MANUAL DE SEGURIDAD

PARA LA PRENSA SALVADOREÑA

ASOCIACIÓN DE PERIODISTAS DE EL SALVADOR

Seguridad digital

COORDINACIÓN E IMPLEMENTACIÓN
Asociación de Periodistas de El Salvador (APES)

APOYO FINANCIERO
El programa Internacional para el Desarrollo de la Comunicación (IPDC, siglas en inglés) una iniciativa de la UNESCO

REDACCIÓN DEL MANUAL
Alba Miriam Amaya

REVISIÓN
Junta Directiva APES
Patricia Montalvo, APES

DISEÑO Y DIAGRAMACIÓN
Roxana Córdova y Wilder Díaz

IMPRESIÓN
TBU

PUBLICADO
Marzo 2021, San Salvador, El Salvador

PRESENTACIÓN

A fin de fortalecer la libertad de la expresión y ayudar a las y los periodistas a mitigar y bajar los riesgos de seguridad relacionados con su labor, la Asociación de Periodistas de El Salvador (APES) con el apoyo del Programa Internacional para el Desarrollo de la Comunicación (IPDC, por sus siglas en inglés), una iniciativa de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) ha desarrollado el Manual para la Prensa Salvadoreña.

El manual está vinculado con el mandato de la UNESCO como agencia de las Naciones Unidas encargada de promover la libertad de la expresión y su rol como la agencia coordinadora de la implementación del Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad. Además, este manual se diseñó en el marco del Objetivo de Desarrollo Sostenible 16: "promover sociedades justas, pacíficas e inclusivas", y en la búsqueda de aportar a la garantía y cumplimiento del derecho a la libertad de expresión en El Salvador.

El documento ha tomado en cuenta información recopilada por Reporteros Sin Fronteras (RSF), el Comité de Protección a Periodistas (CPJ, por sus siglas en inglés), la Federación Internacional de Periodistas (FIP) y otros recursos especializados para la seguridad de la prensa en diferentes áreas como los manuales desarrollados por Deutsche Welle (DW), recomendaciones de IREX INC y el Centro Dart para Periodismo y Trauma, por mencionar algunos.

Si bien, los derechos humanos son interdependientes, indivisibles y progresivos, el enfoque de este manual es el derecho a la libertad de expresión porque es el eje transversal del trabajo de la prensa. Pero -si siempre ha sido así- ¿por qué sacar este documento ahora? Porque, en El Salvador, las condiciones para ejercer y gozar plenamente de este derecho muestran retrocesos preocupantes: el ranking internacional de RSF evidencia el descenso progresivo de la libertad de prensa en El Salvador -desde 2012- lo que llevó al país a ocupar el puesto 81 en 2019. (Ranking RSF, 2019).

Una investigación de la APES sobre la situación de la prensa en 2020 confirmó que las condiciones para ejercer el periodismo ya presentaban síntomas preocupantes desde las dos décadas pasadas, pero -en los últimos años- se ha profundizado la crisis a extremos alarmantes. Dicho estudio detalla que, en el pasado reciente, hubo

un incremento en restricciones a la prensa. Además, el documento subraya preocupaciones acerca del manejo de la pauta publicitaria gubernamental y las consecuencias para la libertad de la expresión.

En El Salvador, las vulneraciones a la prensa incluyen no solo violencia física también hostigamiento, amenazas, eliminación de material como fotografías, videos, restricción al acceso a la información y al ejercicio periodístico, ataques verbales y digitales. Todas las anteriores fueron registradas por el Centro de Monitoreo de Agresiones a la Prensa de la APES. De acuerdo a los resultados de un diagnóstico sobre la situación de la prensa en El Salvador realizado en 2020 por la asociación, quienes ejercen las vulneraciones no solo son funcionarios públicos, sino que también grupos delincuenciales. Estos últimos con mayor presencia en la zona oriental y occidental del país.

Por ello, este manual propone una serie de recomendaciones que se sugiere sean observadas cuidadosamente -junto con otras fuentes acerca del tema- para identificar y prevenir riesgos antes, durante y después de las coberturas. Esto ya sea a nivel individual, grupal, como medio de comunicación u otro, dada la importancia de la planificación y preparación, así como la comprensión del contexto, para prevenir el impacto de riesgos y reforzar prácticas seguras que robustezcan la libertad de prensa.

Esta herramienta recopila consejos de periodistas y de organizaciones nacionales e internacionales con base en experiencias similares a las que se viven en El Salvador y que abarcan los ámbitos digitales, físicos y psicosociales. Este libro abarca consejos para la seguridad digital. Para consejos sobre seguridad física y auto-cuido debe revisar los cuadernillos aque conforman este manual.

Cabe mencionar que este documento no pretende ser la única herramienta utilizada por la prensa en El Salvador, sino que se recomienda sea complementada con otros manuales, recursos, talleres e instrumentos para así poder diseñar un plan de acción para el auto-cuido y autoprotección a fin de mitigar los riesgos relacionados con el trabajo periodístico.

ÍNDICE

Seguridad Digital

GLOSARIO DE TÉRMINOS
SOBRE SEGURIDAD DIGITAL

Astroturfing: es una técnica de propaganda que consiste en que pocas personas generen contenidos en Internet que parezca que son populares y espontáneos.

Ataque DDoS (Denial of Service): busca que un servidor o un sitio web deje de funcionar ya sea sobrecargando el ancho de banda o acaparando sus recursos hasta agotarlos. Lo usual es que se envíen múltiples solicitudes simultáneas para que el servidor se vuelva inestable o esté indisponible.

Ataque DoI (Denial of information): busca difundir masivamente mensajes, a través de programas informáticos –conocidos como bots– para inundar los canales de información con noticias falsas y así dificultar el acceso a la información real.

Deep Fakes: es la manipulación de videos en la que colocan el rostro de una persona en el cuerpo de otra para crear información falsa o para dañar su imagen.

DoubleSwitch: consiste en la vulneración de la cuenta de una persona, usurpar su identidad y difundir información falsa a fin de desacreditarle.

Doxxing: es la búsqueda y recolección de información en la web (seudónimos, fotos, videos, número de tarjeta bancaria, etc.) y luego difundirlos para perjudicar a la persona.

Email bombing: consiste en usar programas para inscribir el correo electrónico de una persona en varios sitios web (a menudo pornográficos) para que no pueda consultar sus propios mails debido a la gran cantidad que recibe.

Hashtag poisoning: es cuando se ataca desde las redes sociales utilizando una etiqueta que une a varias cuentas para insultar o amenazar a una persona.

Mass Report: es cuando se señala masivamente a la cuenta de una persona como "ofensiva" para que la red social la suprima. Es una forma de censura se ve también cuando las reglas de moderación de las redes sociales se ponen al servicio de los gobiernos.

Memes: es la modificación de fotos o videos para crear montajes humorísticos que circulan en las redes sociales. El doxxing puede adquirir la forma de memes.

Pornografía no consentida: es el uso de fotografías sexuales con el objetivo de perjudicar a una persona. Incluye los fotomontajes de imágenes personales, tomadas de las redes sociales, que son alteradas con elementos de sitios pornográficos.

Phishing: es cuando se envía un mensaje con un enlace que conduce a un sitio web con el que se piratea la cuenta de correo para tener acceso a información privada.

Social Bots: son programas informáticos que, de forma automática y de bajo costo, pueden hacer retuits, likes, follow, propagar información falsa o emprender ciberataques.

RECOMENDACIONES EN SEGURIDAD DIGITAL

Este apartado recopila recomendaciones para la protección digital y recordamos que ningún equipo o aparato vale más que la vida, la integridad o la seguridad.

Iniciamos este apartado haciendo énfasis en el cambio de hábitos sobre el uso de software y/o aplicaciones para el celular, así como la revisión constante de actualizaciones en los temas que se abordarán ya que -con el avance de la tecnología- es posible que varias recomendaciones aquí detalladas queden obsoletas en el transcurso del tiempo.

Actualmente, se reporta una tendencia a ataques digitales a los sitios web periodísticos, duplicación de cuentas de periodistas en redes sociales y amenazas, campañas de desprestigio, seguimiento de dispositivos, geolocalización, activación remota de cámara y micrófono, escuchas telefónicas, entre otros. Reporteros sin Fronteras indicó en su informe "Acoso en Línea a periodistas", (2018) como en tan solo seis meses documentaron decenas de casos en 32 países, sus doce oficinas y secciones, así como de su red de corresponsales. Fue entonces que RSF agregó diferentes tipos de ataques en línea contra periodistas como categorías de agresión a la prensa.

Según el Comité de Protección a Periodistas (CPJ, por sus siglas en inglés), la seguridad digital debe verse como la protección del trabajo periodístico ante los riesgos de pérdida: si el disco duro de la computadora se arruina, se pierde la tarjeta de memoria de la cámara, el teléfono celular se destruye, etc.; de divulgación de información que debería de permanecer privada; o de la interrupción de la comunicación por Internet o por teléfono. En tal sentido, es necesario reflexionar sobre:

- Si hay una interrupción en el correo electrónico, ¿qué tanto afectaría esto el desarrollo del trabajo?
- ¿Cómo dañaría la falta de Internet en una investigación periodística?
- Si no se pueden hacer llamadas por el celular, o si hay una interrupción completa al acceso de redes ¿se perjudicaría el trabajo?
- ¿Cómo se afectaría mi trabajo si soy víctima de cíber-acoso o de campañas de desprestigio?
- ¿Se perjudicaría mi labor si me roban las credenciales del correo electrónico o de las redes sociales?

También, hay que recordar que es difícil saber cuándo alguien ha revisado el material en el que se trabaja y que, una vez los datos se pierden -o si alguien ha copiado algún archivo que debería permanecer en secreto- es imposible revertir el daño. Lo más seguro, según CPJ, es contar con un número pequeño de herramientas fáciles de usar, así como simples técnicas y hábitos.

El cambio de hábitos y su refuerzo, cabe recalcar, es primordial y mucho más importante que el cambio de las técnicas o herramientas. Esto es porque si hay buenos hábitos será más fácil elegir bien los instrumentos necesarios (y no al revés). Así pues, a continuación, se enumeran recomendaciones generales de medidas para la protección de diferentes áreas digitales a fin de minimizar los riesgos.

Manejo de perfil

1. Verificar los contactos que se mantienen en redes sociales
y seleccionar los criterios de confidencialidad. Considerar borrar toda la información personal publicada en línea.

2.Considerar el uso de un perfil profesional y uno personal en redes sociales.
Activar la configuración de privacidad (quién puede encontrarte, qué pueden compartir, qué se puede etiquetar, entre otros).

3. Valorar el compartir fotografías familiares o comprometedoras
-fuera del círculo de confianza- ante el riesgo de que las copien y las alteren para luego intentar intimidar o detener una publicación.

- No compartir imágenes que muestren el uniforme escolar de hijas o hijos o de otros miembros de la familia
- No compartir fotografías de las instituciones educativas donde asisten familiares.
- No compartir datos de la familia, tales como edad, dirección, preferencias, hábitos.
- No utilizar la geolocalización para los lugares de visita frecuente.
- No publicar los planes de vacaciones.
- No compartir fotografías de la fachada del hogar o del automóvil que utiliza donde se identifiquen las placas, calcomanías características, etc.

4. Recordar que el teléfono celular de trabajo no debe contener fotografías
personales de ningún tipo.

5. Si se considera que no generaría ansiedad adicional
o que puede llegar a alterar su nivel de alerta, valorar el crear una alerta en Google para saber cuándo alguien menciona su nombre.

6. Eliminar el número de teléfono personal de las publicaciones en línea
o en respuestas automáticas de correos electrónicos.

7. Activar la verificación de dos pasos para las cuentas de correo electrónico
y autenticación segura (con una aplicación de verificación de segundo factor como FreeOTP, Google Authenticator o Microsoft Authenticator) para ingresar a las redes sociales.
Se recomienda priorizar el uso de una aplicación de segundo factor y no del envío de un código de verificación por SMS porque -si el teléfono está intervenido- quien vigila puede leer el mensaje SMS e ingresar sin su conocimiento. Recordar que los SMS se transmiten sin cifrado.

Ataque a los sitios web

Reporteros Sin Fronteras (RSF) define a un ataque DDoS (Denial of Service) como la denegación de servicio que busca que un servidor, servicio o estructura web deje de funcionar ya sea a través de sobrecargar el ancho de banda o acaparando sus recursos hasta agotarlos. En el ataque DDoS, se reciben múltiples y simultáneas solicitudes para que el funcionamiento del servidor se vuelva inestable o no esté disponible. Ante esto:

- Si el ataque es contra el medio de comunicación, solicitar soporte técnico y protección a través de empresas como CloudFare, Incapsula u organizaciones sin fines de lucro que promueven derechos humanos, la privacidad del medio y apoyan en el análisis forense digital, tales como Defflect (DDoS) Qurium
- Si el ataque es contra un sitio personal, solicitar soporte técnico y protección a través de AccessNow (https://www.accessnow.org/help-es/) o Artículo 19 (https://articulo19.org/).

Medidas para proteger software y hardware de computadora portátil

El hardware es todo lo que sí se puede tocar en una computadora: el teclado, la pantalla, el ratón, los discos duros, las USB, los circuitos, etc. El software es lo que no se puede tocar en una computadora: los programas, el sistema operativo, las aplicaciones (o apps), etc.

Para la protección de hardware:

1. Solicitar mantenimiento preventivo y limpieza externa del equipo
de parte de personal de informática del medio.
Si se trabaja de forma independiente, se recomienda buscar el apoyo de empresas o profesionales de informática para que brinden asesoría. Este mantenimiento y limpieza debería realizarse con un mínimo de cada seis meses.

2. Proteger la pantalla de la computadora con un acetato de privacidad que sirva como filtro para restringir la visión lateral y así evitar las miradas indiscretas. Estos acetatos se pueden encontrar en tiendas especializadas o en línea a través de compañías como Amazon.

3. Revisar que los cables, puertos y conectores
de la computadora estén en buen estado.

4. Hacer una copia de seguridad periódica del disco duro.
La periodicidad dependerá de la cantidad de la información: puede ser cada dos semanas o una vez al mes. Entre más frecuente sea la actualización de la información, menor deberá ser el intervalo de tiempo entre las copias de seguridad.

5. Ejecutar un saneamiento digital: refrescar o eliminar los datos
de todos los dispositivos de almacenamiento de archivos como tarjetas SD, memorias USB, discos duros externos, entre otros. Esto se puede hacer también al formatearlos.

6. Al terminar de trabajar, apagar la computadora
en lugar de ponerla en modo de suspensión.

7. Luego de una cobertura, limpiar el equipo sí estuvo expuesto a líquidos
o agentes químicos. Recordar que la cámara y el micrófono de la computadora o el teléfono celular pueden ser activados remotamente por terceras personas. Ante esto, y dada la necesidad de hacer reuniones virtuales que impide desinstalar el micrófono o cámara, lo que la mayoría de periodistas hace es el viejo truco de tapar el lente con cinta adhesiva o una calcomanía.

Para el caso que se tengan conversaciones sensibles, se recomienda evitar tener sus dispositivos cerca.

Para la protección de software:

1. Instalar una versión actualizada del sistema operativo
de sus plataformas, ya sea de Windows, Linux, Mac, u otros.

2. Actualizar regularmente el sistema operativo y programas instalados.

3. Establecer una contraseña para ingreso y bloqueo (pantalla de bienvenida).
Hay que recordar siempre bloquear la pantalla al levantarse del escritorio o la mesa de trabajo para evitar que terceras personas tengan acceso a leer, editar, revisar o extraer información. Esta es una medida para garantizar la privacidad.

4. Cifrar archivos sensibles, o el disco duro por completo,
en la computadora con programas como Veracrypt, https://www.veracrypt.fr/code/VeraCrypt/

5. Desactivar la asistencia remota y el escritorio remoto.

6. Solo descargar software directamente desde el sitio web oficial,
no de sitios web de terceros (aunque sea barato porque puede traer malware).

7. No usar computadoras públicas en cibercafés, hoteles o aeropuertos
para conversaciones confidenciales o para acceder a sus memorias USB. Hay que asumir que estas computadoras están infectadas. No ingresar contraseñas en computadoras públicas. Si no tiene otra opción, asegurarse de usar una navegación privada y borrar el historial del navegador una vez finalizado el trabajo.

8. Evitar guardar información sensible en la nube.

Contraseñas:

1. No usar la misma contraseña para diferentes cuentas.

2. Lo mejor es utilizar un administrador de contraseñas
como Keypassxc y bitwarden, pero siempre es necesario apoyarse en equipos profesionales para su uso e instalación. Si no se tiene acceso a un administrador de contraseñas, se recomienda:

- Escoger contraseñas seguras y mantenerlas en secreto.
- No seleccionar contraseñas con información personal que sea fácil de descifrar (como la fecha de nacimiento, el apellido o el nombre de la mascota).
- Las contraseñas deben ser complejas y con un mínimo de 15 caracteres para que sea segura.
- Incluir caracteres especiales, letras en mayúsculas y minúsculas, así como números.

Una forma para crear una contraseña segura es pensar en una frase y convertirla en su propio código. Por ejemplo:

- "Siempre siento hambre a las ocho de la noche": 100PRe100toHamBr@8:00
- "¡Mi vestido de quinceañera no fue rosado!": MiVesTD15AñNFRosa2!

3. Proteger la lista de contraseñas en un archivo cifrado o en una memoria USB cifrada en lugar de una página de papel o un archivo de texto.

Medidas y aplicaciones para proteger los dispositivos móviles

Cada teléfono celular funciona con sistemas operativos y aplicaciones diseñadas para sus plataformas que dependen tanto de la empresa fabricante como de la versión del equipo que se compra. Sin embargo, hay recomendaciones que aplican para los distintos sistemas operativos:

1. Proteger el celular con una contraseña.
No usar un patrón de bloqueo ni seguridad biométrica (huella digital y rostro).

2. Proteger la pantalla del celular con un acetato de privacidad
que sirva como filtro para restringir la visión lateral y así evitar las miradas indiscretas. Estos acetatos se pueden encontrar en tiendas especializadas o en línea a través de compañías como Amazon.

3. Hay que instalar un antivirus en el teléfono celular,
al igual que con la protección de la computadora, como se explica más adelante. Si no se cuenta con un antivirus instalado, hay opensource o gratuitos como:

- Malwarebytes
- Avast
- McAfee
- Sophos

4. Limitar los intentos de desbloqueo del celular
(revisar el manual del fabricante para ver si la opción está disponible).

5. Instalar aplicación de VPN (Virtual Private Network)
como RiseUp VPN, Orbot, Psiphon u otras aplicaciones que brinden privacidad.
Recordar que un dispositivo con un VPN mal configurado es tan inseguro como si no lo tuviese. Consultar a especialistas en informática.

6. Cifrar el teléfono celular
(revisar el manual del fabricante para ver si la opción está disponible).
Antes de usar aplicaciones, es necesario revisar en detalle los pasos a seguir, las autorizaciones que se dan y las apps que se instalan.

- Activar las opciones de copia de seguridad.
- Valorar el uso de aplicaciones para el cifrado de datos que permitan que el texto guardado no sea visible a proveedores de servicio Consultar a especialistas en informática
- Recordar que, al cifrar, hay que tener cuidado de no perder la contraseña. De lo contrario, no se podrá recuperar el acceso al teléfono.
- No usar el celular como una memoria USB: borrar continuamente audios, fotografías para las publicaciones, entre otros.

7. Revisar, en la configuración del dispositivo,
los permisos que se da a cada una de las aplicaciones instaladas y el acceso que tienen a los datos.

8. No descargar apps de entretenimiento indiscriminadamente
ya que pueden contener malware.

9. Analizar la configuración de las fotografías y vídeos captados por el celular
y la información que captan en metadatos (fecha, hora, tipo de cámara, ubicación GPS, etc.).
- Revisar el manual del equipo sobre la configuración de los archivos de imagen y audio.
- Valorar el uso de aplicaciones de edición que permitan eliminar la información de metadatos.

10. Valorar el uso de aplicaciones populares y su seguridad para chatear
sin intervención de terceros:
- Se recomienda utilizar aplicaciones como Signal Private Messenger en lugar de WhatsApp. Si se mantiene la aplicación de WhatsApp activar el pin de seguridad de la aplicación
- Borrar diariamente todas las conversaciones sensibles de las aplicaciones de chat.

11. Considerar el uso de navegadores con complementos de seguridad instalados
o uno que cuente con paquete de anonimato.
- Se recomienda utilizar aplicaciones como Firefox o TOR en lugar de Chrome, por ejemplo.

12. Si algo es muy importante, prestar atención al tiempo invertido
en una conversación telefónica ya que cada vez es más rápido localizar el origen de una llamada o una conexión a Internet.
- Considerar evitar el tema en una llamada telefónica y esperar a tener la conversación en persona
- Si es necesario hablar por teléfono, considerar el uso de códigos sencillos, o palabras clave, previamente acordadas entre interlocutores.

Es necesario recordar que, aunque hay formas de proteger los datos en el teléfono celular, las llamadas de voz y los mensajes de texto pasan siempre por un proveedor de servicio, por lo que la comunicación entre la persona usuaria y la empresa proveedora puede ser vulnerada por cualquiera que tenga el conocimiento y el equipo para hacerlo. Para optimizar la seguridad propia:

1. Desactivar el Bluetooth si no se va a ocupar.
De preferencia usarlo en lugares seguros y no en espacios públicos
2. Desactivar las funciones de geolocalización en las aplicaciones y en el celular.
3. Para citas que requieran tomar precauciones adicionales con fuentes que han pedido el anonimato, no llevar el celular personal ni el de trabajo. Usar un teléfono descartable ya que, si se compromete, no costará deshacerse de él.

Además, es necesario prestar atención a las medidas que se tomen para prever el robo, extravío, confiscación o daño del teléfono celular ya que una vez que cualquiera de estas posibilidades ocurra no se podrá hacer mucho si no se han tomado precauciones. Por ello, hay que asegurarse de:

1. Configurar la función de borrado a distancia.
2. Mantener el celular "limpio": no guardar datos importantes como fotografías familiares, datos de fuentes confidenciales información bancaria etc
3. Codificar los contactos del directorio, es decir dotarlos de un apodo para proteger tanto a las listas de confianza como a las fuentes que han pedido anonimato .
Considerar revisar el pin de la tarjeta SIM y cambiarlo para incrementar la seguridad -en caso de robo o extravío- y así evitar que sea utilizado por terceras personas.
4. Borrar registro de llamadas y SMS de forma periódica.
5. Cambiar las contraseñas de cualquier cuenta que haya sincronizado con el teléfono (cuentas de correo electrónico, redes sociales, etc.).

6. Avisar a las personas que podrían ser afectadas por la pérdida del celular.

7. Reportar a los diferentes grupos de chat

-en los que se encuentre enrolado el dispositivo- para ser dado de baja por el administrador y así evitar intromisiones de terceras personas.

Si el celular ha sido vulnerado y se estima que las llamadas están siendo grabadas:

- Destruir el aparato -aún si es de alta gama- y conseguir otro con un número nuevo.
  Si no se reemplaza completamente, y el teléfono está comprometido, no se solucionará nada al asociarlo al número anterior.
  • Tomar en cuenta que es posible controlar la ubicación de un teléfono celular, aun cuando está apagado, por lo que, si se lleva el nuevo celular a la casa o a la oficina, se asociará el nuevo aparato a esa ubicación.
- Comprar una tarjeta SD nueva.

- No transferir las aplicaciones.

Navegación:

1. Revisar que el protocolo HTTPS

esté siempre presente al inicio de la dirección web en la barra del navegador ya que brinda una conexión segura.

2. Recordar que una conexión pública de Wi-Fi no es segura,

aún si -al conectarse- aparece un sitio web que pide introducir una contraseña.

3. Robustecer la seguridad del router en casa u oficina:

- Revisar el manual del router para cambiar la contraseña predeterminada por el fabricante. La ubicación de la configuración dependerá del fabricante y de la unidad específica. También se puede revisar la guía para asegurar redes caseras de Derechos Digitales
- Crear una contraseña segura: larga (de al menos 15 caracteres), complicada y difícil de descifrar.

4. Inhabilitar la opción de Recordar contraseñas de su navegador seleccionado.

5. Borrar el historial de navegación continuamente.

6. Considerar el uso de navegadores con complementos de seguridad

instalados o uno que cuente con paquete de anonimato o formato privado. Para ello, se puede consultar con especialistas en informática. Entre los navegadores más comunes están:

- Tor
- Brave
- Mozilla Firefox

7. Instalar complementos de seguridad y privacidad a su navegador, tales como:

- Ulocker
- https everywhere
- Privacy Badger

Para más opciones de complementos revisar la sección de Recursos.

Antivirus:

1.Solo utilizar una aplicación de antivirus -o actualizar el que ya se tiene- tanto para las laptops, tablets, teléfonos celulares, etc. La coexistencia de dos antivirus podría bloquear recurrentemente el uno al otro y dará conflictos engorrosos. Algunos antivirus con versiones gratuitas son:

- Malwarebytes
- Avast
- McAfee
- Sophos
- Total AV
- Norton

● Activar la actualización automática del antivirus y otras aplicaciones anti-malware.
● Establecer recordatorios para comprobar actualizaciones.

2. Activar un Firewall o cortafuegos.

Correo seguro:

1. Recordar que algunos servicios de correo electrónico como Hotmail, Gmail u Outlook pueden ser interceptados por terceros, por lo que hay que utilizar servicios de correo cifrado como Tutanota, Protonmail o afines.

2. Para el envío de información delicada, es recomendable utilizar títulos en el correo (o en el espacio de "asunto" del mensaje) con frases ajenas al tema y que no hagan referencia a la importancia de lo compartido. Valorar el uso de frases de tipo SPAM por ejemplo: ¡Gane un viaje a Europa!

3. No hacer click en enlaces sospechosos o de dudosa procedencia.

4. No abrir ningún archivo adjunto.
Corroborar con el remitente si se trata de un adjunto legítimo y aun así analizarlo con el antivirus.

5. Tener cautela con enlaces o imágenes dentro de mensajes de correos electrónicos porque pueden traer enlaces a virus.
No abrir correos no deseados (conocidos como SPAM).

6. No enlazar las cuentas de redes sociales, ni usar credenciales de servicios asociados como Gmail a las redes sociales.

7. Considerar crear una cuenta de correo electrónico anónima para trabajos delicados para que no esté asociada a su dirección física, teléfono celular, lista de contactos u otro dato de identificación.

Programas para guardado seguro de la información en computadora portátil

Para poder determinar la información que se necesita proteger de forma particular, es necesario poder contestar:

● ¿Cuáles son los datos clave que hay que proteger ante todo?
● ¿Quién podría buscarlos y por qué?
● ¿Qué medidas tengo a mi alcance para protegerlos?
● ¿Cuáles son las consecuencias de no proteger mis archivos?

Para ello, a continuación se brindan algunas recomendaciones generales:

1. Utilizar paquetes para cifrar los archivos tales como Veracrypt que es multiplataforma. Si la computadora cuenta con Windows Pro, usar el cifrador BitLocker.

2. Guardar los archivos en una memoria USB fácil de ocultar y cifrarlas:
Dentro de la USB o nube, crear un contenedor o carpeta cifrada que sirva para almacenar información sensible.

3. Guardar archivos en un disco duro externo con la capacidad suficiente para lo que se necesita.

4. Guardar dos copias de seguridad de todos los documentos vitales una vez a la semana:
- Una en un dispositivo de almacenamiento (memoria USB o disco duro) cifrado con una contraseña segura No guardar las copias de seguridad en la computadora
- Otra en la casa de un contacto de confianza o en la nube, recordando que si se pierde acceso a la cuenta en la nube, se perderá acceso a la copia de seguridad.
- Eliminar el metadata de los archivos de Microsoft Office (creación del documento, lectura, edición, etc.):
  - Abrir un documento y elegir Archivo en el Menú de Inicio.
  - Hacer click en Información y buscar Preparar para compartir.
  - Hacer click en Comprobar si hay problemas y luego en la opción Inspeccionar el documento.
  - Borrar la información personal, comentarios y contenido invisible.

5. Si se revisan documentos que una fuente compartió o de una plataforma como Wikileaks, y no se sabe si tiene virus o malware, no abrir los documentos descargados mientras se está en línea, ya que esto puede ocasionar involuntariamente que la computadora divulgue información.

6. Valorar los riesgos de la manipulación de archivos con información sensible mientras se encuentra en una zona de alto riesgo:
- A veces, es prudente esperar a salir del área para mandar la información al medio.
- Otras, es preferible enviar los datos rápidamente o transmitirlos en directo por redes sociales y eliminarlos del equipo en caso de decomiso o robo También, se puede subir a la nube para su posterior uso y eliminación.
- Una opción es intercambiar las memorias de la cámara cuando ya se tenga material sensible o subirla a la nube en el momento.

Acoso en línea

Una de las formas que se ha usado para atacar a la prensa es a través del acoso en línea por redes sociales. Las agresiones suelen surgir posterior a la publicación de información considerada como dañina para un grupo o individuos señalados en las publicaciones de los medios y se presentan como mensajes o comentarios que incluyen, pero que no se limitan a, el descrédito personal, la burla y el insulto. En el caso de mujeres periodistas, este acoso también incluye connotaciones sexuales que implican mayor carga psicoemocional (RSF, 2018).

Aunque a escala mundial, este tipo de ataques contra la prensa vienen del anonimato que brindan las cuentas falsas, también denominadas trolles, el Centro de Monitoreo de la Asociación de Periodistas e El Salvador (APES) ha registrado ataques de esta naturaleza cuyos perpetradores incluyen a funcionarios públicos, partidos políticos y sus seguidores, entre otros. Para conocer más sobre el tema y recomendaciones específicas se recomienda visitar el sitio **acoso.online.**

Ante un ataque de este tipo, se recomienda:

1. Denunciar ante la APES y buscar su asesoría.
2. Solo si se cuenta con un análisis de riesgo y un plan de mitigación de las consecuencias, revelar la identidad de la/el acosador o la cuenta desde donde se está recibiendo el ataque.
3. Valorar el moderar los comentarios, dentro de la configuración de su cuenta en redes sociales, para buscar reducir las oportunidades de ataques y minimizar el impacto.
4. Primará la solidaridad gremial por lo que se espera que -aún si no es quien sufre de acoso en línea, pero sí es testigo- apoye a la víctima y acuerpe su denuncia.
Esto incluye al equipo completo dentro del medio o al grupo de colegas de distintas empresas.

Ante la publicación de una amenaza implícita (por ejemplo: gente como vos deben recibir un disparo):

1. Denunciar ante la APES y buscar su asesoría.
2. Analizar el marco legal vigente y saber que es una amenaza a la vida, por lo que debe considerarse acciones legales.
3. Considerar silenciar o bloquear la cuenta.

Ante la publicación de una amenaza explícita (por ejemplo: voy a matarte):

1. Acudir a la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores para asistencia de plan de seguridad domiciliar.

2. Formalizar la denuncia ante la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores y:
- Si se confía en las autoridades gubernamentales, denunciar ante la Policía y/o ante Fiscalía General de la República
- Denunciarlo ante organizaciones internacionales.

3. Documentar todo lo sucedido para tomar medidas posteriores ante las autoridades u organismos internacionales. Lo que hay que documentar:
- Número de amenazas.
- Fecha, hora y captura de pantalla de amenaza.
- Número de personas involucradas.
- Severidad del ataque (implícita y explícita).

4. Notificar a la lista de contactos prioritarios o personas de confianza y coordinar el monitoreo de las cuentas de redes sociales.

Ante la publicación de insultos o críticas:

1. Denunciar ante la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores y buscar su asesoría.
2. Si es una crítica al trabajo, considerar interactuar o no con la persona.
3. Si es muy fuerte la afectación:

- Considerar salir de línea hasta que se recupere.
- Considerar silenciar o bloquear la cuenta.

Ante la publicación de comentarios difamatorios:

1. Denunciar ante la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores y buscar su asesoría.
2. Analizar el marco legal vigente para saber si se puede considerar como un delito.
3. Considerar interactuar con la persona, bloquearla o silenciarla.
4. Solicitar a la lista de contactos prioritarios o personas de confianza que comenten o denuncien la publicación en redes sociales.

Ante la suplantación de identidad en redes sociales:

1. Denunciar ante la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores y buscar su asesoría.
2. Denunciar el caso ante la red social.
3. Analizar el marco legal vigente para saber si se puede considerar como un delito.

Recordar que es un ataque digital y hay que tomar medidas de mitigación:

- Denunciar la suplantación de identidad ante las plataformas de redes sociales y solicitar verificación.
- Solicitar a la lista de contactos prioritarios o personas de confianza que supervisen sus publicaciones en redes sociales.

En línea, también existen los ataques denominados doxxing que consisten en obtener información personal que están en la web -como las fotos, vídeos, número de tarjeta bancaria, etc.- para luego publicarla y así afectar a la persona (RSF, 2018). Ante revelación de información privada (doxxing):

1. Acudir a la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores para asistencia de plan de seguridad domiciliar.
2. Formalizar la denuncia ante el gremio y:

• Denunciar el caso ante la Policía y la Fiscalía General de la República.
• Denunciarlo ante organizaciones internacionales como Troll-Busters.com o Access Now.

3. Documentar todo lo sucedido para tomar medidas posteriores ante las autoridades u organismos internacionales. Lo que hay que documentar:

- Número de publicaciones.
- Fecha, hora y captura de pantalla de publicación.
- Número de personas involucradas.
- Severidad del ataque (implícita y explícita).

4. Notificar a la lista de contactos prioritarios o personas de confianza y coordinar el monitoreo de las cuentas de redes sociales.

Ante revelación de información privada (pornografía no consensual o revenge porn):

1. No bloquear el contenido o la persona.
2. Formalizar la denuncia ante la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores y:
- Si se confía en las autoridades gubernamentales, denunciar ante la Policía y la Fiscalía General de la República
- Denunciarlo ante organizaciones internacionales como cyberbullying.org

3. Buscar asistencia legal particular o a través de la APES, ASPIES, CAFOCARES u otras asociaciones de periodistas o comunicadores.

4. Documentar todo lo sucedido para tomar medidas posteriores ante las autoridades. Lo que hay que documentar:
- Número de publicaciones.
- Fecha, hora y captura de pantalla de publicaciones.
- Número de personas involucradas.

RECURSOS

Recomendaciones en seguridad para redes caseras,
Derechos Digitales.

Sobre la Gobernanza en el Internet,
RedPaTodos (Video)

Extensiones de Navegador para proteger tu privacidad,
LifeHacker

Algunas herramientas para la privacidad para la navegación en Internet,
GitLab (En inglés)

Para más información y medidas en caso de acoso en línea:

Misoginia en internet: bombardeo a campo abierto contra las periodistas,
Fundación Karisma

Combatir la violencia en línea contra las mujeres,
Organización de Estados Americanos

Pornografía no consentida. Cinco claves para denunciar y resistir su publicación,
Acoso online.

Ataques digitales, ¿cuáles son y cómo identificarlos?,
Protege.LA

Contra la violencia de género en línea,
Dominemos la tecnología.

13 formas de agresión relacionadas con la tecnología contra las mujeres,
Social Tic.

Construir un internet feminista,
Luchadoras – México

http://troll-busters.com/
(En inglés)

BIBLIOGRAFÍA

Andrés A., Lehnhoff G. (2018). **Plaza Pública:** Así investigamos (y así nos cuidamos). Guatemala. Deutsche Welle Akademie.
Disponible en:
https://www.plazapublica.com.gt/sites/default/files/doc/Manual_mod_JUN15.pdf

Ferrier M. (2018). Attacks and Harassment:
The Impact on Female Journalists and Their Reporting. Estados Unidos. Trollbusters-IWMF.
Disponible en:
https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf

Fundación Karisma, (2013). Sobre la gobernanza en el internet. RedPaTodos.
Disponible en: https://www.youtube.com/watch?v=HU2Vbo_SxIs

GitLab, (2020). Privacytools. 24 de marzo 2020.
Disponible en: https://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034

Guerra, Carlos (2020). Recomendaciones en seguridad para redes caseras de cara al teletrabajo.
Derechos Digitales América Latina. Marzo 2020.
Disponible en:
https://www.derechosdigitales.org/wp-content/uploads/Recomendaciones-de-seguridad-en-Redes-caseras-de-cara-al-teletrabajo.pdf

Henry, Alan, (2015). The best browser extensions that protect your privacy. Lifehacker. 31 de Agosto 2015.
Disponible en: https://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034

IREX. (2018). Programa de estudio de entrenamiento básico de SAFE: Entrenamiento de seguridad para profesionales de medios de comunicación y comunicadores sociales a través del lente único de la conciencia física, la identidad digital y el cuidado psicosocial. Estados Unidos. IREX.
Disponible en:
https://pdfslide.tips/documents/programa-de-estudio-de-entrenamiento-bsico-de-safe-parte-del-programa-de-estudio.html

IWPR. (2018). Manual de seguridad holística para periodistas de Cuba. Cuba. IWPR.
Disponible en :
http://translatingcuba.com/wp-content/uploads/2018/08/pdfholisticsecurityguideforcubanjournalistses_CYMFIL20180822_0001.pdf

OEA, (2019). Combatir la violencia en línea contra las mujeres. Un llamado a la protección. White paper series. Edición 7.
Disponible en: https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf

Protégé.LA, (sin fecha). Ataques digitales, ¿cuáles son y cómo identificarlos? SocialTIC.
Disponible en: https://protege.la/ataques/

Reporteros Sin Fronteras. (2018). Acoso en línea a periodistas: Cuando los trolls arremeten contra la prensa. Francia. RSF.
Disponible en: https://rsf.org/sites/default/files/rapport_cyber_violence_es_0.pdf

Smyth F. (2012). Manual de seguridad para periodistas:Cubriendo las noticias en un mundo peligroso y cambiante. Estados Unidos. Committee to Protect Journalists (CPJ).
Disponible en: https://cpj.org/es/2012/04/manual-de-seguridad-para-periodistas-del-cpj/

SocialTIC, (2018). 13 formas de agresión relacionadas con la tecnología contra las mujeres. Blog.
Disponible en: https://socialtic.org/blog/13-formas-de-agresion-relacionadas-con-la-tecnologia-contra-las-mujeres/

Tennyson S. (2012). SpeakSafe: Manual para trabajadores de medios de comunicación sobre prácticas online y de tecnología móvil más seguras. Estados Unidos. Internews.
Disponible en: https://protege.la/wp-content/uploads/2018/05/0001_guia_SpeakSafe.pdf

Toledo, Amalia. (2016). Misoginia en internet: bombardeo a campo abierto contra las periodistas. Fundación Karisma. 24 de febrero 2016.
Disponible en: https://web.karisma.org.co/misoginia-en-internet-bombardeo-a-campo-abierto-contra-las-periodistas/

MANUAL DE SEGURIDAD PARA LA PRENSA SALVADOREÑA

ASOCIACIÓN DE PERIODISTAS DE EL SALVADOR
APES