Mujeres Activistas por el software libre

2 Guía

Herramientas de cuidado digital:

¿cómo te puedes vacunar frente a las violencias digitales?

Créditos

Investigación:

Nerissa José, Aguilera Arteaga
María Germana, Oliveira Blazetic
María Ángela, Petrizzo Páez

Diseño e Ilustración:

Sandra ,Triana Duarte

@sandra_triana77

@activistassl
@activistassl
contacto@activistasxsl.org
http://activistasxsl.org

Mujeres Activistas XSL

Caracas, marzo 2022

Presentación

Mujeres Activistas por el Software Libre.

Es es un colectivo de mujeres venezolanas que viene trabajando desde el 2009 en acciones para empoderar a las mujeres en el uso efectivo de herramientas de tecnologías libres, habilitándolas en la identificación, prevención y mitigación de situaciones riesgosas para ellas, de forma de impactar positivamente en su entorno y reducir la brecha de género digital.

Desde el 2011 nos interesamos en indagar sobre aspectos de seguridad digital que afectan a mujeres y cuya resolución pasa por un conocimiento especializado de los riesgos y vulnerabilidades de nuestro uso en la Red. Un año después iniciamos talleres sobre cibercuidados para colectivos activistas e iniciamos el proceso de atención a víctimas y sobrevivientes de Violencias Digitales Basadas en Género (VDBG).

De esa experiencia, hemos compilado este trabajo que hoy te presentamos en formato de talleres de formación que, si bien venimos trabajando desde hace ya varios años, también actualizamos de forma permanente para poder acercar esta información a más y más mujeres de nuestro país.

Cada uno de nuestros talleres está acompañado de una guía en la que detallamos la información que presentamos. Esta guía que verás ahora, es posible gracias al apoyo recibido a través del Fondo de Mujeres del Sur y su programa Liderando desde el Sur, en el año 2022.

2 Guía

Herramientas de cuidado digital:

¿cómo te puedes vacunar frente a las violencias digitales?

¿Qué aprenderemos con esta guía?

- A navegar de forma segura en internet.
- A evitar la violencia digital.
- Aplicar medidas de seguridad digital en nuestras redes sociales, plataformas y servicios a los que accedemos.
- Cuidar nuestra privacidad en las redes sociales
- ¿Qué significa estar segura en Internet?
- ¿Qué significa mantener tu privacidad en Internet?

Buenas prácticas Generales de Cibercuidado

***Cuida lo que publicas*,** antes de publicar algo, piensa en cómo eso pudiera afectarte en un futuro (incluso cercano), recuerda que todo lo que publiques puede quedar en manos de terceras personas (como las empresas que prestan los servicios) o que incluso no puedas borrarlo.

- No publiques fotos indicando el sitio donde estás actualmente, publica en pasado.
- No publiques fotos donde tengas algún uniforme, de tu trabajo o de tu escuela.
- Desactiva la ubicación en tus dispositivos.
- No publiques los lugares en donde estarás o cuales son tus planes del día.

Cuidado con las apariencias, recuerda que todo lo que ves en Internet no necesariamente es real, y la facilidad que brinda la tecnología para crear ilusiones nos dificulta muchas veces a distinguir la realidad de una mentira.

- ¿Utiliza una imagen real? Puedes usar herramientas para la búsqueda de imágenes en línea para verificar si la imagen fue tomada de otro sitio.
- Si conoces su correo electrónico también puedes usarlo para verificar si está en otros sitios, o incluso si cuenta con algún otro registro en línea como su curriculum si es una persona, o si ese correo pertenece efectiva mente a una empresa o negocio.
- ¿Tiene publicaciones recientes? De lo contrario podría ser una cuenta creada solo para atraer personas, y dar una falsa imagen de realidad.

Investiga siempre, intenta conocer lo más que puedas a las personas que están detrás de las cuentas que sigues en tus redes sociales, las personas con quien hablas en línea, las páginas web o blogs que frecuentas.

- A quiénes siguen, qué comparten, cuál es el tono de sus comentarios, cómo responden a los comentarios de otros, entre otras cosas te pueden dar una idea de cómo son la o las personas detrás de la tecnología.
- ¿Es una persona o una empresa? ¿Cuál es la intención de la cuenta o de esa empresa?
- ¿Qué interés puede tener en seguirte y ver tus publicaciones? ¿Estás dispuesta a compartir lo que publicas con alguien que no conoces o con empresa u organización?

Cuidado con lo que envías, incluso las herramientas más seguras pueden ser vulneradas, recuerda que ningún sistema informático está libre de vulnerabilidades, solo que algunos son más seguros que otros.

- Conoce a quien envías fotos y archivos personales, asegúrate que realmente puedes confiar en esa persona.
- Utiliza herramientas que te garanticen el mayor grado de seguridad, y aún así, piensa en las formas en que podría vulnerarse. Por ejemplo, una herramienta que no permita la captura pantalla (print screen), podría tomarle una foto a la pantalla con otro dispositivo.

- Si vas a practicar sexting con cualquier persona, conocida o no, procura informarte sobre las herramientas y estrategias que puedes usar para mejorar tu privacidad. Por ejemplo, no envíes fotos de cuerpo entero, en donde también este expuesto tu rostro o marcas particulares como tatuajes y lunares entre otros.

Conoce las herramientas que usas, infórmate todo lo que puedas sobre las herramientas que usas y cómo funcionan, busca redes de apoyo en materia tecnológica que te permitan mantener en contacto con personas que sean especialistas en el área y busca información en sitios especializados en seguridad informática donde analicen esas herramientas.

- Evalúa cuáles son las opciones de privacidad y seguridad de las herramientas que utilizas.
- ¿Tienen rastreo de ubicación? ¿Utilizan el GPS de tus dispositivos?, ¿Existe la opción de desactivarlo?
- ¿Qué empresa u organización controla la herramienta y que datos obtienen de ella? ¿Existe la opción de borrar los datos?

Recuerda que la tecnología es un medio y una herramienta que puede ser usada para la difusión de datos e información, pero al mismo tiempo puede servir para la recolección de toda esa información, y que las empresas que brindan estos servicios nunca lo hacen gratis: **si el servicio es gratis, el producto eres tú.**

La tecnología no está exenta de los problemas sociales que enfrentamos en el mundo off-line, sino que son trasladados y muchas veces magnificados gracias a su uso sin las debidas precauciones.

Buenas prácticas para el uso de contraseñas

Una contraseña, es un conjunto de caracteres usado como mecanismo de autenticación, comúnmente implementado para comprobar la identidad de la persona o aprobar algún tipo de acceso. Esta puede ser una una frase, una palabra, un número, o la unión de diferentes letras, números y símbolos.

Actualmente, usamos contraseñas para a nuestra computadora o teléfono celular, acceder a nuestra cuenta de banco, a nuestras cuentas de redes sociales, etc. Todas estas interacciones nos obligan a recordar una gran cantidad de datos, por lo que podemos caer en la tentación de aplicar algunas malas prácticas que pueden poner en riesgo nuestra privacidad.

Por ello debemos tener en cuenta las siguientes recomendaciones:

- *No compartas tus contraseñas*, intenta no escribir tus contraseñas, ni en papel, o en algún dispositivo electrónico, y menos las almacenes en algún servicio en línea como texto.

- *Evita por todos los medios usar la opción "recordar contraseña" de los navegadores*, ya que tus contraseñas podrían quedar expuestas ante cual quier ataque cibernético, e incluso por cualquier persona que físicamente pueda acceder a tu equipo.

- *Usa contraseñas seguras, esto significa:*
  - Que tengan más de 12 caracteres, mientras más larga mejor.
  - Usar letras (mayúsculas y minúsculas), números y caracteres especiales (/,*,%,&,$...).
  - Si vas a generar las manualmente, usa alguna técnica como la mnemotecnia, o el diceware. Aunque siempre recomendamos usar herramientas especializadas para la generación de contraseñas seguras.

- *No uses la misma contraseña para acceder a diferentes cuentas,* esto es más fácil decirlo que hacerlo, ya que por lo general tenemos más de una cuenta de banco, más de dos cuentas en redes sociales, posiblemente uno o más correos electrónicos, y además estamos inscritas a otros ser vicios en línea como: educación en línea, servicios básicos (TV, conexión a internet, teléfono), que incrementan el número de contraseñas que tendremos que crear para acceder a cada una. Para ayudarte existen aplicaciones llamadas “Gestores de contraseñas” que te permiten guardar todas tus contraseñas de forma segura, tan solo tendrás que recordar la contraseña maestra (para acceder a la propia aplicación).

- *No uses contraseñas cortas, fáciles de descifrar, o muy sencillas*, usar nuestra fecha de cumpleaños, número de identificación, o cualquier dato personal e incluso de nuestra familia. Los datos personales usualmente son cortos, y solo usan letras o números por lo que son fáciles de descifrar sobre todo para las aplicaciones usadas para estos fines. Algunos gestores de contraseñas también pueden ayudarte a generar contraseñas seguras, incluso existen servicios en línea para esto sin necesidad de instalar alguna aplicación.

- *Utiliza algún gestor de contraseña*, busca información sobre las aplicaciones para gestionar contraseñas tanto para instalar en tu computadora como en tu teléfono móvil, es importante buscar datos y opiniones de personas expertas sobre estas aplicaciones, luego descargarlas y probarlas, quédate con la que encuentres más cómoda y fácil de usar para tí. Estas aplicaciones además de almacenar todas tus contraseñas también pueden ayudarte a generar contraseñas seguras.

- *2FA,* utiliza factor doble de autenticación *(two-factor authentication)* siempre que esté disponible, esto agrega otra capa de seguridad además de nuestras contraseñas para el acceso a nuestras cuentas.

Buenas prácticas de cuidados digitales en la navegación en Internet

Un navegador web, es una aplicación (software) que nos permite acceder a la Web. Esta aplicación interpreta la información de los sitios web (páginas web) para que podamos visualizarla de forma correcta, bien sea texto, imágenes o videos, entre otros.

Actualmente los navegadores web permiten una gran cantidad de acciones que podemos ejecutar sin necesidad de descargar alguna otra aplicación, como juegos, realizar búsquedas en bases de datos en línea, corregir textos, modificar imágenes, grabar videos, etc.

Los navegadores web son usados principalmente para realizar búsquedas en Internet, a través de los “buscadores” o motores de búsqueda, que son sistemas que buscan archivos almacenados en servidores (máquinas locales o remotas que pueden ser accedidas, dados ciertos parámetros, a través de Internet). Estas búsquedas utilizan algoritmos, que cada vez son más complejos, y hace algunos años vienen generando polémicas en cuanto a la privacidad para las personas que los usan.

Existen muchos navegadores web, al igual que muchos motores de búsqueda, principalmente desarrollados por empresas, las cuales buscan de alguna forma obtener principalmente datos; esos datos les brindan información sobre nuestros gustos, desde la ropa que usas hasta tu ideología política. Principalmente, lo hacen a través de los metadatos que son enviados y compartidos a través de Internet.

Esos metadatos, en un principio servían para comprobar la compatibilidad de formatos, o dispositivos; pero su uso ha evolucionado y actualmente son usados también para invadir la privacidad. Por ello han surgido organizaciones o personas organizadas, que han desarrollado navegadores que mejoran la posibilidad de una navegación segura y con mayor privacidad.

Por todo esto es importante:

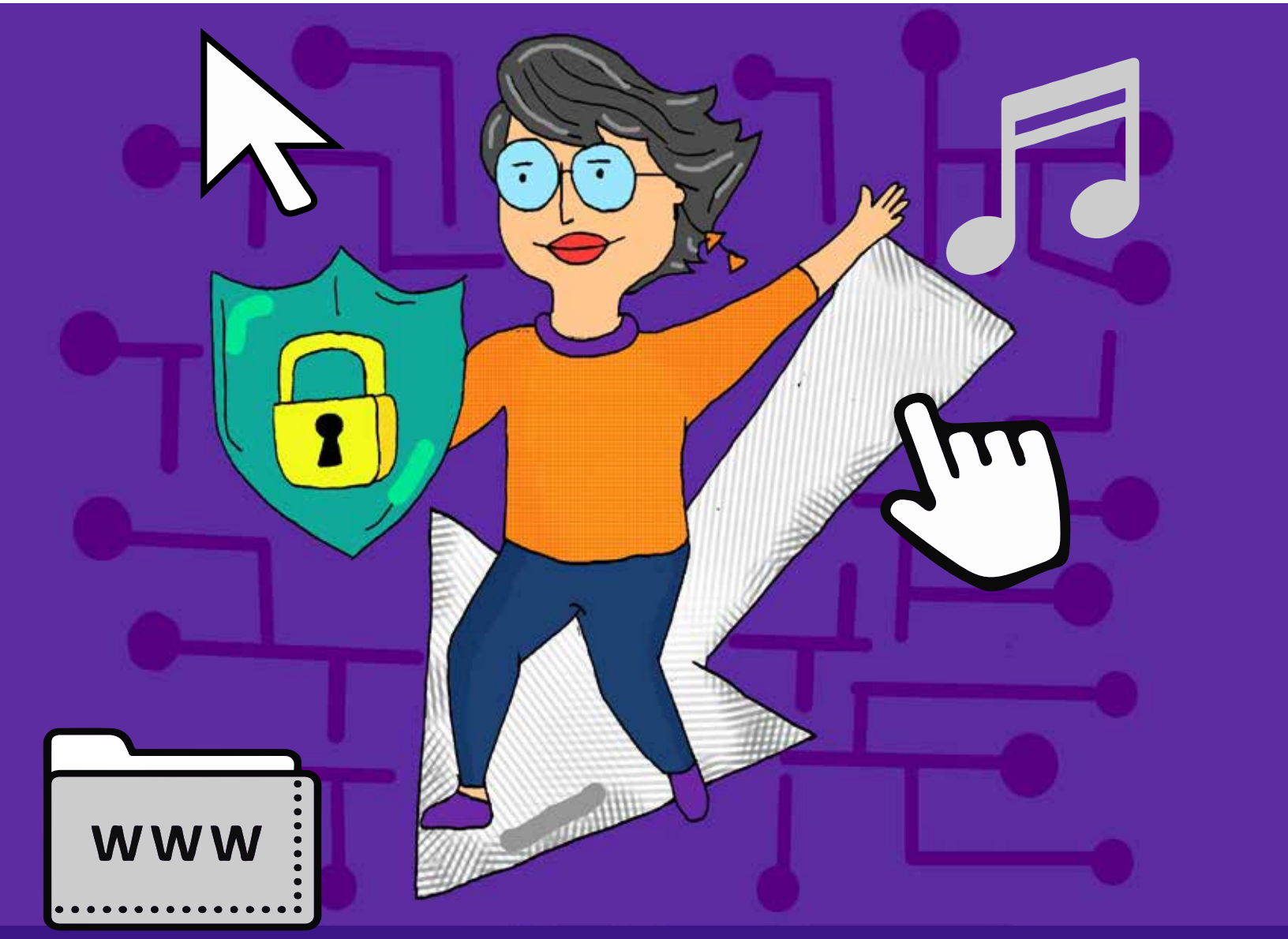
- ***Infórmate,*** accede regularmente a sitios especializados de noticias sobre seguridad informática para informarte sobre las vulnerabilidades de las herramientas que usas para navegar en Internet, busca información sobre los navegadores y motores de búsqueda existentes sobre todo los más usados, así como los más seguros, sigue personas especialistas en el tema o busca redes de apoyo que puedan recomendarte herramientas y estrategias seguras de navegación en Internet.

- ***Descarga y prueba,*** según la información que hayas podido obtener, los navegadores y motores de búsqueda seguros, y quedate con el que más cómoda te sientas

- ***Piensa en tu privacidad en todo momento,*** cuando uses equipos sobre los cuales no tienes control, por ejemplo, en la escuela, en la universidad o en el trabajo, busca navegador instalado y advierte sus debilidades. Analiza el entorno: las herramientas a tu disposición y el control que tienes sobre los dispositivos y valora las búsquedas que puedes realizar. Y recuerda

borrar siempre tu historial de navegación y las cookies al término de tu sesión de trabajo.

- *Mantén el control*, si debes realizar actividades en Internet que puedan poner en riesgo tu seguridad tanto física como en-línea, asegúrate de usar un dispositivo que puedas controlar (realizar actualizaciones e instal aciones de software, realizar configuraciones como usuario administrador) y herramientas que te aseguren en un mayor porcentaje tu privacidad. No ingreses a tus redes sociales o correo electrónico personal, ya que esto puede exponer tu identidad incluso si estás usando herramientas seguras o el modo anónimo.



Buenas prácticas para uso de correos electrónicos de forma segura

En 1965 se desarrolló el servicio MAIL, que permitía el envío de mensajes entre usuarios de una misma máquina, con terminales remotas, estas máquinas eran conocidas como Mainframe. Pero el primer mensaje a través de la red (en aquel entonces ARPANET) fue emitido en 1971, y, a partir del 1977, el correo electrónico se convierte en un servicio de red estandarizado.

Desde aquel entonces, el correo electrónico ha sido convertido en una de las principales herramientas del uso de Internet, bien sea que lo usemos directamente desde nuestro navegador o a través de una aplicación de correo electrónico instalada dispositivo. Hoy por hoy, millones de personas hacen uso de él para facilitar sus comunicaciones alrededor del mundo, siendo incluso necesario para poder acceder a cuentas de redes sociales u otros servicios, como listas de correo, foros, muy utilizado por servicios de telefonía, bancarios, etc.

Lamentablemente, los servicios de correo electrónico más usados actualmente, son aquellos que menos respetan nuestra privacidad, por lo que han desatado la polémica y son los principales acusados por los movimientos en pro de los derechos digitales, ya que son quienes acceden a la mayor cantidad de datos sobre nuestra vida, actividades, contactos, conversaciones privadas, fotos, etc. Datos que son vendidos a otras empresas o proporcionados a los gobiernos.

Por todo esto es necesario que al seleccionar un servicio de correo electrónico tengas presente:

- *Jurisdicción,* ¿Donde está localizado el servicio de correo electrónico? Todo el correo electrónico que envías o recibes quedará almacenado en alguna máquina, incluso podría estar almacenada tu contraseña y otros datos personales, por ello es importante saber donde estarán

almacenados esos datos. Por ejemplo, si vives en un país catalogado por EEUU como terrorista o enemigo entonces es posible que un servicio ubicado en ese país no respete tu privacidad ya que estará obligado a proporcionar datos e información al Gobierno de los EEUU.

- ***Exportación***, ¿El servicio de correo electrónico que utilizas permite la exportación de datos? Algunos servicios permiten que puedas exportar tanto tus correos electrónicos como tus contactos, esto puede ser útil para para realizar respaldos pertinentes, dependiendo de la información que manejes a través de tu correo electrónico.

- ***Encriptación***, esta es una técnica de cifrado o codificado que permite hacer que los mensajes sean inteligibles para los receptores no autoriza dos, es decir, que si un mensaje es interceptado en el camino por alguien o alguna aplicación no autorizado no podrá ser leído/entendido. Por eso es importante conocer si tu servicio de correo electrónico proporciona encriptación de extremo a extremo, esto es que el mensaje es cifrado por el emisor y que solo puede ser descifrado por el receptor, o si tanto los correo como los archivos adjuntos son encriptados en reposo, es decir, que tanto los correos como los archivos almacenados en el disco de la máquina (servidor de correo electrónico) están cifrados.

- ***Seguridad,*** infórmate sobre las políticas y estándares del proveedor del servicio de correo electrónico, puedes verlas siempre en el contrato que aceptas al crear una cuenta de correo electrónico.

- **Privacidad,** ¿Cómo protege tu privacidad el proveedor de servicio de correo electrónico? ¿Qué datos son recolectados, por cuánto tiempo son almacenados y por qué? Esto también puede estar contemplado en el contrato de aceptación de servicio, pero también es importante que investigues un poco sobre la empresa u organización proveedora del servicio y si ha sido acusada de violaciones a la privacidad, o tiene

algunas vulnerabilidades conocidas.

- **Otras características,** indaga sobre otras características que brinda el proveedor de correo electrónico, como calendarios, aplicaciones móviles, comunicación con clientes de correo de terceros, que puedan interesarte o ser necesarias para el uso que vas a darle al correo electrónico, y por supuesto, otras opciones de seguridad.

- **¿Qué necesitas?**, esta es una de las principales preguntas al evaluar cualquier servicio, es decir, pregúntate para qué estás buscando el servicio y para qué lo vas a usar, esto te permitirá evaluar qué tanto puedes permitir y que no es negociable.

Buenas prácticas para tener videoconferencias exitosas y seguras (sin machitrolles)

Probablemente te has enterado por algún medio, bien sea por televisión, noticias en línea o a través de las redes sociales, sobre casos de filtración de información personal o abusos en las videoconferencias, las cuales se han incrementado estos últimos años, creando una necesidad de uso de aplicaciones para este tipo de comunicación. Muchas personas han comenzado a usar herramientas tecnológicas para realizar reuniones y eventos en línea, pero lamentablemente algunas veces con consecuencias negativas para su privacidad o a lo menos una mala experiencia en algún evento o reunión.

Para evitar problemas y mejorar nuestras experiencias con estas herramientas de comunicación:

- *Asegúrate de verificar y configurar los ajustes*, antes de entrar a una videoconferencia, tomate tu tiempo para asegurarte que cada opción está configurada según tus requerimientos. Prueba el audio y video, y piensa desde donde estarás conectada y si algo en el lugar pudiera estar

revelando algo de tu privacidad, como: donde vives, o alguno de tus intereses, fotos de familiares o amigos.

- *Tomate el tiempo para conocer la herramienta*, no es necesario que seas una experta, pero es importante que sepas usarla al punto de saber rápidamente cómo reaccionar a situaciones inesperadas. Saber donde están ubicadas las opciones de silenciar el micrófono, apagar la cámara o salir de la reunión, es importante para asegurar las condiciones mínimas de privacidad, y poder reaccionar a tiempo en caso de requerirlo.

- *Cuida las capturas de pantalla*, muchas veces queremos compartir lo que hacemos en nuestras redes sociales, y las capturas de pantalla se han convertido en algo habitual en estas reuniones. Si deseas evitar que se revelen tus datos, puedes cambiar tu nombre y usar una imagen genérica, o simplemente no usar ninguna. Y si eres tú quien desea hacer una captura de pantalla, recuerda preguntar antes de hacerla, sobre todo si es una reunión privada.

- *Las invitaciones a la reunión*, deben hacerse directamente por la persona anfitriona. Evita enviar enlaces a alguna videoconferencia si no eres quien está a cargo de los contactos, ya que pudieras enviar en enlace a la persona equivocada. Informa a la persona anfitriona si es necesario invitar a la reunión a alguien más, o confirmar algún contacto.

- *Cuida el enlace de invitación*, cuando seas anfitriona el enlace de invitación es la llave para entrar a la videoconferencia, entonces, a menos que sea estrictamente necesario no dejes el enlace en sitio públicos ya que cualquiera podría acceder a la reunión. En caso que sea una videoconferencia pública asegurate de que la herramienta que usarás tiene opciones adecuadas para proteger la privacidad tanto de las personas anfitrionas como de los ponentes y participantes, muchas

herramientas de videoconferencia tienen opciones para rrestringir el uso de los micrófonos y vídeos, o compartir la pantalla, e incluso chats privados para ponentes y anfitrionas.

- *Usa más seguridad*, si es posible, considera usar otro nivel de seguridad como un código de ade acceso para entrar en la reunión o una inscripción previa, esto pudiera reducir los problemas de accesos no deseados. Recuerda compartir el código de acceso y el enlace de la videoconferencia por medios separados para que ese nivel extra de seguridad realmente haga una diferencia.

- *Modera la reunión,* si eres la propietaria de la reunión pero no te es posible moderarla, asigna a una persona para que cumpla con este rol. Es posible que te veas tentada a realizar varias tareas al mismo tiempo, cómo ser anfitriona y al mismo tiempo moderar, o ser ponente y también moderar la reunión, ¡nuestra recomendación es que no lo hagas! lLa persona que modera la reunión debe estar lista para realizar acciones con rapidez como bloquear, silenciar o expulsar a añguien detener la presentación, bloquear la reunión, etc.

- *Considera la trasmisión en vivo (streaming),* pudiera que sólo necesites transmitir tu mensaje, no necesariamente en una videoconferencia donde las personas que participan puedan hablar al mismo tiempo. El streaming puede permitirte evitar interrupciones, y un mayor control de quienes pueden o no compartir video al mismo tiempo, pero además puedes tener la opción de utilizar chats privados o de preguntas para el público en general.

- *Conoce al proveedor de servicio,* al seleccionar una herramienta, conoce quién es el proveedor del servicio, que opciones de privacidad ofrece y cuales son son políticas de seguridad, hazte preguntas como ¿el proveedor indica explícitamente qué datos recopila y cómo se protegen?

¿el proveedor specifica cuánto tiempo se retienen los datos y con qué propósito?

Buenas prácticas de cuidados digitales en nuestras computadoras

El computador se ha convertido en una de las principales herramientas para realizar nuestros trabajos, investigaciones, entretenimiento y más. El uso diario del computador y todos los datos que almacenamos en él lo han convertido en uno de los blancos principales de los cibercriminales, bien sea computadores que están conectados a redes empresariales o nuestros computadores personales, los cuales no están exentos de poseer información relevante para su provecho. Pero más peligroso aún son algunas empresas proveedoras de servicios servicios en las cuales usualmente confiamos y que se valen de nuestros datos para realizar estudios de mercado, venta de esos datos a otras empresas, o proveerles a gobiernos para nuestra vigilancia. Así que no solo existen cibercriminales confesos si no que al mismo tiempo debemos protegernos de este tipo de organizaciones, y cada día nuestros datos son más valiosos.

Utiliza un Sistema Operativo seguro, si aun usas sistemas operativos poco seguros (como Windows), investiga y prueba sobre sistemas operativos más seguros como alguna distribución de GNU/Linux, informate sobre cursos para aprender a usarlo y busca grupos que puedan ayudarte a aprender y resolver dudas y problemas.

- *Instala un Antivirus*, incluso si usas un sistema operativo seguro siempre es buena idea contar con un antivirus con el cual puedas escanear cualquier archivo o dispositivo externo. Y si usas un sistema operativo poco seguro, esto debe ser una prioridad, y recuerda siempre tener el antivirus actualizado ya así que esto te ayudará a limitar la posibilidad de infección de tus archivos, así como posibles entradas no autorizadas a tu sistema.

- *Mantén tu sistema operativo actualizado,* igual que cualquier aplicación (como el antivirus) es siempre recomendable que el sistema operativo de tu computador esté actualizado ya que si tendrás disponible todos los arreglos de posibles “huecos” de seguridad que puedan poner en riesgo tu privacidad.

- *Respalda tus datos,* hoy día existen muchos servicios para realizar respal dos en la “nube”, pero con estos es importante igualmente tener en cuenta todas las recomendaciones de seguridad aquí descritas. Por esta razón, una de las mejores formas de realizar tus respaldos sería usando un dispositivo físico de tu propiedad el cual además puedes controlar quien accede a él y mantener libre de archivos maliciosos a través del uso de antivirus u otras herramientas de análisis.

- *Revisa cualquier dispositivo externo, pendrive (USB)*, disco duro externo, o cualquier dispositivo móvil que conectes a tu computador antes de su uso. Esto es importante, pues debes analizarlo en busca de virus o archivos maliciosos que puedan poner en riesgo tu privacidad.

- *Utiliza navegadores web seguros*, cuando accedes a Internet estás expuesta a cualquier amenaza externa, desde un simple virus que pueda arruinar tus archivos hasta un “troyano” que pueda poner en riesgo tu seguridad. Los navegadores web pueden ayudarte o no a limitar los riesgos a los que estamos expuestas en Internet, es por eso que es importante que tengas en cuenta el navegador que estás usando y

conocerlo más que puedas, ya que esto te permitirá saber cómo tu nave gador puede ayudarte con tu privacidad.

- *Cuidado con lo que llega a tu correo electrónico*, hoy día el correo electrónico se ha convertido en una de las herramientas más usadas para el cibercrimen, a través de distintas estrategias que incluyen la ingeniería social como, como el envío de enlaces maliciosos que pueden llevarte a i nstalar aplicaciones que pueden dañar tu computador o acceder a tus datos, o mediante el envío de correos electrónicos que simulan ser de organizaciones legítimas como como, bancos o redes sociales, solicitando información con la cual buscan acceder a las contraseñas de tus cuentas. Recuerda en todo momento tener en cuenta que ninguna empresa o institución debería pedirte tus datos personales a través de un correo electrónico. Por eso, revisa siempre los enlaces que son enviados a tu correo, accede a las páginas web desde la barra de dirección de tu navegador, y verifica en todo momento el correo emisor de todo lo que recibas.

- *Verifica la seguridad de las páginas web que visitas*, al acceder a un sitio web, asegúrate que la información del sitio que visitas se encuentre indicada como protegida por un certificado de seguridad. Esto puedes visualizarlo en la mayoría de los navegadores, con la imagen de un candado cerrado junto a la URL. Básicamente, te dirá si el sitio web es "seguro" o no seguro" sin embargo, recuerda que incluso los sitios web "seguros" no son 100% seguros porque pueden usar cookies que invadirán tu privacidad.

- *Cuidado con las descargas,* algunos navegadores tienen una función de seguridad que te pregunta si deseas continuar con una descarga. Es posible que te indiquen que el archivo que va a descargar contiene materiales que pueden dañar su computadora. Además, antes de abrir los archivos descargados, asegúrate de revisarlos antes con un antivirus, ya que también pueden contener virus.

- *Gestiona tus contraseñas*, todo lo que indicamos anteriormente sobre las contraseñas, es igualmente aplicable para proteger tu computador. Recuerda aplicar el mayor número de consejos para hacer de tus contraseñas lo más seguras posibles y evitar accesos no autorizados a tus equipos.

- *Utiliza bloqueadores de sitios web*, además de las funciones de seguridad integradas en los navegadores, también existen add-ons o extensiones que permiten bloquear ciertos sitios disponibles en la web, así como el rastreo de información privada a través de las cookies por ejemplo. Estas extensiones bloquean sitios web potenciales que pueden contener o estar involucrados en fraude, phishing, estafas y otras amenazas. También puedes programar estas extensiones para bloquear ciertos sitios con palabras clave. También pueden ayudar a bloquear sitios y anuncios emergentes.

- *Evita usar Wi-Fi públicas*, no confíes en las redes Wi-Fi públicas, cualquier persona malintencionada podría acceder a la Wi-Fi usando aplicaciones especiales para ello, y con el propósito de robar contraseñas o acceder a equipos poco protegidos. Te sugerimos que utilices una red privada virtual o VPN que encripta tu conexión.

- *Desconéctate,* si no necesitas una conexión a Internet, es mejor que te desconectes, esta es una medida preventiva que te ayudará a evitar que las amenazas de seguridad ingresen a tu computadora a través de Internet.

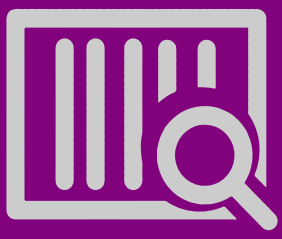
Además de todas estas recomendaciones aquí propuestas, es importante que desarrolles la suficiente confianza para gestionar y configurar tu computador, busca grupos de ayuda, cursos y apoyo en personas del área de tecnología que contribuyan a mejorar tus conocimientos y habilidades.

DECÁLOGO DE LA SEGURIDAD Y PRIVACIDAD EN LOS DISPOSITIVOS MÓVILES

1

¿Quienes soy? –> Código IMEI

Significa Mobile Equipment Identity (identidad internacional de equipo móvil) es un código único en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, no debe compartirse con nadie. Se consigue marcando *#06# Este número se guarda realizando una captura o se anota, en caso de extravío es más fácil bloquear el número si se tiene esta información.



Conociendo otros códigos secretos

2

*#21# ó *#62# Son importantes para garantizar nuestra privacidad, nos informa si tenemos desvío de llamadas y se consigue esta información marcando uno u otro código en el teléfono móvil.

3

¿Estoy infectada?

Si tu teléfono móvil se recalienta, está muy lento y tiene una excesiva carga, se abren y cierran aplicaciones mediante comportamiento inesperado, es posible que tu teléfono esté infectado, ya que hay muchos virus y malware para dispositivos móvil. Una buena práctica, que recomendamos, consiste en que cada cierto tiempo se instale un antivirus y se utilice para escanear el móvil. Hay muchos de pago para android, uno gratuito que recomendamos es bitdefender.

AUTHY

Configura tu autenticación de 2 pasos o 2FA

4

Es un método de seguridad adicional que se debe activar a todas nuestras cuentas de correos, redes sociales, wallets, etc. Recomendamos instalar y utilizar authy

DECÁLOGO DE LA SEGURIDAD Y PRIVACIDAD EN LOS DISPOSITIVOS MÓVILES

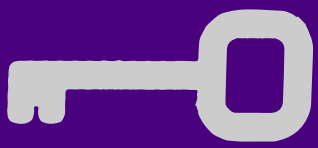
5 Cuida tu historial de navegación y cookies

Como buena práctica es recomendable borrar cookies e historial de navegación cada cierto tiempo, programa una alarma cada mes para realizar esto:

1. Abre la aplicación Chrome en tu teléfono o tablet Android.
2. En la parte superior derecha darle click a los 3 puntos y luego toca Historial
3. En la parte superior, elige Borrar datos de navegación
4. Marca las casillas "Historial de navegación" "Datos de sitios y Cookies" y "Imágenes y archivos almacenados en ca ché".
5. Toca Borrar datos

6 Usa un gestor de contraseñas

Un gestor de contraseñas es como una caja fuerte donde se guardan todas las contraseñas de tus cuentas y sólo tienes que recordar una llave maestra que es la que luego te da acceso a todas las demás claves y cuentas. Revisa este video de Chica Geek sobre este tema: https://www.youtube.com/watch?-v=S6OolNvhGxM



DECÁLOGO DE LA SEGURIDAD Y PRIVACIDAD EN LOS DISPOSITIVOS MÓVILES

Crea una bóveda secreta para tus archivos y multimedia privada

7

Son aplicaciones que aparentan ser o tener una utilidad, como una calculadora o un reloj y en realidad te ofrecen la posibilidad de guardar archivos, fotos, videos y estos estarán protegidos mediante clave.

8

Navegación privada con DuckDuckGo

Duckduckgo es un navegador y también buscador que ofrece niveles de privacidad aceptables ya que impide que los rastreadores que están en todas las páginas de servicios que visitamos lleguen a nosotros/as, una vez que lo instalen y abran la app inmediatamente les comenzará a llegar información de los sitios que visitamos.

TOR el Dios sin 'H' del anonimato

9

TOR es un sistema que incluye un navegador web y que oculta nuestra dirección IP al hacer que nuestra comunicación pase por varios servidores antes de llegar a destino, y lo mismo al volver. Esta es una forma fácil de evitar ser rastreadas mientras navegamos. Para android recomendamos usar Orbot que es una aplicación que se conecta a la red Tor y cifra todo el tráfico de manera que se establezca una comunicación anónima

10

Realiza Protección física de tu teléfono móvil

La protección física es una de las tres capas de la seguridad de los dispositivos móviles, las otras dos capas son la gestión segura de aplicaciones y la protección de datos, vistos en los anteriores puntos del decálogo. Sin embargo no sirve de nada aplicar estos puntos si no se realiza la protección física, para hacerlo es necesario que pongamos protección de acceso, es decir usar contraseñas de acceso, huellas dactilares y otros elementos de autenticación.

Buenas prácticas para el uso seguro del teléfono celular.

Nuestro teléfono celular se ha convertido hoy día en uno de los dispositivos más usados, gracias a su versatildad para transporte, uso y manejo, así como la posibilidad de conectarnos a la Internet casi en cualquier lugar. Es nuestra agenda de contactos, accedemos a nuestro correo electrónico y nuestras redes sociales, almacenamos archivos, fotos, videos personales, y accedemos a nuestras cuentas bancarias o pagos electrónicos. Entonces, luego de todo lo que hemos aquí descrito, ¡te podrás imaginar lo importante de mantener tu teléfono celular protegido!.

- *Usa un código de acceso,* y es importante destacar que el código de acceso establecido de fábrica no es una buena idea. Usa un código de acceso establecido por tí, e intenta utilizar las recomendaciones dadas en esta misma guía para las contraseñas como; no usar fechas de nacimiento, o el mismo código en todos tus dispositivos Esto limitará la probabilidad de accesos indeseados, dejar tu teléfono sin un código de acceso sería como dejar tu casa sin puerta de entrada, cualquier persona podrá entrar y acceder a todas tus cosas.

- *Ten cuidado con las aplicaciones que instalas,* verifica e investiga todas las aplicaciones que instalas, una aplicación puede parecer muy buena e inofensiva, recomendada por alguna de tus amigas, pero recuerda siempre estar al tanto de su funcionamiento y si la instala, debes estar pendiente de los permisos que estas dando a la aplicación, una aplica ción de calculadora, por ejemplo, no debería pedirte acceder a tu GPS.

- *Cuidado con los enlaces,* así como en nuestros computadores, también navegamos en Internet a través de nuestros teléfonos celulares, asegura te allí también de usar navegadores seguros, que te ayuden a minimizar l os riesgos. Pero sobre todo, siempre debes estar atenta de los sitios a los que accedes, de los enlaces donde haces clic, y la información que suministras.

- *Mantén tu teléfono actualizado,* al igual que nuestra computadora, nuestro teléfono celular es un dispositivo electrónico que funciona con un siste ma operativo y una serie de aplicaciones, que necesitan estar actualizadas con las últimas revisiones que te permitan estar protegida de cualquier “hueco” de seguridad.

- *Evita usar Wi-Fi públicas,* con nuestros teléfonos celulares tenemos la costumbre de querer estar siempre conectadas, pero como ya hemos dicho en esta guía, el uso de redes públicas pudiera poner en riesgo nuestra seguridad, evitar su uso en lo posible es la mejor forma de protegernos, y en caso de ser inevitable su uso, usar aplicaciones que limiten los riesgos como una VPN o encriptación.

- *Respalda tus datos con regularidad,* al igual que con nuestro computador es importante realizar respaldos regulares de nuestros datos.

- *Tu tarjeta Sim y SD son importantes,* si decides vender el teléfono, o incluso si debes llevarlo a reparar o revisión técnica, remueve la tarjeta SIM y tu tarjeta de memoria externa.

Aplicaciones y tips que incrementa tu seguridad digital

Existen muchas aplicaciones para distintos tipos de tareas que puedes usar, y cada día son desarrolladas muchas más. En ese mar de aplicaciones es comprensible sentirse abrumada, de allí eso la importancia de contar con alguna fuente de información confiable y/o grupos de apoyo que puedan guiarte hacia la elección de las aplicaciones que más se adapten a tus necesidades.

A continuación te mostramos algunas y te explicamos por qué y en cuáles contextos contexto podrían usarse, igualmente recuerda que esto podría cambiar en el tiempo, ya que se podrían encontrar nuevos riesgos de seguridad en estas aplicaciones o sus objetivos de desarrollo podrían cambiar.

Protegiendo nuestros accesos

El ingreso a cualquier herramienta o servicio en Internet generalmente implica tener un usuario y contraseña que nos identifique. La gestión de nuestras contraseñas es cada vez más importante y abrumadora, con la cantidad de servicio que accedemos todos los días, con ellas resguardamos desde nuestras redes sociales hasta nuestras cuentas bancarias (o criptomonedas), es necesario entonces contar con herramientas que nos faciliten esta tarea, como los gestores de contraseñas que nos ayudan a mantener lo más simple posible la tarea de recordar y preservar seguras todas nuestras contraseñas.

- KeePassXC
- KeePassDX (para Android)

Aunque utilices el modo de navegación "privado" o "de incógnito" en tu navegador, tu dirección IP y ubicación reales aún pueden ser vistas en cada sitio web, anuncio y rastreador que se carga en tu navegador. Además, todas tus actividades permanecen visibles para tu proveedor de servicios de Internet (ISP). Y como hemos aprendido recientemente, los ISP registran todo lo que haces en línea y comparten los datos con terceras partes. Por eso es fundamental utilizar una buena VPN (Virtual Private Network) para la privacidad digital básica. Una VPN cifra, protege y anonimiza tu tráfico de Internet, al mismo tiempo que puede desbloquear contenido de cualquier parte del mundo (ya que existen contenidos o páginas web que pueden permitirte o no ver la información de acuerdo al lugar desde donde te estés conectando).

Hablando ahora sobre Navegadores, que puedes usar en conjunto con una VPN, tendremos que tener en cuenta: la seguridad ¿Como te proteje el navegador de vulnerabilidades, virus u otras amenazas en la red? y la privacidad ¿Qué datos recolecta el navegador sobre tí y a quien le está compartiendo esos datos?

TOR

Firefox

Brave

También es importante tener en cuenta los navegadores para móviles:

DuckDuckGo

FireFox Focus

Bromite

Comunicándonos

No importa que tan irrelevantes sean tus conversaciones, siempre pueden aportar datos necesarios tanto para ciberdelincuentes como para delincuentes corporativos. Tus comunicaciones con otras personas son igualmente importantes, sobre todo si compartes videos, fotos, y más aún si trabajas con información confidencial o realizas actividades de activismo que pueden ser blanco de Gobiernos o empresas.

Correo electrónico

Mailfance

Tutanota

ProtonMail

Mensajería instantánea

Signal	
Telegram	
Wire	

Es importante destacar que el orden de las aplicaciones aquí mencionadas no implica una mayor o menor seguridad o privacidad de las mismas (y que estas no son las únicas), asegúrate siempre de leer sobre las aplicaciones que vas a usar y lo que pueden ofrecerte, y contrastarlo con tus necesidades. Recuerda también que es posible que estas herramientas queden obsoletas, pasen a otras manos (sean compradas por alguna otra empresa) y puedan cambiar sus objetivos. Está siempre atenta a las noticias de tecnología y las revisiones de expertos.

Por último, te recomendamos algunos enlaces para estar informada:

- https://www.welivesecurity.com/la-es/
- https://latam.kaspersky.com/blog/
- https://blog.avast.com/es
- https://restoreprivacy.com (en Inglés)
- https://www.eff.org (en Inglés)
- https://onlineviolenceresponsehub.org (en Inglés)

Y por supuesto, recuerda que puedes contactarnos:

En **Instagram** y **twitter** @activistassl

Mujeres
Activistas
XSL