cualquier tipo de archivo. Este cifrado es particular para cada elemento.
b) Dispositivos periféricos: consiste en cifrar la información contenida en dispositivos externos, por ejemplo, el USB, mediante el cual se almacena o transfiere información hacia el equipo de cómputo u otros aparatos como televisiones o equipos de sonido. La importancia de utilizar el cifrado en este tipo de dispositivos radica en la facilidad que existe para su pérdida, robo o extravío y que conlleva un riesgo alto, si la información contenida no se encuentra debidamente protegida.
c) Disco duro: se cifra todo el contenido de la unidad, es decir, no selecciona qué archivos cifra de manera particular, su funcionalidad consiste en proteger todo lo que se encuentra en el disco duro, dejando inaccesible la información a cualquier usuario que no cuente con la clave de acceso.

El cifrado de tránsito se basa en utilizar un mecanismo para garantizar que la información que se envía de un dispositivo a otro, no pueda ser alterada o sustraída durante el trayecto:

a) Red: consiste en cifrar el canal de comunicación a través de un protocolo seguro, que garantice que la información que será transmitida, en todo momento del trayecto estará integra y mantendrá su confidencialidad. Una red privada virtual (VPN por sus siglas en inglés) permite establecer una conexión privada y segura con otra red para garantizar la confidencialidad de los datos y archivos que sean transferidos por los dispositivos que se conectan a ésta.
b) Correo electrónico: el cifrado en este medio es una medida de seguridad que hace uso de claves públicas y privadas entre remitente y destinatario, para garantizar la seguridad del contenido de un correo electrónico. El cifrado de correo está orientado a proteger su contenido para que, en caso de ser interceptado, sea ilegible para quien lo intercepte.
c) Mensajería instantánea: En la actualidad, los servicios de mensajería instantánea se han convertido en uno de los medios más comunes de comunicación, dada su importancia estos servicios han incorporado un sistema de cifrado en el tránsito de información, ya sean mensaje, voz e imagen. Por ello, es importante que los titulares conozcan cuáles son los servicios de mensajería instantánea que cuentan con la funcionalidad de cifrar la información, de forma que les permita ser más selectivos cuando se trate de elegir una aplicación para comunicarse.

NOMENCLATURA		
Win- Sistema Operativo *Microsoft Windows*	iOS- Sistema Operativo para móviles de *Apple*	ES- Idioma español
Mac OS- Sistema Operativo *Apple*	An- Sistema Operativo para móviles de *Google (Android)*	EN- Idioma inglés

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
ALMACENAMIENTO	Crypto Ghost Aplicación móvil para cifrado de archivos.				x		x		x
	My Lockbox Permite ocultar, bloquear y proteger con una contraseña cualquier carpeta en una computadora.	x					x		x
	Folder Vault Programa para proteger archivos, hacerlos invisibles, cifrarlos a través de una contraseña maestra.	x					x		x
	DiskCryptor Programa para el cifrado de todas las particiones del disco duro y de dispositivos móviles.	x					x		x
	Bitlocker Desarrollado por Microsoft, para el cifrado completo de disco duro.	x				x		x	x
	FileVault Aplicación desarrollada por Apple integrada en su sistema operativo para el cifrado de disco duro.		x			x		x	x
	Veracrypt Soporta la creación de espacio de almacenamiento virtual cifrado.	x	x				x		x
	Configuración de contraseña de bloqueo para iOS.			x			x	x	x
	Configuración de contraseña de bloqueo para Android.				x		x	x	x

Tipo	Nombre - descripción	Sistema Operativo				$		Idioma	
		Win	Mac OS	iOS	An	Sí	No	ES	EN
TRÁNSITO	GPG4Win A través de esta herramienta los usuarios pueden enviar correos electrónicos y archivos de forma segura a través del cifrado y la firma digital.	x	x				x		x
	Hot Spot Shield Herramienta que ofrece protección para la conexión web a través del cifrado de tráfico.	x	x			x	x	x	x
	Express VPN Servicio de red privada virtual de alta velocidad, seguro y fácil de usar. Cuenta con una configuración instantánea.	x	x	x	x	x		x	x
	Nord VPN Permite la navegación segura a través del servicio de red privada virtual.	x	x	x	x	x		x	x
	IPvanish VPN Servicio de VPN que ofrece seguridad y privacidad para la conexión a la web.	x	x	x	x	x		x	x
	WhatsApp Cifrado de extremo a extremo.	x	x	x	x		x	x	x
	Facebook Messenger Cifrado de extremo a extremo a través de la opción de comunicaciones secretas, éstas no están disponibles en la versión web.	x	x	x	x		x	x	x
	Skype Cifrado AES de 256 bits y RSA de 1536 o 2048 bits.	x	x	x	x		x	x	x
	Telegram Cifrado AES simétrico de 256 bits, un cifrado RSA de 2048 bits y un intercambio seguro de claves Diffie-Hellman.	x	x	x	x		x	x	x
	iMessage Cifrado de extremo a extremo.		x	x			x	x	x
	Signal Servicio de mensajería y llamadas con cifrado extremo a extremo.	x	x	x	x		x		x

RECOMENDACIÓN 10

Cuida tu entorno físico

¿Por qué es importante el cuidado del entorno físico para la protección de los datos personales?

Es importante recordar que además de las medidas de seguridad para el entorno digital que fueron mencionadas a lo largo de esta serie de recomendaciones, es importante considerar medidas para la protección del entorno físico, ya que existen descuidos o errores humanos que pueden poner en riesgo la seguridad de los datos personales.

De este modo, las personas malintencionadas utilizan prácticas que se aprovechan del descuido del entorno, para obtener información de las personas, entre ellas están las siguientes:

a) Ingeniería social: se refiere al conjunto de acciones no técnicas a través de las cuales se puede obtener información mediante el

RECUERDA...

SÓLO BASTA UN DESCUIDO PARA PONER EN RIESGO TU INFORMACIÓN PERSONAL

engaño, para ello, se emplean técnicas psicológicas y habilidades sociales que permiten obtener información, accesos a sistema o la ejecución de actividades más elaboradas.

b) Espionaje por encima del hombro (*shoulder surfing*): consiste en observar discretamente por la espalda de la víctima, las teclas que digita, la pantalla del monitor o de cualquier dispositivo, con el objeto de obtener alguna información que pueda ser de utilidad, como por ejemplo contraseñas de acceso.

c) Escuchar secretamente (*eavesdropping*): consiste en escuchar con detenimiento la información que se intercambia en una comunicación, con la finalidad de obtener contraseñas, códigos, información confidencial o que pueda resultar de interés para el atacante. Esta técnica también puede realizarte en el entorno digital a través de escuchar lo que se intercambia en la red de datos o en la línea telefónica.

¿Qué puedo hacer para proteger mi entorno físico?

A continuación, se presentan algunas recomendaciones para protección del entorno físico:

- Evita el uso de redes públicas para realizar transacciones bancarias o compartir información sensible.
- No realices compras por Internet en lugares públicos, dado que no es posible controlar quién puede mirar la pantalla del dispositivo y de este modo tener acceso a datos bancarios o información personal.
- Al vender o regalar un dispositivo, se recomienda realizar un borrado seguro de la información que se encuentra almacenada.
- Activa un control de acceso para todos los dispositivos y la opción de bloqueo automático a partir de cierto tiempo de inactividad.
- Deshabilita las conexiones **bluetooth** y **Wi-Fi** si no se están utilizando.
- Guarda los dispositivos en un lugar seguro al caminar por la calle o viajar en el transporte público o automóvil.
- Cuida la información que se comunica a través de las conversaciones en lugares públicos.
- Usa protectores de pantalla con filtro de privacidad.
- Cubre la cámara *web* cuando no las estés utilizando.
- Verifica qué tan expuesto estás al robo de identidad, esto puede realizarse a través del *Vulnerómetro*, herramienta creada por el INAI para que los usuarios sean conscientes sobre el tratamiento que se realiza de sus datos personales, disponible en http://micrositios.inai.org.mx/vulnerometro/.

Finalmente, es importante mencionar que la consideración de las recomendaciones tanto del entorno digital como físico, contribuirán a fortalecer la seguridad de los datos personales y reducir la posibilidad de cualquier uso, acceso, pérdida o modificación no autorizada.

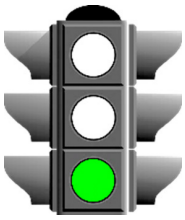
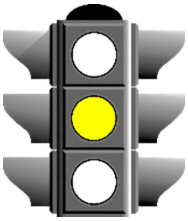
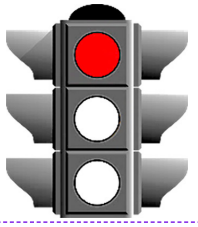
TEST

¿Cómo te proteges en el entorno digital?

Selecciona con una **X** la respuesta que corresponda para cada una de las preguntas y con base en tus resultados conoce tu nivel de protección actual.

No.	Pregunta	Sí	A veces	No
1	¿Identificas cuál de la información que manejas debe estar cifrada?	☐	☐	☐
2	¿Cifras la información que tienes en tu equipo de cómputo o dispositivos móviles?	☐	☐	☐
3	¿Cuentas con una contraseña robusta para controlar el acceso a tus dispositivos o cuentas?	☐	☐	☐
4	¿Utilizas la autenticación de dos pasos para el acceso a tus dispositivos o cuentas?	☐	☐	☐
5	¿Tienes instaladas extensiones o complementos adicionales en tu navegador para mejorar su seguridad o privacidad?	☐	☐	☐
6	¿Usas buscadores que integren medidas de seguridad para proteger tu navegación?	☐	☐	☐
7	¿Respaldas la información contenida en tus dispositivos?	☐	☐	☐
8	¿Cuentas con alguna herramienta que te permita buscar o borrar tu dispositivo?	☐	☐	☐
9	¿Descargas software de sitios diferentes a las oficiales?	☐	☐	☐
10	¿Verificas los permisos y accesos que otorgas al software o aplicaciones que instalas?	☐	☐	☐
11	¿Actualizas periódicamente tu sistema, software o aplicaciones?	☐	☐	☐
12	¿Sabes cómo se configuran las actualizaciones de tus dispositivos?	☐	☐	☐
13	¿Has leído las configuraciones de privacidad de las redes sociales que utilizas?	☐	☐	☐
14	¿Tomas alguna medida de seguridad antes de publicar información en tus redes sociales?	☐	☐	☐
15	¿Cuentas con un antivirus instalado en tus dispositivos móviles y/o equipo de cómputo?	☐	☐	☐
16	¿Actualizas tu software antivirus de forma frecuente?	☐	☐	☐
17	¿Sabes qué es la ingeniería social?	☐	☐	☐
18	¿Eres precavido sobre la información que compartes cuando conversas en lugares públicos?	☐	☐	☐
19	¿Respaldas con frecuencia la información que se almacena en tus dispositivos o equipo de cómputo?	☐	☐	☐
20	¿Revisas los respaldos una vez que se realizan para verificar su integridad?	☐	☐	☐

Resultados

Mayoría de "Sí"		Las medidas de seguridad que actualmente tienes implementadas protegen de forma adecuada tu información y/o datos personales. Eres un usuario consciente de la importancia de mantener protegidos todos los dispositivos y medios que empleas en tu vida diaria y tomas con seriedad el cuidado de tus datos personales.
Mayoría de "A veces"		Cuentas con algunas medidas de seguridad que brindan un nivel de protección básico a tu información y datos personales. Eres un usuario que conoce sobre la importancia de proteger tu información personal, pero que necesita generar una mayor conciencia. Aunque cuentas con mecanismos para tu protección es recomendable que actualices o fortalezcas las medidas con las que actualmente proteges tus datos personales.
Mayoría de "No"		No cuentas con medidas de seguridad que brinden protección a tu información y datos personales, lo cual implica que estés más expuesto a una pérdida, robo, extravío o copia no autorizada de tus datos. Como usuario desconoces cómo proteger los dispositivos y medios que usan o almacenan tu información personal.

Referencias

1. *10TopTenReviews, Privacy, consultable en: http://www.toptenreviews.com/software/privacy/*
2. *10TopTenReviews, The Best Computer Protection Software, consultable en: http://www.toptenreviews.com/software/security/best-computer-protection-software/*
3. *10TopTenReviews, The Best Email Encryption Software, consultable en: http://www.toptenreviews.com/software/privacy/best-email-encryption-software/*
4. *10TopTenReviews, The Best Encryption Software, consultable en: http://www.toptenreviews.com/software/security/best-encryption-software/*
5. *10TopTenReviews, The Best Identity Theft Protection Services of 2017, consultable en: http://www.toptenreviews.com/services/protection/best-identity-theft-protection-services/*
6. *10TopTenReviews, The Best Internet Browser Software, consultable en: http://www.toptenreviews.com/software/internet/best-internet-browser-software/*
7. *Cloudwards, 99 Free Tools to Protect Your Privacy, consultable en: https://www.cloudwards.net/99-tools-to-protect-your-privacy/*
8. *CSO Magazine, Top 5 tools to protect internet privacy, consultable en: https://www.csoonline.com/article/3213931/privacy/top-5-tools-to-protect-internet-privacy.html*
9. *Digital Trends, These Are The Best Password Managers For Protecting Your Data Online, consultable en: https://www.digitaltrends.com/computing/best-password-managers/*
10. *Electronic Frontier Foundation, The 7 Privacy Tools Essential to Making Snowden Documentary CITIZENFOUR, consultable en: https://www.eff.org/deeplinks/2014/10/7-privacy-tools-essential-making-citizenfour*
11. *Electronic Frontier Foundation, Tools from EFF´s Tech Team, consultable en: https://www.eff.org/pages/tools*
12. *Electronic Privacy Information Center, EPIC Online Guide to Practical Privacy Tools, consultable en: https://www.epic.org/privacy/tools.html*
13. *HACK*BLOSSOM, Guía de Seguridad Digital para Feministas Autogestivas, consultable en: https://es.hackblossom.org/cybersecurity/*
14. *Lifewire, The Best Search Engines of 2017, consultable en: https://www.lifewire.com/best-search-engines-2483352*

15. *Lifewire, Top 7 File Syncing Apps, consultable en: https://www.lifewire.com/best-file-syncing-apps-2378054*

16. *Net Alert, Secure Accounts, consultable en: https://netalert.me/secure-accounts.html*

17. *PRISM Break proyect, Prism-Break, consultable en: https://prism-break.org/en/*

18. *Privacytools.io, Privacy? I don´t have anything to hide, consultable en: https://www.privacytools.io/*

19. Reset the Net, Privacy Pack, consultable en: https://pack.resetthenet.org/

20. Restore Privacy, Privacy Tools, https://restoreprivacy.com/privacy-tools/

21. *TechAdvisor, The best web browsers for 2017, consultable en: http://www.techadvisor.co.uk/test-centre/software/best-web-browsers-for-2017-3635255/*

22. *Techradar, The best free password manager and generator 2017, consultable en: http://www.techradar.com/news/software/applications/the-best-password-manager-1325845*

23. *TechRadar, Top 5 best encryption tools of 2017, consultable en: http://www.techradar.com/news/top-5-best-encryption-tools*

24. *The best free backup software 2017, TechRadar, consultable en: http://www.techradar.com/news/the-best-free-pc-backup-software*

25. *The Intercept, Edward Snowden explains how to reclaim your privacy, consultable en: https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/*

26. *Tom´s guide, Best Ad Blockers and Privacy Extensions, consultable en: https://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html*

27. *Tom´s guide, Best Antivirus Software and Apps 2017, consultable en https://www.tomsguide.com/us/best-antivirus,review-2588.html*

28. *ZDNet, 14 privacy tools you should use to stay secure, consultable en: http://www.zdnet.com/pictures/the-best-privacy-tools-for-staying-safe-secure-online/*

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales