RR presenta

SEGURIDAD 360°

Herramientas prácticas de seguridad integral para periodistas mesoamericanos

SOCIALTIC

Tecnología digital para el cambio social

ARTICLE 19

Organización internacional de derechos humanos por la defensa de la libertad de expresión y el derecho a la información.

El periodismo en Guatemala, Honduras, Nicaragua y El Salvador se ejerce entre políticas autoritarias, la persecución y la criminalización judicial. Es en este contexto que el periodismo independiente se ve amenazado y, con él, la libertad de expresión y el derecho de los ciudadanos a acceder a la información.

La Redacción Regional (RR) está convencida de que hacer periodismo en Centroamérica para vigilar los abusos del poder es más necesario que nunca y **diseñamos esta guía con herramientas prácticas para que los periodistas protejan su seguridad física, jurídica, emocional y digital.**

En estas páginas encontrarás:

-Cómo construir un protocolo de seguridad física en 9 pasos

-Qué hacer en casos de emergencia

-Cómo se encuentra tu seguridad y privacidad digital

-Tipología de los ataques digitales y las medidas para atenderlos

-Salud mental en contextos de macrocriminalidad

-Herramientas jurídicas de protección

Esperamos que esta pequeña guía te sirva para hacer mejor tu trabajo.

La Redacción Regional es el primer equipo periodístico dedicado a una cobertura en profundidad del autoritarismo, corrupción, violencias y desigualdad en Centroamérica

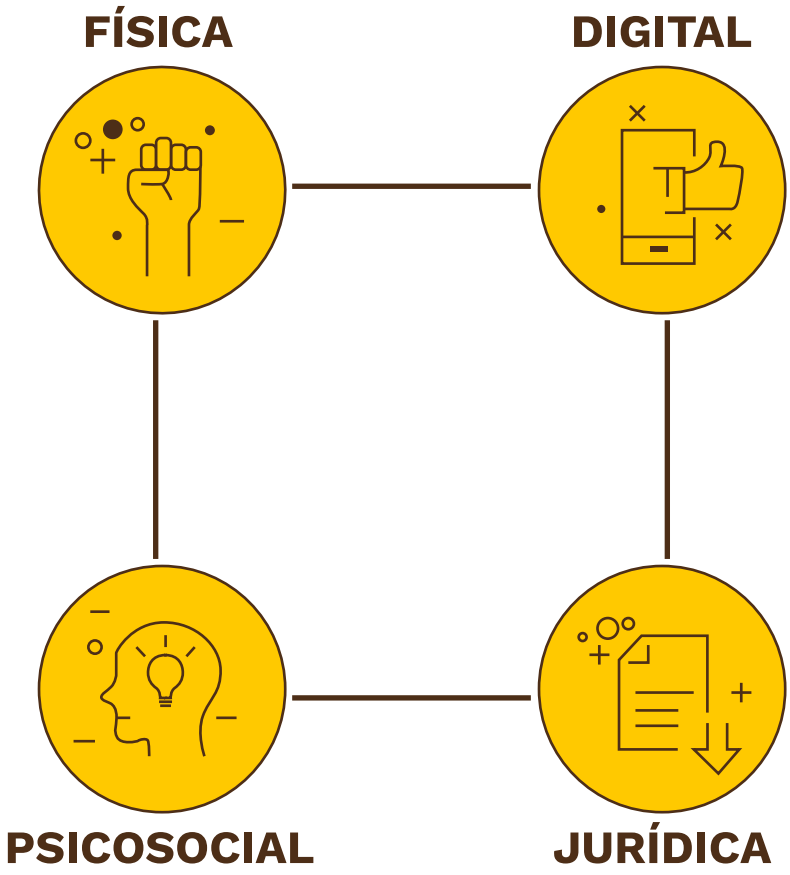
Este manual recoge insumos de periodistas de Dromómanos (México), No-Ficción (Guatemala), La Prensa Gráfica (El Salvador), Contracorriente (Honduras) y Divergentes (Nicaragua).

Sígue nuestro trabajo en redaccionregional.com

¿Qué es seguridad integral?

Por Artículo 19

Las distintas dimensiones que abarcan la seguridad las dividimos en cuatro categorías para darte herramientas de prevención y autoprotección para reducir las amenazas en cada una ellas:



Para mantener **seguridad física:**

Elabora un protocolo de seguridad en 9 pasos

Este plan te ayudará a saber qué medidas tomar ante una amenaza.
Recuerda: es mejor tener un protocolo de seguridad **simple y realista** que tener uno muy elaborado que nunca se cumplirá.

Se empieza por dividir el protocolo en 4 etapas:

DIAGNÓSTICO — **PLANIFICACIÓN** — **IMPLEMENTACIÓN** — **EVALUACIÓN**

Como parte del diagnóstico:

1 Analiza la cancha de juego

Hacer un análisis de contexto te ayudará a identificar las circunstancias en las que llevas a cabo tu labor. Debes tomar en cuenta los aspectos políticos, económicos, sociales, tecnológicos, legales y ambientales y la posición en la que te ubicas dentro de cada contexto.

TIPS

Aunque puede hacerse de manera individual, el formato ideal es una lluvia de ideas.

El contexto no necesariamente está ligado a tu trabajo directamente, pero sí puede provocar un impacto. La siguiente tabla te facilitará el análisis:

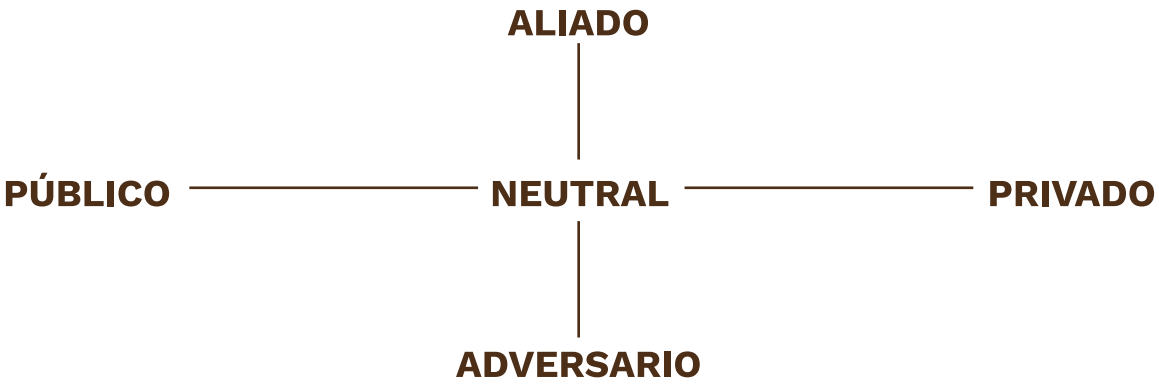
CONTEXTO	ASPECTOS FAVORABLES	ASPECTOS DESFAVORABLES
LOCAL		
INTERNACIONAL		

Otra herramienta. El Método PESTEL te puede ayudar a considerar más elementos:

Políticos	Económicos	Sociales	Tecnológicos	Ecológicos	Legales
¿Qué pasa en el gobierno? ¿Poder?	¿Crisis? ¿Inflación?	Demografía, culturas, grupos de poder, patriarcado	Comunicación, redes, recursos	Cambio climático, megaproyectos	Lesgilación, partidos en el congreso

2 Mapea a los actores, ¿quiénes?

Identifica a las y los actores que puedan tener impacto en tu seguridad. Te permitirá saber de dónde pueden provenir las amenazas y si los actores capaces de dañarte son sensibles o no al costo político.



Pregúntate

- Si estás trabajando en una investigación periodística, ¿quién o quiénes podrían reaccionar ante tu trabajo y de qué maneras?
- ¿Quién o quiénes tienen la capacidad y voluntad de protegerte?
- ¿Quién o quienes tienen la capacidad y voluntad de atacarte?
- ¿Qué actores son neutrales, pero dependiendo del contexto que analices podrían convertirse en aliados o adversarios?
- ¿Cómo se relacionan todas las y los actores entre sí?

La siguiente tabla te facilitará el análisis:

ACTORES	¿ES ADVERSARIO, ALIADO O NEUTRAL?	SU VOLUNTAD DE AGREDIR (PROBABILIDAD DE ATAQUE)	SU CAPACIDAD DE AGREDIR (PODER)

3 ¿Qué medidas tomas para mantenerte seguro?

Pregúntate

- ¿Qué te hace sentir segura/o insegura/o?
- ¿Qué experiencias previas, tanto tuyas como de tu entorno, te proveen de elementos para protegerte?
- ¿Cómo afrontas los riesgos de forma instintiva?, ¿eres consciente de esto?
- ¿Qué medidas de seguridad tomas y en qué nivel las aplicas?

La siguiente tabla te facilitará el análisis:

CONTEXTO	INSUFICIENTE	FRÁGIL	BÁSICA	AVANZADA	PROFESIONAL
POLÍTICA DE SEGURIDAD GENERAL					
MANEJO DE CRISIS					
RECURSOS					
CAPACITACIÓN					
REPORTES DE INCIDENTES					

4 La fórmula de riesgo: R= V + A / C

Existen dos aproximaciones para medir el riesgo y se complementan entre sí:

- El riesgo es igual a la probabilidad y el impacto de que se materialice una amenaza.

El nivel de probabilidad e impacto dependerá de las capacidades y vulnerabilidades, así como de la probabilidad e impacto que tenga la materialización de una amenaza. Todo depende de tu contexto.

- El riesgo es la suma de tus vulnerabilidades y amenazas externas, disminuido por tus capacidades.

Una vulnerabilidad es aquel factor interno que puede afectar negativamente tu seguridad. Una amenaza es un factor o acción externa. Y tus capacidades son tus fortalezas, vínculos o áreas de conocimiento que benefician a tu protección.

R = A + V / C

R = Riesgo
A = Amenazas
V = Vulnerabilidades
C = Capacidades

Para evaluar el riesgo calcula la probabilidad y el impacto de las amenazas (situaciones o factores externos) que identificaste.

Enfócate en aquellas con mayor impacto y probabilidad.

La siguiente tabla puede ayudarte como referencia:

AMENAZAS DETECTADAS	PROBABILIDAD 1 = muy baja 10 = muy alta	NIVEL DE IMPACTO 1 = muy baja 10 = muy alta	RIESGO

Una vez que identificaste las amenazas en cuanto a probabilidad e impacto, debes multiplicarlas entre sí, los números más altos son aquellas amenazas que debes atender primero.

Cuando las identifiques debes establecer cuáles son tus vulnerabilidades y capacidades antes estas.

TIPS

Considera las capacidades que tienes en lo individual y en lo colectivo.

Para cada amenaza, enlista las vulnerabilidades y capacidades que tienes para contrarrestar cada vulnerabilidad.

Ejemplo. Amenaza: Allanamiento de oficinas

Vulnerabilidades	Capacidades
Puertas sencillas, sin chapas de seguridad. No hay cámaras ni alumbrado.	Hay respaldo de información. Hay seguro en caso de robo y redes de apoyo como sociedad civil.

"Los riesgos nunca llegan a cero, ser consciente de tus vulnerabilidades y capacidades no es suficiente, es necesario establecer qué medidas tomarás para fortalecer tus capacidades. Mientras más medidas tomes es menos probable que algo te suceda".

No olvides la perspectiva interseccional en el diagnóstico.

Es indispensable entender que existen condiciones estructurales como el género, la posición socioeconómica, la etnia, la situación migratoria, entre otros, que al ser construcciones socioculturales impactan la posición que cada persona tiene en un contexto determinado.

Etapa de **planeación**. Consiste en diseñar medidas antes, durante y después de la experimentación de algún tipo de violencia.

5 Toma medidas preventivas

Son acciones permanentes que rigen tu día a día y el de la organización. Para el manejo de la información, la comunicación, la seguridad en oficina, bitácora de incidentes, seguridad en contextos de riesgo: protestas, desastres naturales, elecciones, planes de monitoreo en caso de viajes, entre otros.

6 Toma medidas de contingencia

Son los acuerdos, medidas y acciones a seguir en caso de sufrir una agresión o en caso de una emergencia.

- Mantener la calma
- En caso de ser posible, identifica a tu agresor/es
- En caso de ser posible enviar geolocalización a quien te monitorea
- En caso de agresiones en la esfera digital o por teléfono: no responder, tomar capturas de pantalla e los mensajes y guardar número, url, entre otros.

“Las medidas de contingencias se diseñan con base en discusiones colectivas e individuales, pero conocer los riesgos a los que te enfrentas y acordar medidas en caso de sufrir agresiones específicas pueden mejorar la forma de reaccionar”.

7 Toma medidas de contención

En caso de sufrir un ataque o agresión es importante que de forma individual y con tu medio lleguen algunos acuerdos con respecto a qué medidas tomarán. Te recomendamos como mínimo:

- Tomarse tiempo para procesar, reflexionar y descansar
- Socializar y solicitar apoyo si lo necesitas. Puedes acercarte a tu jefa/e alguna colega o con quien más confianza tengas (apoyo psicosocial).
- ¿Qué viste?
- ¿Qué sentiste/pensaste?
- ¿Cómo lo afrontaste?
- Después de un tiempo, hay que analizar las medidas tomadas y establecer qué no funcionó y por qué y qué se puede mejorar, así como si es necesario modificar los acuerdos, medidas, entre otros.

8 Implementa

Materializa las medidas de seguridad acordadas. Pueden dividirse en:

- Establecer responsabilidades: ¿quién estará a cargo de qué?
- Implementación de las medidas acordadas, si acordaron que cada integrante del medio debe entregar 2 contactos de emergencia, se debe notificar a todas y todos de esta petición y las razones por las cuales se está solicitando, quién tendrá acceso a los contactos y bajo qué circunstancias se comunicarán con los contactos.
- Establecer fechas límites. Para cada medida acordada es importante establecer tiempos límites para facilitar su ejecución.

9 Evalúa

Evalúa tus protocolos de seguridad cada determinado tiempo, después de algún contexto de riesgo o posterior a una agresión o ataque.

TIPS

Toma en cuenta que un protocolo de seguridad no es estático y que debe adecuarse a las necesidades de cada persona, medio o colectivo, así como adaptarse a cambios en el contexto.

Algunas preguntas base para la evaluación de tu protocolo son:

- ¿Qué funcionó y qué no? ¿Por qué no funcionaron las medidas?
- ¿En cuál etapa detectamos fallas en el protocolo? ¿Diagnóstico, planeación o implementación?
- ¿Qué podemos hacer para mejorar cada etapa?
- ¿Existen medidas dentro del protocolo que son innecesarias?
- ¿Cómo me sentí al implementar las medidas acordadas?
- ¿Qué estoy dispuesta/o hacer para mejorar mi protocolo?
- ¿Qué recursos puede brindar el medio para mejorar el protocolo?

Guía en caso de emergencia

Por Artículo 19

Llenar esta guía de forma individual y/o con tu medio te servirá para enfrentar situaciones en las que la integridad o vida de alguien corre peligro y en las que se debe actuar de forma expedita.

Primer contacto
¿A quién se tiene que avisar primero? Si eres periodista independiente, ¿quiénes son tus contactos de emergencia y quién se encarga?

Análisis y documentación
Quién se encarga de documentar el incidente y cómo se comunicará.

Coordinación / toma de decisiones
Quién toma la decisión sobre la respuesta a esta emergencia y quién decide si se deben iniciar procedimientos legales.

Apoyo emocional, ¿cuáles son las medidas?

Red de apoyo
Enlista las organizaciones y personas con contactos de confianza.

Autoridades
Cuáles autoridades locales, estatales o federales podrían apoyar y los números.

Apoyo Legal,
¿con qué se cuenta y quién es el responsable?

Difusión
Qué redes mediáticas serían útiles para difundir información que ayude en caso de una emergencia.

Servicios públicos.
A qué servicios públicos se recurre (policía, ambulancia, bomberos, taxis de confianza, otros) y sus números. Responsables de contacto.

Otra herramientas para ti

Artículo 19 tiene una serie de recomendaciones para mantener tu seguridad física antes, durante y después de las coberturas de protestas sociales. Puedes descargarlo aquí.

Para mantener **seguridad digital:**

Conoce cómo viaja tu información cuando navegas en Internet

Por PROTEGE.LA y SocialTIC

Cuando quieres conectarte a Internet, tus dispositivos buscan una red inalámbrica (WiFi) o un plan de datos para conectarse, el punto de acceso de esta red es el router o módem.

Este aparato se encarga de distribuir los datos, es decir, enviar y recibir información por la red.

TIPS

Para proteger tu conexión a internet, cambia la contraseña que viene por defecto del módem y comprueba la configuración de seguridad.

Después del módem, tus datos llegan a tu proveedor de servicios de Internet, es decir, empresas que proveen la conexión.

El proveedor envía tus datos a la red social o sitio web que estás visitando (por ejemplo, Facebook, Google).

Los sitios web que visitas viven en los servidores de distintas páginas y servicios. Al conjunto de servidores se le conoce como “la nube” por su capacidad de almacenar archivos. Cuando subes archivos “a la nube” en realidad estás guardándolos en las computadoras de alguien más.

Facebook entrega tus datos a otro proveedor de Internet para que lleguen a su destino final.

El proveedor envía tus datos al módem de la destinataria.

Después de recorrer este camino, tu mensaje llega al dispositivo de la destinataria.

Es importante tener en cuenta que hay empresas y gobiernos que observan tus datos en el trayecto y en el caso de las empresas, recolectan estos datos para venderlos.
Esto va en contra del derecho a la privacidad y de una red libre y neutral.

Checklist

Después de repasar la ruta de la información, verifica esta lista para saber cómo se encuentra tu seguridad y privacidad digital:

- [ ] Hice un respaldo de mi información más importante recientemente.
- [ ] Utilizo contraseñas de al menos 20 caracteres.
- [ ] Actualizo mis contraseñas cada 30 días.
- [ ] Tengo activada la verificación de 2 pasos.
- [ ] Todos mis aparatos tienen PIN, clave o contraseña de bloqueo de pantalla.
- [ ] Tengo un antivirus instalado y actualizado.
- [ ] Mantengo al día las actualizaciones de mis sistemas operativos y aplicaciones.

- [ ] He revisado la “Configuración de privacidad y seguridad” de mis aplicaciones y cuentas.
- [ ] Verifico que los sitios que visito tienen HTTPS.

¿Cómo te fue? Puedes hacer esta checklist periódicamente y si identificas vulnerabilidad en un punto, usa estos **ocho consejos**:

1 **Respaldo**
Haz copias actualizadas de tu información de manera regular (elige si semanal o mensualmente) y guárdalas en lugares seguros contra daño y robo.

2 **Contraseñas**
Una contraseña se considera segura cuando es: única, privada, larga, combina números letras+símbolos y tiene caducidad. Evita el “12345” y repetir contraseñas.

TIPS

Para almacenar y usar contraseñas seguras:
LastPass 1Password

3 Verificación de dos pasos

Para proteger tu información y cuentas en línea, activa la verificación de 2 pasos, así tienes doble capa de seguridad (contraseña + código)

4 Bloqueo de dispositivos

En tus equipos tienes y compartes mucha información; bloquea el acceso con contraseña, PIN o patrón.

TIPS

Utiliza BitLockeren en el caso de Windows para tener una contraseña de cifrado previa a la de usuario. Mac lo hace solo.

5 Antivirus

Los virus no sólo afectan computadoras, ¡también celulares! Instala antivirus actualizado en todos tus equipos.

TIPS

Norton y McAfee son programas antivirus recomendados para proteger tus equipos personales.

5 **Sistema operativo y aplicaciones**
Mantén actualizado el sistema operativo y las aplicaciones de tus equipos. Las actualizaciones corrigen fallas de seguridad.

6 **Configuración de seguridad y privacidad**
Entra a la sección de privacidad y seguridad de tus apps y cuentas, revisa y cambia lo que desees. También recuerda cerrar tus sesiones al finalizar.

7 **Navegación segura**
Observa la URL de los sitios que visitas, los que tienen HTTPS y el candadito verde son sitios que protegen lo que haces y compartes en línea.

Otra herramientas para ti

En estas Checklists de Seguridad Digital en línea podrás revisar qué tan sanos están tus dispositivos, recibir consejos para mejorar tus hábitos y el cuidado de tu información.

ABC para clarificar y tomar acciones

Seguridad: mecanismos que aseguran la integridad de la información.

Privacidad: mecanismos de control sobre la información.

Anonimato: mecanismos que asocian la información a una identidad.

Identifica un ataque digital y toma acción

En un espectro de violencia donde las agresiones toman distintas formas, son múltiples y se relacionan, hay una tipología que busca describir los eventos y elementos asociados a los ataques digitales, algunos de los riesgos que conllevan y medidas digitales de prevención.

TIPOLOGÍAS

Mediante **vulneraciones técnicas**	Mediante **conductas humanas**
Implican abusar del diseño de la tecnología para modificar o romper aspectos técnicos con fines maliciosos.	Implican abusar del componente humano y las relaciones sociales con tal de generar un daño.
Daño, pérdida o robo de dispositivos **Medidas:** - Respaldar periódicamente la información en medios de almacenamiento externos. - Almacenar los dispositivos en lugares físicamente seguros (a salvo de daños y robo).	**Interacción directa** a través de redes sociales, correos o chat. **Interacción indirecta** suele ser silenciosa.

- Elegir el lugar y medio de almacenamiento adecuado en función de la información que se desea proteger.
- Bloquear el acceso de los dispositivos configurando usuarios y contraseñas.
-Cifrar la información privada y sensible.

Para cifrado de archivos se puede utilizar Cryptomator.

Para cifrado de dispositvos coompletos se puede utilizar VeraCrypt, Filevault o Cryptsetup, dependiendo del sistema operativo.

- Configurar mecanismos de bloqueo y formateo remoto mediante la opción “Encontrar mi dispositivo” de Google, Apple o Microsoft.

Accesos no autorizados a dispositivos, cuentas y servicios en línea

Medidas para dispositivos:
- Bloquear el acceso de los dispositivos configurando usuarios y contraseñas.
- Cifrar la información privada y sensible.

Para cifrado de archivos se puede utilizar Cryptomator.

Para cifrado de dispositvos coompletos se puede utilizar VeraCrypt, Filevault o Cryptsetup, dependiendo del sistema operativo.

Directas

Conductas ofensivas, intimidatorias, discriminatorias o que incitan al odio, amenazas, acoso, hostigamiento, extorsión

Acción Inmediata:
- Buscar apoyo con personas de confianza y organizaciones especializadas como SocialTIC (regional), IREX (regional), Comité para la Protección de los Periodistas (regional), IFEX-ALC (regional), Voces del Sur (regional), Asociación de Periodistas de El Salvador (El Salvador), Protection International Mesoamérica (Guatemala), PEN (Guatemala y Nicaragua) y Asociación por la Democracia y los Derechos Humanos de Honduras.
- Documentar (registrar las agresiones y respuesta de las plataformas).
- Utilizar las herramientas de silenciar, bloquear o reportar.
- Si incurre en un delito y decides hacer una denuncia pública y con las autoridades, aumenta tu seguridad e identifica redes de apoyo.

Medidas de prevención:
- Separar o dividir información de acuerdo a cada perfil (público o privado).
- Configurar las opciones de privacidad de cuentas digitales, controlando qué información es visible y quiénes la pueden ver.
- Conocer las normas de comunidad y utilizar las opciones que incluyen las plataformas para dar de baja contenido ofensivo o intimidatorio (silenciar, bloquear o reportar). La respuesta de las plataformas dependerá del tipo de ataque.

Medidas para cuentas y servicios en línea:

- Utilizar contraseñas seguras.
- Utilizar la verificación de dos pasos.
- Configurar códigos de recuperación extra.
- Utilizar un gestor de contraseñas como KeePass.
-Revisar periódicamente en tus cuentas en línea (cada 6 meses)

Denegación de servicios

Medidas si gestionas un servicio:
- Modificar las configuraciones preestablecidas del servicio.
- Utilizar infraestructuras robustas y escalables para soportar ataques de gran volumen como un CDN (Content Delivery Network) o infraestructura elástica.
- Monitorear la actividad del servicio o sistema para detectar actividad sospechosa.

Medidas de prevención si utilizas un servicio:
-Considerar un servicio de respaldo en caso de emergencia.
- Considerar herramientas o servicios descentralizados.
- En casos especiales, considerar servicios offline o analógicos.

Intervención de dispositivos o sistemas

Medidas para dispositivos:
- Evitar caer en phishing.
- Respaldar periódicamente la información en medios de almacenamiento externos.

- Dependiendo del contexto, contar con un registro de incidentes personales o colectivos (que contenga enlaces, capturas de pantallas y fechas) e incluir acciones y respuestas relacionadas.
- Contar con una red de apoyo que pueda responder ante la solicitud de aspecto físico, legal, digital, emocional.

Indirectas

Doxing - Búsqueda y distribución sin consentimiento de información personal, privada, o íntima

Medidas de prevención:
- Revisar las configuraciones de seguridad y privacidad de servicios y cuentas en línea, y verificar qué información es pública.
- Revisar quiénes pueden ver información que es publicada en redes sociales.
- Realizar un “auto-stalkeo” para conocer qué tipo de información existe en internet sobre una persona. El auto-stalkeo consiste en buscar e identificar información publicada sobre una misma(o), también incluye crear alertas asociadas a palabras clave a cerca de una persona o entidad para dar seguimiento de nuevos contenidos relacionados.
- Evaluar qué información personal podría ser usada para solicitar la baja de contenido de algún espacio digital.

- Bloquear el acceso de los dispositivos configurando usuarios y contraseñas.
- Cifrar la información privada y sensible.
- Instalar actualizaciones de seguridad, tanto del sistema operativo como del software (programas o aplicaciones).
- Instalar y utilizar antivirus y un firewall.

Medidas para sistemas:
- Respaldar periódicamente la información e infraestructura de los sistemas.
- Cifrar la información privada y sensible de bases de datos o sistemas de almacenamiento.
- Instalar actualizaciones de seguridad de los sistemas.
- Utilizar sistemas de monitoreo para identificar actividad, incidentes o eventos sospechosos.

Intervención de líneas o infraestructuras de comunicación

Medidas:
- Utilizar medios y herramientas de comunicación cifradas.

HTTPS en sitios web.

Video y Voz, como Jitsi o Big Blue Buttom.

Chat, como Signal.

Envío y recepción de archivos, como Share Rise Up o Send Tresorit.

Distribución de información (imágenes, audios, videos o datos) con fines de dañar o desinformar

Medidas:
- Contar con un grupo de apoyo para prevenir y atender situaciones de amenaza. Ej. Contar con un grupo de contra discurso en línea.
- Establecer y configurar alertas de contenido nuevo en Internet sobre tu persona, como alertas sobre contenido de Google.

Suplantación y robo de identidad

Medidas para suplantación:
- Revisar las configuraciones de seguridad y privacidad de servicios y cuentas en línea, y verificar qué información es pública.
- Identificar los documentos que contienen información personal, manteniéndolos en lugares seguros.
- Documentar la actividad de las cuentas falsas y reportar a la plataforma que corresponda.
- Conocer las herramientas de reporte y atención de incidentes dentro de las plataformas o servicios en línea.

Medidas para robo:
- Activar notificaciones en servicios y cuentas en línea para identificar actividad sospechosa.
- En caso de notificación de intentos de acceso a cuentas cambiar las contraseñas de estas.

Navegación en Internet con servicios VPN, la red Tor o DNS alternativos.

-Verificar la autenticidad de la información a través de firma o huella digital, o de hashes. Ej. llaves o claves de seguridad para cifrado.

- Revisar inicios de sesión en plataformas, así como las carpetas de correo enviado, basura y spam para identificar actividad sospechosa.
- Conocer las herramientas de reporte y atención de incidentes dentro de las plataformas o servicios en línea.

Bloqueo o control de la distribución o publicación de información en plataformas, servicios o espacios digitales

Medidas:
- Utiliza herramientas que aseguren tu privacidad mientras navegas, puedes utilizar el navegador Tor, una VPN o DNS alternativos.
- Elige canales de comunicación que cuenten con cifrado de extremo a extremo. El cifrado de punta a punta protege tu información mientras viajas en Internet.

Remoción de contenidos publicados en plataformas, servicios o espacios digitales

Medidas:
- Cuenta con un registro o documentación de publicaciones y contenidos en línea, esto podría incluir capturas de pantalla o copias de los contenidos.
- Identifica redes de apoyo que puedan monitorear la remoción de contenidos y respuesta en caso de remoción y otras formas de censura.
- Busca la opción de apelar a través de la plataforma.
- Registra evidencia como pantallazos y respuesta de las plataformas.

Hablemos de Phishing

Por PROTEGE.LA y SocialTIC

Es una técnica que se basa en suplantar o falsificar información para incitar a la persona a realizar una acción, como dar clic a un enlace, abrir un archivo infectado, conectarse a una red o sistema falso, o ingresar información en sitios falsos.

Generalmente con el objetivo de robar información, infectar un equipo o sistema de información. Por ejemplo, correos electrónicos o SMS sospechosos solicitando dar clic a enlaces. Los posibles impactos son:

- Robo de información
- Robo de datos para iniciar sesión en cuentas
- Accesos no autorizados a cuentas
- Suplantación de identidad
- Infecciones e intervenciones de dispositivos

Siete medidas de prevención contra el phishing

1. **Verificar e identificar:**
   Origen de la información (emisor)
   Veracidad del contenido
   Veracidad de los enlaces o adjuntos

2. En caso de reconocer información sospechosa o poco confiable, evitar responder, dar clic en enlaces o abrir archivos adjuntos.

3. Evitar compartir información privada o sensible en espacios digitales.

4. Utilizar un navegador web actualizado para identificar sitios sospechosos.

5. Utilizar servicios en línea cómo Should I Click?, URLScan o Virus Total para identificar enlaces maliciosos.

6. Utilizar un antivirus para analizar archivos sospechosos.

7. En caso de requerir abrir archivos que estén potencialmente infectados por malware se puede utilizar “Danger Zone”.

Para mantener **seguridad emocional:**

Identifica los impactos psicosociales en un contexto de macrocriminalidad

Por Alejandra González Marín
Consultora en acompañamiento psicosocial a víctimas de violencias y graves violaciones de derechos humanos.

> ***"Las personas que trabajan en escenarios de violencias no enfrentan experiencias tan traumáticas como las poblaciones afectadas, pero observar o documentar procesos y catástrofes colectivas puede hacer que manifiesten efectos parecidos, tanto en el ámbito físico, como cognitivo, emocional, conductual o espiritual".***

El contexto. Hay elementos que componen la crisis en materia de derechos humanos en la región:

- Macrocriminalidad
- Graves violaciones a los derechos humanos
- Corrupción
- Impunidad

Hechos de violencia sociopolítica que amenazan la integridad personal, asociadas a emociones extremas:

Miedo

Dolor - Enojo

Humillación – Vulnerabilidad

Caos – Estrés

Frustración – Impotencia – Desesperanza

Frente a el contexto de mesoamérica, los aportes del enfoque psicosocial convergen:

El enfoque psicosocial no tiene solo en cuenta al individuo, sino la dimensión familiar y la reconstrucción de redes sociales de dimensiones destruidas como consecuencia de la violencia.

Salud mental y derechos humanos

Los efectos a la salud mental en escenarios de violencia o de graves violaciones a derechos humanos no se da de manera uniforme.

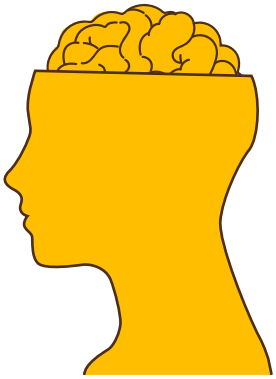
Se debe tomar en cuenta:

1. **La clase social**
2. **El involucramiento en la presunta responsabilidad**
3. **La temporalidad**

(Baró, 1990). Martín – Baró, I (1990). Psicología Social de la Guerra: Trauma y Terapia. El Salvador: UCA editores

- Recoger testimonios / escuchar historias
- Confrontarse con la Impunidad
- Dificultades de Investigación
- Falta de voluntades políticas
- Burocracia
- Problemas de seguridad y/o riesgos por ejercer nuestros derechos

No es fácil porque implica que reconozcas tus propias vulnerabilidades



Falta de realización personal y profesional.

Fatiga física y emocional extrema

Cosificación o despersonalización (deshumanización)

Tómate un momento y pregúntate:

- ¿Cómo me siento? [emociones, pensamientos, funcionabilidad, energía, mi cuerpo]
- ¿Desde hace cuánto tiempo estoy así?
- ¿Cómo me estoy relacionando con las personas más relevantes de mi vida?
- ¿Qué tiene que ver mi trabajo con todo lo anterior?
- ¿Qué tiene que ver el contexto sociopolítico?

¿Sufres burnout?

Es definido como un estado de fatiga o frustración que aparece como resultado de la devoción a una causa, a un estilo de vida o a una relación que no produce las recompensas esperadas. No es agotamiento por el exceso de trabajo, ese que se cura al tomar vacaciones, se trata de una “erosión del espíritu”.

Freudenberger (1974), psicoanalista neoyorquino.

Revisa estas tres dimensiones clave de impactos:

- Agotamiento extenuante
- Sentimientos de cinismo y desapego por el trabajo: distancia, ironía,
- Insensibilidad.
- Sensación de ineficacia y falta de logros.

ESTRÉS VS. BURNOUT	
Se involucra	Falta de involucramiento
Emociones sobrereactivas	Emociones embotadas
Urgencia e hiperactividad	Indefensión y desesperanza
Pérdida de energía	Pérdida de motivación e ideales
Conduce a desórdenes de ansiedad	Conduce al desapego y a la depresión
El daño principal es físico	El daño principal es emocional
Puede llevar a la muerte prematura	Puede hacer parecer que no vale la pena vivir

¿Qué puedes hacer para prevenirlo o revertirlo?

- Aliméntate bien
- Haz ejercicio
- Prioriza actividades recreativas
- Duerme bien
- Vigila tu cuerpo
- Disminuye estresores
- Acude con especialistas

Otra herramientas para ti

En Salud con Lupa han emprendido distintas iniciativas para acercar a sus lectores y a su propio equipo a temas como el estrés y la depresión con series como Hablemos de salud mental y Los otros pacientes.

The Self-Investigation es un proyecto que apoya a los periodistas para abordar su salud mental.

¿Por qué es importante elaborar estrategias de autocuidado?

1. Para afrontar de mejor manera tu situación personal y el contexto laboral y social.

2. Es necesario ser conscientes de la calidad de vida que queremos, en relación a la que estamos teniendo.

3. Porque buscar y construir tu bienestar no es un lujo, sino un derecho.

4. Es una responsabilidad personal frente al escenario de violencia en el que vivimos y desarrollas tu trabajo.

Esta es parte de una de las guías de autocuidado que Artículo 19 ha elaborado. Consúltalas aquí.

Para mantener **seguridad jurídica:**

Conoce algunos conceptos básicos del sistema de protección de Derechos Humanos

Por Dromómanos

El sistema interamericano dota de herramientas a las personas que están en situación de grave riesgo o que les son vulnerados sus derechos humanos.

> ***"Los derechos humanos son los derechos que tenemos básicamente por existir como seres humanos. Estos derechos universales son inherentes a todos nosotros, con independencia de la nacionalidad, género, origen étnico o nacional, color, religión, idioma o cualquier otra condición. Existen sistemas de protección internacional que actúan como complemento a la protección nacional de cada país. Según el país, el ente de protección a periodistas es judicial o administrativo".***

Sistema universal

Sistema de Naciones Unidas

Tiene órganos como el Consejo de Derechos Humanos que examina periódicamente cómo los estados cumplen con los tratados internacionales de DD.HH. Todos los países tienen el deber de presentar ante el Consejo un informe cada cierto tiempo.

Naciones Unidas también posee organismos dirigidos por expertos en derechos específicos que analizan la situación de esos derechos en cada país a nivel mundial y emiten recomendaciones e informes. En la materia de libertad de expresión y de opinión existe una Relatoría Especial. Actualmente está a cargo de Irene Khan.

Los Estados que han firmado tratados internacionales donde reconocen a sus habitantes DD.HH. están obligados a su cumplimiento y facilitar información para los monitoreos de órganos veedores creados para verificar que esos derechos sean efectivamente cumplidos y respetados. Por ejemplo, el Pacto Internacional de Derechos Civiles y Políticos que en su artículo 19, al igual que la Declaración Universal de Derechos Humanos, establece el derecho a la libertad de expresión.

Los órganos contralores de esos tratados se definen como Comités, y dentro de estos se articulan espacios para dirimir reclamos cuando un Estado está incumpliendo con un tratado internacional al cual está adscrito.

Sistema interamericano de protección de Derechos Humanos:

- Es un sistema regional indirecto de promoción y protección de DD.HH.
- Es indirecto porque el acceso al tribunal regional, la Corte Interamericana de Derechos Humanos, está supeditado a que el caso lo presente la Comisión Interamericana de Derechos Humanos.
- Hay dos grandes etapas procesales dentro del Sistema Interamericano:

Una se inicia en la Comisión en su función jurisdiccional. Ante ella se presenta un caso y esta emite un informe de admisibilidad y posteriormente un informe de fondo. En el caso en que el Estado no cumpla con las observaciones de este último se le puede exigir, a pedido de los representantes y como decisión última, que el caso en revisión pase a la Corte Interamericana de Derechos Humanos.

La Comisión Interamericana de Derechos Humanos:

- Fue creada en 1959 con la Carta de la Organización de Estados Americanos (OEA). Actualmente forman parte todos los países de la región menos Venezuela y Nicaragua.
- Integrado por 7 comisionados elegidos por la Asamblea General, pueden tener 2 mandatos de 4 años. También hay una secretaría ejecutiva que lleva adelante las tareas de trámite.
- El órgano de la etapa inicial. Funciona como órgano autónomo de la OEA. Su función principal es promover la observancia y la defensa de los DD.HH. en la región americana en general.

Tiene una dimensión política que busca articular espacios de monitoreo para ver cómo los estados están llevando adelante el cumplimiento de los DD.HH. reconocidos tanto en la Convención Americana de Derechos Humanos como otros tratados a nivel Interamericano.

- También una dimensión jurisdiccional con un sistema de peticiones y de casos. Aquí uno de los elementos más importantes es el de medidas cautelares que buscan proteger a personas que se encuentran en una situación grave, de urgencia y de daño irreparable de algunos de sus derechos humanos.

La Corte Interamericana de Derechos Humanos:

- Creada en 1969 mediante la Convención Americana de Derechos Humanos. Está compuesto por siete jueces y juezas, por una secretaria legal y administrativa, y una secretaría de junta.

- Es el tribunal regional que cumple función judicial internacional. Tiene tres funciones específicas:

1) las medidas provisionales, muy similares a las medidas cautelares.
2) la contenciosa. O sea, el litigio que se inicia la Comisión y que después llega la Corte en el cual una persona representada, puede ser por una ONG, personalmente o por un defensor Interamericano, demanda un estado por un incumplimiento a un tratado de Derechos Humanos Americano. Acá es donde se enmarca la jurisprudencia de la Corte Interamericana, cuando dicta una sentencia. Después continúa una etapa de supervisión de cumplimiento. Es decir, un seguimiento posterior a esa sentencia en mira de que los estados cumplan con las medidas de reparación integral que ha otorgado el tribunal.
3) la consultiva.

- Tanto la Comisión como el tribunal tienen dos instrumentos jurídicos por los cuales se están regulados: el Estatuto de la Corte y de la Comisión y reglamentos internos que son sancionados por los comisionados en el caso de la Comisión y por los jueces en el caso de la Corte. De ellos surgen los estándares interamericanos de derechos humanos.

Algunas herramientas jurídicas para proteger tu labor

Se pueden utilizar juntas o solo una

1 **Para afrontar de mejor manera tu situación personal y el contexto laboral y social.**

- Una persona o grupo de personas que consideran que un Estado le ha vulnerado un derecho humano reconocido en un tratado internacional, como la Convención Americana, demanda a un Estado ante la Comisión Interamericana y después será posible acceder a la Corte por el incumplimiento.
- Esa demanda se llama petición inicial. De ser verificados y comprobados se condena el Estado mediante un informe de fondo, en el caso de la Comisión, o una sentencia, en el caso de la Corte.
- Se declara que tuvo la responsabilidad internacional por violación de derechos y se dictan medidas de reparación integral y garantías de no repetición.

Un llamado importante

Es importante que agotes todos los recursos a nivel nacional para llegar a la etapa supranacional. Hay que denunciar los hechos ante instancias locales (Fiscalía, Defensor de Derechos Humanos, Juzgados), alegar los hechos y, de ser posible, referir testigos, pericias, videos, etc. Aquí también es clave contar con apoyo de organizaciones defensoras de DD.HH. aliadas para que el umbral probatorio y la gestión ante instancias supranacionales tengan más impacto.

2 Medidas de protección

- Es un mecanismo inmediato que busca proteger a una persona o a un grupo de personas que están frente a una situación grave y urgente de sufrir un daño irreparable a sus derechos.
- No hay un prejuzgamiento del caso. Los órganos del sistema no analizan si está configurada la violación al derecho o no. Analizan si existen condiciones a una potencial afectación y actúan en consecuencia
- No se requiere el agotamiento de los recursos internos. No se determinan reparaciones.

El umbral probatorio es cuando el órgano hace un análisis de *prima facie*, los hechos no tienen que estar 100% probados, sino que haya presunción del grave riesgo.

- **Cautelares:**
  Las otorga la Comisión. Reguladas en el artículo 25 del Reglamento de la Comisión. Los requisitos son a) gravedad, b) urgencia, ambas se deben ver en la situación, el riesgo debe ser inminente y que pueda materializarse. Y c) daño irreparable, o sea no puede ser restaurado adecuadamente.
  La Comisión actualmente sólo lo toma cuando hay un peligro a la vida y a integridad de las personas.
  Pueden proteger a una sola persona o ser colectivas.
  Para solicitarlo no se necesita de un abogado, cualquier persona las puede solicitar.

No es necesario tener la ciudadanía del país al que se interpela, pero sí residencia. Se pueden enviar a **cidhdenuncias@oas.org** o vía postal a la Comisión en Washington DC.

Tiene dos funciones:

- **Cautelar:**
  busca preservar una situación jurídica

- **Tutelar:**
  la más útil para periodistas. Busca tutelar ese derecho humano del cual es titular la persona. Quiere evitar un daño irreparable a un derecho humano.

Es difícil que se otorguen. Del 2005 al 2020 la Comisión solo otorgó el 7,51% de las solicitudes de medidas cautelares que recibió. Muy pocas de ellas son por la violación a la ibertad de expresión o de prensa.

Una vez otorgadas hay unos mecanismos de supervisión:

- **Audiencias públicas.** Pueden ser solicitadas por las partes o por la Comisión.
- **Visitas de seguimiento y revisión.** Debe ser con la anuencia del Estado.
- **Reuniones de trabajo.** No son públicas. Participa el relator país.
- **Reuniones bilaterales.** La Comisión con solo una de las partes.

Resoluciones de seguimiento. Sirven para llamar la atención al Estado, porque los factores de riesgo han aumentado, o porque el Estado no ha implementado nada de lo solicitado.

- **Provisionales:**
  Surgen de la Convención y las otorga la Corte.
  Se pueden acceder sin tener cautelares, pero generalmente es una elevación de una situación de grave que ya pasó por la Comisión. Los requisitos son a) extrema gravedad, b) extrema urgencia y, c) daño irreparable.

  - En casos que no están en la Corte: primero se debe pasar por la Comisión y denunciar que las medidas cautelares no se están cumpliento.
  - En casos que sí están en la Corte: deben tener relación directa con el caso.

Seguridad 360

Herramientas prácticas de seguridad para periodistas mesoamericanos

Es gracias al apoyo de la Fundación Panamericana para el Desarrollo (PADF)

Y a los aportes de 25 periodistas provenientes de Nicaragua, Honduras, Guatemala, El Salvador y México que participaron en los Talleres de seguridad integral para periodistas convocados durante 2022 por la Redacción Regional en alianza con Artículo 19 y SocialTic.

Centroamérica, agosto de 2023

PADF
FUNDACIÓN PANAMERICANA PARA EL DESARROLLO