Elementos básicos de seguridad informática para personas defensoras de DDHH

AGOSTO 2021

Protection International

Compilado por: Alexandra Loaiza y Arturo Chub

PROTECTION international

Introducción

La actual situación de inseguridad y los riesgos informáticos que experimentan a diario las personas que adelantan procesos de defensa de derechos humanos, se han incrementado durante la crisis ocasionada por el COVID 19, pues las medidas restrictivas a la movilidad y el aislamiento social, nos han llevado a trasladar la mayoría de nuestras acciones al escenario virtual, en muchos casos desde nuestras propias casas y con nuestros propios recursos, casi siempre limitados.

El presente documento tiene como objetivo brindar algunas herramientas prácticas, que aporten a mitigar estos riesgos. Como en todo proceso de protección, la mitigación de los riesgos tiene una parte técnica y una parte humana. La parte técnica, tiene que ver con el uso de herramientas, lo más seguras posibles; y la parte humana, considera la capacitación de las personas para ser conscientes de los riesgos y desarrollar prácticas que ayuden a prevenirlos, o, a mitigar sus impactos.

Es importante señalar que estas medias podrán resultar útiles, pero no son suficientes para garantizar una gestión efectiva de la información, que es lo que está en riesgo en entornos digitales, pues la seguridad informática, es solo un componente de la seguridad de la información, que se produce, almacena y difunde por diversos medios.

Contexto

Cada vez con mayor frecuencia, las personas defensoras de derechos humanos, aún en entornos rurales, usamos las tecnologías de la comunicación para desarrollar nuestro trabajo. El computador, el celular y la internet, se han convertido en herramientas claves para la labor de defensa de derechos: para mantener la comunicación, romper el aislamiento, activar alertas tempranas, denunciar o visibilizar y documentar los procesos.

Con el uso de estas tecnologías, que definitivamente facilitan nuestro trabajo, también se han incrementado riesgos asociados al acceso, control y uso de información, que podría resultar sensible o poner en riesgo nuestro trabajo, e incluso la vida y la integridad de las personas con las que trabajamos. La inseguridad de la información almacenada o enviada, se está convirtiendo en un problema central, para las personas defensoras de derechos humanos en muchas partes del mundo, y Colombia no es la excepción (Front Line Defenders , 2020).

Estos riesgos se han incrementados dramáticamente, en el marco de la coyuntura provocada por COVID 19- "***Según las cifras más recientes del Centro Cibernético de la Policía Nacional, los delitos informáticos aumentaron un 59% en el primer semestre del año 2020,*** *respecto al mismo periodo del año anterior.*" (Portafolio, 2020)

Es importante señalar que todas las personas, independiente de la labor que desarrollemos, estamos expuestas a riesgos digitales. Los ataques más comunes documentados, por lo tanto, los más importantes a considerar son los siguientes: (Magdits, 2020)

> **Phishing**: Es la técnica que, a través de correos electrónicos con mensajes engañosos, se pretende obtener información del destinatario; tomar control de sus cuentas en línea (correos, cuentas bancarias y suscripciones a servicios); acceder y tomar control de la información que maneja la persona, sus contactos y su dinero, en el caso de cuentas bancarias.
> **Ransomware**: Son programas maliciosos que toman como rehén la información almacenada en computadoras personales o servidores de archivos. Los datos existentes en las computadoras personales o servidores (documentos, hojas de cálculo, presentaciones, fotografías, vídeos, audios, etc.) son encriptados, se vuelven inaccesibles para los/as usuarios/as o propietarios/as y para retomar el control, las personas y las organizaciones deben pagar un rescate en bitcoins. Generalmente el ransomware viene en los adjuntos de correos aparentemente legítimos.

Sin embargo, quienes realizamos una labor de defensa de derechos humanos estamos expuestos a otro tipo de riesgos y amenazas, que están dirigidos a obstaculizar nuestra labor, silenciarnos e

inmovilizarnos. El acceso a nuestra información es vital, para aquellos actores que tienen interés en atacarnos o debilitar nuestro trabajo, es la mejor manera de conocernos, perfilarnos e identificar las condiciones de mayor vulnerabilidad que les permita atacar cuándo sea necesario, sea de manera violenta o no.

Estas amenazas pueden ser: (Protection International, 2009)

La inteligencia contra personas defensoras en el país ha sido utilizada para hacer montajes judiciales, que han llevado a la captura y detención de varias de ellas; también ha sido utilizada para preparar campañas de difamación y desprestigio que son utilizadas para atacar su credibilidad y buen nombre; asimismo ha facilitado los ataques violentos contra defensores/as, las amenazas o la filtración de información a actores armados ilegales que tiene fuerte capacidad de actuación en los territorio.

Por ello, la seguridad de la información, y como parte de ello la seguridad informática, representan un paso fundamental para la protección de nuestro trabajo y de las personas defensoras, y se constituye en una acción preventiva y una barrera extra, que se pone a quien pretende atacarnos.

Herramientas de Seguridad Digital

La experiencia de PI nos indica que la implementación de medidas de protección digital requiere de procesos graduales y progresivos, previamente planificados y acompañados por técnicos con experiencia de trabajo con personas defensoras de derechos humanos. No hay una receta universal para organizaciones de derechos humanos, por ello es importante el análisis de riesgos, y solo sobre la base de las necesidades y capacidades, proceder a diseñar e implementar un plan de seguridad digital.

A modo de ejemplo mostramos a continuación un esquema de un plan gradual y progresivo:

Los criterios para la selección de herramientas de seguridad digital que utilizamos son:

- Optamos por software libre y en segundo término los programas de código abierto. Básicamente porque son auditados de manera independiente.
- Multiplataforma, es decir que funcionan sobre los Sistemas Operativos Windows, Mac iOS y Gnu/Linux. En algunos casos compatible con Android, el sistema operativo más extendido en la telefonía celular.
- Que tenga soporte técnico de sus desarrolladores en el tiempo real.

Recomendaciones para mejorar la seguridad de sus celulares.

1. **Verifique que su sistema está actualizado**
   Android: https://support.google.com/android/answer/7680439?hl=es
   iPhone: https://support.apple.com/es-es/HT204204
   Si verifica que, incluso con la última actualización, su versión tiene más de 9 meses, su Smartphone está fuera de soporte, y es especialmente vulnerable. No lo utilices para obtener información confidencial.

2. **Cree un pin fuerte de, al menos, 6 números. No use un patrón, o pase el dedo.**
   La seguridad de la autenticación biométrica (por ejemplo, las huellas dactilares, el iris o la cara) varía entre los distintos modelos y fabricantes. La autenticación biométrica también implementa una metodología diferente de protección (algo que se tiene, y no algo que se sabe), y por lo tanto también tiene otras vulnerabilidades.

3. **Desinstale todas las aplicaciones que no necesite.**

4. **Verifique que todas las aplicaciones estén actualizadas**, y sólo instale aplicaciones de las App-Stores oficiales. Verifique los permisos de las aplicaciones instaladas y elimine las aplicaciones que invaden la privacidad o limite sus permisos.

5. **Verifique que su Smartphone esté encriptado.** Los iPhone y la mayoría de los nuevos teléfonos de Google ya están encriptados. Sin embargo, los teléfonos de Google más antiguos, y muchos otros teléfonos todavía necesitan ser encriptados. Para más información, consulta
   https://support.google.com/pixelphone/answer/2844831?hl=

6. **Desactive el GPS/localización, el Bluetooth, el NFC y otros sensores siempre que sea posible.**
   Tenga en cuenta que la red del Sistema Global de Comunicaciones Móviles (GSM) lo rastrea, en cualquier caso. Sin embargo, no podrás ser rastreado si has configurado el teléfono en modo avión.

7. **Acostúmbrese a apagar su teléfono** al menos una vez al día para complicar el funcionamiento del malware

Mensajería segura

La mayoría de herramientas de mensajería ofrecen cifrado de la conexión, que se establece entre sus servidores y nuestro teléfono celular, de manera que en el viaje no puede ser leído por intrusos. Pero eso no significa que nuestra información se almacena de manera cifrada en sus servidores. Aún si sus servidores estuvieran encriptados, sus técnicos siguen teniendo acceso a nuestra información. Esa es una gran vulnerabilidad para defensores y defensoras de derechos humanos, puesto que algunos países, con gobiernos autoritarios, han pedido acceso a mensajes compartidos por estas redes.

Proponemos el uso de Signal y Wire por lo siguiente:

Signal: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=es&gl=ES

- Es software libre, completamente auditable.
- En sus servidores solo se almacena el número telefónico, la fecha y hora en que empezó a utilizar el servicio y la última conexión a sus servidores. NO almacena sus mensajes, a menos que realice un procedimiento especial para hacer un respaldo en su teléfono, protegido con una contraseña segura.
- Los datos que transmite Signal son encriptados con una llave que se genera y almacena en cada teléfono celular. Cada dispositivo registrado genera una llave única e irrepetible (en cambio WhatsApp crea y almacena las llaves en sus servidores), por esa razón se puede verificar el código de seguridad de cada contacto que uno tenga.
- Este programa borra los metadatos de las fotografías, vídeos y audios que se comparten a través de Signal. También puede proteger sus chats de pantallazos y una contraseña diferente a la del teléfono.
- Puede crear grupos y los administradores tienen la potestad de incluir o expulsar miembros/as.
- Permite hacer videollamadas.
- Tiene versión para computadoras.

Wire: https://play.google.com/store/apps/details?id=com.wire&hl=es&gl=ES

- También es software libre, y auditable.
- No lleva registro de los números de teléfono celular, aunque sí lleva un registro de la huella digital única que tiene cualquier computadora o teléfono celular.
- Para tener el servicio se requiere de una cuenta de correo electrónico, al cual le enviarán el código para verificar y autorizar el servicio.
- Permite la creación de grupos con un administrador con autoridad para incluir y excluir participantes. La mejor manera para ubicar y agregar a un contacto es mediante el envío del nombre de usuario/a por un medio alternativo.
- Wire se puede utilizar en un celular, y cuenta con un programa especial para computadoras o un navegador de internet como Mozilla-Firefox.
- El proveedor de Wire se dará cuenta y le avisará cuando se ha conectado desde programas y dispositivos diferentes.

Navegación privada

El gran problema de la navegación en internet es la privacidad. La gran mayoría de sitios en internet implementan prácticas antiéticas, recolectan información de nosotros sin pedir nuestra autorización.

Todos los sitios web saben si nos conectamos desde una tablet, un teléfono celular, un computador, el sistema operativo y su versión, la resolución de nuestra pantalla, la versión de nuestro navegador. También hay navegadores que permiten que se instalen en nuestro computador virus, troyanos y programas espía.

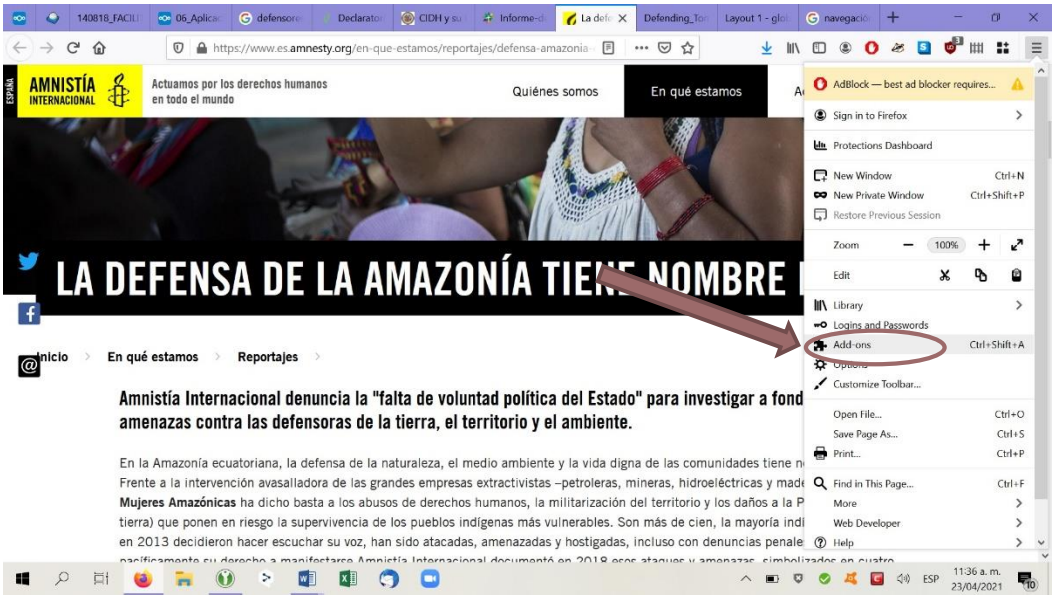
Algunas personas prefieren el navegador de Google, Chrome, porque es un poco más rápido. Su velocidad obedece a que nos individualiza y llega a saber y anticipar qué tipo de información estamos buscando. Google vive de la minería de datos, así que, con su navegador gratuito, no compensa las ganancias que obtiene con los datos que sobre nosotros recolecta.

Proponemos la instalación de Mozilla-Firefox puesto que a sus desarrolladores les preocupa nuestra privacidad. Hay una versión para cualquier sistema operativo y dispositivo (computadora, tablet, teléfono celular).

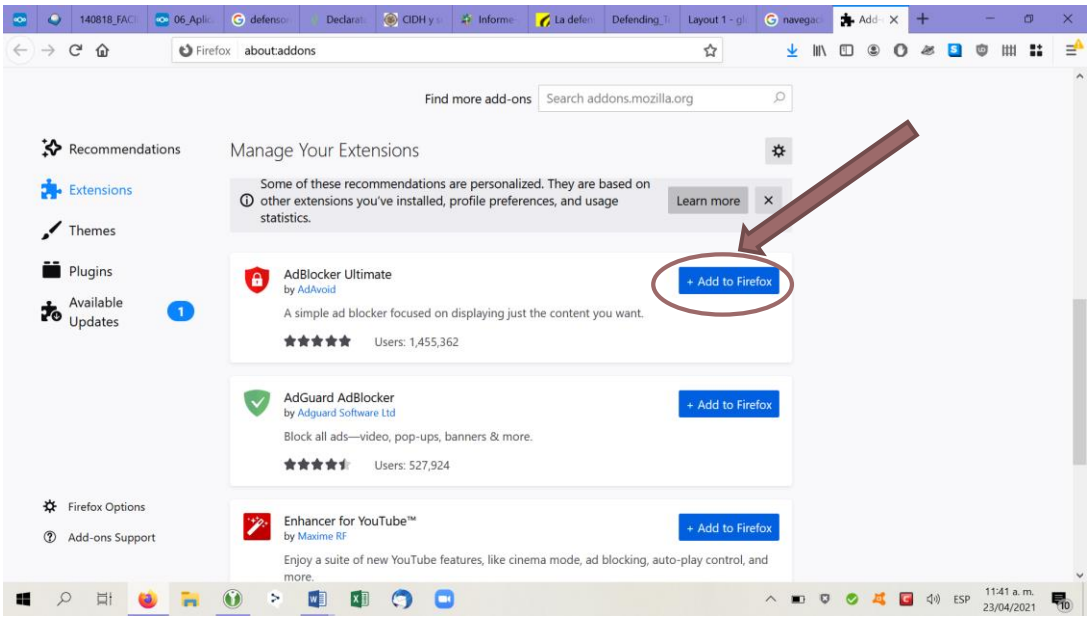
Ha sido desarrollado para protegernos de algunas técnicas de intrusión a nuestra privacidad, por ello es ligeramente más lento para hacer búsquedas. Tiene la opción de navegación anónima, con lo cual no se almacena información de los sitios que frecuenta, ni nombres de usuario, contraseñas, números de tarjetas de crédito, etc.

Complementos: Al programa Firefox se le pueden añadir otros programas más pequeños (llamados complementos o extensiones), pero con funciones muy importantes para resguardar la privacidad en internet.

Para instalarlos nos dirigimos a las tres barras horizontales ubicadas en la esquina superior derecha del navegador Firefox, luego buscamos en el menú desplegable la sección que dice Complementos:



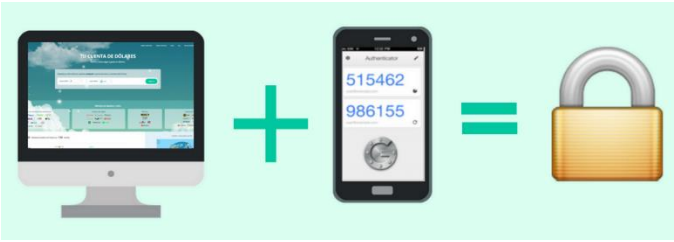
Posteriormente, arriba a la izquierda buscamos la sección **extensiones**, en la casilla titulada buscar más complementos escribimos el nombre del complemento; a la par del mismo estará un botón verde o azul con la leyenda + Agregar a Firefox, hacemos clic sobre el mismo; luego clic en el botón Añadir y finalmente clic en el botón Vale, entendido.



Complemento	Características
HttpsEveryWhere:	Es un programa que reconoce sitios web clonados o inseguros, de manera que si usted tratara de ingresar a una página web clonada, simplemente no se va a conectar o lo redirigirán al sitio legítimo.
UblockOrigin:	Este programa reduce la publicidad que se muestra en los sitios web, haciendo más cómoda y productiva la lectura en algunos sitios. Evita que se abran otras ventanas a causa del sitio que visitamos.
PrivacyBadger:	Ya sabemos que todos los sitios web recolectan nuestra información, pero hay unas prácticas que son ilegales, y el programa los detiene. También bloquea rastreadores de sitios diferentes al cual estamos visitando. También advierte a los sitios web para que no compartan o vendan su información, ni que lo rastreen.
FacebookContainer:	Cuando visitamos un sitio web, este puede estar diseñado para averiguar si al mismo tiempo estamos navegando en otros sitios incluyendo twitter y Facebook. Este programa aísla nuestra sesión de Facebook, de esa manera los otros sitios no saben que tenemos cuenta en Facebook y, evita que esta red social y sus socios sepan qué otros sitios visitamos o leemos.
MultiAccountContainers:	Es un programa que, bien configurado, puede agrupar y aislar las pestañas del navegador de internet Firefox para evitar el rastreo. Por ejemplo, si crea contenedores separados para servicios de gmail, drive y YouTube, Google no almacenará información sobre sus gustos musicales mientras lee su correo electrónico.

Existen cientos de extensiones para Firefox, pero en materia de privacidad estas son las prioritarias.

Autenticación de doble factor



En internet se tienen algunos servicios más sensibles que otros, entre ellos, la Banca en Línea, para las cuales consideramos que hay necesidad de agregar una capa de seguridad, que se llama, autenticación de doble factor o verificación en dos pasos.

Su objetivo es el de asegurarse de que el usuario no solo conoce la contraseña para acceder al servicio, sino que, además es quien dice ser, aportando en el proceso de logueo información, un código, por ejemplo, sobre algo que solo él posee.

Si usted es usuario/a de banca en línea, realiza compras en línea con su tarjeta de crédito, tiene una nube privada con información sensible, es administrador o un usuario regular de un sitio web, considere seriamente utilizar la verificación de dos pasos. En algunos casos consiste en agregar el número de nuestro teléfono celular, una dirección de correo electrónica alterna o dedicada a esta tarea o poseer una tarjeta con códigos o un dispositivo electrónico para generar códigos.

Hoy en día, existen muchos servicios que ofrecen un factor de autenticación múltiple por defecto. Entre los servicios que sí incluyen un factor de autenticación múltiple, encontramos los siguientes:

Facebook	Google	Apple
Twitter	Amazon	Dropbox

No obstante, algunos servicios donde alojamos información crítica no lo implementan, como, algunos servicios bancarios. Por lo cual le recomendamos acérquese a la oficina de Atención al Cliente allí le darán la ayuda que necesita para implementar la verificación de dos pasos.

En cualquier caso, debemos seguir tratando de implementar buenos hábitos relacionados con la creación de contraseñas robustas y con la utilización de herramientas como los gestores de contraseñas para no tener que memorizar todas ellas. Y, por supuesto, de ser posible, siempre utilizar el factor de autenticación doble o múltiple.

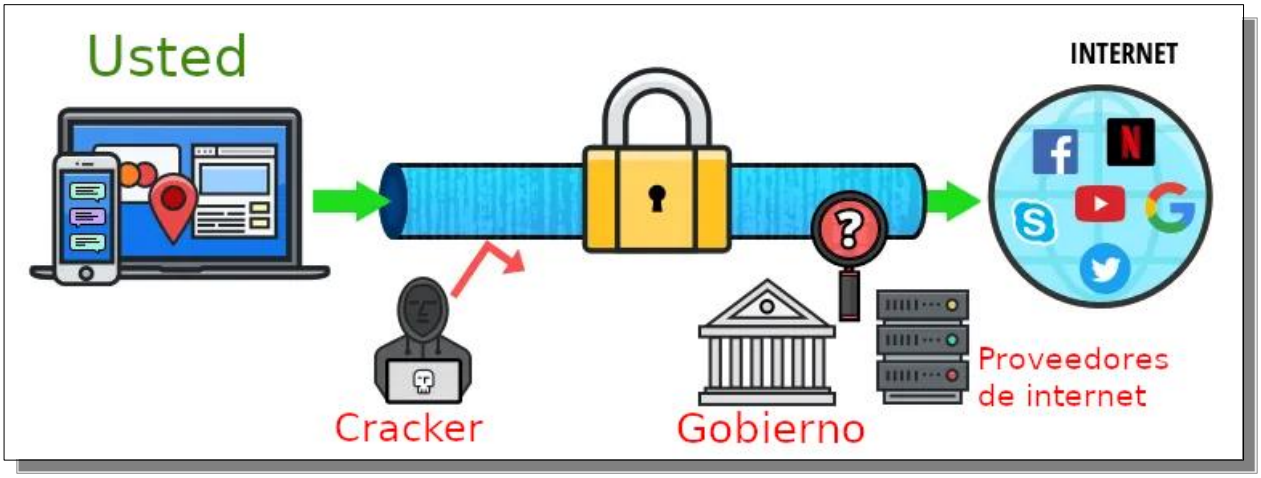
Antirrastreo y antifiltrado

A veces podemos tener acceso a internet inalámbrico o cableado en lugares públicos como centros educativos, hoteles, restaurantes, aeropuertos o dependencias del gobierno, pero no sabemos si éstos están capturando, filtrando o escuchando nuestras comunicaciones. Inclusive algunas

personas defensoras pueden estar siendo monitoreadas por el proveedor de internet residencial o de oficina.

Para evitar este inconveniente se utilizan Redes Privadas Virtuales, VPN por sus siglas en inglés. Una VPN consiste en crear un túnel encriptado entre dos dispositivos ubicados, inclusive, en países diferentes. Uno actúa como servidor y los demás se llaman clientes.

Por ejemplo, si el servidor está en Alemania y usted está en cualquier departamento de Colombia, los sitios web que usted visite entenderán que su dispositivo (computador, tablet o teléfono celular), forma parte de una red de máquinas ubicadas físicamente en Alemania. Por su parte, quien lo está monitoreando o vigilando en Colombia, estará al corriente de que usted se está conectando de manera encriptada a un sitio web ubicado en Alemania, pero no sabrá si usted está viendo su muro de Facebook, enviando un correo electrónico, reenviando un mensaje de WhatsApp o editando un texto en línea en su nube privada.



Fuente: Imagen adaptada. Original recuperado de: https://www.adslzone.net/app/uploads/2019/10/VPN-Schematic.png

Una VPN también tiene la posibilidad de abrir algún servicio que esté censurado o restringido para Colombia.

Existen dos alternativas libres: **Bitmask y RiseupVpn**. Ambas son muy intuitivas y fueron desarrollados por dos grupos muy cercanos y colaboradores entre sí. Ambas tienen servidores en EEUU, Canadá y Europa.

Correo seguro

Llamamos correo comercial a las cuentas que, aunque sean gratuitas son proveídas por empresas como Google (gmail), Microsoft (hotmail, outlok), yahoo, entre otras. El correo sería privado si está hospedado en sitios controlados por nosotros, ubicados en países con legislación fuerte para la protección de datos y que no es gestionada y controlada por un proveedor externo. El correo electrónico es seguro cuando algún programa adicional, como Gpg4Win, encripta su contenido, de manera que, si se tiene una política y práctica de seguridad digital comprometida y disciplinada, se podría tener correo seguro o encriptado en cuentas de Gmail, claro que su implementación es muy compleja.

Protonmail es una alternativa con menor grado de dificultad, porque el cifrado ya está incorporado. Su apariencia es muy parecida a la de cualquier correo comercial, lo cual la hace muy intuitiva. La versión gratuita nos da 500MB de espacio y podemos enviar hasta 150 mensajes al día. Los planes pagados ofrecen hasta 20GB de almacenamiento y 50 direcciones, para lo cual podemos obtener nombres de dominio adecuadas para nuestras organizaciones.

Protonmail es software de código abierto y utiliza un cifrado muy potente. Sus servidores se encuentran físicamente en Suiza, debido a que las leyes de este país tienen altos estándares para garantizar el derecho a la privacidad.

Para crear cuentas de correo es opcional colocar sus datos verdaderos y la colocación de una cuenta de correo para la recuperación de la contraseña. Si por algún motivo se le olvida su contraseña y no colocó una dirección de correo de recuperación, perderá definitivamente el acceso a sus mensajes.

Todos los correos que se intercambian entre usuarios/as de Protonmail están encriptados. El intercambio de correos hacia cuentas ajenas a Protonmail, Gmail, por ejemplo, puede ir o no encriptado. Por supuesto que preferimos utilizar la opción de envío encriptado, para lo cual preferiblemente tendríamos que enviar por una vía alterna y segura la contraseña del mensaje. También existe la opción de delimitar el tiempo de vida de un correo, siendo 4 semanas, 6 días y 23 horas el máximo y el mínimo de una hora. l resto del correo se borrará cuando nosotros así lo decidamos.

Otras herramientas recomendadas

Contraseñas:

Se dice que una cadena es tan fuerte como el eslabón más débil y en informática los programas de cifrado o encriptado son cada vez más potentes, siendo la contraseña el eslabón débil. En la construcción de una contraseña el factor humano es determinante. Con los programas y computadoras actuales una contraseña de 4 dígitos puede ser rota en menos de un minuto. Una contraseña de 8 caracteres, dependiendo de la complejidad de la misma, puede ser rota entre 13 minutos y 57 días como máximo. Por ese motivo se recomiendan frases contraseña, que tengan un mínimo de 16 caracteres, que combinen letras mayúsculas y minúsculas, números, signos y espacios.

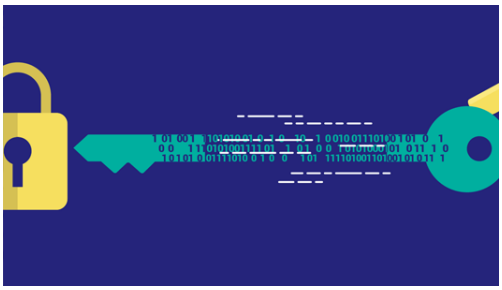
La experiencia nos indica que lo mejor es que cada persona invente su propia metodología para hacer contraseñas fuertes. A continuación, presentaremos varios ejemplos de frases contraseñas:

Felizmente Contento & Sonriente	Matasano$ Fabricante$ 2021
35 Entrenadores & 70 Atletas	El_Leon_21_Es_Vegetariano
mI//bibliotecA//dE//1milloN//dE//pdfS	123 gallinas pavos patos & codornices

Recuerde que la mejor contraseña es aquella fácil de recordar, que no está escrita en cualquier lugar, que por ningún motivo y medio se comparte y que no se utiliza en más de un servicio.

Si desea un programa para gestionar sus contraseñas, le recomendamos KeepassXC, este tiene la capacidad de crear un contenedor encriptado. Usted tendría que memorizarse una sola frase contraseña, la que abriría el contenedor. Dentro de un contenedor de contraseñas de KeepassXC usted puede almacenar la cantidad de contraseñas que desee y el programa le puede ayudar a generar contraseñas y frases contraseñas más seguras.

Cifrado de información:



Cuando decimos cifrado o encriptado de información, nos referimos a la creación de espacios seguros dentro de nuestras computadoras, con un resultado parecido a la instalación de una caja fuerte en una residencia. Para ello se utilizan programas que pueden encriptar carpetas, unidades de almacenamiento externo, fracciones de discos duros o computadoras completas. A continuación, mencionaremos algunas alternativas.

Bitlocker:	Windows trae incorporado, en la mayoría de máquinas, este programa, que le permite encriptar una parte del disco duro o encriptar la computadora completamente. Hay abundante información en línea sobre el procedimiento, pero lo más recomendable es tener la compañía de alguna persona con abundante experiencia en el encriptado y desencriptado de contenedores seguros.
Veracrypt:	Es un programa de código abierto para crear contenedores encriptados que pueden tener un tamaño de 1MB hasta un disco entero. Nuestra recomendación es que inicie creando contenedores que sean fáciles de almacenar en un CD (700MB) o un DVD (4.3GB). Cuando ya esté habituado a la utilización del programa dé el salto para encriptar Memorias USB, discos duros externos y particiones de su disco duro local. Cualquier acción que realice con Veracrypt hágase acompañar por alguien con experiencia y antes de poner un contenedor en marcha o producción, asegúrese de hacer copias de sus archivos en un disco duro externo.
Cryptomator:	este es software de código abierto y está diseñado para encriptar carpetas que se copian en nubes privadas y comerciales. El consejo planteado arriba también aplica para reducir el riesgo de pérdida de información.

Recursos complementarios

- Kit digital de primeros auxilios para defensores de los derechos humanos: https://www.apc.org/es/irhr/kit-digital-de-primeros-auxilios
- Front Line Defenders (2009), « Seguridad y privacidad digital para los defensores de derechos humanos: https://www.iidh.ed.cr/iidh/media/9255/bloque-4-seguridad-y-privacidad-digital-para-los-defensores-de-ddhh-front-line-defenders-2009.pdf
- Autoprotección Digital Contra La Vigilancia: Consejos, Herramientas y Guías Para Tener Comunicaciones Más Seguras https://ssd.eff.org/es
- Línea de Ayuda en Seguridad Digital https://www.accessnow.org/help-es/

Bibliography

Front Line Defenders . (2020, 12 4). *Seguridad Digital* . Retrieved from https://www.frontlinedefenders.org/es/resource-publication/physical-emotional-and-digital-protection-while-using-home-office-times-covid

Magdits, A. (2020, abril 24). *EY.* Retrieved from https://www.ey.com/es_pe/cybersecurity/riesgos-ciberneticos-tiempos-pandemia

Portafolio. (2020, Septiembre 15). Delitos informáticos, la otra pandemia en tiempos del coronavirus. pp. https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642.

Protection International. (2009). *Nuevo Manual de Proteccion para Defensores de Derechos Humanos.* Bélgica.

Protection International. (2013). *Guía de facilitación para el nuevo manual de proteccion .* Belgica.

Protection International. (2017). Herramientas metodológicas. Documento interno de trabajo.