

Reduce tu riesgo

Protocolos de
Seguridad para
Periodistas



Este documento consiste en una serie de protocolos de seguridad adoptados por la Comunidad de Periodistas de la Frontera Norte de México

ÍNDICE	1
INTRODUCCIÓN	3
DESCARGO DE RESPONSABILIDAD	3
PROTOCOLO ANTE LAS AMENAZAS A PERIODISTAS	4
Paso 1: Determina la credibilidad de la amenaza y el nivel de riesgo	6
Paso 2: Documenta la amenaza	7
Paso 3: Consigue ayuda psicológica	7
Paso 4: Protege tus comunicaciones	8
Paso 5: Responsabilidades del círculo de confianza	8
PROTOCOLO DE SEGURIDAD ANTE LA VIGILANCIA	10
PROTOCOLO DE SEGURIDAD ANTE EL ACOSO SEXUAL	13
PROTOCOLO DE SEGURIDAD EN LA INVESTIGACIÓN PERIODÍSTICA	16
PROTOCOLO DE SEGURIDAD CON LAS FUENTES DE INFORMACIÓN	19
PROTOCOLO DE INVESTIGACIÓN EN ZONAS DE ALTO RIESGO	22
PROTOCOLO ANTE EL ACOSO JUDICIAL	26
PROTOCOLO ANTE INCIDENTES GRAVES DE SEGURIDAD	29
Responsabilidades de la dirección en casos de emergencia	31
Otras responsabilidades en el área editorial	32
PROTOCOLOS DE SEGURIDAD DIGITAL	33
Cómo crear una contraseña segura	34
Gestión de contraseñas	35
Autenticación Multifactor	37
Uso de Redes Privadas Virtuales (VPN)	39



Introducción

Estos protocolos son guías y recomendaciones de acción individual o colectiva que el Border Hub ha recogido en su experiencia para que periodistas y personas defensoras que ejercen su oficio en la frontera norte puedan reducir el riesgo de manera significativa en momentos en los que una amenaza de daño grave de tipo físico, legal, psicológico o digital pende sobre sus organizaciones y personas.

Consideramos que escribir, compilar y compartir estos protocolos es muy importante para que las y los periodistas puedan desarrollar su trabajo con la mayor seguridad posible ante actores hostiles que depredan la libertad de prensa y el derecho a la información. También es muy importante que el Border Hub los publique y adopte para lograr una serie de conocimientos, prácticas y tecnologías homologada entre sus integrantes.

Las guías presentadas aquí no son ni estáticas, definitivas o exhaustivas. Son documentos en redacción permanente que deben ponerse a prueba y mejorar en cada experiencia donde una persona dedicada al periodismo o a la defensa de los derechos humanos utiliza los protocolos para mejorar su seguridad.

DESCARGO DE RESPONSABILIDAD

Este texto es posible gracias al apoyo del pueblo de los Estados Unidos a través de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). El contenido de este texto es responsabilidad de su autor, y no necesariamente refleja el punto de vista de USAID o del gobierno de los Estados Unidos.

1. Protocolo ante las amenazas a periodistas



Protocolo ante las amenazas a periodistas

En un número importante de casos recientes de asesinato de periodistas, las víctimas habían sido amenazadas de muerte días, semanas o meses antes del ataque físico. La existencia de una impunidad sistemática, así como de diversas deficiencias, favorecen la tendencia de cumplimiento de las amenazas.

En ese contexto de impunidad, negligencia e ineficiencia, hay una probabilidad muy alta de que las amenazas pueden ser creíbles y su cumplimiento inminente. En esos casos, el margen de acción para los medios ha sido muy limitado.

Ha sido difícil llegar a un consenso entre los medios mexicanos en relación a qué hacer una vez que la amenaza ha sido declarada. Las reacciones han sido diversas: algunos medios deciden sacar a sus periodistas de la zona inmediatamente, antes aún de investigar la naturaleza de la amenaza y la probabilidad de que sea cumplida. En esas respuestas se advierte una tolerancia al riesgo baja y la percepción de que las amenazas pueden ser cumplidas en forma inminente.

En otras ocasiones, los medios deciden mantener a sus periodistas en sus ciudades o poblaciones, en ocasiones porque no hay los recursos suficientes para sacarlos de la zona y en otros casos porque posiblemente la lectura del riesgo arroje que la amenaza tiene menos probabilidades de ser cumplida.

Hay personas y organizaciones que recomiendan acudir a la agencia del Ministerio Público a denunciar la amenaza en forma rápida, y hay otras que opinan que presentar una denuncia ante las autoridades puede aumentar el riesgo para las y los periodistas y el medio. También puede haber diferencias entre medios y periodistas que consideran mejor denunciar en forma pública la amenaza y elevar su perfil público y hay otras que sostienen que hacerlo público puede atraer consecuencias indeseables.

Sigue estos pasos si has recibido alguna amenaza o consideras que puedes estar en peligro:

Paso 1: Determina la credibilidad de la amenaza y el nivel de riesgo

Analiza pronto si la amenaza es creíble o no y si el riesgo es bajo, intermedio o extremo, según las experiencias recientes en tu comunidad, en tu estado o en tu país. El riesgo de la amenaza de un funcionario público puede ir de bajo a extremo, y debes ver qué tan creíble es, qué tan dispuesto está a consumar la amenaza y si eso es algo inmediato o no. Si el funcionario tiene un historial de agresiones a periodistas y demuestra tener la voluntad de atacarlos, entonces considera riesgo alto o extremo. Si la amenaza viene de grupos criminales o de oficiales de los cuerpos de seguridad que están en contubernio con ellos, el riesgo puede ser extremo. Puedes hallar una descripción más detallada del análisis de riesgo en [este documento](#):

Considera estos pasos, si determinas que la amenaza es creíble y que el nivel de riesgo es extremo:

- Irte a un hotel o una casa segura, determinada con tu gente de más confianza.
- También puedes acudir a una instalación militar y pedir protección inmediata.
- Asegúrate de que no estás sujeto a vigilancia en el entorno de tu casa, de tu oficina, y en el trayecto entre uno y otro. Revisa si hay automóviles extraños en los alrededores. Si manejas tu vehículo, asegúrate que nadie te siga en otro vehículo. Desconfía de los vehículos tripulados por tres personas, particularmente si los tres son varones. También pon atención a motocicletas y taxis que muestren movimientos inusuales.
- Evita usar transporte colectivo. Si manejas tu vehículo, no lo hagas de noche. Antes de llegar y salir de un lugar, asegúrate que no haya nadie sospechoso alrededor. Puedes ayudarte de tus vecinos y cámaras de seguridad.
- Una vez que sientas que has tomado medidas precautorias, analiza la posibilidad de presentar una solicitud ante el Mecanismo Gubernamental de Protección de Personas Defensoras y Periodistas. Ten en cuenta que la aprobación de la solicitud puede tomar días, semanas o quizá meses. Así que mientras se decide la protección gubernamental, debes tomar todas las medidas posibles de precaución.
- Decide si lo mejor es salir de la ciudad o del país.

Si decides que la amenaza no es creíble o que el nivel de riesgo es bajo o moderado, adopta los siguientes pasos:

Paso 2: Documenta la amenaza

Es muy importante documentar la amenaza, con los siguientes elementos:

1. Fecha, hora y ubicación del incidente.
2. Presunta identidad de la persona y/o grupo amenazante.
3. Medio de transmisión de la amenaza (por ejemplo: en persona, por teléfono, por correo electrónico, por manta en la calle, por mensaje escrito).
4. Número telefónico y correo electrónico, en caso que se realizara por alguno de estos medios.
5. Anotación textual del mensaje.
6. De ser posible, grabación de la amenaza o captura de pantalla. Estos datos de registro pueden ser importantes en caso de que decidas presentar una denuncia formal ante el agente del Ministerio Público o solicitar la ayuda del Mecanismo Gubernamental de Protección de Personas Defensoras y Periodistas.

Paso 3: Consigue ayuda psicológica

Considera que las amenazas pueden dañar tu integridad, la de tus colegas o la de tus familiares. Así que es importante que tomes pasos para fortalecer tu integridad emocional y evitar que tu preocupación no sea paralizante o que el miedo sea desbordante. Mantén la protección de tu círculo de apoyo, con tu familia y tus colegas.

Aunque determines la baja o alta credibilidad de la amenaza, sería importante que pidas ayuda profesional de una persona especializada en Psicología. Tu medio de comunicación o tu círculo de confianza debe facilitar la ayuda profesional para mantener la estabilidad psicológica de la persona amenazada.

Si necesitas ayuda psicológica urgente, puedes enviar un mensaje a info@bordercenter.net y podemos acercarte a una red de psicólogos y psicólogas dispuestos a ayudar.

Paso 4: Protege tus comunicaciones

En esta etapa, es fundamental que uses comunicaciones encriptadas de punta a punta, es decir, que son transmitidas en forma encriptada y se descifran en el dispositivo de la persona que recibe la comunicación.

Una de ellas puede ser el intercambio de mensajes o de llamadas a través de la aplicación [Signal](#). Si compartes información confidencial en ese momento usa Protonmail, un servicio de correo electrónico encriptado de punta a punta. Es mejor que si te desplazas, tus dispositivos no contengan información sensible o confidencial.

Toma en cuenta que en una situación de amenaza es importante que tus dispositivos no contengan información sensible de tus fuentes, de tus reportajes, o de tu persona. Esto ayuda a limitar el impacto de una acción de espionaje en tu contra o del robo o decomiso de tus dispositivos.

La seguridad digital de los periodistas debe también considerar que las redes sociales y las plataformas digitales han servido para lanzar agresiones digitales contra periodistas. En el apartado de seguridad digital veremos el uso de herramientas que ofrecen privacidad y anonimato digital como [VPN](#), [Tor](#) y [PGP](#). (Ver protocolo de Seguridad Digital)

Paso 5: Responsabilidades del círculo de confianza

Todo periodista que trabaje en situaciones de alto riesgo debe crear o unirse a una red de confianza donde consiga apoyo y solidaridad. Esta red de confianza puede incluir a familiares, amigos, colegas de otros medios de comunicación y del medio con el que colabores o trabajes.

Asegúrate de que la red de apoyo cuente también con sus propios protocolos de actuación en caso de amenazas. Si no los tiene, puedes proponer las siguientes medidas:

1. Atención pronta a colegas que sufrieron una amenaza.
2. Acompañamiento permanente de una persona de confianza.
3. Creación de un círculo de mucha confianza que ayude a la persona amenazada a mantener la ecuanimidad y reunir la mayor cantidad y calidad de información sobre la amenaza, su naturaleza, sus motivos, así como la capacidad y voluntad de la persona amenazante para cumplir con la amenaza y causar daño.

4. Si trabajas en forma regular para un medio de comunicación, informa a tus jefes de las amenazas recibidas y discute con ellas y ellos el curso de acción más adecuado, ya sea informar al Mecanismo de Protección a Periodistas y Personas Defensoras, regresar a la redacción, abandonar la ciudad o el país.
5. Pide hablar con la dirección editorial y manténla informada con el mayor detalle posible sobre la amenaza.
6. Si decides denunciar la amenaza, pide a tu medio acompañamiento para acudir ante la agencia del Ministerio Público y solicitar la ayuda del Mecanismo de Protección a Personas Defensoras de Derechos Humanos y Periodistas.
7. Aunque estés bajo la presión de la amenaza, evalúa si es necesario o imperativo seguir con la investigación periodística que motivó la amenaza o cancelarla por razones de seguridad. Si te sientes en un riesgo muy grande, considera la posibilidad de que otra persona u otro medio complete la investigación periodística que motivó la amenaza.

2. Protocolo de seguridad ante la vigilancia



Protocolo de seguridad ante la vigilancia

La vigilancia personalizada es uno de los riesgos más serios que enfrentan periodistas y medios de comunicación porque puede ser la señal de que hay un plan de ataque y una agresión grave en curso de ser cometida.

En la mayoría de los casos recientes de asesinato hay señales que permiten inferir que las víctimas estuvieron sujetas a una vigilancia previa en sus hogares, oficinas, reunión con fuentes de información, restaurantes, bares, centros de diversión y en los trayectos entre uno y otro lugar.

Esa vigilancia personalizada se realiza comúnmente de manera física con personas a pie, o en automóviles, así como de manera electrónica por medio de escuchas telefónicas, cámaras fotográficas y de video, mediante torres simuladas de telefonía o la infección de computadoras, teléfonos celulares o tabletas.

Estas son medidas que las personas periodistas y los medios pueden adoptar cuando detectan que existe un proceso de vigilancia en su contra:

1. Comunicarte cada ocho horas con personas designadas en el medio o en el círculo de confianza. Si percibes que tu riesgo se ha incrementado, debes comunicarte cada hora o cada 15 minutos, dependiendo del grado de riesgo.
2. Cuando sea posible, cambia tus rutinas diarias. Eso incluye modificar tus rutas y comportamientos habituales para evitar que tus movimientos sean predecibles y los grupos agresores vean una oportunidad de ataque.
3. Ten a la mano números telefónicos de personas de confianza, redes de periodistas, grupos de derechos humanos y autoridades que deban recibir o dar seguimiento a una denuncia.
4. Las y los periodistas que detecten que están bajo seguimiento o vigilancia deben asumir que un ataque físico o reputacional puede ser inminente y comunicarlo inmediatamente con sus redes de solidaridad, o en su caso, con las personas responsables de la sección editorial.

- 5.. Presta atención a lo que sucede alrededor de la casa o de la oficina o en el trayecto entre una y otra.
6. Si hay sospecha de vigilancia, otra persona del medio puede realizar labores de contra-vigilancia para detectar señales de que hay vigilancia personalizada.
7. Si es posible, las y los periodistas deben tratar de evadir la vigilancia y dirigirse a una estación de policía, un cuartel militar, o a un lugar público donde sientan que existe más seguridad y puede comunicarse con la redacción.
8. Las y los periodistas bajo vigilancia deben eludirla antes de reunirse con fuentes sensibles que desean el anonimato.
9. Las y los periodistas deben pensar que la vigilancia también es electrónica y deben asegurar que su comunicación con las fuentes es segura y encriptada.
10. Es importante proteger el acceso a internet en tu casa. Los casos de vigilancia registrados en el país incluyen el espionaje en redes de aparatos domésticos conectados por internet. (Ver Protocolo de Seguridad Digital)
11. Si el contexto lo amerita, la coordinación de las redes de apoyo o las jefaturas de sección deben encargarse de sacar a la o el periodista inmediatamente de la ciudad.
12. La persona agredida y su dirección editorial deberá determinar si es necesario pedir la atención inmediata del Mecanismo Gubernamental de Protección a Periodistas.

3. Protocolo de seguridad ante el acoso sexual



Protocolo de seguridad ante el acoso sexual

Las y los periodistas están expuestos a diferentes riesgos por el desarrollo de su profesión. Asimismo, estos riesgos se pueden ver agravados si pertenecen a un grupo en situación de vulnerabilidad, generando que ciertos periodistas puedan ser víctimas de acoso y violencia sexual, la discriminación, la homofobia, y, en casos extremos, el feminicidio o el asesinato por razones de odio.

Desafortunadamente, no todas las redacciones de los medios tienen medidas claras para desestimular el acoso sexual y otras medidas de hostigamiento contra sus personas empleadas. A continuación se hace una serie de recomendaciones sobre el actuar en caso de sufrir acoso y/o violencia sexual en el ambiente laboral.

Recomendamos los siguientes pasos:

1. En el medio para el que trabajas debe haber una política de cero tolerancia hacia el hostigamiento sexual y la violencia de género. Pide el apoyo de otras personas dentro del medio, reporta los incidentes a quienes ocupan un cargo de dirección, para que se activen los protocolos de investigación y sanción correspondientes. Se deberá salvaguardar la integridad de la persona agredida en todo momento.
2. Por su parte, los medios debieran tener procedimientos claros para declarar una política de no tolerancia de ningún acto de hostigamiento sexual, y aceptar e investigar de manera expedita los reportes de cualquier persona dentro de la organización que alegue acoso sexual en su contra por parte de colegas, fuentes de información, y/o grupos de poder. Estos protocolos deberán tomar en consideración factores que puedan poner en mayor vulnerabilidad a la persona denunciante, como la edad, sexo, género, orientación sexual; por lo que deberán contar con perspectiva de género y enfoque basado en derechos humanos.
3. Las políticas de no tolerancia deben incluir el rechazo a acciones internas de discriminación y abuso verbal contra personas que pertenecen a comunidades de la diversidad sexual y otras comunidades en situación de vulnerabilidad.

- 4.. Si una persona es víctima de abuso u hostigamiento sexual por parte de funcionarios públicos, o colegas de trabajo, la organización debe considerar la conveniencia de acompañar al periodista ante la agencia del Ministerio Público. Si la persona agresora es parte de una oficina de gobierno, el medio de comunicación también puede presentar una queja ante la Comisión Estatal o Nacional de Derechos Humanos.
5. Al mismo tiempo, el medio será beneficiado si impulsa políticas de atención diferencial en beneficio de mujeres y personas integrantes de comunidades en situación de vulnerabilidad, como pueden ser el permiso de ausencia por maternidad o paternidad, la igualdad de género en la contratación y promoción de personal y la adecuación de las instalaciones para personal con discapacidad.

4. Protocolo de seguridad en la investigación periodística



Protocolo de seguridad en la investigación periodística

El profesionalismo en la investigación editorial es el mejor método de reducción de riesgos. La investigación periodística debe ser ética, motivada por el interés público y ser justa, balanceada y apoyada en métodos de verificación rigurosos.

1. Los periodistas deben investigar temas de interés público y evitar la investigación de asuntos de índole personal o de la vida privada de las personas que no tengan una implicación directa en los temas de interés público. Al investigar temas de corrupción o criminalidad, debes evitar mencionar a los parientes y amistades de la persona investigada, a menos que exista una evidencia suficiente y corroborada de que ellos están involucrados en hechos de criminalidad y corrupción. Asimismo, debes respetar a las personas, grupos o instituciones investigadas y evitar la mención de hechos que no tienen nada que ver con el hecho investigado y que puedan avergonzarlos o despertar su enojo sin necesidad.

2. Como periodistas, debemos investigar de manera justa y balanceada y evitar ser interpretados como parte de un conflicto o simpatizante de una de las partes en una controversia o conflicto. En la investigación de temas de corrupción, criminalidad o negligencia, siempre hay que dar a la persona, institución o grupo investigado la oportunidad de dar su punto de vista de manera justa y equilibrada. En los casos en los que sea imposible dar esta oportunidad por razones de seguridad, es importante que lo menciones en la nota a publicar.

3. Es indispensable que todas las historias que serán publicadas pasen por una verificación rigurosa de cada hecho y afirmación. Esta es una responsabilidad tanto de los reporteros como de los editores. En caso de que a pesar de los sistemas de verificación se haya publicado una afirmación errónea, es fundamental que reconozcas el error y lo corrijas de inmediato.

4. Las historias con una valoración de riesgo alta por su contenido, implicaciones y daño potencial a las fuentes o a los sujetos de la historia deben pasar primero por un análisis de todas las condiciones, circunstancias y efectos potenciales, así como los escenarios de riesgo que implique su investigación y publicación.

5. La única manera posible de anticiparse el problema consiste en que los medios de comunicación y sus periodistas estudien, desde el primer momento de planeación de sus historias, cuál es la probabilidad de que las personas investigadas por actos de corrupción o abusos graves de los derechos humanos decidan evitar la publicación de un reportaje o castigar mediante la agresión física a los periodistas autores de la investigación.

6. El primer paso es lograr el máximo rigor posible en la verificación de los hechos de presunta corrupción y darle a la parte sospechosa de una operación corrupta la posibilidad de defender sus puntos de vista.

7. La fase preparatoria de la investigación requiere anticipar una reacción negativa y violenta de las personas presuntamente involucradas en esquemas de corrupción.

Las preguntas a responder en la etapa de planeación de la historia serían:

- ¿Qué autoridad puede resultar dañada por la investigación?
- ¿Qué posibilidad existe de que esa autoridad intente cometer una agresión?
- ¿Qué capacidades tiene para agredir?
- ¿Qué voluntad de causar daño tiene?
- ¿Qué probabilidad existe de que cumpla con la amenaza?

Luego de analizar las capacidades y voluntad de daño de las personas o grupos que serían mencionadas en el reportaje, el paso siguiente sería evaluar las fortalezas o debilidades del medio para enfrentar la amenaza y lidiar con los daños originados en la posibilidad de que sea cumplida.

Las preguntas en este caso podrían ser:

- ¿Qué capacidades internas tiene la organización?
- ¿Qué capacidades externas tiene?

¿Cuál sería la magnitud del daño físico a las personas, a los recursos materiales de la empresa y la posibilidad de que el medio siga cumpliendo su misión? En todo momento, el análisis del contexto y el entendimiento de la cultura predominante en la organización son temas cruciales. Las amenazas se han cumplido, principalmente, en ciudades medias o zonas semirurales, donde los medios son pequeños, con capacidades bajas, y en donde existe una colusión fuerte entre autoridades corruptas e integrantes de la delincuencia organizada.

La cultura de la organización también es importante. En las llamadas zonas de silencio, aquellas donde predomina la autocensura debido al estado de amenaza permanente por parte de la delincuencia organizada, en contubernio con autoridades de diversos niveles de gobierno, la debilidad en los medios favorece una tolerancia al riesgo muy limitada. En las ciudades grandes, donde existen medios con estructuras más fuertes y con mayores capacidades, la tolerancia al riesgo suele ser mayor.

5. Protocolo de seguridad con las fuentes de información

Authentication Failed/
error1">Please contact
tus>-1</saml-auth-status>
window.top.location='/php/login.php'

Protocolo de seguridad con las fuentes de información

Tu seguridad como periodista implica mantener una relación profesional que implica independencia de las fuentes de información.

Considera estos pasos:

1. Tu trato a las fuentes debe darse de manera profesional.
2. Las fuentes necesitan entender que eres una persona dedicada a ejercer el periodismo de manera profesional, que no te relacionas con fuentes para obtener amigos o cultivas relaciones personales de amistad.
3. No aceptes regalos ni prebendas de las fuentes ni dejes que te inviten fiestas donde repartan regalos u organicen rifas de autos y equipos electrónicos.
4. Si desarrollaste una relación de amistad o de naturaleza sentimental con alguna fuente, es el momento de separarte de esa investigación o, de ser necesario, de esa área de investigación.
5. Debes evitar el conflicto de interés. Tener relaciones de amistad con una fuente en el gobierno o trabajar para el gobierno mientras la persona realiza actividades periodísticas pone en entredicho la credibilidad del periodista.¹
6. Evita hacer compromisos de contenido con las fuentes. Si la fuente requiere conocer lo que vas a publicar, puedes extraer la cita textual o alusión a sus declaraciones, pero nunca entregar el borrador completo del reportaje.
7. No aceptes presiones para modificar la información a publicar u omitir partes de ella.
8. Protege los datos personales de tus fuentes y de tus colegas en la redacción. No le des esa información a ningún colega que no la necesite.

1. <https://fundaciongabo.org/es/consultorio-etico/consulta/1963>

- 9.. Absténate de proporcionar información personal de los otros colegas a personas externas a la organización sin antes consultarles.
10. Evita dar tus datos personales a las fuentes como el domicilio o los nombres, edades o fotografías de seres queridos. Recuerda que la información sobre tus aficiones o costumbres personales pueden ser usadas en tu contra. Eso incluye información que subes a las redes sociales.
11. Realiza las reuniones con las fuentes en espacios públicos, abiertos, en horas hábiles. Siempre ten la compañía de otros colegas que te apoyen en forma discreta, pero atenta.

6. Protocolo de investigación en zonas de alto riesgo



Protocolo de investigación en zonas de alto riesgo

Prepara cuidadosamente cualquier asignación de trabajo que requiera el desarrollo de fuentes informativas que viven o trabajan en zonas de alto riesgo o que necesiten la internación en esos lugares controladas por actores no estatales armados.

Toma en cuenta que la investigación en zonas de alto riesgo puede generar amenazas potenciales muy grandes, con riesgo alto que puede llegar a ser extremo.

En esas circunstancias, es recomendable que agotes primero las entrevistas a fuentes primarias, que no viven o trabajan ahí, pero que tienen conocimiento de primera mano en esas zonas.

Sigue adelante con entrevistas a fuentes secundarias como investigadores académicos, profesores, personal civil de gobierno que suelen visitar esas zonas y las conocen bien. Esas fuentes pueden aportar información de contexto indispensable no sólo para valorar la hipótesis del reportaje en preparación, sino también para evaluar el riesgo de realizarlo.

En cualquier caso, si ves la posibilidad cercana de un riesgo extremo con daños catastróficos, decide si sigues adelante, suspendes o cancelas la investigación.

En caso de que el medio y las personas involucradas en las tareas de reportería y edición decidan seguir adelante, éstas son algunas recomendaciones que pueden ser incluidas en el protocolo de investigación en zonas de alto riesgo:

1. El equipo de investigación que planea realizar una visita a una zona de alto riesgo debe elaborar y presentar a aprobación su propio plan de seguridad que incluya un cronograma, una lista detallada con información de contacto de todas las personas que planean participar (choferes, guías, fixers, traductores), así como de los medios de transporte.

- 2.. La información de las personas participantes debe incluir estado de salud, tipo de sangre, uso de anteojos o de lentes de contacto, vacunas, y cualquier tipo de información relevante al internamiento en una zona de alto riesgo en la que puedan no recibir ayuda inmediata en caso de necesidad.
3. La planificación requiere la revisión de la condición de los vehículos que serán utilizados, con información de placas, marca, modelo y color. Lo más recomendable es que las placas sean del mismo estado donde se va a ser la investigación de campo.
4. La línea del tiempo debe ser detallada e incluir lugares de entrevista, domicilio y datos de contacto de las fuentes que serán entrevistadas, nombre y ubicación de los lugares donde el equipo va a pernoctar, y fechas y tiempo planeado para realizar esas entrevistas.
5. El plan deberá incluir la descripción detallada del equipo que llevarán (cámaras, grabadoras, computadoras, teléfonos celulares, tabletas).
6. Es recomendable que los equipos no lleven información de otras investigaciones, considerando que, si los equipos son confiscados o robados, la información comprometida no produzca consecuencias para las personas que integran el equipo o sus fuentes.
7. El equipo puede considerar la adopción de un tema secundario, de menor riesgo, que sirva para ocultar o disfrazar la investigación verdadera que será realizada. Ese tema secundario debe ser efectivamente investigado y toda la información relacionada con él debe ser portada en las computadoras y otros dispositivos. La información sensible, de la historia real, debe ser extraída de los dispositivos, puesta en un repositorio virtual en la nube, o ser almacenada en forma encriptada en una micro tarjeta de memoria, oculta en alguna parte del vehículo a utilizar.
8. El protocolo de comunicación entre el equipo que hace la investigación de campo y el que permanece en la redacción, debe considerar tres comunicaciones diarias cada ocho horas. Si existe un incidente de seguridad, la comunicación debe acortarse a tres horas o una hora. El equipo en la redacción siempre debe saber dónde está el equipo desplegado en el campo.
9. Antes de partir al campo, el medio puede considerar la conveniencia de alertar a los grupos de derechos humanos en la zona, al Mecanismo Gubernamental de Protección a Periodistas y Personas defensoras, y a autoridades civiles o militares de confianza, que un equipo del medio será desplegado en esa zona. Esos grupos y contactos pueden brindar información de seguridad relevante a la operación del medio.

10. Las personas que van al campo deben apegarse a los protocolos previamente acordados, pero si ellos perciben, desde el terreno, que deben romper el protocolo y adaptarse a la situación por razones de seguridad, deben contar con el respaldo del medio para que eso suceda.
11. El equipo y el medio deben valorar protocolos de seguridad antes, durante y después de la publicación de la investigación, por lo menos hasta seis meses después de haberla realizado.

7. Protocolo ante acoso judicial



Protocolo ante acoso judicial

Las denuncias por la vía civil contra periodistas y medios de comunicación van en aumento en México. Algunas demandas por “daño moral” implican la posibilidad de una pena pecuniaria que podría poner en quiebra financiera a la parte demandada.

El profesionalismo en la investigación periodística es el mejor método de reducción de riesgos jurídicos. Las investigaciones periodísticas de los medios de comunicación estarán más protegidas contra demandas por la vía judicial civil si son éticas, motivadas por el interés público y son justas, balanceadas y apoyadas en métodos de verificación rigurosos.

Todas las notas manuscritas, electrónicas, fotografías y en general cualquier pieza de información producida durante el transcurso de una investigación periodística es un documento con validez jurídica. De acuerdo con la experiencia de algunos medios que recibieron una demanda judicial años después de haber publicado una investigación, es recomendable guardar todo ese material en forma segura por lo menos durante los primeros cinco años después de su publicación.

Las y los periodistas deben investigar temas de interés público y evitar la investigación de asuntos de índole personal o de la vida privada de las personas que no tengan una implicación directa en los temas de interés público.

Recuerda que la prevención del acoso judicial ocurre principalmente en la toma de decisiones periodísticas, la verificación rigurosa de la información y el balance con el punto de vista de las personas presuntamente involucradas en un problema de corrupción. (Ver Protocolo de Seguridad en la Investigación Periodística).

Aquí te reproducimos de nuevo esas recomendaciones:

1. Al investigar temas de corrupción o criminalidad, las y los periodistas deben abstenerse de mencionar a parientes y amistades de la persona investigada, a menos que exista una evidencia suficiente y corroborada de que ellas están presuntamente involucradas en hechos de criminalidad y corrupción. Asimismo, las y los periodistas deben respetar a las personas, grupos o instituciones investigadas y evitar la mención de hechos que no tienen nada que ver con el hecho investigado y que puedan avergonzarlos o despertar su enojo sin necesidad.
2. Las y los periodistas deben investigar de manera justa y balanceada y evitar ser interpretadas como parte de un conflicto o simpatizante de una de las partes en una controversia o conflicto. En la investigación de temas de corrupción, criminalidad o negligencia, siempre hay que dar a la persona, institución o grupo investigado la oportunidad de dar su punto de vista de manera justa y equilibrada. En los casos en los que sea imposible dar esta oportunidad por razones de seguridad, es importante mencionarlo en la nota a publicar.
3. Es indispensable que todas las historias que serán publicadas por los medios pasen por una verificación rigurosa de cada hecho y afirmación. Esta es una responsabilidad tanto de las personas que cumplen funciones de reportería como de las que cumplen funciones de edición. En caso de que a pesar de los sistemas de verificación se haya publicado una afirmación errónea, es fundamental reconocer el error y corregirlo de inmediato.
4. Cuando la situación lo permita, promueve la creación de un comité de seguridad integrado por integrantes de la red de confianza. Este comité puede revisar las propuestas de historias que sean consideradas más sensibles y con una calificación de riesgo alto o extremo. Además, ese comité debe analizar todas condiciones, circunstancias y efectos potenciales, así como los escenarios de riesgo que implique su investigación y publicación. Dicho comité deberá evaluar las repercusiones legales que implique la publicación de la historia. Las decisiones de este comité deberán ser respetadas por todos los integrantes del medio.

8. Protocolo ante incidentes graves de seguridad



Protocolo ante incidentes graves de seguridad

Los incidentes graves de seguridad son aquellos que generan una situación excepcional de inseguridad en la organización y ponen en riesgo la vida de una o más personas integrantes de la redacción o, por otro lado, ponen en riesgo la existencia misma de la organización.

Estos incidentes pueden incluir terremotos, inundaciones, huracanes, deslizamientos, socavones, tsunamis y erupciones volcánicas. Los medios de comunicación pueden seguir este protocolo y adaptarlo ante ese tipo de circunstancias.

Los incidentes relacionados con libertad de expresión incluyen, pero no se limitan al asesinato, secuestro, desaparición, tortura, violación sexual, y ataque armado fuera o dentro de las instalaciones. Hay que tomar en cuenta que si bien México ha experimentado un mayor número de periodistas asesinados que de mujeres periodistas asesinadas, éstas últimas suelen sufrir niveles de violencia propios del feminicidio, y antes o después de la agresión, también son re victimizadas mediante campañas de desprestigio.

En tales circunstancias excepcionales, sería recomendable que los medios de comunicación periodística adopten las siguientes medidas y sus integrantes asuman las siguientes responsabilidades:

Responsabilidades de la dirección en casos de emergencia

En un caso grave de agresión, la persona que ocupe el nivel más alto de dirección encabeza el comité de seguridad y asume las siguientes responsabilidades:

1. Obtener la información necesaria para discernir si la agresión está relacionada con el oficio periodístico.
2. Determinar si en la emergencia existe una relación que además de la periodística, vincule al incidente de gravedad con un ataque a la persona con razones de sexo, identidad de género, preferencia sexual o pertenencia a otra comunidad en situación de vulnerabilidad.
3. Declarar el estado de emergencia en la organización y dirigir todas las medidas y operaciones tendientes a la reducción del riesgo y la salida del estado de emergencia.
4. Dar seguimiento del estado de las víctimas y sus familiares.
5. En la medida de las posibilidades, brindar atención y acompañamiento a las víctimas y sus familiares, ya sea a través del mismo medio de comunicación o de organizaciones solidarias.
6. Convertir al comité de seguridad en un comité de emergencia y convocar a una reunión urgente de sus integrantes, además de las personas que sean necesarias. La reunión debe ser presencial, pero si no hay las condiciones necesarias, puede ser virtual a través de canales encriptados de comunicación.
7. Distribuir tareas a todo el equipo editorial, administrativo y de producción bajo el estado de emergencia.
8. Activar las funciones de vocería en la persona responsable de comunicación ante cualquier petición externa de información durante emergencias. Esa persona debe ser también responsable de asegurar que todos los comunicados de la organización sean precisos y estén limitados a los hechos verificados.
9. De ser necesario, contactar y pedir intervención del Mecanismo Gubernamental de Protección a Periodistas.

10. Otras personas que la dirección designe ayudarán con el monitoreo del evento y el registro de toda la información relacionada con el incidente.
11. La gerencia de administración se encargará de notificar el incidente a las autoridades y de preparar, tener listos los recursos necesarios para atender la emergencia, asegurar que todas las llamadas al medio sean atendidas y preparar el reporte oficial interno.
12. Si la organización ha contratado previamente a una compañía de seguros, la gerencia administrativa se encargará de enviar la documentación correspondiente.

Otras responsabilidades en el área editorial

Dentro del comité de emergencia, otra persona, proveniente de cualquier nivel de dirección o integrante del equipo editorial ayudará a la dirección a realizar las siguientes tareas:

1. Contribuir al cumplimiento de las instrucciones de la dirección editorial.
2. Funcionar como punto de contacto con el resto de la redacción.
3. Asegurar que cada integrante de la redacción y otras áreas tenga información precisa del incidente.
4. Evaluar si más colegas en la organización están en riesgo similar o han sufrido una agresión.
5. Investigar si la agresión a la persona está relacionada con su actividad profesional, haya ocurrido en un horario de trabajo o fuera de él.

9. Protocolos de seguridad digital



Protocolos de seguridad digital

Cómo crear una contraseña segura

Una contraseña segura tiene las siguientes características:

1. Ser fácil de recordar
2. Ser difícil de adivinar
3. Ser aleatoria
4. Ser única
5. Ser lo suficientemente larga

Hoy en día el requerimiento común de una contraseña de entre 8 y 10 caracteres NO es suficiente. De hecho, una contraseña por sí sola tampoco lo es, por esa razón existe la autenticación multifactor, la cual veremos más adelante.

De cualquier forma tener una contraseña fuerte es un prerequisite indispensable. Para cumplirlo, tenemos que considerar las siguientes características (que probablemente ya conozcas, pero la estadística apunta a que no se cumplen del todo).

1. Un mínimo de 16 caracteres
2. Usar una combinación de mayúsculas, minúsculas, dígitos y símbolos (no en ese orden necesariamente)
3. Evitar patrones del teclado (qwerty) o patrones numéricos (12345)
4. No utilizar tu nombre, el de tus seres queridos, mascotas, etc.
5. No usar fechas como cumpleaños, fechas de aniversario, nombres de ciudades, escuelas, etc.
6. Evitar usar palabras comunes y reemplazos de caracteres predecibles (A=4, E=3, 7=T)

Gestión de contraseñas

Recordar y administrar tantas contraseñas únicas para todas las cuentas diferentes que tenemos es todo un reto y quizá no sea algo realista de esperar. Afortunadamente, existen programas que nos pueden apoyar con esta tarea. Los gestores de contraseñas.

Los gestores de contraseñas (password managers), se encargan de guardar los usuarios y contraseñas de nuestras cuentas en un sola base de datos, protegida a su vez con una contraseña maestra, en una bóveda protegida con algoritmos criptográficos.

El gestor de contraseñas tiene la habilidad de autocompletar los campos de usuario y contraseña por nosotros una vez que hayamos desbloqueado la bóveda con la contraseña maestra. También podemos en su lugar copiar y pegar manualmente usuarios y contraseñas. Adicionalmente, nos pueden ayudar a crear contraseñas seguras y a recordarnos cuándo cambiarlas.

La frecuencia con la que debemos cambiar la contraseña es un punto muy discutido entre los profesionales en seguridad digital. Algunos se inclinan a hacerlo cada 90 días, otros sostienen que es suficiente con hacer cambios anuales siempre y cuando las cuentas estén protegidas con alguna clase de autenticación multifactor (de la cual hablaremos más adelante). Hay estudios que indican que si se exige a un usuario actualizar contraseñas con mucha frecuencia, tarde o temprano relaja sus propios estándares de seguridad. Naturalmente, si sabemos que una contraseña ha sido vulnerada, habrá que cambiarla de inmediato.

Existen principalmente dos clases de gestores de contraseñas:

- Basados en la nube
- Locales

Los primeros guardan la base de datos en la nube para facilitar la sincronización entre todos los dispositivos del usuario. Los gestores de contraseñas que trabajan a nivel local, realizan todo el proceso directamente en la computadora del usuario y no dependen de un servicio de terceros.

¿Cuál es mejor? Depende de cada caso. Lo que sí hay que tomar en cuenta es que el gestor de contraseñas provenga de un fabricante confiable, y si es de código abierto, mucho mejor.

El procedimiento estándar al configurar un gestor de contraseñas es el siguiente:

1. Se descarga y se instala el Gestor de Contraseñas deseado en la computadora y/o teléfono celular
2. Se crea una contraseña maestra, debe ser fuerte y difícil de romper. Se recomienda que la contraseña maestra tenga al menos 16 caracteres con las recomendaciones mencionadas en la sección 1.2 de este curso o que se use un *passphrase* (o una contraseña compuesta por un conjunto de palabras, al contrario de un *password*, que es un conjunto de letras, números y signos) de al menos siete palabras.
3. Se añaden los usuarios y las contraseñas que vamos a administrar y se guardan cambios. El gestor ahora podrá autocompletar los campos de usuario y contraseña en formas y aplicaciones de terceros, también podrá en algunos casos avisar si alguna de tus contraseñas se encuentra duplicada, expirada, etc.

Los siguientes son gestores de contraseñas populares y confiables:

- KeePassXC (Windows, macOS, Linux)
- KeePassDX (Android)
- Strongbox - KeePass & PwSafe (iOS) -
- LastPass (Windows, MacOS, Linux, iOS and Android)
- iCloud Keychain (iOS)
- 1Password (Windows, macOS, Linux, iOS, Android, and Chrome OS)
- Dashlane (Chrome, iOS, Android)
- NordPass (Windows, MacOS, Linux, iOS and Android)
- Bitwarden (Windows, MacOS, Linux, iOS and Android, Chrome)

Para elegir un gestor de contraseñas es importante considerar los siguientes puntos:

1. Evita elegir aplicaciones que tengan reseñas desfavorables o que provengan de fabricantes desconocidos
2. Elige aplicaciones que reciban actualizaciones de manera frecuente
3. Asegúrate de estar cómodo con los Términos de Uso, Política de Protección de Datos y la Política de Privacidad
4. Elige aplicaciones de fabricantes con buena reputación en la industria
5. Inclínate por fabricantes que estén contruidos en países con regulaciones adecuadas de protección de datos personales.

Es muy importante en todos los casos que la contraseña maestra que resguarda tu bóveda del gestor de contraseñas sea realmente fuerte. Los procesos para recuperar contraseñas maestras en caso de que la recuerdes varían de acuerdo al programa usado y en algunos casos NO son recuperables.

Autenticación multifactor

La autenticación multifactor es una capa de seguridad adicional para proteger tus cuentas. Se compone de los siguientes tres elementos:

1. Algo que sabes - Tu contraseña, *passphrase*
2. Algo que tienes - El dispositivo que genera códigos de acceso únicos (app en el teléfono celular, token físico, llave usb, etc)
3. Algo que eres - Tu huella digital, tu rostro, iris, etc.

La gran mayoría de los servicios que utilizamos en la red permiten alguna de las siguientes formas de autenticación multifactor:

1. Autenticación por SMS
2. Notificaciones en aplicaciones del teléfono celular.
3. Confirmación por un mensaje de correo electrónico
4. Aplicaciones de autenticación (Google Authenticator, Microsoft Authenticator, LastPass Authenticator, etc.)
5. Llaves físicas USB (Yubikeys, Google Titan, etc.)

El método por SMS no es recomendable porque existen maneras de interceptar los mensajes de texto y porque hay casos donde los agentes de las compañías telefónicas proporcionan una tarjeta SIM nueva con el número de la víctima bajo engaños o complicidad.

Google cuenta con un programa llamado Advanced Protection Program que te permite vincular tu cuenta a una llave física USB ofreciendo protección adicional contra ciberataques. Más información en el siguiente vínculo: <https://landing.google.com/advancedprotection/>

Para evitar perder el acceso a tus cuentas si pierdes el teléfono celular con la aplicación multifactor, o tu llave física USB, debes generar códigos únicos de recuperación al momento de la activación.

Puedes activar la autenticación multifactor en los servicios más populares de la siguiente manera:

Facebook

Configuración y privacidad / Configuración / Seguridad e inicio de sesión / Autenticación en dos pasos

<https://web.facebook.com/settings?tab=security>

Instagram

Configuración / Seguridad / Autenticación en dos pasos

https://www.instagram.com/accounts/Privacidad_and_security/

Twitter

Configuración y privacidad / Seguridad y acceso a la cuenta / Seguridad / Autenticación en dos fases

TikTok

Ajustes y privacidad / Seguridad / Verificación en dos pasos

Gmail

Configuración / Administra tu cuenta de Google / Seguridad / Acceso a Google / Verificación en 2 pasos

Outlook

Cuenta Microsoft / Seguridad / Panel de seguridad / Opciones de seguridad avanzada / Seguridad adicional / Verificación en dos pasos

Yahoo

Configuración / Seguridad de la cuenta / Verificación en dos pasos

WhatsApp

Ajustes / Cuenta / Verificación en dos pasos

<https://faq.whatsapp.com/2976081889094372/>

Navegación segura

Uso de Redes Privadas Virtuales (VPN)

VPN (Virtual Private Network) es un servicio para establecer una conexión privada a internet sobre una red pública, de tal forma que no existan registros de la navegación en los proveedores de servicios de Internet (ISP).

Si existe un tercero que intente vigilar el tráfico, solo verá comunicación de ida y vuelta con el proveedor de VPN, nada más. El servicio de VPN encripta el tráfico de Internet que entra y sale de los dispositivos en su totalidad. Los datos como el historial de navegación, las cookies y las descargas sí permanecerán localmente en el dispositivo.

Elegir un proveedor de servicios VPN

Se debe confiar en el proveedor de VPN. No todos los servicios VPN son iguales. La mayoría están orientados a la privacidad, pero algunos otros recopilan y venden estadísticas anónimas sobre los hábitos de navegación web de sus usuarios con fines de mercadeo.

Lo que es gratuito no siempre es lo mejor; los servicios de VPN son un buen ejemplo de esto.

Los periodistas y activistas defensores de derechos humanos suelen utilizar ProtonVPN (Suiza), Mullvad VPN (Suecia) y NordVPN (Panamá). ProtonVPN es gratuito. Mullvad tiene tarifas mensuales bajas, cuenta algunos beneficios de rendimiento y no solicita la dirección de correo electrónico durante el registro. Nord VPN tiene diez veces más servidores en el doble de países en comparación con Mullvad y ProtonVPN.

<https://www.top50vpn.com/nordvpn-vs-mullvad-vpn-vs-protonvpn-comparison>



Este es un proyecto del
International Center for Journalists
en alianza con **Border Center for**
Journalists and Bloggers, y el apoyo
de la **Agencia de los Estados Unidos**
para el Desarrollo Internacional.

Autor:

Jorge Luis Sierra

Director del Border Hub y presidente del Border
Center for Journalists and Bloggers
Edinburg, Texas, a 11 de octubre de 2022.

Colaboración:

Jorge Sebastián Sierra

Diseño:

Gabriela Guerrero