

SEGURIDAD DIGITAL:
CONCEPTOS Y HERRAMIENTAS
BÁSICAS



Edición: Mayo 2020.

Autora: Oriana Hernández

Diseño y diagramación: Aliz Segovia

Colaboradores: Carlos Guerra, Mario Felaco

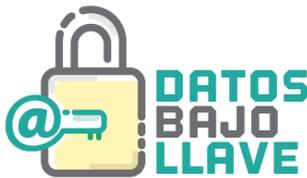
Esta guía ha sido desarrollada como parte de la iniciativa
“**Datos Bajo Llave**” de la organización Conexo.

Para consultar más recursos te invitamos a visitar:

<https://conexo.org/datos-bajo-llave/>

Versión de esta guía en html:

<https://conexo.org/conceptos-y-herramientas-basicas>



ÍNDICE

PARA QUIÉN ES ESTA GUÍA	04
QUÉ ES SUSCEPTIBLE DE SER INTERVENIDO. QUÉ DEBEMOS PROTEGER ANTES DE COMENZAR	05
1 CONTRASEÑAS	09
a. Cómo crear contraseñas seguras	
b. Evita estos hábitos	10
Recomendaciones	13
Usar frases como contraseñas	
Usar administradores de contraseñas	
Cambiar las contraseñas de servicios más importantes para mantener tu privacidad	14
2 AUTENTICACIÓN DE DOS FACTORES (2FA o DOBLE PASO)	15
a. Qué es la autenticación de dos factores	
b. Cómo activar la autenticación de dos factores	16
c. Servicios de uso frecuente donde se puede activar la autenticación de dos factores	17
Recomendaciones	18
3 TELÉFONO MÓVIL	20
a. Llamadas:	
Recomendaciones	
b. Mensajería:	21
SMS	22
Mensajería instantánea o chats	
Whatsapp	23
Signal	24
Recomendaciones	25
c. Rastreo	26
Recomendaciones	
d. Protección física de la información en teléfonos móviles	
Recomendaciones	
e. Otros hábitos	27
4 PHISHING	28
Qué es el phishing	
Recomendaciones	

5 MALWARE	31
Qué es el malware	
Qué podemos hacer para detectar y eliminar malware de nuestros equipos	
Recomendaciones	32
6 NAVEGACIÓN SEGURA, EVASIÓN DE CENSURA Y ANONIMATO	33
Redes inalámbricas	
Recomendaciones	
HTTPS	34
VPN	36
Qué es una VPN	
Ventajas y desventajas de usar una VPN	37
Ventajas	
Desventajas	
Recomendaciones	38
TOR	39
Recomendaciones	40
7 CORREOS ELECTRÓNICOS SEGUROS	41
Recomendaciones	
8 PROTECCIÓN FÍSICA DE LA INFORMACIÓN	45
Recomendaciones	
9 SEGURIDAD EN REDES SOCIALES	48
Recomendaciones	
REFERENCIAS	50
CHECKLIST DE SEGURIDAD DIGITAL	51



PARA QUIÉN ES ESTA GUÍA

Esta guía ha sido escrita pensando en periodistas, defensores y defensoras de derechos humanos, activistas y personas que, independientemente de su espacio de desarrollo profesional, desean iniciarse en el camino de la seguridad digital y la privacidad. La adopción total o parcial de las recomendaciones que se ofrecen dependerá de los riesgos que enfrenta la persona u organización interesada en implementarlas. Es por ello que antes de comenzar recomendamos que se realice una evaluación de riesgos.

La guía de [SAFETAG](#) define el riesgo como “**la evaluación actual de la probabilidad de que ocurran eventos dañinos. El riesgo se evalúa comparando las amenazas que enfrenta un agente con sus vulnerabilidades y su capacidad para responder o mitigar las amenazas emergentes**”, así:

$$\text{Riesgo} = \frac{\text{Amenaza} \times \text{Vulnerabilidad}}{(\text{Capacidad})}$$



Amenaza: es un posible ataque que tiene el potencial de dañar la vida, la información, las operaciones, el medio ambiente y/o la propiedad.



Vulnerabilidad: Es un atributo o característica que hace que una entidad, activo, sistema o red sea susceptible a una amenaza dada.



Capacidad: es la combinación de fortalezas, atributos y recursos disponibles de una persona u organización que pueden usarse para reducir el impacto o la probabilidad de amenazas.

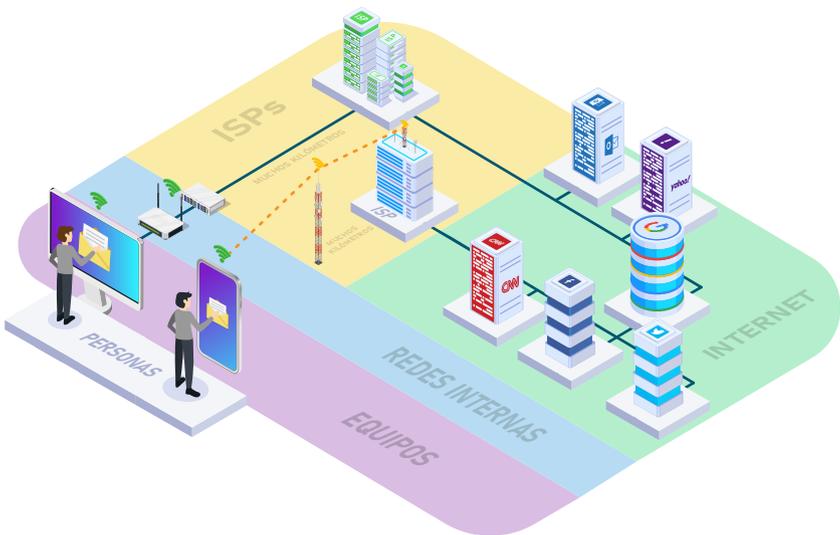


Para más información sobre cómo realizar un completo análisis de riesgo recomendamos consultar el manual “[Seguros y Documentados para el Activismo](#)” (SDA).



QUÉ ES SUSCEPTIBLE DE SER INTERVENIDO Y QUÉ DEBEMOS PROTEGER

Cuando hablamos de seguridad digital normalmente nos referimos al conjunto de acciones que podemos llevar a cabo para proteger y tener control sobre nuestras comunicaciones, información y, en general, sobre nuestros datos, procurando garantizar su disponibilidad, integridad y confidencialidad, pero, **¿qué es exactamente lo que debemos proteger?, ¿cómo hacerlo?, ¿dónde comenzar?** Una manera de explicarlo es a través de la siguiente imagen:



En la imagen te mostramos cómo es el recorrido regular de la información cuando navegamos en Internet. Vemos como una persona, utilizando su computadora, se conecta a una red wi-fi para enviar, por ejemplo, un correo electrónico. Para ello la información pasa, en primera instancia, por la infraestructura de su proveedor de servicios de Internet o ISP y a continuación entra a la Internet, específicamente al servidor de Google.

A continuación, para que la información pueda ser consultada por el destinatario, este debe tener un equipo (en este caso un teléfono móvil) que accede a Internet a través de su propio ISP.



ANTES DE COMENZAR

Las siguientes son algunas premisas relacionadas al mundo de la seguridad que son útiles de conocer antes de empezar a poner en práctica el contenido de esta guía:



En seguridad digital se dice que “**la cadena es tan fuerte como el eslabón más débil**”. Si eres parte de una organización, es muy conveniente que todos los miembros puedan poner en práctica las recomendaciones acordadas, así lograrán estar más seguros. Como individuo, es recomendable ver tu seguridad como un todo y no pensar que con una sola medida ya estarás seguro: piensa que quizás exista otra manera de tener acceso a tus datos distinta a la que aseguraste.



La mayor parte de la mejora de tu seguridad depende de que puedas cambiar tus hábitos, otra parte depende de que comiences a utilizar nuevas herramientas o aplicaciones y otra de que configures correctamente herramientas o servicios que ya usas.





Aunque pongas en práctica todas las recomendaciones de esta guía **tu información nunca estará 100% segura**. Solo estarás disminuyendo la probabilidad de ocurrencia o el impacto de tus riesgos, por ello es conveniente que puedas realizar con regularidad una evaluación de los mismos y diseñar planes para su mitigación.



Hablamos de **seguridad holística** cuando de forma coordinada se utilizan herramientas y tácticas para el bienestar y la seguridad **psicosocial, física y digital**. Te invitamos a consultar recursos que abordan técnicas para mejorar tu seguridad física y psicosocial, así como a consultar recursos adicionales a esta guía en la parte de seguridad digital.



Las herramientas que te presentamos a continuación se caracterizan por tener en cuenta la **seguridad** y **privacidad** de las personas que las usan; se someten a auditorías independientes; están bien valoradas por la comunidad de seguridad digital; son generalmente transparentes sobre su operación (incluyendo sus fallas) y no tienen costo monetario (o tienen al menos una versión de este tipo).



1 | CONTRASEÑAS

Una contraseña es un texto cuyo uso permite a las personas acceder a determinado tipo de información, cuentas de determinados servicios, entre otros.

Hoy en día, a pesar de que existen múltiples formas de autenticación (pines de 4 o 6 dígitos, patrones, reconocimiento de voz y facial...), las contraseñas siguen siendo la **principal puerta de acceso a nuestras cuentas de usuario** y dispositivos. Es por ello que tener contraseñas de acceso seguras, que difícilmente puedan ser hackeadas, es fundamental.

En este capítulo te enseñamos cómo crearlas, qué hábitos son convenientes que cambies y qué alternativas para la administración de tus contraseñas existen en el mercado.

A CÓMO CREAR CONTRASEÑAS SEGURAS

Las **contraseñas seguras** son aquellas que incorporan en su diseño los siguientes elementos:



Longitud: Mientras más larga, más segura será la contraseña. Cuando diseñamos contraseñas es recomendable hacerlas tan largas como sea posible o como el servicio o dispositivo lo permita. Aunque no hay un consenso sobre cuál debería ser el mínimo, 15 caracteres es un número recomendable. ¿El máximo? Incluso 100 caracteres o más.

Uso de distintos tipos de caracteres: mayúsculas, minúsculas, números y símbolos.



Que no sea predecible: Otra de las técnicas empleadas para descifrar contraseñas es el uso de la “ingeniería social”. Aunque inicialmente consiste en usar la psicología para obtener información de la víctima, las características de este tipo de información hacen que pueda ser obtenida a través de las publicaciones que se realizan en redes sociales y otros sitios de Internet. En este sentido la recomendación es no utilizar información personal (nombres de mascotas, fechas importantes, nombres de familiares, datos personales) en el diseño de las contraseñas.



Una de las técnicas utilizadas por los atacantes para descifrar contraseñas son los llamados “**ataques de fuerza bruta**”, que consisten en ingresar al sistema todas las combinaciones posibles de contraseñas en forma sistemática y secuencial.

También encontramos los “**ataques de diccionario**” en donde se prueban todas las palabras registradas y sus combinaciones, por lo que aquellas contraseñas que consisten, por ejemplo, en palabras comunes, serán fácilmente descifradas por el atacante.

En este sentido, si consigues incorporar todas las características que hemos descrito anteriormente en tus contraseñas, harás que una persona malintencionada deba emplear mayores recursos (tiempo y hardware, principalmente) y **difícilmente** pueda dar con la contraseña.

B

EVITA ESTOS HÁBITOS



Repetir contraseñas: Si hackean una de tus cuentas, pueden hackear todas. Recordemos el caso en junio de 2016 de Mark Zuckerberg, CEO de Facebook, quien utilizó la clave de acceso de LinkedIn en Twitter. Los atacantes habían robado en 2012 una base de datos de contraseñas de LinkedIn y gracias a eso lograron acceder a la cuenta de Twitter de Zuckerberg.



Malas respuestas para las preguntas de seguridad:

Muchos servicios ofrecen como alternativa de recuperación de cuenta preguntas que al ser respondidas correctamente permiten de nuevo el acceso al servicio. La recomendación es **responder a estas preguntas de seguridad con contraseñas en sí mismas**, así evitaremos que terceras personas accedan a nuestros datos por esta vía.

Correos de recuperación no seguros: Al igual que en el punto anterior, otra vía de acceso a nuestras cuentas puede ser a través de correos electrónicos alternativos o de recuperación. La **recomendación** en este caso es cambiar la contraseña y las respuestas a las preguntas de seguridad del correo de recuperación por contraseñas seguras, así estaremos cerrando otra puerta de acceso a nuestros datos. La eliminación del correo electrónico de recuperación es también una alternativa que recomendamos llevar a cabo cuando sea posible.



Dejar copias físicas o digitales accesibles: Las notas en el celular, los documentos de texto en el computador, las notas adhesivas en los monitores y las anotaciones de contraseñas en pizarras y libretas son considerados como **malos hábitos** si nuestro objetivo es tener la mayor seguridad posible en nuestras cuentas.

Acceso en equipos que no son de confianza: No es recomendable acceder a nuestras cuentas de usuario desde ordenadores y equipos que **no son de confianza**. Algunos equipos pueden estar infectados con **programas espías capaces de capturar tus contraseñas**.



Compartir contraseñas: Las contraseñas contienen información privada que no debería ser compartida con ninguna otra persona. Si se trata de una cuenta a la que varias personas tienen acceso, como suele ser el caso de las redes sociales de una organización, es importante compartir la contraseña por **vías seguras** y almacenarlas también en lugares seguros.



Guardar contraseñas en el navegador: Debido a las vulnerabilidades que se han registrado en diversos momentos, los navegadores no se consideran lugares seguros para el almacenamiento de nuestras contraseñas. Adicionalmente, es común que los navegadores nos pregunten si deseamos almacenar en ellos una contraseña que acabamos de ingresar. Lo mejor para evitar clicar en “**aceptar**” es ir a la configuración del navegador y **deshabilitar la opción de guardar contraseñas**.



Exceso de confianza: Cada vez son más las técnicas engañosas en las que los usuarios pueden estar facilitando su información sin autorización a desconocidos. Navega siempre en **sitios seguros** (con **HTTPS**), chequea que la dirección del sitio web en la barra superior sea correcta y **desconfía** de cualquier anuncio, correo electrónico, llamada, entre otras formas de comunicación, que soliciten información personal.



Cuidado con el cambio frecuente de contraseñas: Estudios han demostrado que el cambio frecuente de contraseñas **podría no ser tan seguro** debido a que el usuario tiende a realizar pequeños cambios sobre la contraseña anterior formando patrones cada vez **más fáciles** de adivinar y, estos patrones también son conocidos por los atacantes. Si has diseñado una contraseña con todos los elementos que hemos descrito anteriormente como seguros, entonces **no será necesario** realizar un cambio frecuente de esta contraseña a menos de que se sospeche que ha sido tomada por un tercero no autorizado.





RECOMENDACIONES

1

USAR FRASES COMO CONTRASEÑAS

El uso de una frase es una alternativa de contraseña segura que consiste en utilizar una secuencia de palabras como acceso a nuestras cuentas. **Lo importante es que sea larga** y no se corresponda con información personal. Por ejemplo:



USO FRASES COMO CONTRASENAS

Esta última bien podría ser una clave segura y tendría la ventaja de ser de fácil memorización. **Añadiremos más seguridad** si intervenimos la frase incorporando números, símbolos o cambiando algunas de las letras, por ejemplo: “**UsoFr@sesC0m0Contr@sen@\$**”, o agregando más palabras.

2

USAR ADMINISTRADORES DE CONTRASEÑAS

Una alternativa más definitiva para la creación, almacenamiento y gestión de contraseñas, es el uso de un “**administrador de contraseñas**”. Actualmente existen varios servicios con versiones de escritorio, aplicaciones o de almacenamiento en la nube. Algunos de ellos son: [LastPass](#), [1password](#), [Passpack](#), KeePass en sus múltiples versiones ([KeePassXC](#) de preferencia entre ellas), [Dashlane](#), entre otros.

LastPass

1Password

PASSPACK

KeePassXC

DASHLANE

Aunque hay variaciones entre ellos y tomar la decisión de usar uno u otro dependerá de nuestras necesidades específicas, la característica más importante es que todos permiten almacenar de forma segura nuestras contraseñas y, una vez que hemos cargado en el servicio toda la información, solo tendremos que recordar la clave de acceso a nuestro administrador de contraseñas, tal y como funciona una caja fuerte.

3

CAMBIAR, AL MENOS, LAS CONTRASEÑAS DE LOS PRINCIPALES SERVICIOS Y EQUIPOS

Si hasta este punto de la guía consideras que tus contraseñas, o los hábitos que tienes sobre ellas, no son los mejores, te invitamos a realizar estos cambios comenzando por los siguientes servicios y equipos:



ACCESO A LA COMPUTADORA Y TELÉFONO MÓVIL



CORREOS ELECTRÓNICOS



BANCOS



SERVICIOS EN LA NUBE



REDES SOCIALES



2

AUTENTICACIÓN DE DOS FACTORES (2FA O DOBLE PASO)

A

QUÉ ES LA AUTENTICACIÓN DE DOS FACTORES

La **autenticación de dos factores**, también llamada de **dobles pasos**, consiste en activar un segundo elemento (además de la contraseña) para lograr acceder a nuestras cuentas. De esta manera estaremos **más seguros** porque se necesitan ambas vías de autenticación para lograr obtener el acceso. Este segundo elemento puede ser:



Algo que sabes: Consiste en **agregar** una segunda contraseña para lograr obtener el acceso a tu cuenta.

Algo que tienes: Consiste en introducir un **código** que solo tú podrás obtener a través de un mensaje de texto, una aplicación o un dispositivo específico o token.



Algo que eres: Consiste en utilizar la **identificación biométrica**, es decir, las características del cuerpo de una persona, para verificar su identidad. Por ejemplo, a través de huellas dactilares, cara o iris. Debido al riesgo de filtración de datos y lo vulnerables que pueden ser estos métodos, la **autenticación** a través de información biométrica no es método que recomendamos cuando esta información es almacenada en servidores externos.

B

CÓMO ACTIVAR LA AUTENTICACIÓN DE DOS FACTORES

Es recomendable **activar el doble factor** en todos los servicios que tengan esta opción. Dependiendo del servicio la autenticación de dos factores puede consistir específicamente en:



Envío de un SMS: El código llegará a tu **teléfono móvil** a través de un mensaje de texto.

Aplicaciones de autenticación: Encontrarás el código de acceso dentro de una aplicación que **no requiere señal telefónica o Internet** para funcionar.



Segunda clave: introducir una **segunda clave** o código de **6 dígitos** (este es el caso de *Whatsapp*).

Token: envío de un **token** de autenticación.



Activación de una llave de seguridad: estas son **piezas de hardware** que se conectan a través de puertos USB o de forma inalámbrica para realizar la autenticación.

Otras opciones pueden incluir **notificaciones** a algún dispositivo, envío de un código a través de un correo electrónico asociado o dispositivos físicos que **generan códigos**.

C

SERVICIOS DE USO FRECUENTE DONDE PUEDE ACTIVAR LA AUTENTICACIÓN DE DOS FACTORES

Estos son algunos de los principales servicios donde **podrás activar** la autenticación de dos factores:



Puedes consultar <https://twofactorauth.org> para una lista más completa.



RECOMENDACIONES

Debido a que los **mensajes de texto son inseguros** y es posible que no puedas obtener el código de acceso en caso de que estés fuera de tu país de residencia, te recomendamos que actives el **doblo factor** a través del uso de una aplicación móvil de autenticación.

Esta aplicación es **segura** y siempre podrás obtener tus códigos de acceso sin importar en dónde te encuentres. Las aplicaciones que recomendamos son:



AUTHY

Disponible en [iOS](#) y [Android](#)



Google Authenticator

Disponible en [iOS](#) y [Android](#)

Para activar cualquiera de las dos deberás:

1

Descargar de la tienda **Play Store** (usuarios Android) o **AppStore** (usuarios iOS) la aplicación de autenticación que elijas.

2

Dirigirte a las **configuraciones de seguridad** del servicio en donde desees activar el doble factor.

3

Escanear el **código de barras** con tu celular y seguir las instrucciones.

De ahora en adelante cada vez que desees **acceder** a una cuenta donde hayas activado el doble factor, el servicio te pedirá tu contraseña y también el **factor de autenticación**.



Te recomendamos tener uno o dos “**dispositivos de confianza**”. De esta manera siempre podrás acceder a tus servicios en caso de robo o extravío de tu teléfono móvil ya que en los dispositivos que hayas marcado como de “**confianza**” el servicio sólo te pedirá la clave pero no el código de autenticación para acceder.

Recomendamos también buscar la opción de **códigos de emergencia** o de seguridad, en los servicios que lo permitan para que puedas tener acceso a tus cuentas en caso de no poder acceder a los otros métodos de autenticación. Estos códigos se deben guardar de la **manera más segura posible**, por ejemplo, en un administrador de contraseñas.

Algunas aplicaciones ofrecen el servicio de respaldar los códigos únicos en servidores en la nube: **no recomendamos utilizar esta opción a menos que sea para migrar a otro dispositivo y luego volver a deshabilitarla.**



3 | TELÉFONO MÓVIL

Este capítulo ofrece recomendaciones con relación a las llamadas, chats, rastreo y protección física de la información contenida en los dispositivos móviles.

A

LLAMADAS:

Cuando realizas una llamada tradicional desde una línea fija o de un teléfono móvil, la llamada no se cifra de extremo a extremo. Si estás usando un teléfono móvil, la llamada puede estar débilmente cifrada entre el teléfono, las torres de teléfonos celulares y el resto de la red telefónica.

A medida que la conversación viaja a través de la red, es vulnerable a la interceptación por parte de la compañía telefónica y, por extensión, del cualquier gobierno o cualquier otra organización que tenga poder sobre esta. También existen técnicas que otras personas pueden usar para escuchar este tipo de llamadas si están cerca de tu teléfono.



RECOMENDACIONES



Es muy recomendable que abandones el hábito de realizar llamadas usando una **línea fija cableada o desde tu línea móvil telefónica** y comiences a llamar únicamente desde **aplicaciones que cifren** las llamadas de extremo a extremo, como *Whatsapp* o *Signal*.



En caso de que sea **indispensable** realizar la llamada a través de líneas telefónicas tradicionales, **evita** hacer mención a **temas sensibles** que pongan en riesgo tu seguridad.



LO QUE DEBES SABER SOBRE EL CIFRADO

Generalmente, **cifrado** se refiere al proceso matemático de hacer que un mensaje sea ilegible, excepto para la persona que posee la clave para descifrarlo en forma legible.

Existen dos formas principales en las que se aplica el cifrado: el **cifrado en reposo** y el **cifrado en tránsito**.



El **cifrado en reposo** se refiere a la codificación de la información almacenada en un dispositivo.



El **cifrado en tránsito** se refiere a codificación de la información que se está moviendo a través de una red de un lugar a otro.

En Internet hay dos maneras — **frecuentes** — de cifrar los datos en tránsito:

A

Cifrado en la capa de transporte (HTTPS a través de TLS): El cifrado de la capa de transporte protege los mensajes a medida que viajan desde un dispositivo a los servidores de un servicio, aplicación o sitio web y desde estos servidores al dispositivo de potenciales destinatarios. En el medio, el proveedor de servicios de mensajería (o el sitio web que está navegando, o la aplicación que está utilizando) puede ver copias no cifradas de tus mensajes.

B

Cifrado de extremo a extremo (E2E): El cifrado de extremo a extremo protege los mensajes en tránsito desde el remitente hasta el receptor. Garantiza que la información se convierta en un mensaje secreto por su remitente original (el primer "extremo") y que sólo sea decodificado por su destinatario final (el segundo "extremo"). Nadie, incluyendo los administradores de la aplicación que estás usando, puede **"escuchar"** y acceder a tu actividad.

Tomado de "[¿Qué debo saber sobre el cifrado?](#)" del programa Surveillance Self-Defense de la Electronic Frontier Foundation.



SMS

No es recomendable comunicarse a través de **mensajes de texto (SMS)** ya que el proveedor de servicio, o incluso personas cerca de tu teléfono, pueden llegar a leerlos con facilidad.



MENSAJERÍA INSTANTÁNEA O CHATS

Quando decimos que una aplicación de chat es **segura** nos referimos a que **cumple con varias características** entre las cuales destacan: cifrado en tránsito, cifrado de extremo a extremo, documentación de procesos, auditorías independientes, transparencia en la operación (incluyendo la comunicación de las fallas a los usuarios), entre otras.



No todas las aplicaciones que encontramos en el mercado cumplen con estas características de seguridad. **Te recomendamos** que, en adelante, cuando desees usar una nueva aplicación de mensajería, **verifiques** con cuáles de estas características cumple y evalúes si es conveniente su uso.



A continuación te mostramos las características de *Whatsapp*, por tratarse de la aplicación de mensajería más utilizada, y de *Signal* que es la alternativa que consideramos más segura y respetuosa de tu privacidad.

WhatsApp

Entre las características positivas que posee *Whatsapp* de cara a nuestra seguridad tenemos:



Cifrado en tránsito



Cifrado de extremo a extremo



Posibilidad de activación de un **código como doble factor** de autenticación.

Sin embargo, posee algunas otras características que pueden representar una amenaza para nuestra seguridad, por ejemplo:



Comparte información con *Facebook*.



Almacena una cantidad importante de **metadatos**.



Incentiva la **creación de respaldos** de las conversaciones en la nube, los cuales pueden ser vulnerados mediante técnicas conocidas.



En algunos dispositivos *Android* almacena automáticamente imágenes, videos y notas de voz en diversas áreas del teléfono, haciendo que esta información quede **accesible aún después de borrar** una conversación en el chat.



Es de código cerrado, por lo que no es posible conocer con exactitud cómo trabajan sus algoritmos y sus posibles vulnerabilidades.



Signal

Signal cuenta con un conjunto de características positivas de cara a nuestra seguridad. Son las siguientes:

-  **Cifrado** en tránsito
-  **Cifrado** de extremo a extremo
-  Posibilidad de activación de un **código como doble factor** de autenticación.
-  Posibilidad de **activación de caducidad** de mensajes para todos los miembros de una conversación.
-  **Almacena sólo los metadatos necesarios** para su funcionamiento.
-  **No comparte** información con otras compañías.
-  A pesar de tener la opción de hacer respaldos en la nube, **no incentiva** su activación.
-  **Su código se encuentra disponible**, por lo que siempre puede ser auditado por terceros.



¿QUÉ SON LOS METADATOS?

“Los metadatos a menudo se describen como todo excepto el contenido de tus comunicaciones. Puedes pensar en los metadatos como el equivalente digital del sobre de una carta”.

Tomado de “[Por qué los metadatos son importantes](#)” del programa Surveillance Self-Defense de Electronic Frontier Foundation.

Los tipos más comunes de metadatos son números de teléfono, direcciones de correo electrónico, nombres de usuario, datos de geolocalización, fecha y hora de tus llamadas telefónicas, información sobre el dispositivo que estás usando, el asunto de los correos electrónicos, entre otros.



RECOMENDACIONES



Descarga *Signal* y comienza a usarla para tener tus conversaciones más sensibles, incluso con grupos, de forma segura.

Adicionalmente, **te recomendamos activar la caducidad de mensajes** para cada conversación: esta característica borra automáticamente los chats para todos los involucrados pasada una determinada cantidad de tiempo (desde 5 segundos hasta 1 semana dependiendo de lo que elijas).



EN LA CONFIGURACIÓN DE SIGNAL:

- 1 Activa el bloqueo de registro:** equivalente a la verificación en dos pasos de *Whatsapp*. Consiste en un PIN que la app te solicitará al registrar tu número de teléfono en un nuevo equipo celular.
- 2 Desactiva las copias de seguridad** (habilitadas sólo en *Android*).
- 3** Chequea que los “**dispositivos enlazados**” sean únicamente los autorizados por ti.



EN LA CONFIGURACIÓN DE WHATSAPP:

- 1 Activa la verificación** en dos pasos.
- 2 Activa** la característica “**Mostrar notificaciones de seguridad**”.
- 3 Desactiva las copias de seguridad** y borra los respaldos que hayas hecho anteriormente.
- 4 Chequea que en “Whatsapp Web/Escritorio”** estén enlazados únicamente los dispositivos autorizados por ti.

C

RASTREO

Tanto tu equipo celular como el chip son rastreables y están continuamente transmitiendo información a las antenas de telefonía móvil, haciendo posible determinar tu ubicación. **Apagar el teléfono una vez que has llegado a un lugar no es una buena práctica si deseas ocultar en dónde te encuentras.**



RECOMENDACIONES



Si deseas tener una reunión con una persona y no deseas que se conozca tu ubicación, lo recomendable es acordar la fecha y hora del encuentro por una vía segura (como *Signal*), dejar el teléfono encendido donde normalmente estarías y acudir a la reunión sin tu equipo celular u otro dispositivo que pueda ser rastreado.

D

PROTECCIÓN FÍSICA DE LA INFORMACIÓN EN TELÉFONOS MÓVILES

Para la protección física de tu teléfono móvil y de la información contenida en él, te recomendamos las siguientes prácticas:



RECOMENDACIONES



Contraseña de acceso: añade una contraseña de acceso a tu teléfono que sea alfanumérica (que haga uso del teclado completo). No se recomienda el uso de patrones, pines de 4 o 6 dígitos o reconocimiento de voz o facial como forma de acceso al teléfono.



Cifra el dispositivo: Tener una contraseña de acceso no es suficiente para proteger la información contenida en tu dispositivo móvil. Lo **único que evitará** que alguien pueda tener acceso a tu información en caso de robo o extravío es la activación del cifrado (o encriptado). Los **teléfonos inteligentes** más recientes activan el cifrado automáticamente al colocar una contraseña de acceso, sin embargo, en dispositivos más antiguos es conveniente revisar si está activada esta característica en las configuraciones de seguridad.



Activa Find My Device (Android) o Find My iPhone (iOS): te recomendamos activar con antelación **Find My Device**, si eres usuario *Android*, o **Find My iPhone** si eres usuario *iOS*. Con esta característica podrás rastrear, recuperar, bloquear o incluso restablecer a la configuración de fábrica a tu teléfono perdido o robado accediendo a tu cuenta Google o Apple, según sea el caso. Al marcar tu dispositivo como perdido **ninguna persona, salvo tú, podrá desbloquearlo.**

E

OTROS HÁBITOS

En la mayoría de los casos, el malware en los teléfonos tiene forma de aplicación. Para evitarlo es recomendable:

- ✓ **Descargar** las aplicaciones únicamente de las **tiendas oficiales** (*AppStore* o *PlayStore*).
- ✓ Descargar solo **las aplicaciones necesarias**.
- ✓ **Revisar con frecuencia** qué permisos (como acceso a cámara o micrófono) tiene cada aplicación.
- ✓ **Evitar** cargar el teléfono usando cables o puertos USB en dispositivos desconocidos.
- ✓ **Actualizar el sistema operativo**, así como las aplicaciones, tan pronto exista una nueva versión disponible.
- ✓ **Respalda frecuentemente** la información más importante en la nube u otros dispositivos.



4 | PHISHING

QUÉ ES EL PHISHING



El *phishing* es una **técnica de ataque** que busca engañar a la víctima para que entregue información sensible, descargue un **archivo** infectado o ingrese su contraseña en una página falsa.



Es probable que recibas mensajes de correo electrónico, *Whatsapp* o SMS con links, archivos o software malicioso que aparentemente provienen de emisores conocidos como *Facebook*, *Twitter*, *Google*, alguna entidad bancaria, entre otros, diciendo que se ha comprometido tu cuenta y que debes acceder a esta **urgentemente** para recuperarla. Si esto te ocurre es muy probable que te encuentres frente a un ataque de phishing.

En las siguientes líneas te ofrecemos algunas recomendaciones que te ayudarán a **reconocer estos ataques** así como la mejor manera de evitarlos.



RECOMENDACIONES



Desconfía de mensajes que instan a tomar acciones rápidas o de urgencia: Muchas veces estos mensajes se aprovechan de situaciones de riesgo o emergencia para convencer a la víctima de tomar acciones apresuradas.



Antes de tomar cualquier acción verifica en páginas oficiales: Si tienes sospechas de que la información que recibes puede ser cierta, la recomendación es que verifiques la información directamente en las páginas oficiales de las entidades bancarias, compañías de correo, entre otras, según sea el caso. Si, por el contrario, el mensaje de alarma que recibiste no se refiere a cuentas comprometidas sino a personas o familiares en riesgo, la sugerencia es que, antes de tomar cualquier acción, intentes contactarte directamente con la persona aparentemente afectada. **En ninguno de estos casos es recomendable seguir vínculos incluidos en el mensaje sospechoso.**



Verifica el emisor del mensaje: Si pretende ser un mensaje de parte de una red social o compañía de correo electrónico, verifica que las cuentas de correo utilizadas sean las oficiales. Si dice ser alguien conocido, **verifica con la persona por otro medio** (preferiblemente en persona) y pregunta si en efecto ha enviado estos mensajes y a quién.



No descargues ningún archivo, instales software o abras ningún enlace web antes de verificar su procedencia y veracidad: para verificar a dónde se dirige un link acortado te recomendamos utilizar unshorten.me o unshorten.it



Mantén actualizado el software: Los ataques de phishing que utilizan **malware** con frecuencia se basan en vulnerabilidades en el software para instalar malware y comprometer tus dispositivos.



Utiliza un administrador de contraseñas con relleno automático: Otra ventaja del uso de los administradores de contraseña que tienen la característica de **relleno automático** de los campos de usuario y contraseña, es que esta información está asociada al URL donde se completa esta información. Si el atacante consigue dirigirte a un sitio web malicioso, tu administrador de contraseñas **no reconocerá** el lugar que pretende robar tu información.



Utiliza Google Drive para previsualizar documentos. En lugar de descargar los documentos que recibas te recomendamos que los cargues en *Google Drive*. Esto convertirá el documento en una versión web, lo que, casi con seguridad, te impedirá instalar software malicioso. Antes de dar click asegúrate de que efectivamente es una previsualización de *Google Drive*, algunos mensajes malintencionados se han aprovechado de ese nivel de confianza e intentan emular el diseño gráfico de esa interfaz para obtener clicks.



Activa la autenticación de dos factores. Como explicamos anteriormente, la activación del **2FA** hará que el atacante no pueda ingresar a tus cuentas de usuario, a pesar de que llegara a tener la contraseña de acceso, debido a que requerirá de este segundo factor de autenticación que solo tú posees.



Para mejorar tus habilidades de detección de phishing te invitamos a realizar el test de phishing diseñado por *Jigsaw* en conjunto con Google: <https://phishingquiz.withgoogle.com/>.

QUÉ ES EL MALWARE



El *malware* es cualquier programa, aplicación o código que ejecuta acciones no deseadas en nuestros dispositivos. Estos **pueden llegar a nosotros** a través de correos electrónicos maliciosos, descargas en Internet, memorias USB, documentos infectados o cualquier otro canal por el que recibimos información.



El *malware* puede hacer cualquier acción que un programa legítimo haría pero con **malas intenciones**, entonces podría, entre otras cosas, ver tu cámara, tus archivos, el texto que escribes en el teclado (que generalmente incluye contraseñas), borrar tu información e incluso puede hacer tu equipo inutilizable. El malware **puede afectar cualquier equipo capaz de ejecutar código**, por lo que nuestras computadoras, teléfonos celulares e incluso equipos de red y dispositivos del “Internet de las cosas”, como televisores inteligentes o equipos del hogar conectados a Internet, pueden ser afectados por malware.

QUÉ PODEMOS HACER PARA DETECTAR Y ELIMINAR MALWARE DE NUESTROS EQUIPOS



A pesar de que no se puede asegurar que no tenemos malware operando en nuestros equipos, especialmente por las técnicas cada vez más creativas usadas para esconderlo y hacerlo pasar por aplicaciones benignas, la gran mayoría de software malicioso es conocido y **puede ser detectado y eliminado**. Sin embargo, la mejor estrategia que podemos adoptar no es detectar y eliminar malware en nuestros equipos, sino evitar que los infectemos. En primer lugar, esto se logra mayormente teniendo **hábitos rigurosos** en el uso de nuestros dispositivos.



RECOMENDACIONES



Mantener el sistema operativo y demás software **actualizado y original**. Ten en cuenta que las actualizaciones también aplican para las aplicaciones del teléfono móvil y los navegadores.



Instalar sólo **aplicaciones de confianza** y obtenidas usando canales oficiales.



Instalar y mantener actualizado un **programa antivirus**. Actualmente las opciones comerciales gratuitas tienen niveles de protección similares o equivalentes a las versiones pagas. **Evita tener más de un antivirus instalado** ya que estos no se llevan bien entre sí y pueden ralentizar tu computadora y no detectar correctamente amenazas reales. Un antivirus que recomendamos que ofrece una versión sin costo es [Avira](#).



Instalar un programa **antimalware** que complemente al antivirus buscando más tipos de amenazas a través de otro tipo de técnicas. Todos los virus son un tipo de malware, pero el malware incluye mucho más que solo virus. Los antivirus y los antimalware **sí pueden convivir instalados a la vez**. Como antimalware recomendamos [Malwarebytes](#).



Revisar las recomendaciones contra el phishing ofrecidas en esta guía, debido a que se ha demostrado que esta es la vía **más utilizada** para infectar a usuarios con malware.



Evitar o limitar las **actividades riesgosas** como la búsqueda y uso de software no legítimo o “**pirata**”, frecuentar sitios web de streaming de series y películas o descargar aplicaciones de **páginas no oficiales**.



6

NAVEGACIÓN SEGURA, EVASIÓN DE CENSURA Y ANONIMATO

Al usar Internet existe información privada o sensible que **no queremos revelar a terceros no autorizados** (datos personales, comunicaciones con denunciantes anónimos, fuentes periodísticas, entre otros). A continuación te ofrecemos algunas recomendaciones para que tu navegación en Internet sea **más segura**.

REDES INALÁMBRICAS



La **protección** de la redes inalámbricas, especialmente a través de una correcta configuración y uso del router, es esencial para evitar el monitoreo y ataques a nuestra red. Te sugerimos que lleves a cabo las siguientes recomendaciones para la protección de tus **redes caseras**:



RECOMENDACIONES

- ✓ **Configurar** una contraseña de acceso a la red.
- ✓ **Deshabilitar** las funciones WPS y UPnP.
- ✓ **Seleccionar** el protocolo WPA2 (o WPA3 si está disponible) en lugar de WEP o WAP que ya no son considerados seguros.
- ✓ Habilitar una **red de invitados**, de ser posible.
- ✓ Actualizar el router.
- ✓ **Descargar una aplicación de mapeo de red** para verificar que todos los equipos conectados son conocidos. Algunas sugerencias son [Ping Tools](#) (Android) y [Fing Network Scanner](#) (iOS) o utilizar las facilidades que ofrezca tu router.
- ✓ Tener **software antivirus** y antimalware instalado, actualizado y activado.

Adicionalmente, recuerda que las **redes públicas** son especialmente peligrosas. Evita acceder a este tipo de redes y si es necesario que accedas, **has uso de una VPN**.



Para más información sobre la protección de redes inalámbricas puedes consultar la guía de Derechos Digitales “Recomendaciones de seguridad en redes caseras de cara al teletrabajo” (marzo, 2020).

HTTPS

HTTPS es un **protocolo de transmisión de datos** que añade cifrado en la capa de transporte, protegiendo la información que envías al navegar en Internet, desde el dispositivo que utilizas hasta los servidores del sitio que quieres consultar.

Cuando navegas en páginas web con HTTPS evitas que terceros, incluyendo tu proveedor de servicios de Internet (ISP), **puedan capturar** la información que intercambias con el sitio que estás consultando. Esto no sucede en las páginas que no tienen activado el protocolo HTTPS sino que, por el contrario, tienen HTTP.

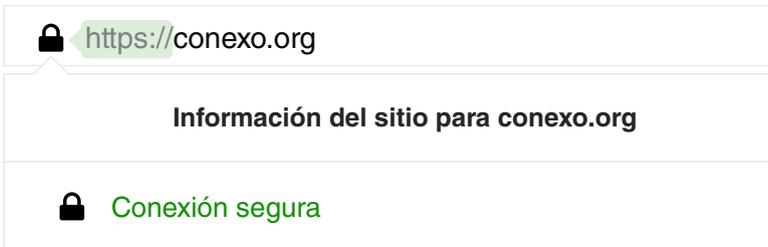
En la siguiente imagen vemos lo que sucedería con **la información que viaja a través de HTTP y la que viaja a través de HTTPS**, donde los cuadrantes de la izquierda representan lo que se ve en pantalla y los de la derecha lo que se transmite en la red:



Observamos que con **HTTP** la información de usuario y contraseña puede ser **capturada de manera legible** debido a que el canal por donde pasa esta información no está cifrado, mientras que con el protocolo **HTTPS**, tal captura de datos **no es posible** porque la información viaja a través de un canal cifrado.



Al usar **HTTPS** tu proveedor de servicios de internet, aunque puede ver que estás consultando un determinado URL, **no puede ver en qué parte específica de la página te encuentras** ni la información que intercambias con el sitio (como usuarios y contraseñas).



La implementación del protocolo HTTPS en una página web determinada depende enteramente de los encargados de la administración de dicha página a través de la instalación de **certificados TLS/SSL**. Como usuario solo puedes escoger navegar únicamente en páginas con HTTPS para estar seguro o, al menos, evitar intercambiar información que páginas que aún utilicen el protocolo HTTP.

El uso de HTTPS no asegura que la comunicación sea con el servicio deseado: **recomendamos** estar muy al tanto de que la dirección web sea la correcta y de que no hayan errores de cifrado.



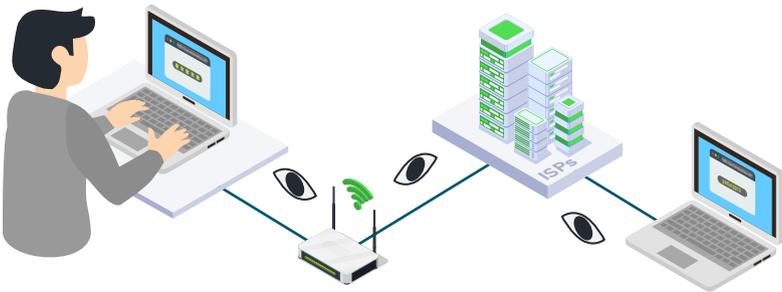
Si eres parte de la administración de una página web y deseas activar un certificado TLS/SSL para implementar HTTPS, una alternativa es hacerlo a través de [Lets Encrypt](#) que es una autoridad de certificación gratuita, automatizada, y abierta que otorga los certificados digitales que se necesitan para poder habilitar HTTPS de una manera amigable.

VPN



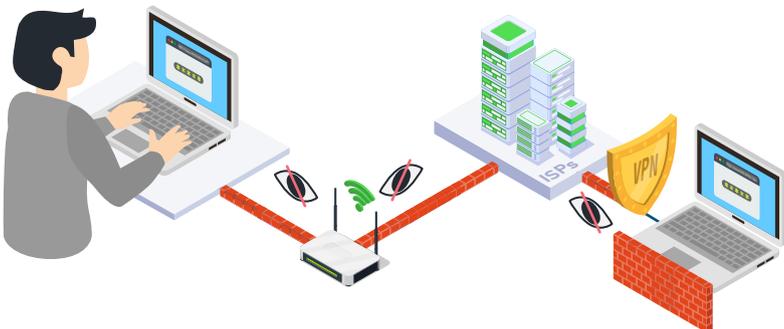
Qué es una VPN: Una VPN (RED PRIVADA VIRTUAL) es una tecnología que establece un **túnel seguro** de comunicación entre **dos o más dispositivos**, lo que le permite navegar por la web de forma más segura y privada, incluso si se usa una red Wi-Fi pública.

La siguiente es una gráfica de cómo funciona una **conexión sin VPN**:



Vemos cómo el usuario **accede a internet** a través de una red wifi y, a continuación, a partir del router se envía la información al proveedor de servicio de Internet (ISP) para posteriormente llegar hasta el servidor del sitio web que desea consultar. En este tipo de conexión sin VPN el ISP es capaz de ver cuáles son las páginas en las que navega el usuario así como la información que transmite si la página que consulta no cuenta con HTTPS.

La siguiente es una gráfica de cómo es una **conexión con VPN**:



VENTAJAS Y DESVENTAJAS DE USAR UNA VPN

VENTAJAS



Cifrar la información que envías en el tramo que va desde el origen (tu dispositivo) hasta el servidor VPN. Esto es una ventaja cuando, por ejemplo, necesitas navegar en una página que no tiene configurada una conexión HTTPS o tienes sospechas de que tus comunicaciones están siendo vigiladas.



Ocultar a tu proveedor de servicio de Internet (ISP) las páginas en las que navegas.



Ocultar tu identidad al servicio que quieres consultar como destino final (Ejemplo: google.com). Esto sucede porque el destino final supone que quien realiza la consulta es el servidor VPN.



Tener acceso a los sitios que han sido bloqueados por tu proveedor de servicios de Internet.

DESVENTAJAS



Es posible que al activar una VPN percibas que tu conexión se vuelve más lenta. En este caso, te recomendamos encenderla solo cuando vas a navegar en páginas sin HTTPS o sensibles, cuando quieras consultar sitios bloqueados o cuando realices trabajos de investigación. También puedes intentar cambiar de servidor VPN a uno más cercano a ti.



Un servicio de VPN, así como otros servicios que ayudan a lograr el anonimato (Ej. TOR), **también pueden ser bloqueados.** Si reconoces algún bloqueo denuncialo a través de los medios que tengas a tu disposición para que la comunidad que apoya el Internet libre ayude a restablecer el servicio u ofrezca otras alternativas de conexión.



Acerca de la navegación privada o en modo incógnito

La navegación privada, también llamada en modo incógnito o en ventana privada, es una función de privacidad en algunos navegadores web que **evita que se almacene permanentemente de forma local** (en los dispositivos) el historial de navegación, cookies y caché web, para evitar que puedan ser recuperados por terceros más adelante. Es importante no confundir esta característica con la navegación con HTTPS o con VPN.



RECOMENDACIONES

Descarga una VPN para cada uno de tus dispositivos móviles y computadoras que puedas tener encendida de forma permanente para obtener las ventajas de seguridad que te hemos descrito anteriormente. Si no puedes mantener la VPN siempre encendida por razones de ancho de banda, entre otras, te recomendamos utilizarla, al menos, para la navegación durante trabajos de investigación u otros similares, cuyo conocimiento por parte de terceros pueda ponerte en riesgo.

Las siguientes son algunas de las VPN que te sugerimos utilizar:



SITIO WEB	TunnelBear	Psiphon	ExpressVPN	Mullvad
PLANES Y COSTOS	Sin costo hasta 500MB mensuales. Existen planes pagos disponibles.	Sin costo.	12,95 USD por mes. Hasta 5 dispositivos conectados simultáneamente por cuenta. Existen otros planes disponibles.	5,5 USD por mes. Hasta 5 dispositivos conectados simultáneamente por cuenta.
DISPONIBLE EN	iOS, Android, MacOS, Windows y como extensión en los navegadores Chrome, Firefox, y Opera.	iOS, Android y Windows.	iOS, Android, MacOS, Windows, Linux y como extensión en los navegadores Chrome y Firefox.	iOS, Android, MacOS, Windows y Linux.
KILL SWITCH	✓	✗	✓	✓



Característica “Kill switch”

La característica denominada “*kill switch*”, que no poseen todos los servicios de VPN, consiste en bloquear todo el tráfico de Internet si por alguna razón la conexión se cae y la aplicación de VPN se desconecta. De esta forma se impide, entre otras ventajas, que puedan revelarse al ISP las páginas que estaban siendo consultadas antes de que se interrumpiera la conexión, es decir, se garantiza que el tráfico (y los datos) no se filtren accidentalmente fuera del túnel seguro.

¿Utilizas servicios de streaming?

Si eres usuario frecuente de servicios de streaming (retransmisión continua generalmente de audio y video), [EdgeWise Connect](#) es una VPN capaz de cambiar la transmisión de datos desde Wi-Fi a los datos móviles del celular, evitando que puntos de acceso lentos o que no funcionen interrumpan tus actividades en línea. Cuando el usuario vuelve a estar dentro del alcance de una red Wi-Fi en funcionamiento, EdgeWise moverá automáticamente el tráfico a Wi-Fi para conservar los datos móviles. En su versión gratuita ofrece 3 horas de conexión diaria.



TOR

La red Tor es una red de servidores distribuidos en diferentes partes del mundo que tiene como objetivo principal **facilitar el anonimato** de los usuarios al pasar los datos de estos por múltiples servidores antes de llegar al punto de destino. La mejor analogía es con un servidor VPN, con la diferencia de que la red Tor utiliza una cadena de servidores que cambia para cada sesión de usuario.

Esta plataforma mantiene protocolos de comunicación propios que dificultan el análisis de los datos interceptados, sin embargo, no está diseñado para competir con el cifrado que emplean las infraestructuras de VPN.





RECOMENDACIONES



Descargar [Tor Browser](#) para conectarse a la red Tor y navegar de forma anónima, acceder a sitios bloqueados por tu ISP o visitar sitios propios de la red Tor (a través de los llamados “servicios onion”). Ten en cuenta que, así como sucede con el uso de la VPN, con Tor también puede ocurrir que la conexión a internet se vuelva más lenta.



Si deseas **anonimato** y, al mismo tiempo, contar con las ventajas del cifrado en tránsito de las VPN, puedes navegar en *Tor Browser* con la VPN encendida. Será como añadir una capa de seguridad sobre otra.



Para **proteger tu privacidad** frente al comercio de datos, te recomendamos instalar en el navegador la extensión [UBlock Origin](#) y [Privacy Badger](#) que bloquean los rastreadores de recopilación de datos. También puedes considerar migrar a *Firefox* debido a que es la alternativa de navegador que ofrece más opciones para resguardar la **privacidad de los usuarios** a través de la eliminación del historial de navegación y cookies una vez que cierras la sesión, entre otros.



7 | CORREOS ELECTRÓNICOS SEGUROS

Los **correos electrónicos** son uno de los medios que más empleados para comunicarnos y, al igual que con el resto de las herramientas que hemos abordado en esta guía, es importante que aprendamos cuáles son las características de seguridad que debemos buscar en los servicios que utilizamos y cuál es la configuración más adecuada para ganar **mayor seguridad y privacidad**.

Lo primero que debes saber es que no todos los servicios de correo electrónico incluyen las mismas características de seguridad, por ejemplo, **no todos permiten** la autenticación de dos factores, así mismo, no todos ofrecen cifrado de extremo a extremo. A continuación te mencionamos las características de seguridad que son convenientes que busques en los servicios de correo que utilizas, así como una tabla comparativa con las características de seguridad de algunos de los servicios de correo.



RECOMENDACIONES

Lo fundamental es que los servicios de correo electrónico que utilizas cuenten con:



HTTPS: para la transmisión de datos en tránsito de forma segura.



Autenticación de dos factores (2FA).



Actualizaciones continuas en las versiones escritorio, aplicaciones y versiones web.

La siguiente **recomendación** es que puedas decidirte, al menos para los temas más sensibles, por opciones de correo que ofrecen cifrado de extremo a extremo o la posibilidad de que cifres tu mismo tus correos a través del uso de PGP/GPG. Como explicamos en líneas anteriores, este tipo de cifrado permitirá que **solo tú y el destinatario** (no la compañía proveedora) pueda ver el contenido del correo.



¿Qué es PGP/GPG?

PGP (Pretty Good Privacy) es un protocolo que utiliza una combinación de métodos de cifrado como la criptografía de claves públicas para mantener los datos seguros. Este proceso se puede utilizar para cifrar archivos de texto, correos electrónicos, archivos de datos, entre otros.

Por su parte, **OpenPGP** es un estándar de PGP para uso público.

GNU Privacy Guard, también llamado **GnuPG** o **GPG** es una implementación completa, gratuita y de código abierto del estándar OpenPGP.

Al utilizar este tipo de cifrado **necesitarás** una llave — virtual — privada capaz de descifrar el contenido de tus comunicaciones y archivos a la que sólo tú tendrás acceso, por lo cual es muy importante que almacenes esta llave en un lugar seguro.

Adicionalmente, **consulta** en dónde está registrada la compañía y en dónde alojan sus servidores. Esto es importante porque las compañías deben ajustarse a la legislación del lugar donde operan, lo que significa que, si lo indica la ley, una compañía puede estar obligada a facilitar información de los usuarios a su gobierno.

Por ejemplo, las compañías que ofrecen servicios de correo que tienen sede en Europa deben ajustarse al **Reglamento General de Protección de Datos de la Unión Europea**. Este reglamento está catalogado como la normativa general más respetuosa a la privacidad y seguridad de los usuarios que está vigente hasta ahora. A partir de aquí los países miembros de la Unión Europea deben implementar sus leyes de protección de datos.



¿USAS GMAIL? CHEQUEA TAMBIÉN LO SIGUIENTE:

- ✓ En la [Revisión de Seguridad](#) en tu cuenta Gmail **verifica** que tengas activa la verificación en dos pasos, que los dispositivos conectados sean conocidos, que las contraseñas de aplicación se correspondan con los servicios que has activado por esta vía y que la “actividad reciente relacionada con la seguridad” no muestre actividad sospechosa.

- ✓ En la ruta **Configuración > Filtros y direcciones bloqueadas**, chequea que no exista ningún correo al que se reenvíe la información que recibes.
- ✓ En la ruta **Configuración > Reenvío y correo POP/IMAP**, a menos que utilices un cliente de correo como Outlook, es recomendable que inhabilites ambas opciones (POP e IMAP).
- ✓ Los [Informes de transparencia de Google](#). Estos incluyen reportes relacionados a la privacidad y seguridad de la compañía, solicitudes de retiros de contenido e informes adicionales. Particularmente puedes consultar las [solicitudes de información sobre usuarios en todo el mundo](#).



OTRAS RECOMENDACIONES:



Revisa la **configuración** de seguridad y privacidad, incluyendo dispositivos y conexiones recientes.



Evalúa **utilizar distintas cuentas de correo** para tus actividades, así puedes mantener separadas las comunicaciones personales de las profesionales.



Evalúa **utilizar correos desechables** para servicios o herramientas que quieras probar y requieran de un registro con correo electrónico. Una recomendación es 10minutemail.com.



Toma un tiempo para **revisar las políticas de privacidad**, particularmente los datos que recopila el servicio, el uso que le dan y cómo se comportan frente a la solicitud de información por parte de terceros.

A continuación te mostramos la siguiente tabla comparativa con las principales características de algunos servicios de correo:



	Gmail	Tutanota	Protonmail
HTTPS			
AUTENTICACIÓN DE DOS FACTORES			
LOCALIZACIÓN	EEUU	Alemania	Suiza
CIFRADO DE EXTREMO A EXTREMO			
PGP/GPG Y POSESIÓN DE LA LLAVE PRIVADA	Es posible configurar PGP/GPG a través de la configuración de Mailvelope en el correo electrónico (consulta si tu proveedor lo permite) o de Enigmail + Thunderbird. En ambos casos solo el usuario tendrá acceso a la llave privada.	El cifrado con PGP/GPG ocurre de forma transparente para facilitar su uso, sin embargo, para que esto suceda, el servidor de la compañía conserva la llave privada y no es posible para el usuario obtener una copia.	El cifrado con PGP/GPG ocurre de forma transparente para facilitar su uso, sin embargo, para que esto suceda, el servidor de la compañía conserva la llave privada. Adicionalmente es posible para el usuario descargar una copia.
PLANES Y COSTOS	Sin costo hasta 15GB (con anuncios). GSuite por \$5.40 USD/usuario/mes (30GB en Drive). Otros planes disponibles.	Sin costo hasta 1 GB de almacenamiento (sólo dominio de Tutanota). 1,20 euros mensuales hasta 1 GB de almacenamiento (dominios personalizados). Otros planes disponibles.	Sin costo hasta 500 MB de almacenamiento. 5 euros mensuales hasta 5 GB de almacenamiento. Otros planes disponibles.
DISPONIBLE EN	Browser, iOS y Android.	Browser, iOS, Android, Windows, MacOS y Linux.	Disponible en Browser, iOS y Android.



8

PROTECCIÓN FÍSICA DE LA INFORMACIÓN

Nuestros archivos pueden ser **vulnerables a ataques** durante las comunicaciones (al momento de enviarlos/recibirlos) debido a que las mismas pueden estar comprometidas o siendo monitoreadas.

También son vulnerables en los **equipos donde reposan**, debido a que pueden caer en manos equivocadas y volverse inaccesibles. Las siguientes son recomendaciones para la protección de tus archivos frente a estos posibles ataques.



RECOMENDACIONES

CIFRADO DE ARCHIVOS

Es recomendable que cifres tus archivos en los dispositivos que los contienen para evitar que terceros puedan acceder a ellos frente a situaciones de robo, extravío, entre otras. Este cifrado puedes llevarlo a cabo de las siguientes maneras:



Cifrado completo de disco duro: A través de la activación de **FileVault** (usuarios MacOS), **Bitlocker** (usuarios Windows), **LUKS** (usuarios Linux) o **Veracrypt** (para cualquier sistema operativo).

Para **activar el cifrado del disco completo** es necesario configurar con contraseña de acceso al equipo que impida que terceros puedan obtener la información. extraer el contenido del disco fácilmente aún sin tener la contraseña de acceso.



FileVault



BitLocker



LUKS



VeraCrypt



Para el cifrado de teléfonos móviles consulta la sección “Teléfono Móvil” de esta guía.



BitLocker no se encuentra disponible en Windows 10 Home. Para activarlo necesitamos obtener la versión profesional del sistema operativo de Microsoft (Windows 10 Pro).



Cifrado de otros volúmenes de almacenamiento: Una alternativa al cifrado completo del disco duro es cifrar volúmenes de almacenamiento extraíbles tales como unidades USB o volúmenes específicos en el disco duro. Herramientas que permiten llevar esto a cabo son **VeraCrypt** (usuarios MacOS y Windows) y **BitLocker** (usuarios Windows).

BORRADO DE ARCHIVOS



Cuando eliminas un archivo en tu computadora, incluso cuando vacías la “papelera”, realmente no estás borrando la información, solo estás indicando que ese espacio que ocupa el archivo puede ser sobrescrito en cualquier momento con nueva información. En este sentido, es posible recuperar los datos “**borrados**” con algún software disponible o métodos forenses.



Si deseas **borrar de forma segura** la información contenida en unidades de disco tradicionales — no en los discos de estado sólido (SSD) — o en unidades USB, lo recomendable es utilizar programas especializados como [CCleaner](#) o [Eraser](#) que sobrescriben el espacio que ocupaba la información “eliminada” de forma que haría muy difícil su recuperación.



El **borrado seguro** en unidades SSD, unidades flash USB y tarjetas SD es muy difícil debido a su diseño (utilizan una técnica denominada “**nivelación del desgaste**”). Para la protección de los archivos contenidos en estas unidades se recomienda la **activación del cifrado completo del disco** en conjunto con estrategias del respaldo y otras medidas adicionales tales como evitar llevar consigo los equipos con información sensible durante viajes, entre otras.

RESPALDO DE ARCHIVOS

Para garantizar la disponibilidad de la información es importante que puedas hacer respaldos o copias de seguridad de tus archivos. Lo recomendable es que los respaldos se realicen a través de **servicios/herramientas seguras** y tomes en cuenta los siguientes criterios sobre tus copias:

- ✓ Cifradas.
- ✓ Fácil restitución.
- ✓ Ubicación física distante al o los sitios que pueden ser vulnerados.
- ✓ En internet.
- ✓ Frecuentes.
- ✓ Copias incrementales.

Existe una estrategia de respaldo bastante conocida llamada “**Backup 3-2-1**” que consiste en:

- ✓ Tener al menos tres (3) respaldos de tus datos.
- ✓ Almacenarlas en dos (2) medios diferentes (físico y virtual).
- ✓ Conservar una (1) copia en un lugar fuera de las instalaciones que podrían ser vulnerables.



En esta sección te hemos ofrecido alternativas para la protección de tus archivos en los equipos que los contienen, sin embargo, no debes olvidar **tomar medidas de protección en el espacio físico** donde se encuentran estos equipos, como tu casa u oficina.



9 | SEGURIDAD EN REDES SOCIALES

En los últimos años las **redes sociales** se han convertido en una de las principales vías para comunicarnos, informarnos e intercambiar ideas pero, al igual que otros medios, también pueden ser utilizadas por atacantes que pueden comprometer nuestros datos y nuestra seguridad. Por otro lado, las redes sociales constituyen una de las principales fuentes de **comercio de datos** y funcionan en una forma que está afectando la privacidad de sus usuarios.

Para **evitar estas amenazas** te ofrecemos las siguientes recomendaciones relacionadas no solo con la seguridad sino también con la privacidad de tu información:



RECOMENDACIONES



Define si tu participación en la **red social** será a través de tu nombre o un alias.



Define el correo electrónico que estará **asociado a tu cuenta**. Si es personal, de trabajo o uno anónimo creado para este fin.



Cuando selecciones tu **foto de perfil** evalúa si usarás la misma en todas tus redes, si mostrarás tu rostro y si tiene el potencial de mostrar más información sobre ti que la que deseas revelar.



Configura una **contraseña segura de acceso** y toma en cuenta el resto de las recomendaciones que te ofrecemos en la sección de **Contraseñas** de esta guía, por ejemplo, cómo configurar las respuestas a las preguntas de seguridad.



Activa la autenticación de dos factores.



Evita tener **conversaciones sensibles** a través de los chats o mensajes directos en redes sociales.



Revisa las opciones de privacidad y seguridad. Por ejemplo, selecciona si deseas que te encuentren a través de tu número de teléfono o escoge quién puede ver tus publicaciones, entre otros. En Twitter es recomendable que **desactives las opciones de ubicación en los tweets** al igual que las opciones de etiquetado de fotos por terceros.



Configura las **notificaciones** de forma que puedan avisarte cuando exista una **actividad sospechosa** en la cuenta, por ejemplo, el intento de inicio de sesión en un nuevo equipo.



Toma un tiempo para **revisar las políticas de privacidad**, particularmente los datos que recopila el servicio, el uso que le dan y cómo se comportan frente a la solicitud de información por parte de terceros.



Recuerda que, aunque realices las configuraciones adecuadas, todo lo que subes en las redes tiene la posibilidad de hacerse público. **Evalúa antes de publicar** la conveniencia de compartir una determinada información.



REFERENCIAS

- Citizen Lab. (Última actualización: 22 de febrero, 2020). Improve your online safety with advice from experts. Recuperado de: <https://securityplanner.org/#/>
- Derechos Digitales. (Junio 2018). ¿Confiable y seguro? Un vistazo a las potenciales vulnerabilidades de WhatsApp. Santiago de Chile. Recuperado de: <https://www.derechosdigitales.org/wp-content/uploads/Confiable-y-seguro.pdf>
- Guerra, Carlos. (2018). SDA Seguros y Documentados para el Activismo. Santiago de Chile. Recuperado de: https://sdamannual.org/assets/pdf/sda_es.pdf
- Electronic Frontier Foundation. Surveillance Self-Defense. Tips, Tools and How-Tos for Safer Online Communications. Recuperado de: <https://ssd.eff.org/>
- Tactical Tech. The Holistic Security Manual. Berlín, Alemania. Recuperado de: <https://holistic-security.tacticaltech.org/>
- Derechos Digitales.(2018). Torificate. Recuperado de: <https://tor.derechosdigitales.org/torificate>
- Internews. SAFETAG. A Security Auditing Framework and Evaluation Template for Advocacy Groups. Recuperado de: <https://safetag.org/guide/>
- Guerra, Carlos. (Marzo 2020). Recomendaciones de seguridad en redes caseras de cara al teletrabajo. Santiago de Chile. Recuperado de: <https://www.derechosdigitales.org/wp-content/uploads/Recomendaciones-de-seguridad-en-Redes-caseras-de-cara-al-teletrabajo.pdf>
- Fundación Karisma. (Noviembre 2016). Seguridad, Protección y Privacidad de Twitter. Recuperado de: <https://web.karisma.org.co/pagina-principal/que-hacemos/campanas/seguridad-proteccion-y-privacidad-de-twitter/>
- Protege.la y SocialTIC. (Junio 2018). Checklist de Seguridad Digital para tu Computadora, Celular y Cuentas en Línea. Recuperado de: <https://protege.la/checklist-de-seguridad-digital-%E2%9C%85/>

CHECKLIST PARA MEJORAR LA SEGURIDAD DIGITAL

BASADO EN LA GUÍA
"SEGURIDAD DIGITAL: CONCEPTOS Y HERRAMIENTAS BÁSICAS"
DE CONEXO

Mayo, 2020

A

CONTRASEÑAS

- Tus contraseñas son largas o utilizan diferentes tipos de caracteres y no son predecibles.
- Evitas repetir contraseñas de acceso entre los distintos servicios/equipos que utilizas.
- Respondes a las preguntas de seguridad para la recuperación de cuentas con información no predecible o contraseñas.
- Has configurado de forma segura los correos alternativos de recuperación de cuentas.
- Evitas dejar copias accesibles con información de acceso a tus cuentas de usuario y equipos.
- Evitas acceder a tus cuentas de usuario desde equipos que no sean de confianza.
- En caso de ser necesario, compartes tus contraseñas únicamente por canales seguros y las cambias cuando deje de ser necesario compartirlas.
- Evitas guardar contraseñas en los navegadores web.
- Cuando cambias tus contraseñas, creas nuevas contraseñas evitando el uso de patrones.
- Utilizas administradores de contraseñas para la creación y almacenamiento de las mismas.

B

AUTENTICACIÓN DE DOS FACTORES

- Si eres usuario de Whatsapp, has activado la verificación en dos pasos.
- Si eres usuario de Signal, has activado el bloqueo de registro.
- Para los servicios que aplique, has activado la autenticación de dos factores a través de aplicaciones de autenticación, token o llaves de seguridad en lugar de mensajes de texto (SMS).
- Has activado la autenticación de dos factores en todas las cuentas de usuario que utilizas que permiten esta característica. (Ejemplo: correos electrónicos, redes sociales, entre otros).
- Has guardado de manera segura los códigos de recuperación de emergencia que ofrece el servicio (si aplica) al habilitar la autenticación de dos factores.

C

TELÉFONO MÓVIL

Llamadas y mensajería instantánea o chats

- Al menos para conversaciones sensibles, realizas llamadas haciendo uso de aplicaciones con cifrado de extremo a extremo, evitando las líneas fijas o móviles.

- Al menos para conversaciones sensibles, envías mensajes haciendo uso de aplicaciones de mensajería instantánea con cifrado de extremo a extremo, evitando los SMS.

- Si eres usuario de Whatsapp, has activado la verificación en dos pasos.

- Si eres usuario de Whatsapp, has activado las notificaciones de seguridad.

- Si eres usuario de Whatsapp, verificas los códigos de seguridad (llaves de seguridad) de las personas con las que chateas a través de otros canales seguros.

- Si eres usuario de Whatsapp, has desactivado las copias de seguridad y eliminado los respaldos que pudieron hacerse anteriormente.

- Si eres usuario de Whatsapp, has revisado que en "Whatsapp Web/Escritorio" estén enlazados únicamente los dispositivos autorizados por ti.

- Si eres usuario de Signal, has activado el bloqueo de registro.

- Si eres usuario de Signal, has activado la caducidad de mensajes, al menos para las conversaciones más sensibles.

- Si eres usuario de Signal, verificas las cifras de seguridad (llaves de seguridad) de las personas con las que chateas a través de otros canales seguros.

- Si eres usuario de Signal (en Android), has desactivado las copias de seguridad.

- Si eres usuario de Signal, has revisado que en "dispositivos enlazados" estén únicamente los dispositivos autorizados por ti.

Rastreo

- Cuando acudes a reuniones sensibles, tomas medidas para evitar el rastreo a través de tu equipo celular y chip.

Protección física de la información en teléfonos móviles

- Has añadido una contraseña de acceso a tu equipo celular, preferiblemente alfanumérica.

- Has activado o verificado que esté activa la funcionalidad de cifrado de la información contenida en el equipo celular y en la tarjeta SD.

- Has activado Find My Device (usuarios Android) o Find My iPhone (usuarios iOS).

- Descargas las aplicaciones de tu teléfono móvil únicamente de las tiendas oficiales (AppStore o PlayStore).

- Tienes como hábito descargar solo las aplicaciones necesarias.

- Revisas qué permisos (como acceso a cámara o micrófono) otorgas a las aplicaciones que usas y desactivas aquellos innecesarios para el funcionamiento de la app.

- Evitas cargar el teléfono usando cables o puertos USB en dispositivos desconocidos.
- Mantienes actualizado el sistema operativo, así como las aplicaciones.
- Respaldas frecuentemente la información más importante en la nube o en volúmenes cifrados.
- Mantienes la funcionalidad de Bluetooth apagada cuando no esté en uso.

D

PHISHING

- Desconfías de mensajes que instan a tomar acciones rápidas o de urgencia, verificando su legitimidad por vías alternas.

Delante a la recepción de mensajes sospechosos:

- Consultas canales oficiales del ente al que se hace referencia como alternativa de verificación segura de la información.
- Consultas por vías alternas con las personas a las que se hace referencia como alternativa de verificación segura de la información.
- Evitas hacer clic en los vínculos incluidos en el mensaje recibido.
- Verificas el emisor del mensaje.
- Evitas descargar archivos o instalar el software adjunto al mensaje.
- Verificas la veracidad de los vínculos acortados incluidos en el mensaje a través de herramientas como unshorten.me, unshorten.it o getlinkinfo.com.
- Mantienes actualizado el software de tus equipos.
- Utilizas un administrador de contraseñas con relleno automático de los campos de usuario y contraseña para tus cuentas de usuario.
- Tienes activada la autenticación de dos factores para todas tus cuentas de usuario que lo permiten.

E

MALWARE

- Mantienes el sistema operativo y demás programas (navegadores, aplicaciones, procesadores de texto, entre otros) actualizado y original.
- Instalas y mantienes actualizado un programa antivirus en tu computador.
- Instalas y mantienes actualizado un programa antimalware en tu computador.
- Analizas las unidades USB, automática o manualmente, a través de un antivirus o antimalware antes de ejecutar un programa o archivo contenido en él.
- Sigues las recomendaciones contra el phishing ofrecidas en la guía de seguridad de Conexo para evitar la instalación de malware a través de esta vía.
- Evitas o limitas actividades riesgosas como la búsqueda y uso de software no legítimo o "pirata", visitas a sitios web de streaming de series y películas, o descargas de aplicaciones desde páginas distintas a las oficiales.

F

NAVEGACIÓN SEGURA, EVASIÓN DE CENSURA Y ANONIMATO

Redes inalámbricas

- Has configurado una contraseña de acceso a la red.
- Has deshabilitado las funciones WPS y UPnP.
- Has configurado el uso del protocolo WPA2 o WPA3 (si está disponible) en lugar de WEP o WPA.
- Has habilitado una red de invitados, de ser posible.
- Mantienes el router actualizado.
- Utilizas aplicaciones de mapeo de red para verificar que todos los equipos conectados son conocidos.

Navegación

- Verificas que la páginas en las que navegas utilizan HTTPS.
- Evitas la navegación, o al menos el intercambio de información, en páginas que aún utilizan el protocolo HTTP.
- Mantienes tu navegador actualizado.
- Al menos para la consulta de temas sensibles que puedan ponerte en riesgo, navegas a través de una VPN o haciendo uso de Tor en tus dispositivos móviles y computadoras.
- Cuando accedes a internet haciendo uso de redes públicas o no confiables, navegas a través de una VPN.
- Cuando seleccionas un servicio de VPN, tomas en cuenta que posea la característica "kill switch".

G

CORREOS ELECTRÓNICOS SEGUROS

Los servicios de correo electrónico que utilizas cuentan con:

- HTTPS para la transmisión de datos en tránsito de forma segura.
- Autenticación de dos factores (2FA).
- Actualizaciones continuas en las versiones escritorio, aplicaciones y versiones web.

¿Eres usuario de Gmail?

- Has configurado una clave de acceso segura de acuerdo a las recomendaciones ofrecidas en la guía de seguridad de Conexo.
- Has activado la verificación en dos pasos.
- Has configurado de forma segura el correo electrónico de recuperación.
- Has realizado la "Revisión de Seguridad" de tu cuenta Gmail.
- En la ruta Configuración > Filtros y direcciones bloqueadas, has chequeado que no exista ningún correo al que se reenvíe la información que recibes que no haya sido configurado por ti.
- A menos que utilices un cliente de correo como Outlook, en la ruta Configuración > Reenvío y correo POP/IMAP, has inhabilitado las opciones POP e IMAP.

Otros:

- Al menos para temas sensibles o que puedan ponerte en riesgo, utilizas servicios de correo que ofrecen cifrado de extremo a extremo o cifras tú mismo tus correos a través del uso de PGP/GPG.
- Has revisado y ajustado las configuraciones de seguridad y privacidad en los servicios de correo electrónico que utilizas.
- Utilizas distintas cuentas de correo para tus diferentes actividades profesionales y personales.
- Conoces las políticas de privacidad de los servicios de correo electrónico que utilizas, al menos en lo relacionado con los datos que recopilan, el uso que le dan y cómo se comportan frente a la solicitud de información por parte de terceros.

H PROTECCIÓN FÍSICA DE LA INFORMACIÓN

- Has activado o verificado que esté activa la funcionalidad de cifrado de la información contenida en el equipo celular y en la tarjeta SD.
- Para los archivos contenidos en el computador, has activado el cifrado completo del disco duro a través de la activación de FileVault (usuarios MacOS), BitLocker (usuarios Windows), LUKS (usuarios Linux) o Veracrypt (para cualquier sistema operativo).
- Para los archivos contenidos en otros volúmenes (por ejemplo, discos externos), has activado el cifrado a través de las herramientas correspondientes.
- Para la información contenida en unidades de disco tradicionales — no en los discos de estado sólido (SSD) — o en unidades USB, borras la información a través de programas especializados como CCleaner o Eraser.
- Realizas respaldos o copias de seguridad de tus archivos siguiendo las recomendaciones de la guía de seguridad de Conexo (copias cifradas, de facilidad de restitución, ubicación física distante al o los sitios que pueden ser vulnerados, en internet, frecuentes e incrementales).
- Has desarrollado políticas de seguridad en caso de viajes profesionales y personales.

I SEGURIDAD EN REDES SOCIALES

- Has escogido conscientemente si tu participación en las redes sociales es a través de tu nombre o un alias.
- Has escogido conscientemente el correo electrónico asociado a tu cuenta (anonimo, personal o profesional).
- Has escogido conscientemente la foto de perfil de tus cuentas en redes sociales de forma que eviten mostrar más información sobre ti que la que deseas revelar.
- Has configurado una contraseña segura de acceso.
- Has configurado de forma segura el correo electrónico de recuperación.
- Has configurado de forma segura las respuestas a las preguntas de seguridad.
- Has activado la autenticación de dos factores.

- Evitas tener conversaciones sensibles a través de los chats o mensajes directos en redes sociales.
- Conoces, revisas y configuras según tus necesidades las opciones de privacidad y seguridad en las redes sociales.
- Configuras, cuando están disponibles, las notificaciones de forma que puedan avisarte cuando exista una actividad sospechosa en la cuenta, por ejemplo, el intento de inicio de sesión en un nuevo equipo.
- Conoces las políticas de privacidad de las redes sociales que utilizas, al menos en lo relacionado con los datos que recopilan, el uso que le dan y cómo se comportan frente a la solicitud de información por parte de terceros.
- Tomando en cuenta que todo lo que subes en las redes tiene la posibilidad de hacerse público, evalúas, antes de publicar, la conveniencia de compartir una determinada información.