Ministerio de Comunicación
Estado Plurinacional de Bolivia

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Programa de Formación Dual en Periodismo ProPeriodismo

DW Akademie

Fundación para el Periodismo
Periodistas trabajando para periodistas

SEGURIDAD DIGITAL PARA PERIODISTAS

Santiago García Gago – santiago@radioslibres.net
Módulo 10 – Periodismo Crossmedia II
Octubre, 2108. La Paz, Bolivia.

EL PERIODISMO DEL SIGLO XXI

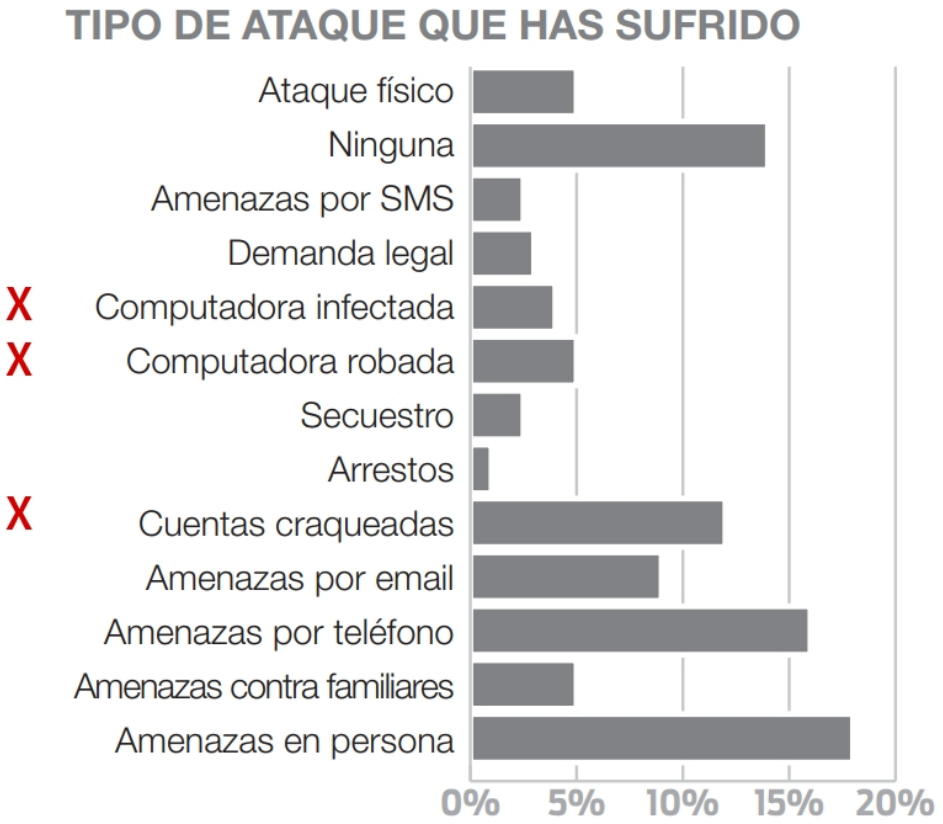
· La mayoría del trabajo actual de un periodista se realiza online y con herramientas digitales

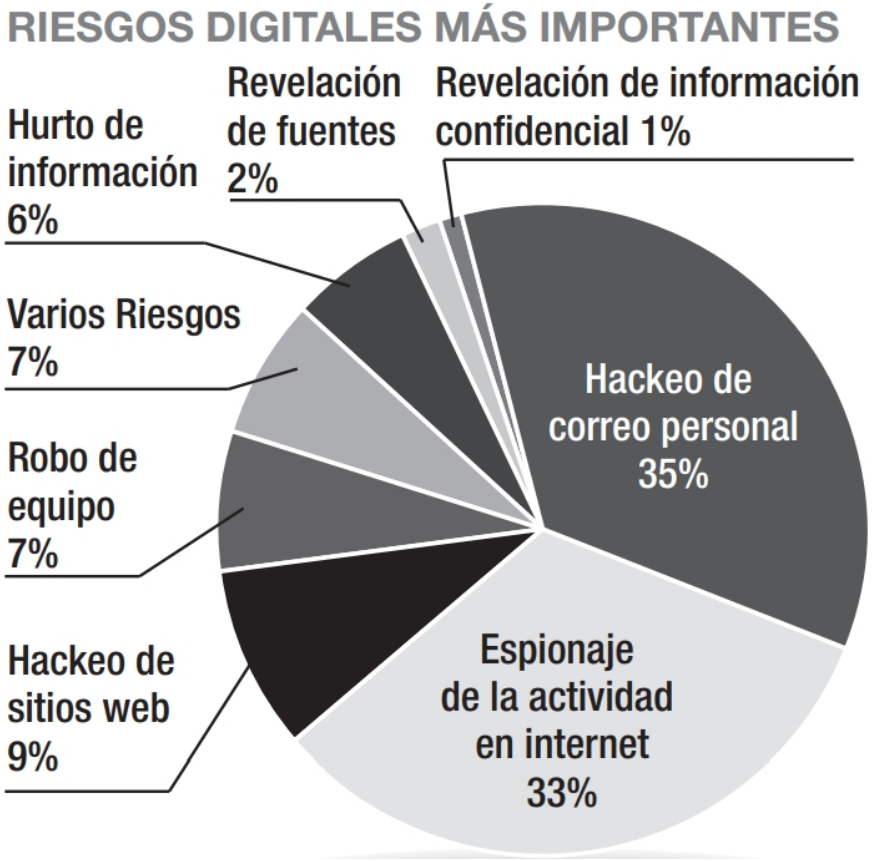
· Por lo general, las y los periodistas usan servicios y plataformas digitales externas para compartir su información: correos de Gmail o Hotmail, WhatsApp…

· Muy pocos son los que toman medidas de seguridad digital como cifrar sus correos, usar mensajería segura, usar contraseñas fuertes y no copiarlas en sus libretas de anotaciones…

· Estas falta de protocolos de seguridad digital les pone en riesgo a ellos mismos pero, también, a sus fuentes.

¿EN REALIDAD ES NECESARIO?





Fuente: resultados de la encuesta entre periodistas y blogueros mexicanos
Desarrollado ICFJ Knight International Journalism Fellow
https://freedomhouse.org/sites/default/files/Digital%20and%20Mobile%20Security%20for%20Mexican%20Journalists%20and%20Bloggers%20-%20Spanish.pdf

BAZAR DE HERRAMIENTAS SEGURIDAD DIGITAL

· Ser conscientes de la necesidad de tomar medidas de seguridad digital, al igual que cuando asistimos a cubrir una marcha tomamos medidas de seguridad física.

· Usar gestores de contraseñas seguros para guardar nuestras contraseñas. (KeepassXC)

· Cifrar nuestros dispositivos (VeraCrypt / BitLocker).

· Usar chats seguros (Wire, Signal).

· Instalar alguna herramienta que nos permita enviar correos cifrados (Enigmail + Thunderbird / Mailvelope).

GESTOR CONTRASEÑAS

· Sirven para guardar todas nuestras contraseñas de una forma segura.

· Nos ayuda a generar contraseñas fuertes.

· Es una simple base de datos, no cambia las contraseñas de nuestras plataformas o servicios.

· Tenemos una sola contraseña maestra para acceder al programa y dentro guardamos el resto.

· La contraseña maestra debe ser larga (al menos 24 caracteres, con mayúsculas y minúsculas, números y algún símbolo).

· ¡No la olvides! ¡Pero no la anotes en ningún papel!

GESTOR CONTRASEÑAS

· Una recomendación es usa alguna frase, título de libro del que te acuerdes siempre y el año en que lo habías leído, por ejemplo:

@ El Amor En Tiempos Del Cólera 1981

· Para recordarla, puedes anotar en algún sitio una regla nemotécnica, te ayudará a recordarla sin escribirla literalmente:

@ Libro Preferido Añoleído

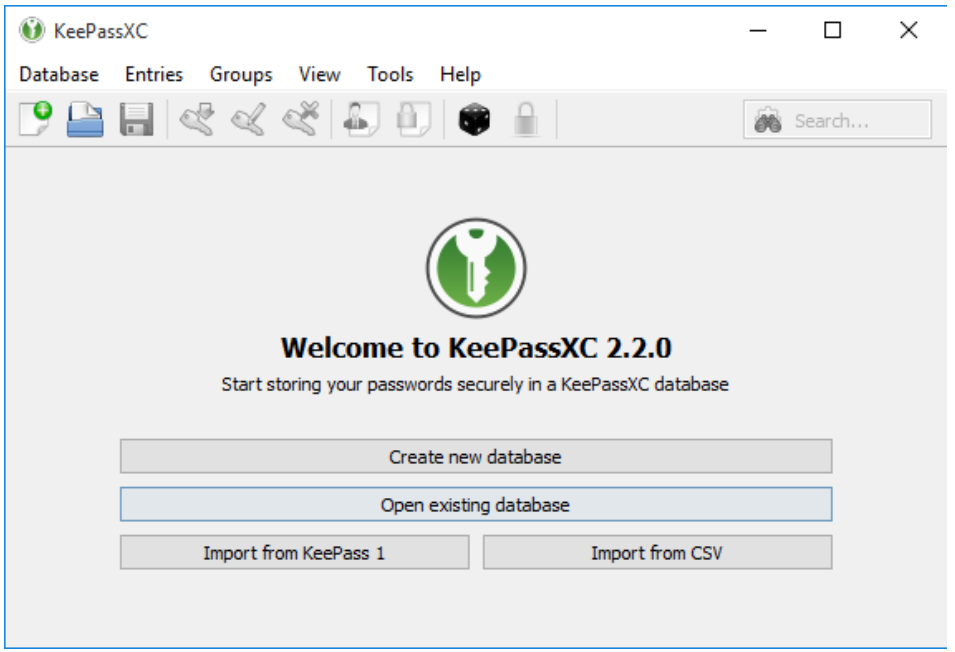
· El archivo de la base de datos de los llaveros digitales se guarda cifrado, por lo tanto puedes guardar un respaldo en otra computadora o en la nube.

GESTOR CONTRASEÑAS

· Recomendamos usar: **Keepass https://keepassxc.org/**

Versión Adroid: https://play.google.com/store/apps/details?id=keepass2android.keepass2android

Manual: *https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassxc*



CIFRADO DE DISCO / ARCHIVOS

· Nos permite proteger carpetas o archivos de nuestros dispositivos. Si alguien los roba o accede sólo verá caracteres inteligibles , pero al ingresar la clave y descifrar los archivos podremos acceder a ellos.

Para Windows

· **BitLocker/BitLocker To Go:** *preinstalada en Windows. Software privativo: la seguridad que brindan no puede ser verificada independientemente.*
Manual de BitLocker (en): https://securityinabox.org/en/guide/basic-security/windows/#windows-full-disk-encryption-with-bitlocker

· **VeraCrypt:**
https://launchpad.net/veracrypt/trunk/1.23/+download/VeraCrypt%20Setup%201.23.exe | **Manual VeraCrypt Windows:**
https://securityinabox.org/es/guide/veracrypt/windows/

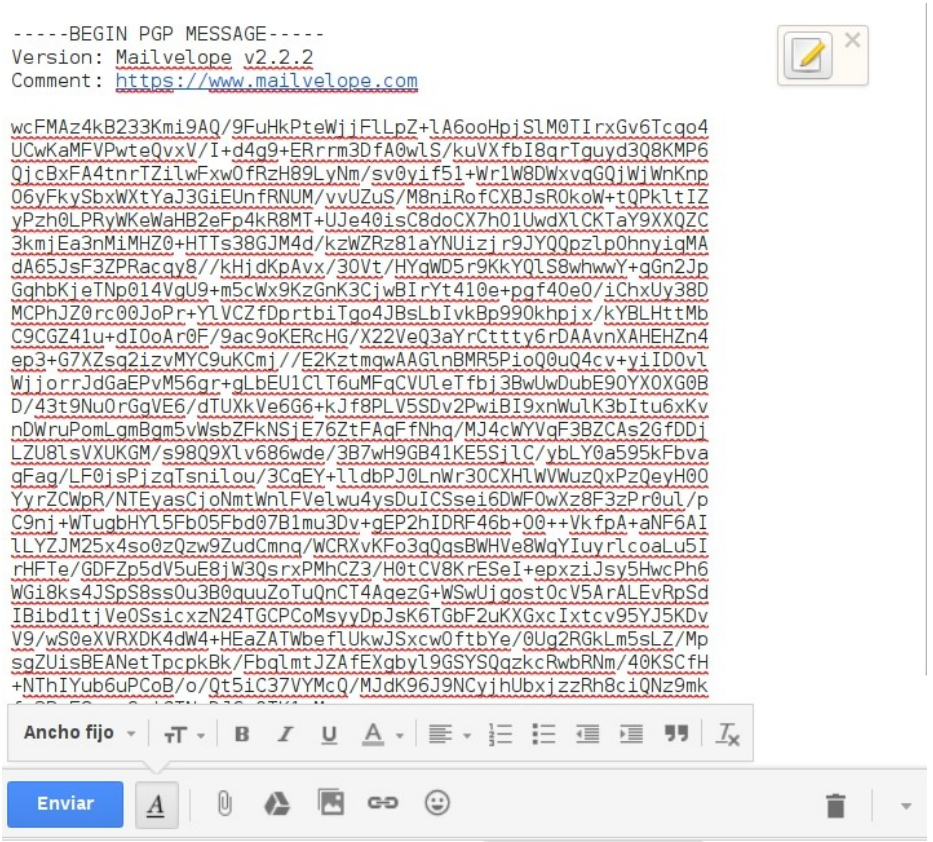
CIFRADO DE EMAIL GPG (GNU Privacy Guard)

· Forma segura de intercambiar correos con fuentes o equipos de investigación periodística.

· El mensaje se transmite de forma cifrada por lo que los intermediarios (servidores de correo, por ejemplo) no pueden leerlos.

· La persona a la que mandamos el correo cifrado debe tener nuestra llave pública y nosotros la de ella. De esa forma, podemos cifrar el correo y ella descifrarlo.

Así se ve un mail cifrado:



CIFRADO DE EMAIL GPG (GNU Privacy Guard)

MAILVELOPE: extensión para navegadores

· **Firefox:**
https://addons.mozilla.org/firefox/downloads/latest/mailvelope/
· **Chrome:**
https://chrome.google.com/webstore/detail/kajibbejlbohfaggdiogboambcijhkke

Tutorial paso a paso :
https://securityinabox.org/es/guide/mailvelope/web/

GESTOR DE CORREOS

Mozilla Thunderbird - https://www.thunderbird.net/es-ES/
Enigmail - https://addons.mozilla.org/es/thunderbird/addon/enigmail/

Tutorial de correo electrónico seguro:
https://securityinabox.org/es/guide/thunderbird/windows/

CIFRADO DE EMAIL GPG EN ANDROID

PARA ANDROID

Gestor de correos K-9
https://play.google.com/store/apps/details?id=com.fsck.k9&hl=en

Open Key Chain / App de cifrado:
https://play.google.com/store/apps/details?
id=org.sufficientlysecure.keychain

MENSAJERÍA INSTANTÁNEA CIFRADA

Comparativa de seguridad de mesajería (inglés, próximamente en castellano):
https://www.securemessagingapps.com/

Wire: https://wire.com/
Signal: https://signal.org/
Telegram: https://telegram.org/
Tox: https://tox.chat/
-> **cliente para Android:** Antox: https://github.com/Antox/Antox

OTRAS HERRAMIENTAS

Buscadores alternativos
Duck Duck Go https://duckduckgo.com/
Searx en disroot https://search.disroot.org/
StartPage https://www.startpage.com/

Extensiones privacidad
Privacy badger https://www.eff.org/privacybadger
https everywhere https://www.eff.org/https-everywhere
Adnauseam https://adnauseam.io/

Visualizar/testear a los trakers
Trackula https://addons.mozilla.org/en-US/firefox/addon/trackula/
lightbeam https://addons.mozilla.org/en-US/firefox/addon/lightbeam/
Panopticlick https://panopticlick.eff.org/

Navegar anónimo
Tor https://www.torproject.org/ - https://tor.derechosdigitales.org/

OTRAS RECURSOS

Seguridad en una caja: https://securityinabox.org/es/ (la versión más completa está en inglés)

Autoprotección digital: https://ssd.eff.org/es

Privacy Tools (inglés): https://victorhck.gitlab.io/privacytools-es/

Por qué mantener tus comunicaciones digitales seguras: https://securityinabox.org/es/guide/secure-communication/

Correos seguros: Riseup: https://riseup.net/es | Tutanota: https://tutanota.com/es/ | ProtonMail: https://protonmail.com/ | Disroot: https://user.disroot.org/

SEGURIDAD DIGITAL PARA PERIODISTAS

Gracias al Espacio Hackfeminista de LaBekka.red por la sistematización de estas herramientas. Con sus datos elaboramos la mayor parte de esta presentación.

Santiago García Gago – santiago@radioslibres.net
Módulo 10 – Periodismo Crossmedia II
Octubre, 2108. La Paz, Bolivia.