MANUAL DE SEGURIDAD HOLÍSTICA PARA PERIODISTAS DE CUBA

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

PRÓLOGO

Ejercer y defender la libertad de expresión en Cuba es peligroso. Las y los periodistas de la isla son víctimas constantes de intimidaciones, agresiones físicas, interrogatorios ilegales, detenciones arbitrarias, allanamientos de oficinas y casas, confiscación de equipo e información, ataques digitales, intercepción de comunicaciones, limitaciones de viaje e incluso encarcelamiento.

Las agresiones contra periodistas buscan generar miedo. Tienen como objetivo imponer censura a medios y autocensura a periodistas. Aunque las agresiones no se pueden evitar, sí es posible reducir el nivel de vulnerabilidad y daños. Para eso es necesario diseñar protocolos de protección que incluyan conocimientos y herramientas holísticas.

El objetivo de este manual es fortalecer las capacidades de prevención, autoprotección y seguridad para ejercer cualquier actividad informativa en el contexto adverso cubano. Este manual contiene información y herramientas que cada medio o periodista puede adaptar de acuerdo a sus necesidades y circunstancias. El contenido pretende ser un documento vivo, sujeto a modificaciones a medida que cambia el contexto o que se conozcan nuevas formas para minimizar vulnerabilidades.

En este documento se abordarán cuatro temas principales:

Este manual ofrece una visión integral, multidimensional y contextualizada de los riesgos y amenazas a los que se enfrentan los y las periodistas en Cuba. Aborda los riesgos desde el punto de vista físico, legal, psicológico y digital. De esta manera se pueden promover estructuras de trabajo seguras, y además, es posible fomentar acciones de cooperación entre periodistas y medios que deriven en denuncias de las agresiones ante instancias internacionales.

Los diferentes apartados de este manual responden, de manera secuencial, a distintas necesidades que las y los periodistas tienen antes, durante y después de realizar su trabajo. Por lo tanto, resulta útil en cualquiera de esas etapas.

ÍNDICE

REGRESAR AL ÍNDICE

I ANÁLISIS INTEGRAL DEL CONTEXTO

El riesgo es el común denominador de la práctica periodística. La seguridad depende de las precauciones que se tomen. Como la mayoría de los ataques a la prensa son imprevisibles, es necesario trabajar en los mecanismos de prevención.

"Prevenir es anticipar. En el ejercicio periodístico son claves para anticiparse: el uso adecuado de las palabras, el entrenamiento, la formación profesional y el respaldo del medio de comunicación **(Article 19 Oficina de México y Centro América, p.7)**"

El primer paso es realizar un *Análisis Integral del Contexto*, que implica: la construcción de un **modelo de amenazas**[1] un **mapeo de riesgos**[2] y un **análisis de riesgo**[3].

Cada vez más periodistas ejercen su profesión como *freelancers*, es importante que en un contexto adverso generen lazos solidarios con otros trabajadores independientes quienes podrían ser el primer apoyo en caso de peligro. Asimismo, en un plan de prevención no puede dejar de haber una seguridad organizacional del medio que contrata a las y los periodistas.

REGRESAR AL ÍNDICE

1.1 ¿Qué es la seguridad organizacional?

Generalmente se habla de la seguridad de las personas que trabajan en situaciones y temas críticos o peligrosos pero pocas veces se menciona la responsabilidad de la organización a la que estas pertenecen, aunque sea de manera ocasional. Y menos aún se habla de la relevancia de pertenecer a un grupo profesional o gremio.

Las direcciones de los medios de comunicación deben responder ante sus colaboradores por cualquier eventualidad derivada de su trabajo. Es responsabilidad de la organización tener planes de emergencia, proveer de herramientas y estrategias que aumenten la seguridad de su equipo periodístico, acercar o facilitar la capacitación necesaria para aumentar la seguridad tanto en términos profesionales como físicos y emocionales.

Además, las organizaciones deben ayudar a la recuperación del o la periodista en caso de haber sufrido una situación traumática. Está demostrado que los grupos organizados son menos vulnerables: es importante conocerse, hablarse y apoyarse.

La seguridad en las organizaciones contempla que cuenten con planes de seguridad y contingencia, que tomen en cuenta el bienestar físico y psico-social de sus empleados, que los inmuebles sean seguros, y que las personas tengan las herramientas de trabajo y conocimientos adecuadas al contexto.

La primera sugerencia es que las direcciones de los medios de comunicación sean conscientes de los peligros y ayuden a incrementar la seguridad de cada integrante de su equipo de trabajo. Cada periodista debería leer manuales como éste que ayuden a su seguridad o acudir a un curso o asesoría sobre seguridad holística. Además, los reporteros y las reporteras tienen el derecho de participar en la planificación de la estrategia de seguridad en su medio o equipo periodístico.

A las y los periodistas freelance se les sugiere formar redes de apoyo que estimulen coproducciones y apoyo mutuo. Además, es importante socializar experiencias: denunciar, establecer patrones, prevenir. A continuación, se presentan algunas herramientas fundamentales para identificar los riesgos que están presentes en el ejercicio del periodismo.

No obstante, cada persona debe ser responsable de su seguridad. Tanto las amenazas como las medidas preventivas deben ser tomadas en serio.

LA SEGURIDAD ES UNA
RESPONSABILIDAD **PERSONAL**

1.2 Modelo de amenazas

La evaluación de amenazas es un conjunto de herramientas metodológicas diseñadas para realizar un mapeo de los posibles actores involucrados, las amenazas que podrían concretarse y su probabilidad de ocurrencia.

El resultado de esta etapa permite tomar medidas de prevención o reducción de afectaciones.

La seguridad desde cualquier punto de vista busca reducir el riesgo a la integridad de una persona, de una organización o de un recurso (tangible o intangible). Partiendo de lo anterior, podemos definir a una amenaza como un evento potencial o real, propiamente indeseable y que puede ser malicioso.

Para que una amenaza exista deben combinarse dos factores: la probabilidad del evento y su impacto.

En conjunto estos dos factores deben ser lo suficientemente importantes para que se necesite tomar medidas. A la combinación de la probabilidad del evento y su impacto se le conoce como riesgo.

A partir de conocer la existencia de una amenaza es posible realizar acciones para minimizar las afectaciones. Para comenzar a enlistar las posibles amenazas se recomienda responder de forma concreta y priorizada las siguientes preguntas:

¿?

¿Existe alguien que tenga algún interés en hacerme/hacernos daño?
¿Por qué?
¿Cómo podría afectarnos?
¿Qué tantos recursos tienen para lograrlo?
¿En el pasado nos ha hecho daño?

El conjunto de respuestas identificadas por cada actor constituye la certeza o no de una amenaza posible. Las amenazas deben ser documentadas periódicamente y observadas bajo diferentes criterios de contexto y tiempo. Cada amenaza tendrá que ser evaluada de acuerdo a los tipos de riesgos que representa (violencia física, hostigamiento, económica), la probabilidad de que suceda y su impacto en las personas y en el medio.

CONSEJO

Para más información sobre Modelo de Amenazas puede consultarse: "Manual de Seguridad para Defensoras y Defensores de Derechos Humanos de FrontLine Defender"
Allí se elaboran una serie de ejercicios complementarios para identificar amenazas.

https://www.frontlinedefenders.org/es/file/1544/download?token=b96Ch9yy

1.3 Mapeo de riesgos

El segundo paso es el **mapeo de riesgos**, la actividad que nos permite detectar los diversos riesgos existentes a partir de la información obtenida de identificar la existencia de una amenaza.

Para clarificar la existencia de riesgos, se recomienda realizar una evaluación personal o grupal de todos los aspectos posibles que representen un riesgo. Para ayudar a realizar este ejercicio, se recomienda responder con alto nivel de detalle las siguientes preguntas:

¿Qué quiero proteger?

¿De qué lo quiero proteger?

¿De quién me quiero proteger?

¿Qué tanto necesito protegerlo?

¿Qué tan fuertes pueden ser las consecuencias de no hacerlo?

¿Cuánto esfuerzo estoy dispuesto a invertir para prevenir el riesgo?

RECUERDA

Estas preguntas deben responderse por cada amenaza detectada. Es muy importante en esta etapa contar con una descripción lo más detallada de los riesgos. Tener mayor información sobre las prioridades a atender para reducir la amenaza nos hará tomar mejores decisiones en favor de la persona, el equipo de trabajo, los colegas que pueda haber involucrados y el medio para el que se está trabajando.

NO OLVIDAR

- El contexto es dinámico y por lo tanto debe ser analizado y actualizado de manera sistemática para detectar amenazas y generar acciones preventivas.
- Incluir todos los cambios (positivos o negativos) por mínimos que parezcan con el fin de hacer un análisis integral de cualquier situación de riesgo.

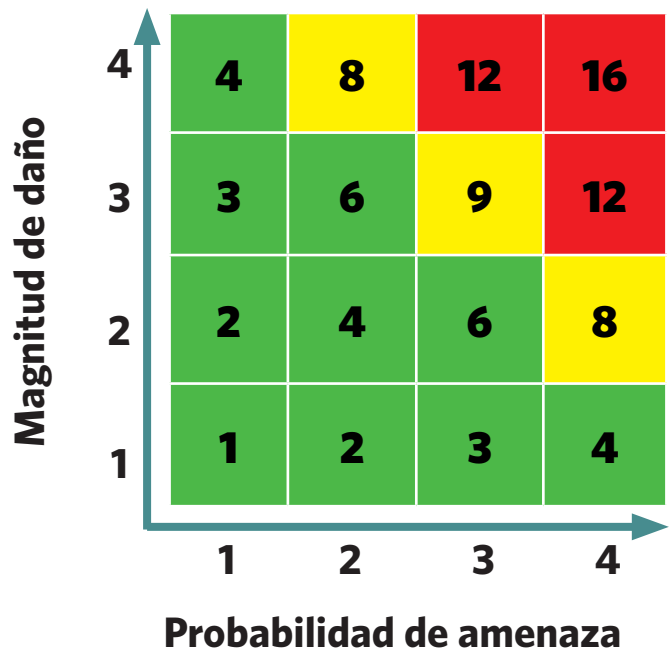
1.4 Análisis de riesgo

El análisis de riesgo tiene como propósito enfocar los esfuerzos en protegernos de aquellas amenazas con mayor probabilidad de ocurrencia.

Una de las herramientas más utilizadas para realizar un análisis de riesgo es la **matriz de riesgo**. Ésta herramienta permite calcular los riesgos basándose en la magnitud del daño posible y la probabilidad de que se concrete. La matriz se elabora utilizando una gráfica de dos dimensiones: en el eje x (horizontal) se representa la probabilidad de amenazas y en el eje y (vertical) se representa la magnitud de daño. En ambos ejes mientras más lejos se encuentre del origen, mayor será el riesgo.

El riesgo de la amenaza se calcula de la siguiente forma:
riesgo = probabilidad de amenaza * magnitud de daño (impacto)

Riesgo = probabilidad de amenaza * magnitud de daño



Alto Riesgo (12-16)
Medio Riesgo (8-9)
Bajo Riesgo (1-6)

Valores:
1 = Insignificante
2 = Baja
3 = Mediana
4 = Alta

REGRESAR AL ÍNDICE

Para asignar valores se pueden tomar en cuenta algunas cuestiones. El riesgo es la probabilidad de que una amenaza se concrete. Ese riesgo se obtiene sometiendo el listado de amenazas a una evaluación totalmente subjetiva de que ésta suceda en un tiempo determinado:

1. **Poco probable**
2. **Probable**
3. **Probable pero no inminente**
4. **Altamente probable /inminente**

El Impacto (medido en magnitud). Se puede analizar el daño que puede causar una amenaza determinada a una persona u organización, dando un valor numérico a cada parámetro:

1. Impacto Nulo: no se percibe riesgo alguno, no existen amenazas ni brechas de seguridad.
2. Impacto Bajo: pueden existir brechas de seguridad informática. Desmoviliza, pero no daña a la persona o medio.
3. Impacto Medio: existe posibilidad de robo de información, amenazas y daños físicos menores. A largo plazo puede provocar desarticulación de la organización.
4. Impacto Alto: hay robo de información, existen amenazas físicas y psicológicas, daños físicos mayores.
5. Impacto Total: Riesgo de muerte, encarcelamiento, tortura, secuestro o desaparición.

Aunque este resultado se expresa de forma numérica el objetivo fundamental del ejercicio es que el valor asignado represente (en un criterio individual o colectivo) la seriedad de la amenaza que puede enfrentar un reportero o una reportera. Esa amenaza es en cuanto a diferentes eventos o circunstancias, generando una herramienta fundamental para la toma de decisiones en el antes, durante y el después.

TIP

Se puede consultar un ejemplo de análisis de riesgo en el Anexo I

1.5 Registro de incidentes

El registro de incidentes de seguridad es una actividad clave para analizar los patrones y la sistematicidad de las agresiones en contra de las personas o las organizaciones. Aunque un incidente parezca insignificante o pequeño, su registro permitirá hacer un análisis eficaz del contexto y permitirá diseñar una estrategia de prevención o disminución del impacto de las agresiones.

Un registro de incidentes permite generar expedientes de agresiones: debe contener la información de la agresión y posibles acciones a tomar en cuenta. Aunque hay muchos modelos, en el **Anexo II** encontrarás un ejemplo de registro de incidentes.

NO OLVIDAR

La mejor herramienta de seguridad es la prevención:

- Monitorear el contexto
- Identificar las amenazas
- Determinar los riesgos
- Conocer tus límites
- Tener un plan de acción
- Registrar los incidentes

II SEGURIDAD HOLÍSTICA

2.1 ¿Qué es?

La seguridad holística es aquella que enmarca tres grandes pilares: seguridad física, psicológica y digital. Los tres pilares interactúan con ambientes específicos tanto personales como laborales. También se debe tomar en cuenta el marco jurídico del país donde se realiza el trabajo periodístico.

Antes de hablar de seguridad tenemos que identificar las fuentes de vulnerabilidad para las y los periodistas en la región, como se muestra en la siguiente figura.

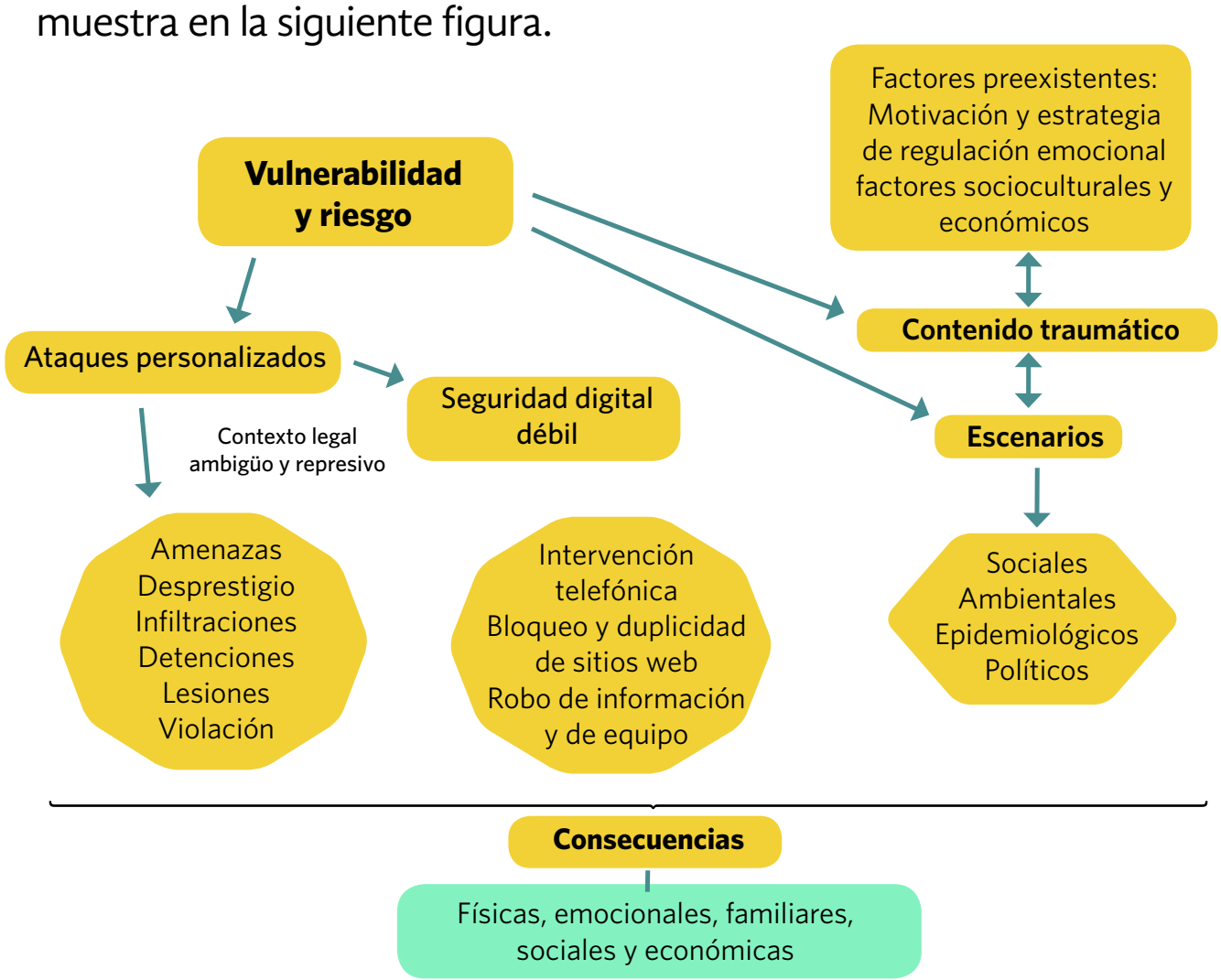


Figura 1. Modelo de vulnerabilidad y riesgo de las y los periodistas en la región (Segarra-Pérez y y Velázquez-Cardoso, 2018).

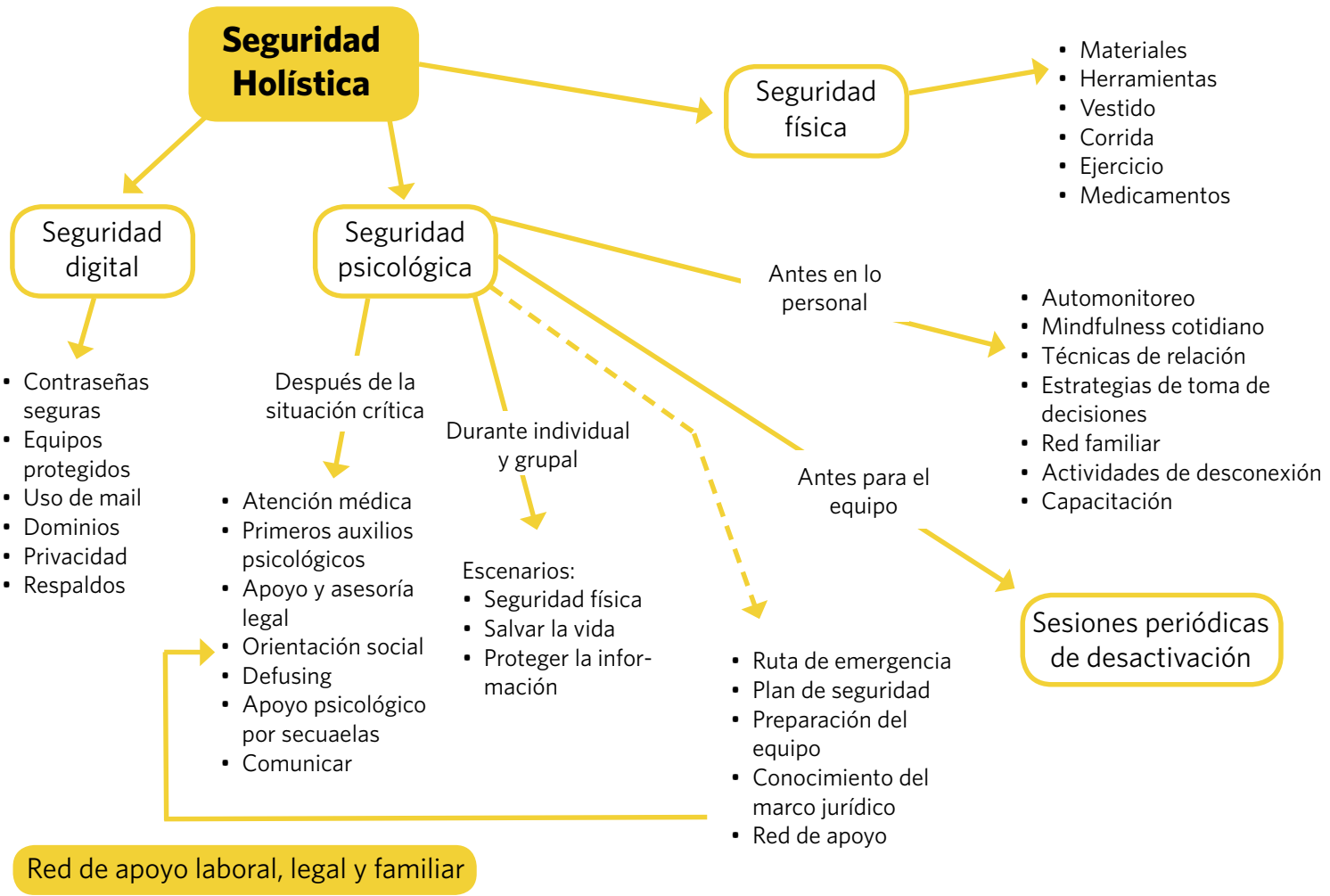


Figura 2. Modelo de seguridad holística (Segarra-Pérez y Velázquez-Cardoso, 2018).

Tomando en cuenta el contenido de los dos modelos que se presentan en la imagen se pueden abordar los diferentes escenarios que viven los equipos de periodistas de forma más amplia, proporcionando herramientas para realizar su trabajo de forma segura.

Enseguida se presentan los tres apartados fundamentales a tomar en cuenta en un equipo de periodistas o de forma individual para aminorar los riesgos.

2.2 Seguridad física

Cuando se va a hacer una cobertura o cuando se haya confirmado una reunión con alguna fuente y/o visitar el lugar de los hechos se tendrán que seguir protocolos de acción según el tipo de tema que se esté cubriendo. En la mayoría de los casos, es más exigente en términos de seguridad cubrir historias sobre corrupción que sobre cultura. En seguida se presentan diferentes medidas a tomar en consideración.

2.2.1 Preparación para una cobertura en terreno / viaje por parte de un equipo

i. Reunión de equipo de trabajo

En esta junta se recabará la información del evento, acciones a tomar y tipo de riesgos que pueden afectar el viaje. La reunión permitirá planear en términos de seguridad y beneficiará la cobertura periodística y la distribución del trabajo.

De acuerdo al contexto en el que se trabaje se debe considerar si la reunión para tomar decisiones debe ser presencial o si se puede hacer vía remota por medio de un canal de comunicación seguro (ver la sección de Seguridad Digital). En la reunión deben participar solamente las personas necesarias.

ii. Comunicación

Se debe establecer con quienes se sostendrá la comunicación, cada cuánto y cómo va estar reportando a la oficina el/la periodista o el equipo de periodistas en terreno. Es importante delimitar cuándo debería haber una preocupación como medio si se pierde comunicación con el equipo o con el o la periodista que realiza la cobertura, y qué hacer en caso de no obtener respuesta o de ser imposible localizarlo. Se sugiere que mínimo dos contactos (uno personal y otro profesional) estén informados del itinerario del o la periodista del equipo (dónde vas a estar, con quién, cuáles van a ser las vías de transporte, y a qué hora).

Y en el caso de viajes determinar una persona encargada del monitoreo de la llegada y salida del equipo y qué medidas tomar en caso de detenciones o desaparición.

iii. Contexto

Una vez confirmada la noticia, así como su cobertura, se deberá reunir toda la información relevante al evento:

1. Ubicación
2. Orografía
3. Clima de 24 a 72 horas
4. Comunicación
5. Accesos
6. Rutas de transporte
7. Estadía
8. Refugio
9. Equipo necesario
10. Regreso
11. Rutas de salida
12. Posibles incidentes
13. Rutas alternas de acción ante incidentes
14. Regreso
15. Reunión de desactivación (Defusing)
16. Información recabada durante la cobertura

iv. Equipo y materiales

El equipo puede variar según la región, medio y evento específico. A continuación, enlistamos un equipo básico que deberá adaptarse de acuerdo a la cobertura y el contexto:

a) Equipo de trabajo

- Cámara y lentes
- Equipo de limpieza para cámara
- Tarjeta extra de memoria para cámara, USB y disco duro externo si es necesario.
- Celular (equipo comunicación)
- Bolsas de plástico resellables o su equivalente para proteger el equipo
- Grabadora de voz
- Batería extra para celular, cámara y grabadora
- Celular extra (modelo básico, solo para llamadas)
- Cargadores para los equipos

b) Equipo de primeros auxilios

- Gasas
- Antiséptico (agua oxigenada, alcohol, yodo...)
- Cabestrillo (tela en forma de Triángulo Escaleno con base de 1 metro)
- Venda
- Antiácido líquido (o algún tipo refresco o leche) para gas lacrimógeno
- Crema para quemaduras
- Analgésicos
- Suero oral (líquido o en polvo)
- Repelente insectos (el shampoo para pelo sirve como repelente en casos de emergencia y no contar con un repelente adecuado)
- Gotas para ojos
- Cinta adhesiva
- Antihistamínicos
- Medicamento para diarrea
- Termómetro
- Bloqueador solar
- Torniquete

c) Maleta personal

- Agua y recipiente para agua
- Cambio de ropa (en bolsa hermética)
- Alimentos secos o enlatados
- Equipo para lluvia
- Lámpara
- Radio
- Toallas húmedas
- Tampones o toallas femeninas
- Condones
- Baterías y pilas externas para celular (nunca dejar celular descargado)
- Cargadores
- Dinero suficiente para cubrir necesidades básicas y transporte a casa en caso de imprevistos
- Lista de teléfonos de emergencia / impreso y guardado en lugar seguro
- Sombrero/lentes de sol
- Lentes armazón o de contacto extra de prescripción (en caso de no contar con unos extras una lupa puede ser una opción para la lectura)

TIP

Los medios de comunicación pueden tener listas de verificación para preparar los materiales y equipos de acuerdo a las necesidades de la cobertura

NO OLVIDAR

¡Tener un kit básico de primeros auxilios en la oficina!

Cada cobertura o reportaje tiene características únicas. El o la periodista y su medio deberán llevar a cabo el modelo de amenazas y preparar el equipo y materiales necesarios para poder realizar una cobertura segura. Recuerda siempre tomar en cuenta las condiciones físicas y psicológicas del equipo de periodistas. Independientemente de si se trata de una cobertura local, en el interior del país o el extranjero es recomendable que cada medio o periodista cuenten con una "hoja de vida" o ficha de datos personales.

Información mínima que debe incluir una ficha personal:

Nombre, teléfono o contacto, contacto de emergencia, teléfono de contacto de emergencia, tipo de relación, información médica, tipo de sangre, alergias, padecimientos crónicos, medicamentos especiales.

Se recomienda que cada redacción elija a una persona del equipo como contacto de monitoreo del o de la periodista o equipo de periodistas que se encuentra en el terreno. Es un muy importante que el protocolo de comunicación sea respetado (horas de llamada, localización, etc).

Al regreso de la cobertura o reportaje el equipo en terreno o el/la periodista deberá curar, en caso de existir, sus heridas físicas y psicológicas, y de ser posible hacer un informe de la experiencia. El intercambio de opiniones con todo el equipo de trabajo puede generar acciones preventivas en futuras coberturas.

NO OLVIDAR

- Seguir el Modelo de Amenazas
- Preparar todo de acuerdo a las necesidades de la cobertura
- Seguir el protocolo de seguridad
- Mantener el sentido común y la calma
- Evaluar siempre si es necesario abandonar el reportaje o cobertura por los riesgos

TIP

- **Viaja con los dispositivos que contengan menos información, si es posible con equipo exclusivo para la cobertura en terreno y totalmente limpio de datos.**
- **Revisa tus herramientas informáticas.**
- **Ten un protocolo de comunicación.**

2.2.2 Tipos de escenarios

I. Escenarios sociales

Son aquellos que involucran interacciones con terceras personas o multitudes.

a) Manifestaciones y disturbios

"Las y los periodistas que cubren protestas o disturbios civiles son susceptibles a ser agredidas/os tanto por civiles como por policías, y en algunos casos por integrantes de los dos grupos al mismo tiempo **(Article 19 Oficina de México y Centro América, p.22)**".

Para la mayoría de los medios es indispensable cubrir este tipo de eventos. Aquí se enlistan algunas recomendaciones generales.

Antes:

- Mapear y conocer la zona (identificar rutas de evacuación y zonas seguras para ti)
- Establecer un protocolo de comunicación:
  - Establecer horarios de contacto para reportarse con la redacción
  - Establecer un punto de reunión en caso de que te separes o pierdas a tu equipo
- Trabajar en equipo o en binomios
- Tomar precauciones para minimizar el riesgo de robo (una mochila pequeña que se ajuste al cuerpo con un kit de primeros auxilios, comida y agua. El equipo voluminoso puede ser una desventaja para retirarse del lugar en medio de multitudes)
- Llevar ropa de telas naturales (las sintéticas son inflamables)
- Llevar calzado cómodo (es preferible que sean cerrados – actúan como protector-)

Durante:

- Caminar a los costados del grupo de manifestantes ya que permite mayor movilidad
- Nunca interponerse entre las autoridades y el grupo de manifestantes
- Conforme se avance, tratar de realizar un mapeo mental de la zona para tener rutas de contingencia
- Poner atención a los objetos arrojados y no acercarse a ellos (podrían ser cocteles molotov, gas lacrimógeno, explosivos caseros u otros)
- Localizar y alejarse de personas potencialmente peligrosas (armadas, encapuchadas)

- Si hay que correr, hacerlo en sentido contrario al grupo de manifestantes o los autos
- Gritar “fuego” es una buena estrategia para llamar la atención
- Evitar lugares solitarios y de difícil acceso

b) Agresiones físicas y con armas punzocortantes

- Si cae o se tropieza tratar de incorporarse cubriendo la cara con las manos y las costillas con los brazos y codos.
- Si no es posible incorporarse, ponerse en cuclillas en posición fetal cubriendo cabeza, cara, costillas y las piernas cerradas.
- En caso de detención, y si no existe una amenaza a la vida, es preferible no resistir ya que con la adrenalina del momento esto puede provocar más agresiones.
- Si la agresión es por personas de la manifestación una vez que sea posible incorporarse es importante buscar un lugar seguro.

1. En algunas ocasiones la gente puede cargar objetos para golpear o herir como son llaves, varillas, cuchillos, palos y piedras, si es el caso lo mejor es alejarse del lugar.
2. Cuando una persona es alcanzada por alguno de estos objetos y hay laceraciones o cortes profundos, la solución es alejarse a un lugar seguro mientras hace presión en la herida con la mano poniendo mayor presión en los orificios de entrada y salida.

3. Una vez en zona segura, la persona puede improvisar un torniquete o poner presión con el cabestrillo de tela que lleva en su equipo, una vez realizado esto tendrá que trasladarse de manera inmediata a un centro médico, hospital o buscar asistencia de personal médico profesional.
4. Después de un ataque de esta índole la víctima puede llegar a presentar síntomas de estrés agudo y estrés postraumático. Es esencial recibir la atención adecuada en estos casos, caso contrario la persona puede tener secuelas de por vida.
5. Contactar al medio de comunicación como se estableció en el protocolo de cobertura para el evento.

CONSEJO

En Venezuela, durante la cobertura de protestas un grupo de periodistas decidió llevar tarjetas impresas con sus datos generales y número de emergencia. Ante una inminente detención en un lugar público, las y los periodistas lanzaban las tarjetas por los aires para que alguna persona la recogiera y avisara a su número de contacto. Se puede incluir un mensaje de alerta para que la persona que obtenga la tarjeta tome en cuenta la importancia de hablar al número de emergencia.

c) Citación oficial

Siempre que una persona sea notificada que debe presentarse ante alguna autoridad es normal que experimente diferentes emociones como el miedo, ansiedad, ira.

"La amenaza tiene como fin amedrentar, atemorizar, quitar del medio a quien afecta intereses. Se instala en la cabeza. Y muchas veces, si la persona no está preparada para afrontarla, logra su propósito de paralizar e incluso puede tomar decisiones equivocadas **(Prensa y democracia, 2009, p.11)**"

Es probable que la persona no pueda dejar de acudir a la cita, por lo que se recomiendan las siguientes estrategias:

1. Detenerse unos segundos
2. Respirar profundamente (respiración diafragmática)
3. Recordar que sólo es una cita, pasará
4. Avisar a la red de apoyo (laboral y familiar) del día, hora y lugar de la cita
5. Hacer un análisis de las posibles preguntas y practicar las respuestas
6. Concentrarse en la rutina y haceres cotidianos, si es difícil, practicar *mindfulness*
7. Recordar que una/o está haciendo su trabajo y esa es la versión de los hechos que es importante contar
8. Pedir orientación legal si es posible

d) Detenciones

1. No discutir: preguntar el motivo de su detención
2. Avisar a la red de apoyo siempre que posible
3. Tratar de ubicar a donde les están trasladando
4. Intentar recordar cada detalle para su posterior narración
5. Si le retiran las pertenencias, protestar
6. Utilizar la técnica de disco rayado para comunicar el mensaje de “sólo estoy haciendo mi trabajo”
7. Recordar que no se ha violentado ninguna ley ni derecho y tratar de mantener la tranquilidad

Posibles escenarios de las detenciones:

- Detenciones en el mismo sitio
- En la casa
- En el trabajo
- Aeropuertos

NO OLVIDAR

- Respetar a la autoridad y su jerarquía
- Intentar mantenerse activo física y mentalmente
- Conocer los derechos legales
- En la medida de lo posible dar aviso e iniciar el protocolo de emergencia

e) Tortura

El mayor número de casos contra la tortura se presenta durante las detenciones.

De acuerdo al Comité Internacional de Cruz Roja **(CICR, 2001):**

"Tortura y violencia represiva se dirigen específicamente contra personas y grupos con el objetivo explícito de causarles dolor, forzarlas a la sumisión y destruir su voluntad política(...)

Alienación, vergüenza, culpa, imposibilidad de sentir confianza, cambio personal, dificultades para relacionarse y dificultades sexuales son aspectos mencionados por sobrevivientes de tortura".

De acuerdo al CICR "Una de las formas más perversas de tortura es su utilización para obtener la sumisión y la colaboración de personas que no están involucradas en un determinado conflicto, pero que son torturadas y extorsionadas para que se infiltren o presten declaración contra supuestos 'enemigos' del Gobierno".

Las personas que no militan en grupos "preparados y entrenados" no cuentan con estrategias para hacerle frente a la tortura, ni tienen por qué, puesto que las reacciones ante cualquier tipo de violencia son normales, esperadas y sobre todo adaptativas.

El CICR considera tortura cualquier abuso, amenaza o coerción, en el marco de detenciones arbitrarias y encierros. Incluye los actos que van desde tocar sin consentimiento u obligar a una persona a desnudarse hasta los de abuso sexual.

NO OLVIDAR

- Aplicar las herramientas psicológicas con las que se cuenta
- Aceptar todo lo que pueda ayudar en el estado físico
- Mantener la calma
- Si es posible documentar el caso y acudir a las instancias internacionales

f) Seguridad en el espacio de trabajo

Muchas veces los espacios de trabajo o redacciones pueden sufrir un robo, allanamiento u otro tipo de ataque que pueda impedir el trabajo periodístico.

Algunas consideraciones generales son:

- No dejar artículos de valor u equipo de trabajo a la vista
- Nunca dejar a la mano notas o información de fuentes
- Realizar un inventario descriptivo de todos los objetos de valor (fotográfico sería ideal) y con los números de serie
- Tener barrotes en las ventanas
- Tener una cerradura fuerte
- Instalar una alarma y cámaras si es posible
- Mantener una comunicación constante con el vecindario

NOTA

Las reuniones de trabajo y sus consideraciones deben de ser especificadas en el protocolo de seguridad de la organización. Por ejemplo, los celulares deben de ser mantenidos fuera de las reuniones o en un lugar que no sea próximo a las discusiones, entre otras.

CONSEJO

Muchas veces las y los vecinos no concuerdan con las actividades periodísticas de determinado medio o equipo periodístico por razones ideológicas o de seguridad, y consideran que su presencia en el barrio llama la atención de las autoridades. Es importante evitar el aislamiento y/o la confrontación con el vecindario y colaborar en las labores del barrio cuando corresponda.

II. Desastres naturales:

a) Huracanes

Estos escenarios pueden preverse gracias a las depresiones y cambios atmosféricos que son medibles y que dan aviso antes de que el fenómeno sea de peligro para las poblaciones, existen varias herramientas y medios para el seguimiento de estos fenómenos.

Riesgo según categoría Saffir – Simpson. Los huracanes están divididos en 5 rangos de destrucción, a continuación, se anexan las categorías y su descripción.

CATEGORIA 1	**74-95 mph | 64-82 nudos | 119-153 km/hora** Estos vientos que son muy peligrosos producirán algunos daños como por ejemplo desprendimiento de tejados y algunas ramas.
CATEGORIA 2	**96-110 mph | 83-95 nudos | 154-177 km/hora** Estos vientos extremadamente peligrosos provocarán daños extensos como Las casas bien construidas podrían recibir graves daños en el techo y el revestimiento exterior. Algunos árboles se desprenderán.

CATEGORIA 3 (mayor)	**111-129 mph | 96-112 nudos | 178-208 km/hora** Habrá daños devastadores: : Las casas presentan daños más graves, Muchos árboles se desprenderán o desarraigarán y podrían bloquear muchos caminos.
CATEGORIA 4 (mayor)	**130-156 mph | 113-136 nudos | 209-251 km/hora** Habrá daños catastróficos: En las casas pérdida de la mayor parte de la estructura del techo y/o de algunas paredes exteriores. La mayoría de los árboles se desprenderán o desarraigarán y se caerán los postes eléctricos.
CATEGORIA 5 (mayor)	**157 mph o más | 137 nudos o más | 252 km/hora o más** Un alto porcentaje de las casas con marcos se destruirán, y se caerán los techos y las paredes. Los árboles y postes eléctricos caídos aislarán las zonas residenciales. Los apagones durarán varias semanas y posiblemente meses.

b) Sismos

Estos escenarios pueden preverse gracias a las depresiones y cambios atmosféricos que son medibles y que dan aviso antes de que el fenómeno sea de peligro para las poblaciones, existen varias herramientas y medios para el seguimiento de estos fenómenos.

Magnitud, escala Richter	Efectos del sismo o terremoto
Menos de 3.5	Generalmente no se siente, pero es registrado
3.5-5.4	A menudo se siente, pero sólo causa daños menores
5.5-6.0	Ocasiona daños ligeros a edificios
6.1-6.9	Puede ocasionar daños severos en áreas donde vive mucha gente
7.0-7.9	Terremoto mayor. Causa graves daños
8 o mayor	Gran terremoto. Destrucción total a comunidades cercanas

En caso de salida para realizar la cobertura periodística de un sismo, hay que preparar una maleta con:

- Agua
- Comida enlatada
- Kit de primeros auxilios
- Silbato
- Radio/pilas
- Una lámpara

Vestir ropa adecuada de acuerdo a las condiciones:

- Calzado cómodo e impermeable
- Ropa de color neutro
- Impermeable
- Pulsera indicando el grupo sanguíneo
- Ningún objeto de valor

ATENCIÓN (SISMOS/HURACANES/INUNDACIONES)

- Respetar las áreas de acceso delimitadas por las autoridades
- Considerar que pueden ocurrir réplicas después del sismo
- Prestar atención a las estructuras que puedan derrumbarse y alejarse de ellas
- Alejarse de lo escombros
- Alejarse del cableado eléctrico
- Evitar zonas con árboles o postes (pueden caer rayos o ramas)
- Evitar fumar (puede haber fugas de gas)
- Evaluar siempre abandonar la zona de riesgo en caso de peligro

c) Epidemiológicos

Los brotes epidemiológicos pueden ser muy peligrosos dependiendo de la rapidez de expansión y la tasa de mortalidad en los seres humanos. Las 48 primeras horas son las más críticas. Algunas de las enfermedades que podrían ocurrir son:

Dengue

Zonas de riesgo:

- Zonas marginadas
- Lagunas
- Estanques
- Época de lluvia

Zika

Zonas de riesgo:

- Zonas marginadas
- Lagunas
- Estanques
- Época de lluvia

Fiebre canícula

Zonas de Riesgo:

- Exposición en mataderos
- Zonas agrícolas
- Agua dulce contaminada - para consumo e/o higiene
- Sistemas de recolección de agua pluvial
- Mascotas domésticas

Cólera

Zonas de riesgo:

- Agua contaminada
- Alimentos contaminados

PRECAUCIONES GENERALES:

- Tener un mapa de la zona de incidencia
- Usar ropa de manga larga y pantalones
- Beber agua embotellada y consumir alimentos cocidos
- Lavarse las manos con frecuencia y tener un desinfectante a mano
- Usar repelente contra insectos (en casos de emergencia que no se tenga acceso a repelentes el champú líquido puede ser de gran ayuda aplicado en las zonas descubiertas)
- No asumir riesgos innecesarios o fuera de su control
- Acudir a un hospital o buscar asistencia médica profesional en caso de algún síntoma

Otras consideraciones a tomar en cuenta durante y después de algún desastre natural:

a) Traslados

Se tiene que investigar y tomar en cuenta que con un movimiento mayor las estructuras y/o carreteras pueden estar comprometidas. Es esencial investigar la mejor ruta para llegar a la localidad o sitio a la cual se pretende ir y localizar las zonas de riesgo consultando a habitantes, colegas o autoridades.

b) En sitio

Localizar un lugar seguro para desplegar el equipo o hacer las entrevistas, evitando entrar a inmuebles si hay duda de que están comprometidos. Recordar que después de un desastre natural hay varias estructuras NO seguras que pueden colapsar o representar un peligro para la vida.

Recordar que la mampostería y vidrios pueden desprenderse después del evento y no caminar por debajo de estos. Retirarse si se detecta olor a gas o gasolina.

Revisar que la zona de trabajo no sea de alto riesgo como puede ser:

- Con una represa cercana
- Industrias petroquímicas
- Puentes
- Laderas
- Costas (si hay alerta de tsunami). En zona de riesgo de tsunami hay que buscar el punto más alto al que se pueda acceder de manera segura.

c) Refugio

Recordar que, con un desastre mayor de esta índole, es probable que tanto hoteles como casas de huéspedes se encuentren sin servicios y/o cerradas por revisión estructural, y/o llenos de personas sin casa, los albergues temporales pueden ser una opción.
Nunca dejar su equipo o información de valor como documentos o USB en un albergue, siempre cargar con todo su equipo y documentos.
Evitar quedarse en una casa u hotel situado en una zona aislada.
Si tiene que quedarse en un refugio, es más seguro acercarse a familias con niñas y/o niños.

d) Retorno

Una vez terminado el trabajo de campo, regresar por una ruta ya establecida que se conozca como abierta y sin daños. Si es necesario regresar al lugar del evento, es recomendable hacerlo después de 72 horas ya que habrá más disponibilidad de las personas afectadas y testigos de cooperar con una entrevista o documental.

NO OLVIDAR

Tener un protocolo de comunicación con el medio (asegurarse que un contacto personal y otro profesional conocen los planes de cobertura, ruta y tiempo mínimo de contacto).

2.2.3 Violencia sexual y de género

"Hombres y mujeres periodistas pueden cubrir las mismas historias y no caben las restricciones por sexo a la hora de hacer un reportaje. Sin embargo, en ciertos casos, se recomienda que las mujeres tomen algunas precauciones concretas para garantizar su seguridad en zonas de riesgo **(Manual de seguridad para periodistas, Reporteros sin Fronteras, 2016)**"

Se recomienda prestar atención a algunos signos de alerta como:

1. Que un grupo o individuo esté detrás en plan de persecución
2. Contacto visual insistente con grupos o personas
3. Obstaculizar el avance o rodearla

En el sitio de una cobertura

- Mantener la distancia de grupos grandes de hombres
- Tratar de no llamar la atención con la ropa o accesorios
- Llevar calzado cómodo para poder movilizarse con rapidez

Retirándose del sitio

- Asegurarse de que nadie la siga
- De ser posible retirarse cuando todavía hay luz
- Evitar zonas de difícil acceso y poca visibilidad
- Mantenerse en comunicación con el equipo de trabajo, familiar o persona de confianza, para que esté monitoreando los tiempos de llegada

Violación

- Al sentir la amenaza se sugiere tratar de desplazarse a un lugar seguro
- Si hay un intento de sujeción, trate de salir corriendo; si esto no es posible y hay más gente cerca, gritar fuerte
- Si observa que su vida está en peligro y tiene posibilidad de huir del sitio, puede usar como arma defensiva un desodorante en aerosol para rociar al atacante en el rostro, esto solo es recomendado en casos extremos ya que, si agrede a un atacante acompañado o que no pueda soltarse de él, es probable que esto incremente la violencia hacia su persona.
- Otra técnica para reducir la posibilidad de una violación es orinarse, esto puede reducir la incidencia, aunque no es infalible
- Si es inminente el ataque sexual y no se tiene otra salida, tratar de cooperar en lo posible con los atacantes, esto suele bajar el índice de violencia
- En una violación tratar de pensar en alguna otra cosa que no sea el evento, recordar que lo que está pasando no fue provocado por su conducta, lo importante y en lo que se tiene que ocupar es de salvaguardar su vida
- Después del evento intentar llegar lo más pronto posible a un hospital para que le puedan brindar el tratamiento necesario contra enfermedades de trasmisión sexual y embarazo

- En caso de violación o agresión sexual contactar a un/a especialista de la salud mental, para poder trabajar en el evento y este no deje secuelas graves en su psique

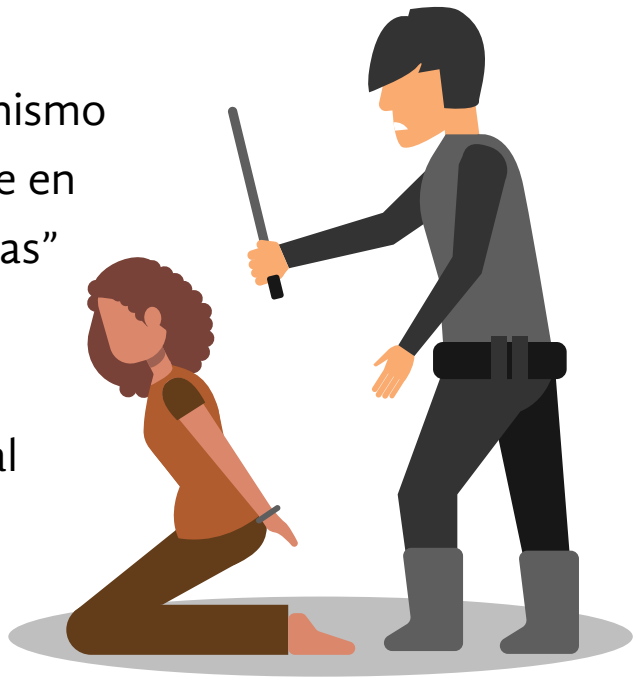
Cuerpos de seguridad o gobierno

Es clave que hombres y mujeres sepan qué hacer en caso de conducta sexual inapropiada por parte de cualquier integrante de las fuerzas de seguridad o del gobierno.

1. Negarse a ser tocada (o) y hacerlo de forma enfática (o). Insistir en el NO.
2. Si se está siendo víctima de una arbitrariedad, recuerde que en ninguna circunstancia provocó ser agredida (o).
3. En caso de violencia no detener sus impulsos y necesidades fisiológicas, es más intentar llevarlas a cabo en el acto.

4. La vida es la prioridad: ninguna historia periodística vale sacrificar la vida.

5. Concentrarse en permanecer en el momento presente, por aversivo que sea.
6. Poner atención a los detalles: favorece la concentración y es clave para describir a fondo la situación en la posterior denuncia del incidente.
7. Recordar que ante todo el organismo responde a los estímulos, así que en caso de sensaciones “inadecuadas” tener en cuenta que solo es una reacción a un estímulo, sin ninguna connotación emocional o cognitiva.



IMPORTANTE

El cerebro y el cuerpo ante situaciones de restricción de libertad reaccionan instintivamente con una pulsión de huida o lucha. Pero cuando no es posible, el último recurso del organismo es paralizarse, guardando así la energía para recuperarse y ponerse a salvo cuando el peligro pase.

NOTA

Las mujeres no son las únicas que pueden enfrentarse a una agresión sexual, por ello los consejos anteriores pueden aplicarse para cualquier persona de cualquier género.

El patrón de las agresiones contra mujeres o minorías podría tener como componente comprometer su integridad sexual y emitir juicios por no "cumplir" los roles tradicionales de género incluyendo: campañas de difamación, golpes, ofensas y amenazas de agravio sexual, así como amenazas y atentados contra la vida personal y profesional de integrantes de su familia.

NO OLVIDAR

En caso de agresión sexual o amenaza de violación:

- Buscar atención médica (la píldora del día siguiente, tratamientos antivirales)
- Buscar apoyo psicológico
- Nunca auto-culparse

2.3 Seguridad psicológica

2.3.1 Prevenir

Las personas que trabajan en contextos violentos, de alto contenido emocional o de mucho peligro, pueden estar expuestas a factores que las vuelven más propensas a ser afectadas. De igual modo, hay factores de protección que aumentan la probabilidad de enfrentar con éxito las adversidades. Ante cualquier amenaza externa toda persona entra en una emergencia psicológica: es esperable y normal.

Para prevenir el trauma ante situaciones estresantes: el primer paso es la preparación de la persona para la situación que va a enfrentar, así como algunos cuidados cotidianos simples pero efectivos. A continuación, algunas sugerencias:

- Promover el cuidado personal (beber bastante agua y alimentarse de forma balanceada, frecuentemente en cantidades pequeñas, por ejemplo).
- Pensar el trabajo a realizar detalladamente, cubriendo las tareas, horario, procesos, etcétera.

- Prepararse para reducir el impacto: las imágenes, los sonidos, y los olores que la persona encuentre a lo largo de la situación traumática formarán las memorias que pueden volver con el tiempo.
- Si el personal que brinda apoyo actúa en papeles de recuperación e identificación de cadáveres, es necesario prepararse para el escenario por el impacto psicológico.
- Es necesario explicar las condiciones de trabajo agotadoras, hablar de las otras organizaciones implicadas y de sus papeles, etc. Ofrecer una descripción gráfica de las imágenes, sonidos, y de los olores que encontrará.
- Para cualquier persona que no pueda manejar el trabajo, ofrecer una salida digna (p.ej. asignar deberes menos agotadores).
- Recordar que es ACEPTABLE parar en cualquier momento. Es importante planear y disfrutar de un período de vacaciones.
- Mencionar la disponibilidad de los servicios de ayuda psicológica y emocional, tanto de auto-higiene como de intervención en crisis, y procurar convertir en requisito la asistencia a las sesiones de auto-ayuda.
- Animar a que las sesiones de auto-higiene sean diarias.

Es necesario desterrar el estereotipo deshumano del/de la periodista que trabaja en cualquier horario, no tiene tiempo para la familia y sus amistades o bebe demasiados cafés, probablemente también fuma y toma antidepresivos para cumplir con su trabajo.

Ante cualquier amenaza externa toda persona entra en emergencia psicológica, sin embargo, las consecuencias pueden ser menos severas si la persona presenta factores protectores.

Factores protectores	Factores de riesgo
Buena salud física	Alta motivación por conseguir la información
Familiares de apoyo	Contar con alguna enfermedad crónica-degenerativa
Situación económica estable	Aislamiento
Capacitación constante	Problemas familiares
Amplia experiencia	Pobreza
Sentido catártico de la historia	Alta empatía, ser una persona emotiva
Actividades sociales	Consumo previo y posterior de alcohol y drogas y socialización
Habilidades de desconexión y conexión alternante	Pérdida de conexión con la rutina ordinaria
Socializar lo ocurrido y contar con una red de apoyo profesional	Pérdidas personales y crisis de vida
A nivel cognitivo: capacidad para solucionar problemas, flexibilidad psicológica	Ser mujer
	Dependencia de otros
	Patologías existentes

Resultados del trabajo el taller de seguridad holístca (Segarra Pérez y Velázquez Cardoso, 2018) y complementado con la investigación Novak y Davidson (2013)

2.3.2 Síntomas de alteraciones del estado de ánimo y estrés

Hay una serie de síntomas relacionados a alteraciones del estado de ánimo y estrés que requieren ser identificados para poder desarrollar alguna estrategia para abordarlos o bien para acudir a un especialista de la salud mental. Esos síntomas son los siguientes

(Ítems del Inventario de Depresión de Beck ,1961):

Depresión

Si se experimentan de forma continua (dos o más semanas) con repercusiones en nuestras actividades cotidianas o relaciones interpersonales varios de los siguientes síntomas se debe buscar ayuda:

- Tristeza y pesimismo
- Sensación de fracaso
- Pérdida de interés en el trabajo y el día a día
- Sentimientos de culpa
- Sensación de estar siendo castigada/o
- Falta de autoconfianza
- Pensamientos suicidas y sobre hacerse daño
- Llanto fácil o incapacidad de llorar
- Agitación y ansiedad
- Incapacidad para tomar decisiones
- Insomnio o exceso de sueño
- Falta de energía, cansancio.
- Irritabilidad
- Cambios en el apetito
- Falta de concentración
- Pérdida de interés sexual

Ansiedad

Si es difícil controlar las preocupaciones y además se experimentan durante mucho tiempo (6 meses o más) los siguientes síntomas,hay probabilidad de que se esté atravesando un trastorno de ansiedad:

- Temblores en las manos y/o piernas
- Incapacidad de relajarse
- Con temor a que ocurra lo peor
- Mareos y fuertes dolores de cabeza
- Ritmo cardíaco fuerte y acelerado
- Inestabilidad
- Temor y miedo
- Nervios
- Sudores fríos o calientes
- Problemas digestivos
- Desvanecimientos
- Temor a morir
- Sensación de ahogo
- Con sensación de bloqueo
- Miedo a perder la vida

Tensión o estrés

El estrés es una reacción adaptativa ante la sensación de peligros reales o imaginarios con características fisiológicas:

- Si la reacción al estrés perdura o se repite de manera continua la persona enferma.
- Tensión muscular
- Dolores en diferentes partes del cuerpo
- Ritmo cardíaco acelerado
- Respiración rápida y superficial
- Visión en túnel
- Disminución de la temperatura en las extremidades,
- Atención selectiva y toma de decisiones deficientes (por estar enfocado a la salida del peligro)
- Sudor

Transtorno de estrés postraumático

Después de ser testigo o tener conocimiento de noticias con alto contenido de violencia o bien por las características sociopolíticas en las que se vive se puede desarrollar el trastorno completo o síntomas propios del trauma que son altamente incapacitantes.

Si se detecta al menos tres de los siguientes síntomas se debe acudir a un especialista (Los síntomas pueden presentarse hasta 6 meses después de la situación traumática):

- Sueños recurrentes relacionados al evento y causantes de angustia.
- Reacciones disociativas (tener la sensación de que se está viviendo de nuevo)
- Recuerdo angustiosos del suceso
- Malestar físico y psicológico (con estímulos que se parecen al evento, por ejemplo olores, colores, imágenes, dolores)
- Ansiedad
- Angustia
- Terror

- Evitación y perdida de la memoria (amnesia disociativa)
- Creeencias negativas sobre el propio desempeño y el evento
- Disminución del interés en los demás y en las actividades cotidianas
- Dificultad para disfrutar otras cosas
- Irritabilidad
- Furia espontánea
- Hipervigilancia
- Sobresalto
- Comportamiento autodestructivo
- Insomnio y problemas de sueño.

NOTA

Es natural y parte del instinto adaptativo reaccionar con estrés a situaciones que pusieron en peligro nuestra vida. Sin embargo, el organismo generalmente regresa a un nivel adecuado de desactivación después de un periodo reducido de relajación. Claro que si el trauma fue muy impactante o repetitivo los síntomas pueden persistir un mes o más. En ese caso se debe acudir a un especialista, pues de no atenderse puede impactar negativamente en las diferentes esferas de vida.

NO OLVIDAR

Este manual pretende ayudar a las y los profesionales del periodismo para que desarrollen y practiquen estrategias para afrontar las reacciones emocionales que se presentan de manera normal y esperada por el tipo de situaciones que pueden presentarse en su trabajo. El objetivo de este manual es brindar herramientas para utilizar antes de acudir a un tratamiento psicológico o psiquiátrico formal.

2.3.3 Trabajar el estrés

A continuación, se muestran técnicas para la desactivación y control del estrés antes y durante los eventos, que se pueden utilizar de manera personal y en poco tiempo.

a)Técnica de *mindfulness*

La atención o conciencia plena es una herramienta que puede ayudar en el entrenamiento de la atención para una regulación emocional más eficiente.

El *mindfulness* es una práctica para ayudar a apagar el "piloto automático" de la vida cotidiana y permitirnos centrar nuestra atención en el estímulo que elijamos como importante, así que puede ser la respiración, un objeto, la mirada de otra persona, la mano, un paisaje, etc., lo importante es ser consciente de cuando se está distraído/a y de manera voluntaria regresar la atención, tantas veces sean necesarias.

EJERCICIO DE ATENCIÓN PLENA:

Cierra los ojos, siéntate con la espalda recta, pero sin tensar, los brazos relajados y los pies separados sobre el piso.

LLeva tu atención a la punta de tu nariz (esperar unos momentos) ahora solo toma en cuenta los sonidos del ambiente que te rodea, realiza un reconocimiento rápido y déjalos estar.

Regresa tu atención a la punta de tu nariz (dar unos segundos)... ahora lleva la atención a tu respiración, siente como entra y sale el aire por tus fosas nasales.

Es importante que no controles o inhales profundamente, se trata de sentir tu respiración, así como es (dejar unos segundos)... si surgen pensamientos, imágenes, recuerdos o cualquier otra cosa que distraiga tu atención, solo observa y déjalos estar, como si fueran fotografías, sin detenerte demasiado.

Regresa la atención a tu respiración, siéntela como si fuera la primera vez que la descubres (dar unos segundos)... si surgen emociones, sensaciones o impulsos, nota que están ahí y déjalos estar.

De manera amable regresa a tu respiración (dar unos segundos).

Si surgen ideas, juicios pendientes, obsérvalos y déjalos pasar, regresando cortésmente a tu respiración, siente como sube y baja el tórax en cada respiración.

Ahora amplía tu percepción al entorno en el que te encuentras, nota los sonidos, temperatura, iluminación, tu cuerpo, la silla, etc.

Y suavemente regresa tu atención al lugar en el que te encuentres y abre los ojos.

b) Técnicas de relajación

La respuesta al estrés es una reacción del ser humano, adaptativa, a peligros reales o anticipados. Cuando percibimos un peligro se activan diferentes mecanismos para proveer de los recursos necesarios para hacer frente a la amenaza, pero una vez superado el peligro, el sistema regresa a su estado de equilibrio. El problema se presenta cuando el cuerpo no se desactiva o cuando la fuente de estrés no desaparece, ahí es cuando pueden practicarse técnicas que ayudan al cuerpo a regresar a un estado de equilibrio.

La ***respiración profunda diafragmática*** es una técnica que genera bienestar al provocar un estado de relajación mediado por la respiración.

La persona promedio respira de 10 a 12 veces por minuto, estando relajada. Cuando se hiperventila se está tomando demasiado oxígeno y exhalando también demasiado dióxido de carbono. Una respiración correcta es un antídoto contra el estrés. Cuando la cantidad de aire que llega al pulmón es insuficiente, la san-

gre no puede oxigenarse, no puede purificarse adecuadamente y los productos de degradación de las células van intoxicando lentamente nuestro organismo. La sangre insuficientemente oxigenada contribuye a los estados de ansiedad, depresión y fatiga. Como el oxígeno que reciben los vasos sanguíneos es muy poco, las células cerebrales trabajan con menos eficiencia. Esta ligera baja de oxígeno en el cerebro, se manifiesta de las siguientes maneras:

- Vértigo, mareo, confusión, trastornos visuales (como la visión borrosa); sentimiento de irrealidad, jadeo

Por otro lado, con la disminución de la cantidad de oxígeno que llega a las células del resto del organismo, se da otro grupo de sensaciones:

- Aumento del ritmo cardíaco (para bombear más sangre al cuerpo)
- Entumecimiento y hormigueo en manos y pies
- Manos frías y húmedas
- Temblor de músculos
- Piernas de gelatina (falta de fuerza muscular en los miembros inferiores)

¿Qué hacer?

a. Acostarse de forma cómoda
b. Explorar signos de tensión
c. Colocar una mano sobre el abdomen y otra sobre el tórax
d. Tomar aire, lenta y profundamente por la nariz hasta el abdomen
    i. Partes bajas del abdomen

ii. Partes medias, mientras que la parte inferior del tórax y las últimas costillas se expanden ligeramente para acomodar el aire que hay en el interior
iii. Por último, llena la parte superior de los pulmones mientras elevas ligeramente el pecho

e. Mantener la respiración unos pocos segundos
f. Sacar el aire lentamente por la nariz
g. Repetir el mismo procedimiento, eliminando todo el aire en pequeños y fuertes soplos por la boca, de forma lenta y gradual.

La ***relajación muscular*** es una técnica que involucra el entrenamiento del contraste tensión-relajación. Se entrena a la persona en alternar la tensión con la distensión de cada área muscular principal: manos, brazos, pecho, hombros, espalda, abdomen, glúteos, muslos, músculos de las pantorrillas, pies, cuello, garganta, mandíbula, ojos y frente. La relajación total se realiza, por lo general, en una silla reclinable o en una colchoneta en el suelo e incluye todas las áreas musculares en la sesión de entrenamiento.

La relajación diferencial puede practicarse en tanto se realizan otras actividades. Aquí la persona relaja deliberadamente aquellos músculos que no estén en uso durante una actividad progresiva. Por ejemplo, mientras se escribe una carta, se puede aprender deliberadamente a soltar la tensión de la frente. Casi siempre, la relajación diferencial se enseña después que la persona ha dominado la relajación muscular total.

Ventajas:

- Alivia tensiones y disturbios emocionales
- Renueva energía y clarifica la mente
- Aumenta la autoestima
- Estimula mente - cuerpo
- Alivia fatiga
- Mayor irrigación sanguínea y linfática
- Depura el cuerpo
- Mejora el tono muscular y reduce la atrofia
- Reduce el tejido adiposo
- Mejora la digestión y el metabolismo, visión, oído y casos de congestión nasal, garganta irritada, calvicie, dolor de cabeza, arrugas, dolor de espalda
- Funciona como un ejercicio pasivo que compensa la falta de actividad física

Ejercicios sugeridos (Vera y Vila, Siglo XXI):

Grupos musculares	Ejercicios
Mano y antebrazo Bíceps	Se aprieta el puño Se empuja el codo contra el brazo del sillón
Frente y cuero cabelludo	Se levantan las cejas tan alto como se pueda
Ojos y nariz	Se aprietan los ojos al mismo tiempo de tal forma que se arruga la nariz.

Grupos musculares	Ejercicios
Boca y mandíbulas	Se aprietan los dientes mientras se llevan las comisuras de la boca hacia las orejas Se aprieta la boca hacia afuera (beso) Se abre la boca
Cuello	Se dobla hacia la derecha Se dobla hacia la izquierda Se dobla hacia adelante Se dobla hacia atrás
Hombros, pecho y espalda	Se inspira profundamente manteniendo la respiración al tiempo que se llevan los hombros hacia atrás intentando juntar los omoplatos. Sentándose en la silla con la espalda recta y sin despegar los glúteos, rotar la espalda hacia la derecha y después hacia la izquierda. De pie, con los pies separados a la altura de la cadera, inclinarse con la espalda recta tomando de una silla, echando hacia atrás la cadera.
Estómago	Se mete hacia adentro, desde el ombligo manteniendo la respiración. Se saca hacia afuera conteniendo la respiración.
Pierna y muslo	Se intenta subir con fuerza la pierna sin despegar el pie del asiento y luego se suelta.
Pantorrilla	Sin subir la pierna se dobla el pie hacia arriba, tirando con los dedos y soltando. Con la pierna estirada jalar los dedos hacia el frente y después hacia abajo tomado de la silla.

2.3.4 Dejar atrás el episodio traumático

a) Desactivación o *Defusing*

Este tipo de técnica se aplica principalmente con los equipos de primera respuesta y operadores sociales, con el objetivo de proporcionar información y apoyo, favoreciendo la ventilación emocional y generar una pausa. Se aplica particularmente al final de cada día de trabajo de terreno de los equipos de primera respuesta, con el fin de elaborar lo acontecido y vivenciado, para permitirles continuar con las tareas de emergencias de días siguientes. Se recomienda en diadas o en grupo al final de día.

Las reglas son:

- Respeto por los sentimientos y pensamientos de el o la compañera.
- Confidencialidad total del contenido que se comparte.
- No se permite la interrupción con información no pertinente al contenido compartido.

b) *Debriefing*

Es una técnica grupal o individual, que ayuda a elaborar los acontecimientos y experiencias vividas en la situación de emergencia o desastre. Es facilitada por un especialista en salud mental. De acuerdo a una revisión (Santacruz Escudero, 2008) sobre la utilidad de la técnica para la elaboración del trauma se concluye que la técnica no está dirigida a personas con patología mental previa, ni previene el estrés postraumático, sino que ayuda a compartir información práctica, aclarar dudas, cohesionar al grupo, organizar la experiencia en hechos, emociones y pensamientos.

El procedimiento es el siguiente:

Fase 1 - Introducción: Explicar los modelos a utilizar y la funcionalidad de los mismos. Determinar la duración, el horario y el lugar de reunión para las sesiones formales (lo ideal es de 1 a 2 horas).

Fase 2 – Descripción de hechos: Se revisa lo que sucedió (e.g., lo que cada persona oyó, consideró, olió, tocó).

Fase 3 – Compartir pensamientos: Promover la lluvia de ideas con respecto a los acontecimientos, tanto de aquellos aspectos operativos como de la situación en general.

Fase 4 – Compartir reacciones emocionales: Revisar y compartir las emociones y sensaciones que cada persona tuvo, en este proceso y de acuerdo con los principios de auto-ayuda, se encontrará que dichas reacciones son similares, lo cual permite reducir la sensación de vulnerabilidad o inadecuación que normalmente se tiene ante la presencia de emociones desbordantes y que al no compartirlas, consideramos que sólo nosotra y nosotros tenemos.

Fase 5 – Compartir los síntomas: Examinar los efectos secundarios físicos y psicológicos que se han presentado en las y los participantes. Irritabilidad, hiperactividad, incremento de la libido, etc.. Al igual que en el caso anterior se reduce la sensación de inadecuación y además el resultado de la catarsis es la reducción en la actuación de los síntomas, es decir “hablar para no actuar”. Ej. Si se sabe que se está irritable y que es algo compartido, habrá menos posibilidades de que se descargue en otras personas o, de que tenga consecuencias.

Fase 6 – De aprendizaje: Recordar que los síntomas que se están experimentando son respuestas normales a la situación anormalmente agotadora a la que se está haciendo frente.

Fase 7 – De reingreso: Este es el tiempo de la conclusión, contestar a cualquier pregunta, y desarrollar un plan para las acciones futuras. En la medida en que se tenga el control de lo que realizaremos, el nivel de tensión se reducirá, de ahí que es fundamental la planeación.

El regreso a casa puede ser una experiencia difícil, la adrenalina, las endorfinas y la cohesión del grupo nos lleva a querer permanecer trabajando más tiempo. Por otro lado, retornar a las rutinas familiares o social con toda la carga emocional y sintomática favorece que surjan problemas familiares, laborales o sociales, de ahí la importancia de desprenderse y descargarse del evento. Algunas sugerencias son:

1. Fomentar el desconectarse de las actividades cuando se disponen a descansar y/o cuando se va a regresar a casa.
2. Lo ideal es que quien va a regresar a casa tenga una sesión individual con un especialista en intervención en crisis o en sesiones abreactivas (debriefing).
3. También es idóneo asistir a otra sesión tras algunos días de haber regresado a casa, y se halla tenido tiempo para reflexionar y descansar.
4. Reconocer que habrá sensaciones ambivalentes con respecto a las tareas incompletas y a las víctimas que permanecen en el sitio, mientras uno consigue ir a casa a reiniciar su vida.

Finalmente, el cuidado de uno mismo/a se inicia en el momento que decidimos o no aceptar la tarea.

Si se acaba de regresar de una emergencia, o se acaba de vivir

una experiencia personal intensa. Ej. Una muerte o una separación, seguramente habra cansancio físico y fatiga emocional.

2.3.5 ¿Cómo afrontar psicológicamente una situación de conflicto?

Para ayudar a una persona que está en situación de emergencia o en situación de conflicto o represión, es bueno repasar algunos **primeros auxilios psicológicos**.

Fases	Procedimiento
1. Acercamiento	• Presentarse • Buscar la catarsis • Un simple ¿cómo está? puede iniciar el diálogo • Cuidar el tono de voz • Cuidar los mensajes no verbales
2. Establecer contacto empático	• Intentar comprender la perspectiva de la otra persona • Ser respetuosa/o • Estar libre de prejuicios • No juzgar
3. Proporcionar Reaseguramiento	• Dar contención • Dimensionar la situación y las emociones • Reorganizar para incrementar la seguridad
4. Estabilizar	• Este paso no siempre es necesario. La fuerte expresión de emociones es una parte natural y no es un síntoma que nos indique la necesidad de estabilizar. • Los signos que debemos detectar para saber si es necesario estabilizar son: - Desorientación - La persona no responde a las preguntas y direcciones que se le dan - Comportamiento regresivo, por ejemplo mecerse. - Reacciones físicas extremas como temblores. • Si alguien presenta los signos anteriores, se deberá ofrecerle atención el tiempo necesario para calmar a la persona y para lograr el contacto.

Fases	Procedimiento
5. Recopilar información: Necesidades y preocupaciones actuales	• Recopilar información sobre la situación actual • Detectar las necesidades del momento • Abordar las preocupaciones relacionadas con la situación
6. Ayudar a Explorar opciones de aspectos que requieran solución inmediata	• Servir de YO auxiliar • Ayudar a la toma de decisiones inmediatas • Dar opciones • No decidir por la otra persona
7. Explorar Redes de Apoyo	• Analizar las redes de apoyo familiar, social e institucional con las que cuenta la persona. • Promover el acercamiento y la utilización de dichas redes.
8. Proporcionar información para aumentar las habilidades de manejo.	• Proporcionar información sobre el proceso psicoafectivo que enfrenta la persona, los síntomas que pueden presentarse posteriormente y las alternativas de manejo para la adaptación a la situación.
9. Canalización	• Evaluar si la condición va a requerir canalización o no, tanto a corto como a largo plazo. • En caso de que la canalización requiera ser inmediata, apoyar a la persona para obtener la ayuda • En caso de que la canalización no sea inmediata, abordar el tema y plantearlo como objetivo. • Ofrecer opciones para la canalización a través de proporcionar los datos de al menos una institución (preferentemente 2).

2.4 Seguridad digital

En un mundo lleno de dispositivos y servicios digitales, tomar acciones a favor de fortalecer nuestra seguridad digital juega un papel prioritario en cuanto a seguridad y privacidad de la información. En el quehacer diario interactuamos con una variedad de plataformas y gestionamos todo tipo de documentos que en algunos casos pueden ser considerados como sensibles por el valor no tangible de la información que contienen.

Además, Internet se volvió el espacio de más fácil acceso para el ejercicio de la libertad de expresión y para la difusión de información de una diversidad de voces de todas las ideas.

Este apartado de Seguridad Digital, pretende aportar conceptos fundamentales sobre los aspectos que deben contemplar a la hora de adoptar medidas de seguridad digital, tanto periodistas y activistas como medios para la gestión de información o la publicación de contenidos.

2.4.1 Seguridad digital para periodistas

La seguridad digital se define como todas aquellas medidas que son adoptadas y dependen exclusivamente de las y los usuarios (a partir de sus interacciones digitales) orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información que el mismo usuario determine como valiosa.

Estas medidas en muchos casos se traducen en cambiar constantemente las contraseñas para evitar posibles intrusos en documentos, dispositivos físicos y virtuales. También, realizar respaldos periódicos de la información para evitar pérdidas en caso de falla en el dispositivo de almacenamiento.

NOTA

El o la usuaria final del servicio o dispositivo es el único responsable de todas las decisiones en seguridad que se toman.

Para tomar conciencia sobre qué es la Seguridad Digital vale la pena tomar un instante para definirla y diferenciarla de otros conceptos similares. Es importante resaltar que la seguridad digital no significa lo mismo que seguridad informática. En la seguridad informática, la seguridad se aborda desde la capacidad de lograr (por parte de quien diseña o produce un servicio o dispositivo) la no existencia de vulnerabilidades que pudieran dar pie a posibles ataques que pongan en riesgo la seguridad digital de las y los usuarios.

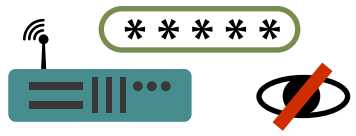
En esta sección, los contenidos están orientados a que las y los periodistas puedan conocer y adoptar buenos hábitos que les ayudarán a incrementar su seguridad digital sin importar la tecnología o servicio que usen ahora o en el futuro. La sección contempla una breve introducción a los conceptos mínimos necesarios sobre seguridad digital, pero también aporta referencias para profundizar en el tema.

2.4.2 ¿Cómo funciona internet?

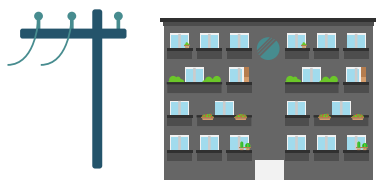
Internet por definición es una gran red de computadoras conectadas por diversos métodos de forma que sin importar el origen o destino de la información se pueden conectar dos extremos de la red. Esto en la práctica es mucho más complejo por ello entender cuáles son las y los agentes, sus capacidades y también los riesgos asociados al navegar por internet es de suma importancia.

A continuación, se presenta un diagrama que ejemplifica brevemente el recorrido de la información cuando se envía o se recibe un mensaje de whatsapp o un correo electrónico.

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.



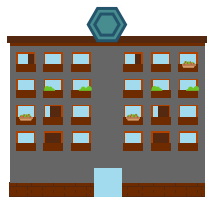
OJO: para proteger tu conexión a internet, cambia la contraseña que viene por defecto del módem y comprueba la configuración de seguridad.



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

El proveedor de datos envía tus datos a la red social o sitio web que está 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 están resguardándolos 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.

(Modelo adaptado de SocialTic, 2018)

REGRESAR AL ÍNDICE

Es importante saber que la red de internet está construida por la participación de diversos actores: por ejemplo, las empresas que proveen el servicio de internet o las empresas que dan servicios como redes sociales o servicios de video. Es decir, cada una de estas entidades representa una aportación a la cadena de internet pero también un riesgo para la privacidad y seguridad de cada persona que utiliza internet.

Al navegar en internet hay que ser consciente de algunas cuestiones:

- Todas las conexiones de internet pueden ser monitoreadas por diferentes agentes de una o varias agencias de seguridad.
- Al usar ciertos servicios de navegación de forma constante, una persona podría ser detectada por realizar una actividad inusual de navegación por diversos agentes de seguridad de la cadena de internet.
- Aunque sin duda hay diversos tipos de riesgos en toda la cadena de internet, es importante priorizar cuál de ellos es más cercano y que consecuencias representa este riesgo.

NO OLVIDAR

Al navegar en internet procurar usar el servicio https:// al visitar un sitio web. por ejemplo **https://www.facebook.com/**

CONSEJO

Una herramienta útil para poder navegar lo más que se pueda con https es HTTPS Everywhere (**https://www.eff.org/https-everywhere**)

2.4.3 Contraseñas y verificación de dos pasos

Uno de los principales problemas al hablar de seguridad digital es lo complejo que puede parecer el buen manejo y uso de contraseñas. La contraseña es el primer gran acercamiento que hay que tener con la seguridad digital ya que permite resguardar el acceso a documentos o servicios privados.

Una contraseña puede ser fácil de olvidar sobre todo cuando es muy compleja. Es más sencillo usar la misma contraseña para todos los servicios, pero en ambos casos esto incrementa el riesgo al robo o la intromisión a documentos privados. Para hacerlo sencillo aquí se presentan recomendaciones de cómo mejorar contraseñas:

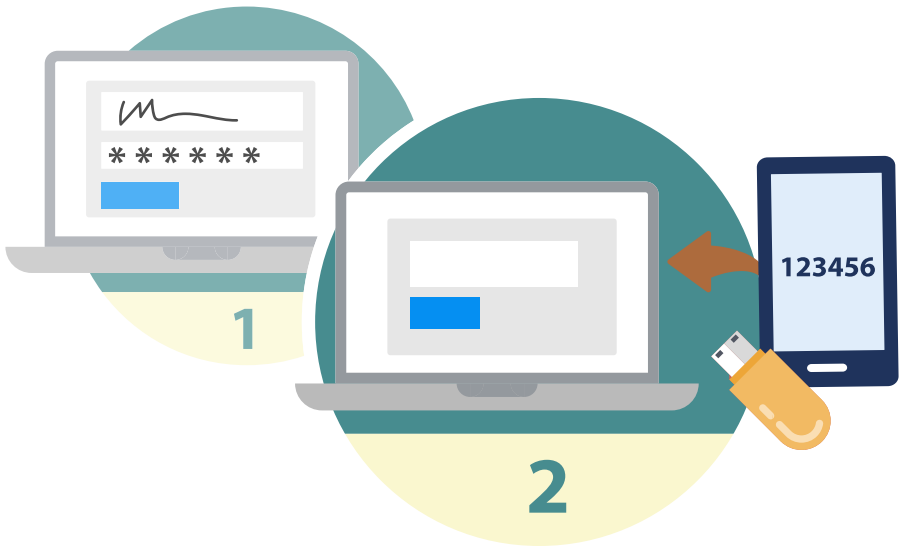
- Deben ser largas, por lo menos 12 caracteres.
- Usar frases en lugar de palabras sueltas, ésto ayuda a recordar. Ejemplo: ¡Parece Que Va a Llover 24 horas!
- Incluyan mayúsculas, minúsculas, números y signos. Algunos servicios permiten espacios en las contraseñas, utilizarlos incrementa la complejidad de la contraseña.
- Hacer una variación entre cada servicio, por ejemplo:
  “Opción 1: Parece Que Va a Llover 24 horas_FB!”
  “Opción 2: P4r3c3 qu3 v4 4 110v3r 24 h0r4s!”
- No dejar pasar mucho tiempo antes de cambiarlas. Cada vez que se hace, este ejercicio es más sencillo.

NO OLVIDAR

- Una buena contraseña debe ser fuerte y de fácil memorización.
- Nunca repetir ni reutilizar contraseñas.

Una vez que ya se esté utilizando una mejor contraseña en las aplicaciones, también se puede habilitar el uso de la verificación en dos pasos, una herramienta sumamente poderosa que se basa en dos componentes: “algo que sé y algo que tengo”.

En la verificación de dos pasos el primero de los pasos es introducir el nombre de usuaria/o y la contraseña en el servicio y el segundo de los pasos es el uso de un código externo y aleatorio que puede ser enviado al teléfono personal mediante SMS o mediante el uso de una aplicación en el teléfono para generar ese mismo código sin esperar a recibirlo.



En la actualidad ya son varias las empresas de servicios que utilizan verificación de dos pasos para sus páginas, por ejemplo:

- Google: **https://goo.gl/7qCfHh**
- Facebook : **https://goo.gl/wjMcCC**
- Dropbox: **https://goo.gl/jw2NLc**

Al realizar la activación de la verificación de dos pasos es más complicado que alguien que no sea la o el usuario pueda acceder a su cuenta personal.

¿Dónde almacenar las contraseñas?

Entre más dispositivos y servicios utilizamos, más contraseñas necesitamos. Por razones de seguridad no es recomendable usar la misma contraseña para más de un servicio o dispositivo.

Uno de los principales problemas que se suelen presentar es recordar tantas contraseñas, con las características que hemos mencionado en párrafos anteriores, a la vez. No es recomendable guardarlas en un papel o "debajo del colchón". Tampoco es útil guardarlas en un bloc de notas en la computadora porque si perdemos la computadora tendrán acceso a todos nuestros servicios y dispositivos.

La solución para almacenar contraseñas es un llavero de contraseñas. Existen varios, pero uno que funciona sin necesidad de conexión a internet es KeePass (**https://keepass.info**).

Para utilizar este llavero hay que crear una "contraseña maestra". Sí, ¡otra contraseña más! que sea compleja: una frase de al menos 20 caracteres que contenga mayúsculas, minúsculas, números, signos y espacios (con la barra espaciadora). Si pones todas tus contraseñas en este llavero, la contraseña maestra será la única que debas recordar.

Con la súper contraseña lista es posible hacer una base de datos que quedará almacenada en un archivo cifrado, o sea, en una especie de caja fuerte, donde se guardarán todas las contraseñas personales. Keepass es multiplataforma y permite ser usado en múltiples dispositivos. O sea, funciona tanto en computadoras

como celulares. Hay un motivo más para recomendar Keepass: es software libre.

Estos pasos recomienda la guía *Security in a Box* hecha por **Front Line Defenders**:

1. Instalar Keepass.
2. Hacer click en *Base de datos* y elegir *Nueva base de datos* en la barra de menú de KeePass.
3. Escoger una contraseña maestra fuerte y fácil de recordar. Escribirla dentro de los campos *Escribir contraseña* y *Repetir contraseña*. La contraseña es irrecuperable, así que hay que memorizarla sí o sí.
4. Guardar la base de datos o el archivo de KeePass en la computadora.

Para guardar las contraseñas:

1. Del lado izquierdo hay una serie de grupos para clasificar contraseñas. Escoger dónde guardar la contraseña.
2. Para guardar una nueva contraseña o alguna ya hecha ir al menú *Entradas* y dar en *Nueva entrada*.
3. Después de guardar y modificar una contraseña hay que seleccionar *Guardar* para salvar los cambios.

Para más información visitar: **https://goo.gl/raJ27p**

CONSEJO

KeePass no solo permite tener un lugar para almacenar las llaves, también permite guardar información considerada sensible.

MUY IMPORTANTE

Tener una contraseña diferente para cada dispositivo y servicio utilizado.

2.4.4 Navegación y comunicaciones seguras (Apps y VPN)

Conocer qué tipo de información generamos y compartimos es de suma importancia, ya que nos permite elegir medios seguros para comunicar. No hay que olvidar que la comunicación de un mensaje o la difusión de archivos se realiza en dos sentidos: como emisores o como receptores.

Cuando navegamos estamos expuestos a distintas amenazas por un sin fin de motivos que van desde errores tecnológicos que se salen de nuestras manos, malos hábitos como usuaria/o o por ataques dirigidos que vulneran la seguridad digital. Para comenzar hay que adoptar los hábitos más básicos para navegar en internet.

RECUERDA

- Para navegar por internet se recomienda utilizar los navegadores Firefox o Chrome, debido a que tecnológicamente los navegadores de Mozilla y de Google superan en rendimiento y reducción de vulnerabilidades a los diseñados por Microsoft (Internet Explorer o Edge) o Apple (Safari).
- Para evitar guardar el historial de navegación se puede usar el *Modo de Navegación Incógnita* de Firefox o Chrome que se activa desde el menú del navegador.
- Verificar que los sitios visitados utilicen HTTPS (secure). Para asegurar que la información enviada y/o recibida desde el sitio viaje de manera cifrada y para asegurar la autenticidad del sitio.
- Se puede añadir complementos con un enfoque de seguridad, privacidad y anonimato a los navegadores. Estos pueden ser bloqueadores de anuncios, bloqueadores de rastreadores, contenedores de sitios, VPN, etc.
- Usar el sentido común, si algún sitio visitado se ve sospechoso o nos sentimos en riesgo, es mejor abandonarlo. Mantener la mente fría antes de dar clic a algún enlace o proporcionar datos personales es de suma importancia y debemos estar atentos a no caer en engaños o provocaciones digitales.

RECOMENDACIÓN

Para evitar el rastreo de los sitios web se puede usar Ghostery (**https://www.ghostery.com/)** o Badger, nuevamente muy recomendados por ser software libre (**https://www.eff.org/es/privacybadger).**

a) VPN

Una pieza importante para navegar de manera segura es el uso de VPNs. Las VPNs o Red Privada Virtual, permiten que la ubicación geográfica del usuario o usuaria se exponga de manera directa y que todo su tráfico viaje de manera cifrada. Existen muchos servicios que ofrecen VPNs gratuitas, sin embargo, no hay que olvidar que el proveedor de la VPN puede rastrear todo el tráfico de un/una usuario/a y realizar un análisis del mismo. Por eso hay que elegir con cautela cual proveedor de VPN es el más adecuado para determinado contexto.

Elegir una VPN puede parecer una tarea complicada debido a la cantidad de proveedores que existen. Podemos apoyarnos en herramientas como The Best VPN (**https://thebestvpn.com/),** un sitio que permite consultar un análisis de los proveedores de VPNs que existen. Para elegir una VPN hay que tomar en cuenta:

- Qué información guardan de las y los usuarios : **https://thebestvpn.com/118-vpns-logging-policy/**
- Velocidad de descarga
- Características de privacidad y seguridad
- Política de jurisdicción y registro
- Disponibilidad para descargar torrents y utilizar Netflix
- Usabilidad y soporte
- Costo
- Compatibilidad con dispositivos, ¿hay un cliente (app) para determinado equipo o dispositivo?

- Disponibilidad de servidores cercanos a la región. No es lo mismo vivir en Europa y tener el VPN en Brasil, que vivir en Brasil y tener el VPN en Chile.
- Si incluye sistema Kill-Switch, bloqueo de internet cuando el VPN deja de funcionar, y si éste es útil.

NO OLVIDAR

Utilizar el servicio de VPN que más se ajuste a las necesidades del/ de la usuario/a.

CONSEJO

Si no existen recursos económicos para adquirir una VPN estas opciones gratuitas son seguras y revisadas por la comunidad de ciberactivistas: Psiphon (**https://psiphon.ca**) y Tunnel Bear (**https://www.tunnelbear.com/**) esta última opción solo regala 500 megas al mes.

b) Apps Cifradas

Hay que asegurarse que la información que se genera y comparte a través de aplicaciones de los teléfonos móviles o tablets se encuentre tan segura como la de los correos electrónicos u otros usos digitales. Para esto podemos apoyarnos en dos tipos de aplicaciones: las que utilizan cifrado y las que operan en redes pequeñas y de confianza (redes mesh).

Las aplicaciones cifradas o encriptadas, son aquellas que utilizan alguna medida de seguridad: en donde el mensaje al momento de enviarse se cifra -viaja cifrado- y al momento de ser recibido se descifra. Esto se conoce como *cifrado punto a punto*. Un extra que añaden algunas aplicaciones es que no almacenan estos mensajes en sus servidores sino en los dispositivos de las y

los usuarios asegurando que la información no quede en ningún otro lugar más allá de las bandejas de entrada de quien envía y quien recibe.

Whatsapp beneficios y riesgos

Whatsapp es la aplicación de mensajería más usada en el mundo. En los últimos años ha mejorado sus sistemas de seguridad en favor de la privacidad, pero como todo en seguridad digital nada es 100% seguro y tiene ventajas y desventajas:

Ventajas:

- Las conversaciones van de un celular a otro de forma cifrada.

Desventajas:

- Da privacidad, pero no anonimato.
- No se pueden eliminar mensajes o hacer que los mensajes se borren después de ser leídos.
- Tener los mensajes e hilos de conversación en el celular es una gran desventaja si se es detenido
- Si no se revisa la configuración o ajustes iniciales, puede generar respaldos en tu celular y en una cuenta de Google Drive.

Algunos ejemplos de aplicaciones cifradas recomendadas y que no guardan mensajes privados en sus servidores son:

- **http://signal.org/** (La principal alternativa a Whatsapp)
- **https://www.wickr.com/** (Ofrece anonimato, no es necesario registrar un número y solo pide un nickname o apodo).
- **https://www.surespot.me/** (Da anonimato, no es necesario registrar un número y solo pide un nickname o apodo).
- **https://ring.cx** (Ofrece anonimato, no pide el registro de un número y solo se necesita un nickname o apodo).

Aplicación para cifrar SMS, pues son transparentes:

- **https://silence.im/** (Solo funciona en dispositivos Android)

Mensajería instantánea, videoconferencia y voz ip:

- **https://jitsi.org/** (La alternativa libre y segura a Skype y Hangout).

Todas las herramientas han sido auditadas y verificadas: funcionan como dicen hacerlo gracias a que son software libre (*open source*). Y cuentan con clientes multiplataforma tanto para móviles como equipos de computo.

2.4.5 Opción off-line: *El mesh*

En una zona sin internet donde es necesario charlar con colegas que están cerca para comunicar información sensible que no se puede decir a viva voz, las aplicaciones *mesh* pueden ser la opción.

Son aplicaciones que operan en redes pequeñas y de confianza que se apoyan en un concepto, *mesh* o *redes en malla*, en donde cada emisor/receptor se considera un nodo y la red se va creando a partir de interconectar todos estos nodos entre sí. Una red de redes. Este sistema vuelve *independiente* la red de Internet ya que todos estos nodos conforman una pequeña red local.

Estas redes y aplicaciones son sumamente útiles para comunicaciones en distancias pequeñas y grupos locales en donde todas/os las y los usuarios se encuentran cerca físicamente. También son sumamente recomendadas en eventos como desastres naturales o manifestaciones, ya que como en el ejemplo anterior, operan en un grupo concentrado físicamente en algún lugar y no dependen directamente de Internet, ayudando así a interconectar rápidamente sin depender de Internet o ayudando a evadir problemas como son la censura o vigilancia.

Algunos ejemplos de aplicaciones mesh recomendadas son:

- **https://www.bridgefy.me/**
- **https://briarproject.org/**
- **https://www.opengarden.com/firechat.html**
- **http://www.servalproject.org/**
- **http://getzombiechat.com/**

2.4.6 Archivos, respaldos y cifrado

El buen cuidado y manejo de archivos es una tarea indispensable día con día, nos ayuda a mantener ordenada nuestra información y a administrar de manera eficiente. A su vez una buena administración nos permite realizar tareas un poco más operativas como lo son los respaldos.

Tener respaldos de información nos permite prevenir que exista una pérdida de información en casos que no tenemos previstos, como un daño a nuestro equipo, una infección por virus, o un robo o extravío de donde sea que se almacene la información.

Los respaldos se recomienda realizarlos con la mayor regularidad posible, ya sea cada dos o cada cuatro semanas. Esto con dos fines, el primero, controlar la información que vamos a respaldar, pudiendo así ser más selectivas/os en los archivos que se respalda, y el segundo, no acumular información en cantidades grandes, así podemos realizar nuestro respaldo rápido y sin complicaciones.

Para realizar un respaldo es posible apoyarse en alguna herramienta que automatice el proceso, ya sea programando para que se ejecute de manera periódica o para que sincronice la información con algún medio extraíble o a la nube. Algunas herramientas recomendadas son:

- Windows, Cobian Backup: **http://www.cobiansoft.com/cobianbackup.htm**
- Mac OS, Time Machine
- GNU/Linux, Déjà Dup: **https://launchpad.net/deja-dup**
- Multiplataforma:
  - Amanda: **http://www.amanda.org/**
  - UrBackup: **https://www.urbackup.org/**
  - Bacula: **http://blog.bacula.org/**
  - **https://www.duplicati.com/**

En el caso del almacenamiento, una buena práctica es tener un respaldo en algún medio físico como un disco extraible y en algún servicio en la nube. Para el medio físico, hay que mantenerlo asegurado procurando evitar sufrir riesgos por golpes, cambios climáticos o robo entre otros. Para la nube actualmente hay soluciones que respetan tu privacidad y resguardar tu información de tal modo que nadie puede husmear en ella.

Cifrado

El cifrado de archivos es una práctica que era considerada compleja para la mayoría de las y los usuarios ya que entender el proceso a primera vista podría ser complicado. Sin embargo ya se ha convertido en una práctica común y un hábito muy fácil y útil para asegurar que terceras personas accedan a información personal.

Fuente: **https://cryptomator.org/**

Para realizar un cifrado existen diversas herramientas: ya sea desde un archivo hasta equipos completo. El cifrado de archivos específicos se recomienda cuando hay que compartir estos archivos por algún medio que no se puede controlar la seguridad al 100 porciento, como un correo electrónico o una memoria USB. El cifrado sirve, es necesario, para asegurar que solamente el/la destinatario/a sea capaz de leer un mensaje.

Para proteger los archivos en una computadora o cifrar la información almacenada en la nube, se puede usar *Cryptomator*: una aplicación para computadora y celular que permite cifrar una carpeta específica de una computadora con un poderoso sistema de seguridad y únicamente usando una contraseña de seguridad. Sin configuraciones complejas ni largos procesos. Aunque hay que tener cuidado: la contraseña es irrecuperable.

En una carpeta cifrada se puede tener guardada información personal importante como fotos de documentos personales, documentos de trabajo u otros archivos considerados valiosos. También permite sincronizar la carpeta con servicios externos como Dropbox y Google Drive, para ello, naturalmente, hay que tener Dropbox o Google Drive instalados en la computadora.

2.4.7 Verificación de apps

Una de las medidas básicas de seguridad digital y sin duda de las más fuertes es la verificación de las aplicaciones y sus fuentes. Como su nombre lo indica, esta actividad se basa en verificar que las aplicaciones y sus fuentes sean originales y oficiales para así asegurar que éstas no han sufrido modificaciones no deseadas. Así es posible prevenir bastantes problemas que van desde la suplantación de identidad por una app o programa hasta la instalación y ejecución de malware.

El primero es la verificación de la fuente en el cual la regla es “No instalar programas o aplicaciones que no vengan de una fuente oficial”. En el caso de programas para equipos de cómputo la fuente es la empresa proveedora y/o desarrolladora del programa.

A la hora de descargar e instalar un programa hay que verificar que el sitio de donde se está descargando sea de la empresa desarrolladora o de un proveedor avalado por ella. Para las aplicaciones basta con que se realice la instalación de la tienda oficial de un sistema operativo o directamente del sitio del desarrollador.

- Evitar el uso de software pirata o crackeado, ya que éste usualmente es modificado y no se tiene la certeza de que no contenga software malicioso.

NOTA

El paquete, las USB en venta o los discos pirata tienen software pirata o crackeado.

- Evitar usar software de países o proveedores que se sabe suelen contener software malicioso como es el ejemplo de China o Rusia. Son países en donde la cantidad de hackers es alta y con facilidad un programa no verificado puede haber sido modificado por una tercera persona y distribuido en páginas falsas para intereses maliciosos.
- En caso de no poder adquirir una licencia de paga, es posible apoyarse en el software libre y de código abierto (FOSS), el cual es una alternativa al software privativo y de paga, y que cuenta con diversos beneficios para quienes buscan herramientas alternativas. Por ejemplo si se busca un word o excel, se puede descargar Open Office (**https://www.openoffice.org/download/)**

- También existen programas para verificar la autenticidad de las aplicaciones utilizadas en los celulares, sean Android o IOS.

En el caso de Android la verificación de Apps se localiza en los "Ajustes" o "Configuración".

Pasos para verificación de apps:

1. Ir a configuración o ajustes y buscar Google.
2. En el menú de Google buscar la sección llamada Seguridad
3. Ya en Seguridad, entrar a Google Play Protect o "Verificar Aplicaciones".
4. Dentro de Verificación de Aplicaciones o Google Play Protect activar el escaneo del dispositivo por amenazas de seguridad.
5. De forma automática el dispositivo Android verificará las APPs que se descargan e instalan.

2.4.8 Seguridad digital para sitios

Actualmente es común que más y más personas u organizaciones tengan sus propios sitios web. Estos suelen ser administrados por personas que no siempre cuentan con un perfil técnico: dada la sencillez que las tecnologías actuales ofrecen.

Para administrar adecuadamente un sitio es necesario ser consciente de los riesgos y amenazas que esto implica y conocer algunas medidas para prevenir más y corregir menos.

Dentro de la inmensidad de amenazas que existen, las más comunes son:

- Ataques distribuidos de denegación de servicios (DDoS)
- Inserción y ejecución de código malicioso que se ejecuta en el servidor
- Inserción y ejecución de código malicioso que se ejecuta en el navegador web

- Inyecciones SQL para alterar o extraer información de las bases de datos
- Robo de cookies o información local temporal
- Cross-site requesting
- Phishing y suplantación de identidad
- Hackeo y robo de servidores

Una de las tecnologías más utilizadas actualmente para el desarrollo y administración de sitios web son los gestores de contenido (CMS), los cuales ya tienen soluciones para todos estos problemas en general y por lo cual se recomienda utilizar uno, así como mantenerlo al día con sus actualizaciones de temas y plugins.

En esta parte de la guía abordaremos cómo realizar conexiones cifradas mediante HTTPS y cómo prevenir daños por ataques DDoS ya que estos son problemas que un CMS por sí sólo no puede solucionar.

a) HTTPS

HTTPS es el protocolo para enviar y recibir información de manera cifrada entre sitios web y el navegador. Es la evolución de un protocolo llamado HTTP, en el cual la información no viaja cifrada.

Si la información no fuera cifrada ésta quedaría expuesta a cualquiera que estuviera monitoreando nuestro tráfico de Internet. Esto se vuelve potencialmente peligroso cuando se pretende navegar de manera anónima o cuando para compartir información privada o sensible como son datos personales o bancarios.

Para que el cifrado del protocolo HTTPS pueda funcionar es necesario utilizar algo llamado certificado. Un certificado es aquel

que se encarga de asegurar que la información se está cifrando. Para obtener un certificado debemos apoyarnos en una entidad certificadora, la cual se encarga de expedir los certificados y dando la seguridad de que el sitio que utiliza el certificado sea quien dice ser.

Usualmente las entidades certificadoras requieren de un pago para expedir un certificado, sin embargo, existe un proyecto llamado *Let's Encrypt*, el cual se encarga de expedir certificados de manera gratuita. Este proyecto surgió como respuesta a la necesidad de incrementar los sitios seguros en Internet por parte de la EFF.

Para utilizar *Let's Encrypt* existen opciones que se adecuan principalmente a tres escenarios:

1) El primero es cuando se tiene un servicio de hosting compartido. El mismo se administra mediante un cPanel.
2) El segundo es cuando se tienen permisos para crear y modificar archivos y carpetas en el servidor mediante FTP.
3) El tercero es cuando se tiene control de una terminal de comandos y acceso al sistema operativo del servidor.

El primero de los casos es el más sencillo y recomendable ya que requiere poca interacción. Para esto, basta con buscar la sección de Certificados SSL, Certificados TTL o Certificados HTTPS , entrar a la opción de *Crear* o *Gestionar certificados*, ingresar los datos requeridos para crear el certificado y después seleccionar la opción *Instalar certificado*. Éstas instrucciones son generales y pueden adaptarse a cualquier panel de administración con algun pequeña variante.

El segundo caso requiere acceder a un sitio para generar certificados basado en *Let's Encrypt* (**https://www.sslforfree.com/).**

En el sitio se ingresa el nombre de nuestro dominio, posteriormente se nos preguntará si deseamos verificar que somos el/la propietaria del sitio de manera manual o automática, cualquiera de las dos opciones requerirá que tengamos acceso a una conexión FTP para subir archivos. Dependiendo de la opción seleccionada se nos pedirá una serie de pasos de archivos a subir y *renombrar* de alguna manera. Es para comprobar que la propiedad del servidor y que se tiene acceso a él.

Finalizadas las instrucciones que nos pida el sitio a realizar en FTP se nos creará un certificado que podemos instalar en nuestro servidor mediante cPanel de manera similar a los explicado en el párrafo anterior, cambiando solamente la parte donde se genera el certificado por una opción para subir certificados ya generados.

Para el tercer escenario es necesario tener acceso a una terminal para administrar el sistema operativo delservidor. En este escenario es posible apoyarse de una herramienta llamada CertBot (**http://certbot.eff.org/).** Se puede instalar en el servidor y solicitarle que de manera automática cree el certificado. Todo esto no toma más allá de 6 líneas de comando en la terminal, es una opción muy sencilla y rápida.

b) Deflect y ataques DDoS

Deflect es un servicio para ONG's, grupos de sociedad civil, activistas y grupos de medios independientes, enfocado en mitigar ataques DDoS (Ataques distribuidos de denegación de servicio). El servicio es *open source* y no tiene costo, el grupo detrás de este servicio es *eQualit.ie*, una ONG enfocada a brindar soluciones de seguridad digital.

Un ataque distribuido de denegación de servicio, DDoS por sus siglas en inglés (Distributed Denial of Service), es un tipo de ataque informático enfocado en bloquear un servicio, casi siempre a través de multiples peticiones de acceso al sitio web.

Este tipo de ataque es muy usual en la actualidad ya que las herramientas para realizarlos se encuentran al alcance de todas las personas y son fáciles de operar. Estos ataques se suelen apoyar en redes de equipos infectados que trabajan para realizar estos ataques sin saberlo, al realizar solo peticiones a los sitios, el trabajo que realiza un equipo infectado pasa desapercibido para el usuario o dueño del equipo.

Actualmente las soluciones que existen para mitigar este tipo de agresiones suelen ser caras por el tipo de infraestructura que necesitan u ofrecen planes que van más allá de lo que un sitio de un grupo de divulgación y/o defensa de algún tema suele requerir. Por lo que no suelen ser accesibles para todos. Como alternativas están los servicios CDN (Content Delivery Network) como pueden ser CloudFlare, Akamai, Incapsula, Amazon CloudFront o SiteLock, que buscan ofrecer servicios para mitigar ataques DDoS con distintos planes de pago y herramientas.

En cualquier caso: levantar un sitio web es relativamente sencillo, por lo que cualquiera que lo desee puede hacerlo. La parte complicada es mantener un sitio con "buena reputación", que sea accesible por usuarias/os legítimas/os y esté disponible siempre que estas personas lo requieran.

El problema es cuando nuestro sitio contiene información que no es cómoda para alguien más y esta persona o entidad decide tomar acciones poco éticas contra nuestro sitio como lo es un ataque DDoS, ya sea para mantener el sitio inaccesible o intimidarnos para dejar de realizar nuestra actividad. Con frecuencia, los costos o herramientas para defendernos no están a nuestro alcance.

Deflect es recomendable para sitios que pueden estar expuestos a este tipo de ataques, y que entran bajo los criterios de elegibilidad de Deflect, estos pueden ser defensora/es de derechos humanos, organizaciones civiles, medios independientes o personas que trabajen en cualquier grupo afín a estos temas,

y por lo contrario, Deflect se rehusa a trabajar o colaborar con grupos que contravienen a la Declaración Universal de Derechos Humanos y que promueven discursos de odio o discriminación.

Deflect funciona sobre una infraestructura bastante robusta que se basa en utilizar múltiples servidores como respaldo "espejo" de nuestro sitio, esto significa que existe una copia de nuestro sitio almacenada en múltiples servidores y que cuando se desea "ingresar" al sitio, realmente estamos ingresando a una de las copias que se encuentran en alguno de los servidores de Deflect. Estos servidores son los que reciben el ataque por lo que nuestro sitio "real" u "original" nunca se ve afectado y permanece anónimo u oculto al atacante.

Para que lo anterior pueda suceder es necesario realizar ciertas configuraciones en nuestro sitio, en concreto es necesario apuntar el DNS de nuestro sitio a donde Deflect nos lo indique, DNS en sí es el encargado de que al escribir "misitio.com", nuestro navegador sepa a dónde dirigirse, esto es importante ya que en este caso nuestro navegador o cualquier que quiera acceder a nuestro sitio (por ejemplo un bot o un atacante) realmente se dirigirá a la copia existente en Deflect.

Cabe mencionar que para poder utilizar Deflect y configurarlo es necesario tener acceso a la configuración de nuestro sitio y a cierta información técnica del mismo, una guía más concreta y específica se puede encontrar en la documentación oficial de Deflect.

c) Configuraciones básicas de WordPress

Para saber si tenemos un sitio seguro que estamos manejando con WordPress, debemos hacernos estas preguntas (tener una bitácora con fechas y registro de incidentes puede ser muy útil):

Dominio

1. ¿La cuenta en el proveedor de dominio tiene una contraseña fuerte?
2. ¿Cuándo caduca el dominio? ¿Se necesita renovarlo pronto?

Servidor

1. ¿La contraseña del Cpanel cumple con las recomendaciones de seguridad?
2. ¿El servidor puede recibir todas las visitas o ya se llegó al límite y se necesita más accesos por mes?
3. ¿Cómo se han ido incrementando los contenidos? ¿Todavía se tiene espacio disponible en el disco duro?
4. ¿Al sitio se accede a través de HTTPS ? ¿Cuándo caduca el certificado SSL?
5. ¿Se tiene configurado el CDN?

Base de datos

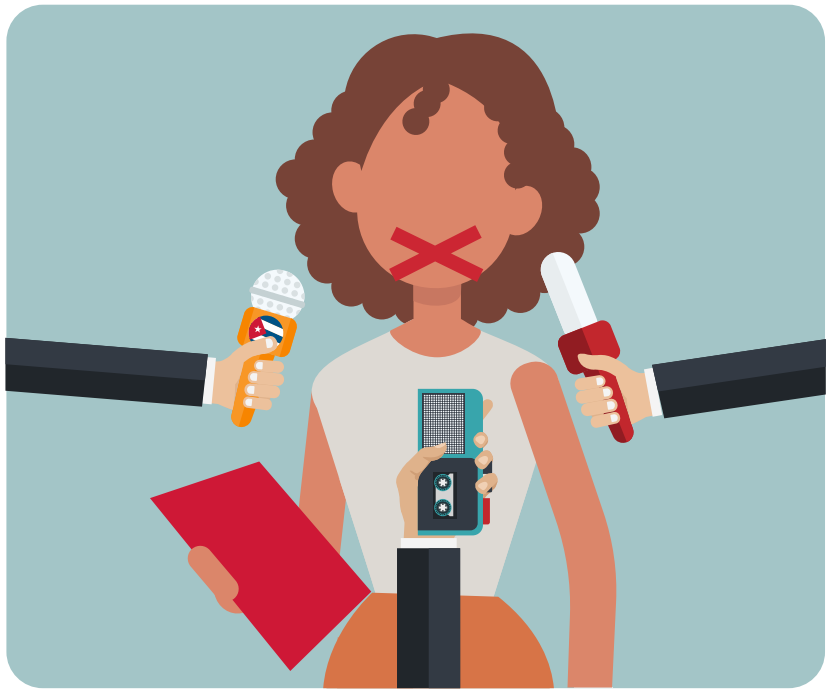
1. ¿Se ha cambiado el usuario por defecto de la base de datos? ¿Se ha elegido una contraseña resiliente para protegerlo?
2. El prefijo de la base de datos es por defecto o se ha configurado adecuadamente?

WordPress:

1. ¿El inicio de sesión todavía es por defecto? ¿O se lo cambio por algo más seguro y personalizado?
2. ¿Cómo se conectan las y los usuarios que pueden realizar cambios en la página? ¿Disponen de un segundo factor de autenticación?

Respaldo:

1. ¿Cuándo fue la última vez que se hizo un respaldo? Si la página se cayera ahora: ¿Qué se perdería de contenido?
2. ¿Se sabe el proceso para restaurar la página?



III. Marco Jurídico

En este apartado se exponen las leyes que más afectan a la labor del periodismo, el libre derecho a la expresión y a la información:

La **Constitución Cubana**, es el documento máximo en el que se dictan las principales directrices y derechos que los ciudadanos tienen.

- **Código Penal**: En él se establecen las funciones y alcances de los funcionarios públicos, así como las sanciones a las que se hacen acreedores en caso de incumplimiento.
- **La Ley 88/99** "De Protección de la Independencia Nacional y la Economía". Más conocida como *Ley Mordaza*, fue creada por el Estado cubano en 1999 para proteger al país contra las amenazas externas a su autonomía, la cual según el informe Situación del Derecho a la Libertad de Opinión y Expresión en Cuba (Cubalex et al., 2016) tiene implicaciones directas para las y los periodistas, comunicadores y defensores de los Derechos Humanos.

Sanciona con cárcel "aquellas acciones que en concordancia con los intereses imperialistas persiguen subvertir el orden interno de la nación y destruir su sistema político, económico y social". Es decir, ningún ciudadano puede difundir sus opiniones acerca de la gestión política, económica y social del actual gobierno y las sanciones pueden ir de los 2 a los 20 años con multas de entre 100 y 250.000 pesos. (La ley 88 completa se puede consultar en el **Anexo III** de este manual).

3.1 Algunas consideraciones

- En Cuba no existen procesos especiales, como el amparo o el *hábeas data*, para la defensa de los derechos constitucionales.
- En materia de libertad de expresión y prensa, no es posible la intervención de los tribunales de la jurisdicción contenciosa-administrativa.
- Las libertades de expresión y prensa en Cuba no pueden ser ejercidas contra el Estado, y solo a partir de la identificación con los intereses de éste es que pueden desarrollarse.
- No se permite la existencia de otros medios de comunicación y prensa que no sean los oficiales o aquellos pertenecientes a las organizaciones sociales y de masas reconocidas por el Estado, los cuales en todos caso deben seguir la política informativa trazada por el PCC.
- No se cuenta con una ley especial que regule el funcionamiento de la prensa, lo cual supone la carencia de una garantía sustantiva en este sentido.

Derechos Humanos

No hay reconocimiento de los Derechos Humanos como tal, porque no aparecen en el ordenamiento jurídico interno (constitución, código penal, etc) que contienen los derechos reconocidos para los ciudadanos; por lo tanto, se desconocen los estándares y organizaciones internacionales de protección.

Artículo 53 de la Constitución, Capítulo VII

Derecho, Deberes y Garantías Fundamentales (siempre conforme a los fines de la "sociedad socialista").

Reconoce a los ciudadanos la libertad de palabra y prensa. La prensa, la radio, la televisión, el cine y otros medios de difusión masiva son de propiedad estatal o social y en ningún caso pueden ser de propiedad privada. Así, las libertades de expresión y prensa solo pueden ejercerse a través de los medios propiedad del estado que son concebidos desde la estructura de poder y sirven de complemento al ejercicio de éste. Por lo tanto, las expresiones contrarias a los intereses del gobierno, sus instituciones y funcionarios son criminalizadas y sancionadas por severas leyes.

El artículo 53 indica que para el derecho a la libertad de palabra y prensa, la Asamblea Nacional (órgano legislativo que ostenta el supremo poder del Estado) debe adoptar normas o medidas eficaces para proteger este derecho. Hasta el momento no lo ha hecho.

Ley de Dignidad Nacional de 1997
Establece penas de prisión de tres a 10 años para cualquier persona que, de manera directa o indirecta, colabore con medios de comunicación del enemigo y aplica para información o productos periodísticos enviados al exterior.

3.2 El Código Penal

Es el principal mecanismo para reprimir y castigar a aquellos que sean abiertamente críticos al gobierno y es la disposición de largo alcance para restringir la libertad de palabra. La ley penal cubana tipifica delitos que en el fondo buscan proteger a las autoridades estatales de opiniones críticas, restringiendo con ello la libertad de expresión. Ente estos delitos se incluye: propaganda enemiga, la clandestinidad de impresos, el desacato, el orden público y tres figuras delictivas dirigidas a proteger el honor: difamación, calumnia e injuria. Se pueden aplicar los siguientes artículos a periodistas.

- **Artículo 73.1**. **Conducta antisocial** al que quebranta habitualmente las reglas de convivencia social mediante actos de violencia, o por otros actos provocadores, viola derechos de los demás o por su comportamiento en general daña las reglas de convivencia o perturba el orden de la comunidad o vive, como un parásito social, del trabajo ajeno o explota o practica vicios socialmente reprobables.
- **Artículo 75.1.** Una persona puede recibir una **advertencia** oficial sin que su actuar esté comprendido en alguno de los estados peligrosos a que se refiere el artículo 73. Se podrá recibir la **advertencia de** acuerdo a los vínculos o **relaciones con personas potencialmente peligrosas** para la sociedad, las demás personas y el orden social, económico y político del Estado socialista.
- **Artículo 91.** Impone **largas penas de prisión o la muerte** para aquellos que actúan contra "la independencia o la integridad territorial del estado".
- **Artículo 103.1**. Tipifica el delito de ***Propaganda Enemiga***, el cual se configura a partir de la incitación, mediante la propaganda oral o escrita o en cualquier otra forma, contra el

orden social, la solidaridad internacional o el Estado socialista (artículo 103.1 inciso a)). También se puede considerar la ocurrencia de este delito, si la acción consiste en confeccionar, distribuir o poseer propaganda del mismo carácter (artículo 103.1 inciso b)). **En ambos casos la sanción es de uno a ocho años de privación de libertad**.

- **Artículo103.2 La difusión de noticias falsas o predicciones** maliciosas tendentes a causar alarma o descontento en la población, o desorden público, **se sanciona con privación de libertad de uno a cuatro años** (artículo 103.2). Y si para los apartados anteriores, se utilizan medios de difusión masiva, la sanción es de **privación de libertad de siete a quince años** (artículo 103.3).
- **Artículo 144.1**. Sobre el ***Desacato***, de acuerdo con éste, el que amenace, calumnie, difame insulte, injurie o de cualquier u ofenda, de palabra o por escrito, en su dignidad o decoro a una autoridad, funcionario público, o a sus agentes o auxiliares, en el ejercicio de sus funciones, la sanción es **privación de libertad de tres meses a un año o multa de cien a trescientas cuotas**.
- **Artículo 200. *El orden público***, es aquel conjunto de normas del Derecho que regulan el orden de la convivencia ciudadana, orden externo y material de la misma. En el apartado primero, se **sanciona con privación de libertad de tres meses a un año o multa de cien a trescientas cuotas**, al que, sin causa que lo justifique, en lugares públicos, espectáculos o reuniones numerosas, dé gritos de alarma o profiera amenazas de un peligro común.
- **Artículo 318.1 Difamación / Artículo 319.1 Calumnia / Artículo 320.1 Injuria**.

  Referente a la ***difamación*** mantiene la prohibición contra la difamación de cualquier institución del Gobierno, organizaciones políticas o “héroes o mártires de la República”

y se sanciona con tres meses a un año de prisión o multa. El delito de ***Calumnia*** se tipifica a partir de que una persona, divulgue hechos falsos que redunden en descrédito de una persona y se sanciona con la privación de libertad de seis meses a dos años o multa de doscientas a quinientas cuotas. El otro delito por el que se protege al honor como bien jurídico-penal es el de ***Injuria*** y establece que "de propósito, por escrito o de palabra, a través de dibujos, gestos o actos ofenda a otro en su honor", será castigado con tres meses a un año de prisión o una multa.

Otras figuras que funcionan como límites a las libertades de expresión y prensa son :

- ***Ultraje a los Símbolos de la Patria:*** se protege a los símbolos nacionales (la bandera, el himno y el escudo nacionales).

- ***Difamación de las Instituciones y Organizaciones y de los Héroes y Mártires:*** establece como acción típica la difamación, denigración, o menosprecio de las instituciones de la república, las organizaciones políticas, de masas o sociales del país, o a los héroes y mártires de la patria.

- ***Clandestinidad de Impresos:*** es un delito que ***funciona como límite específico a la libertad de prensa***. Básicamente se trata de la confección, difusión o circulación de publicaciones sin indicar la imprenta o el lugar de impresión o sin cumplir las reglas establecidas para la identificación de su autor, o de su procedencia, o las reproduzca, almacene o transporte, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas. Es un delito que describe conductas muy variadas, pues abarca desde la confección hasta la circulación.

Apoyo internacional

A continuación, una lista de algunas de las organizaciones que ofrecen apoyos a periodistas y la libertad de expresión:

Apoyo en caso de emergencia:

APLP
Asociación Pro Libertad de Prensa
2006aplp@gmail.com
Calle Independecia #1046 entre Lucha y Esperanza.
Managua Ciudad Habana.
+53 7 609 8400

CIDH
Comisión Interamericana de Derechos Humanos
Para enviar denuncias:
Correo electrónico: **cidhdenuncias@oas.org**
Formulario electrónico: **www.cidh.org**
Correo postal:
Comisión Interamericana de Derechos Humanos
1889 F Street, N.W.
Washington-D.C. 20006 Estados Unidos

Cubalex
Promoción y defensa de los derechos humanos.
Servicio online de asesoría y asistencia legal gratuita.
info@cubalex.org

Fondo de Emergencia de la IWMF brinda a las mujeres periodistas

https://goo.gl/FSqh48

- Pequeñas subvenciones para atención psicológica y médica relacionadas a incidentes y amenazas en el trabajo como periodista;
- Tres meses de asistencia para reubicación temporal en casos de crisis o amenazas;
- Ayuda legal para contrarrestar amenazas de encarcelamiento o censura;
- Asistencia no financiera en forma de información sobre el acceso a recursos adicionales.

Access Now

Help@accesnow.org

Para ataques digitales a defensores de DDHH y periodistas.

Redes

Coalition for Women in Journalism (Coalición para la Mujer en el Periodismo)

http://womeninjournalism.org/home

Red global de apoyo a mujeres profesionales del periodismo. El objetivo es propagar la corresponsabilidad entre las colegas y crear nuevas vías de prosperidad para las mujeres. Además, ofrece asistencia profesional y psicológica en crisis a través de su línea gratuita de ayuda.

International Women's Media Fundations

https://www.iwmf.org/programs/adelante/

Adelante es una iniciativa de la IWMF para apoyar a mujeres periodistas reportando sobre y/o trabajando en América Latina. La iniciativa intenta reducir la brecha de género en la región brindándoles a mujeres periodistas oportunidades y habilidades para amplificar sus voces y avanzar profesionalmente.

Sembra Media

https://www.sembramedia.org/recurso/fondos/

Espacio para informarse sobre Fondos para periodismo: becas, organizaciones donantes e inversionistas

Protection International

https://www.protectioninternational.org/es/node/

Apoya a los defensores y las defensoras de los derechos humanos en el desarrollo de sus estrategias de gestión de seguridad y de protección. Cuenta con diferentes manuales y guías de protección individual y organizacional

AGRADECIMIENTOS

A todas y todos los periodistas y medios independientes por compartir sus experiencias y conocimientos.

La redacción de este manual fue posible gracias al trabajo conjunto y las valiosas contribuciones de:

Gracias también al apoyo y la información compartida a las siguientes organizaciones comprometidas con la libertad de expresión:

BIBLIOGRAFÍA

Aguilar, Paul; Araiza, Sergio. (2018). Seguridad digital básica in a nutshell

American Psychiatric Association. (2013). *Diagnostic and statistical manual of mental disorders* (5th ed.). Washington, DC: Author.

Article 19 Oficina de México y Centro América. *Prevenir para después informar: Guía práctica de seguridad para la cobertura en zonas de riesgo* p. 7

Beck, A.T., Ward, C.H., Mendelson, M., Mock, J. y Erbaugh, J. (1961). An inventory for measuring depression. Arch Gen Psychiatry. 4: 561-571.

Comité Internacional de la Cruz Roja, Tortura: *¿Qué asistencia brinda el CICR a las víctimas?* 26-06-2001. Recuperado el 6 de abril de 2018 en **https://www.icrc.org/spa/resources/documents/misc/5tdphh.htm**

Cubalex et al. (2016). Situación del Derecho a la Libertad de Opinión y Expresión en Cuba. Reporte preparado para el Relator Especial de las Naciones Unidas sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Sr. David Kaye. P. Sin número de edición.

Gallego Díaz Soledad. “Prensa y democracia”, en El País, Suplemento Domingo, 10 de mayo de 2009, p.11.

Gómez, María Ialia, “identificar el riesgo”, ponencia, en el Seminario de la sociedad Interamericana de Prensa, Guatemala, noviembre de 2008.

Madariaga,C. CINTRAS 2002. Trauma psicosocial, trastorno de estrés postraumático y tortura. Chile. En **http://www.cintras.org/textos/monografias/monog_trauma_psicosocial_espanol.pdf** Recuperado el 5 de abril de 2018.

Nieves Vera, M y Vela, J (1995). Cap. 9. Técnicas de relajación. En Caballo, V (comp) Manual de Técnicas de terapia de modificación de conducta. Ed. Siglo XXI. España. Pp 161-181.

Nezu, A.M y Nezu, C.M. (1995). Cap. 22. Entrenamiento en solución de problemas. En Caballo, V (comp) Manual de Técnicas de terapia de modificación de conducta. Ed. Siglo XXI. España. Pp 161-181.

Novakand, J.R. y Davidson, S. 2013. The journalistic structure of feeling: An exploration of Career life histories of Israeli journalists.Volume: 15 issue: 8, page(s): 987-1005. Disponible en **http://journals.sagepub.com/doi/abs/10.1177/1464884913512930.** Consultado el 1 de mayo de 2018.

Reporteros sin fronteras. (2016) Manual de seguridad para periodistas.

Santacruz Escudero, J.M. (2008). Una revisión acerca del debriefing como intervención en crisis y para la prevención del TEPT (trastorno de estrés postraumático). Rev. Colomb. Psiquiat., vol. 37:1.

Secuencia tomada de Vera y Vila Cap. 9. *Técnicas de Relajación. En Caballo, V. Manual de Técnicas de Terapia y Modificación de Conducta*. Ed. S-XXI

Segarra, P., Zellhuber, A, Velazquez-Cardoso, J. (2008) Manual de Situaciones críticas Vinland Solutions S.A. de C.V. México, DF

Washington Coalition of Sexual Assault Programs Published on Washington Coalition of Sexual Assault Programs (**http://www.wcsap.org**): Disponible en: **http://www.wcsap.org/neurobiology-reactions-stress-fight-or-flight-then-freeze,** consultado el 17 de mayo de 2018

REFERENCIAS SEGURIDAD DIGITAL

- **https://socialtic.org/wp-content/uploads/2018/04/ComoViajaTuInfoEnInternet.pdf**
- **https://socialtic.org/blog/como-viaja-tu-informacion-en-internet-consejos-y-herramientas-para-protegerla/**
- **https://edri.org/files/2012EDRiPapers/how_the_internet_works.pdf**
- **https://www.owasp.org/index.php/Modelado_de_Amenazas**
- **https://msdn.microsoft.com/es-es/library/aa561499(v=bts.10).aspx**
- **https://ssd.eff.org/es/module/evaluando-tus-riesgos**
- **https://protejete.wordpress.com/gdr_principal/analisis_riesgo/**
- **https://protejete.files.wordpress.com/2009/07/pres_11_analisis_riesgo.jpg**
- **https://protejete.wordpress.com/gdr_principal/matriz_riesgo/**
- **https://support.kaspersky.com/mx/614**
- **https://www.sslforfree.com/**
- **http://certbot.eff.org/**


ETECSA

ANEXOS

ANEXO I:
Análisis de riesgo

Enseguida presentamos tres ejemplos de posibles amenazas que sufren periodistas a causa de su trabajo. Cada ejemplo tiene su modelo de amenazas, mapeo de riesgo y su análisis de riesgo.

Modelo de Amenazas

Amenaza 1 (A1)

¿Existe alguien que tenga algún interés en hacerme/hacernos daño?

Sí, unos agentes de la "policía política" me han detenido en la calle para advertirme que estoy cruzando la línea en algunos temas, que me dedique a cultura.

¿Por qué?

Han dicho que mi trabajo ya no debe cubrir cosas políticas y económicas, que mi medio hace mucho ruido con eso, que, si hacemos otros temas, ellos no tienen problema.

¿Cómo podría afectarnos?

Citaciones y posibles detenciones por unas horas.

¿Qué tantos recursos tienen para lograrlo?

Ellos son la autoridad, tienen los recursos suficientes para hacerlos.

¿En el pasado nos ha hecho daño?

Hasta el momento no nos había pasado esto.

Amenaza 2 (A2)

¿Existe alguien que tenga algún interés en hacerme/hacernos daño?

Ayer, 30 de junio, le quitaron a la directora del medio el móvil por 30 minutos para una “revisión de rutina” en el aeropuerto.

¿Por qué?

Solo han dicho que era de rutina.

¿Cómo podría afectarnos?

Que nos quiten nuestros equipos de trabajo, como computadoras o celulares, en el aeropuerto al regresar de un viaje.

¿Qué tantos recursos tienen para lograrlo?

Cuando estamos en aduana siempre estamos solos.

¿En el pasado nos ha hecho daño?

Hemos escuchado rumores de otros colegas, pero nunca a nosotros.

Amenaza 3 (A3)

¿Existe alguien que tenga algún interés en hacerme/hacernos daño?

Uno de mis tíos me ha dicho que contará a mi madre a lo que me dedico y dará parte a las autoridades.

¿Por qué?

Me ha dicho que soy una traidora de la revolución y que colaboro con personas que buscan dañar mi país.

¿Cómo podría afectarnos?

Que mi tío diga a las autoridades información de otros colegas que me visitan en mi casa para hablar de trabajo.

¿Qué tantos recursos tienen para lograrlo?

No tiene muchos recursos materiales, pero es muy respetado por el CDR del barrio que es “muy rojo”.

¿En el pasado nos ha hecho daño?

Nunca me había hecho daño, pero se comenzó a molestar por algunas opiniones que hice en una reunión familiar.

Mapeo de Riesgo

Amenaza 1 – Intimidación (A1)

¿Qué quiero proteger?

Mi integridad física y emocional. Además, no quiero tener antecedentes penales.
Mi medio no quiere ser intimidado.

¿De qué lo quiero proteger?

Hostigamiento ¿De agresiones emocionales y legales?

¿De quién me quiero proteger?

“seguridad del estado”.

¿Qué tanto necesito protegerlo?

Vamos a dejar de publicar noticias de economía y política que tengan que ver directamente con funcionarios de alto nivel.

¿Qué tan fuertes pueden ser las consecuencias de no hacerlo?

Nos van a detener.

¿Cuánto esfuerzo estoy dispuesto a invertir para prevenir el riesgo?

No logramos llegar a un consenso, pero por el momento no haremos investigaciones de largo aliento sobre funcionarios de alto nivel.

Amenaza 2 – Movil (A2)

¿Qué quiero proteger?

Mi información personal en mis equipos.

¿De qué lo quiero proteger?

De decomisos.

¿De quién me quiero proteger?

Revisiones “aduanales”.

¿Qué tanto necesito protegerlo?

Que me extraigan información.

¿Qué tan fuertes pueden ser las consecuencias de no hacerlo?

Que mi información personal quede a la disposición de las autoridades y sean publicadas en blogs.

¿Cuánto esfuerzo estoy dispuesto a invertir para prevenir el riesgo?

Voy a cambiar mis hábitos de seguridad en equipos.

Amenaza 3 – Familiar (A3)

¿Qué quiero proteger?

Mi vida profesional y privada.

¿De qué lo quiero proteger?

Una ruptura familiar, con mis amistades y ser detenida o acosada por mi trabajo periodístico.

¿De quién me quiero proteger?

Mi tío.

¿Qué tanto necesito protegerlo?

Que termine en un escándalo público y legal por las denuncias de mi tío, necesito protegerme.

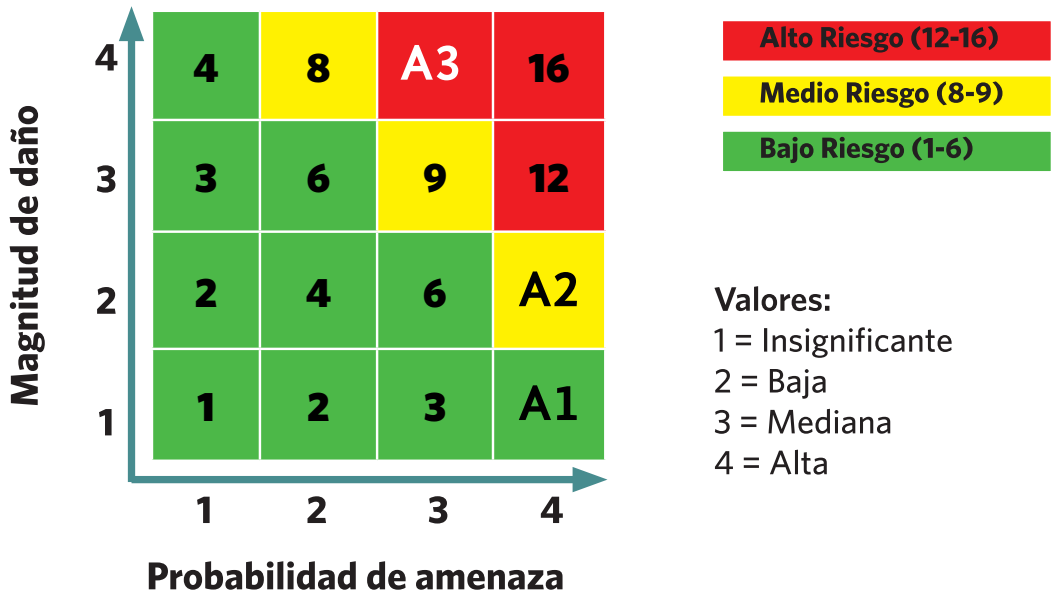
¿Qué tan fuertes pueden ser las consecuencias de no hacerlo?

Muy fuertes, terminar enfrentada a mi familia, amigos y aislada, sola.

¿Cuánto esfuerzo estoy dispuesto a invertir para prevenir el riesgo?

Todo, pero no sé qué hacer, ni cómo explicar a mis colegas.

Riesgo = probabilidad de amenaza * magnitud de daño



Conclusiones

Las tres amenazas tienen una probabilidad alta de ocurrir. La A1 tiene una alta probabilidad de ocurrir, pero una magnitud del daño que las personas involucradas consideraron de “bajo riesgo”. La A2 tiene una alta probabilidad de ocurrir, pero la magnitud del daño es considerado mediano si es que se siguen las recomendaciones de seguridad holística que sugieren van a seguir. Lamentablemente la A3 tiene una magnitud de daño alta, pues que ocurra ya no depende de nosotros sino de un agente externo que por razones ideológicas puede afectar nuestra vida privada, las otras dos amenazas pueden ser paleadas por acciones que dependen de nosotros y nuestros medios.

ANEXO II:
Registro de incidentes

Expediente interno

Tip: recuerda guardar esta información en un lugar seguro y tener un backup.

Nombre del caso:
Documenta:
Fecha: 02 de noviembre de 2015
<u>Datos de la víctima</u>
Nombre Completo:
Edad:
Fecha de Nacimiento:
Domicilio:
Estado Civil:
Teléfonos:
Correos Electrónicos:
Datos de trabajo:
Otros datos importantes:

Descripción de hechos (Debe ser lo más detallado posible):

Antecedentes del caso:

Documentación y pruebas sobre el caso (Debe agregarlos como anexos a su carpeta de expediente):

¿Qué va a hacer el medio o grupo de periodista para ayudar a la protección de la víctima?:

(Deben ser metas a corto, mediano y largo plazo. Es una planeación cronológica, detalla lo de la sección anterior).

Acciones Jurídicas y no jurídicas:

ANEXO III:
Ley 88

RICARDO ALARCON DE QUESADA, Presidente de la Asamblea Nacional del Poder Popular de la República de Cuba.

HAGO SABER: Que la Asamblea Nacional del Poder Popular en su Primera Reunión Extraordinaria de la Quinta Legislatura, celebrada los días 15 y 16 de febrero de 1999, ha aprobado lo siguiente:

POR CUANTO: El Gobierno de Estados Unidos de América se ha dedicado a promover, organizar, financiar y dirigir a elementos contrarrevolucionarios y anexionistas dentro y fuera del territorio de la República de Cuba. Durante cuatro décadas ha invertido cuantiosos recursos materiales y financieros para la realización de numerosas acciones encubiertas con el propósito de destruir la independencia y la economía de Cuba, utilizando para tales fines, entre otros, a individuos reclutados dentro del territorio nacional, como ha reconocido la Agencia Central de Inteligencia desde el año 1961, en informe que fuera divulgado en el año1998.

POR CUANTO: La Enmienda "Torricelli" incluida en la ley de Gastos para la Defensa de 1992, promulgada por el Gobierno de Estados Unidos de América, previó el suministro de medios materiales y financieros para el desarrollo de actividades contrarrevolucionarias dentro de Cuba, y mediante la Ley de 12 de marzo de 1996, conocida como Ley Helms - Burton, se amplió, intensificó y codificó la guerra económica contra Cuba y detalla el suministro de tales recursos a individuos que serían empleados en el territorio nacional para cumplir los propósitos subver-

sivos y anexionistas del Imperio, habiéndose reconocido públicamente, desde esa fecha y en reiteradas ocasiones, la entrega de dichos fondos del Presupuesto Federal de Estados Unidos para esos fines.

POR CUANTO: La Ley del Presupuesto Federal para 1999, promulgada el 21 de octubre de 1998 por el Gobierno de Estados Unidos de América, fijó un límite mínimo de dos millones de dólares para la realización de actividades contrarrevolucionarias dentro de Cuba y el 5 de enero de 1999 el Presidente de ese país anunció planes para engrosar, con recursos de entidades e individuos, los fondos federales que se destinan a la promoción y ejecución de dichas acciones.

POR CUANTO: Las acciones anteriormente mencionadas constituyen una permanente agresión contra la independencia y soberanía de la República de Cuba, violatoria del Derecho Internacional y de los principios y normas que rigen las relaciones entre los Estados, y de manera persistente esta agresión se ha ampliado e intensificado durante cuarenta años, se ha refrendado incluso mediante las decisiones legislativas antes mencionadas y se ha proclamado como política de Estado contra nuestro país, empleándose para su consecución cuantiosos recursos oficiales, a la vez que se promueve el empleo de los que destinen a esos fines otras entidades privadas e individuos.

POR CUANTO: Constituye un deber ineludible responder a la agresión de que es objeto el pueblo cubano, derrotar el propósito anexionista y salvaguardar la independencia nacional, tipificando como delitos las conductas que favorezcan la aplicación de la mencionada Ley “Helms-Burton”, el bloqueo, la guerra económica contra Cuba, la subversión y otras medidas similares que hayan sido adoptadas o sean adoptadas en el futuro por

el Gobierno de Estados Unidos de América, mediante disposición o regulación, con independencia de su rango normativo, así como otras medidas que propendan a fomentar o desarrollar esa política agresiva contra los intereses fundamentales de la Nación.

POR CUANTO: Es propósito de esta Ley sancionar aquellas acciones que en concordancia con los intereses imperialistas persiguen subvertir el orden interno de la Nación y destruir su sistema político, económico y social, sin que en modo alguno menoscabe los derechos y garantías fundamentales consagrados en la Constitución de la República.

POR CUANTO: En cumplimiento de lo dispuesto en la Ley de Reafirmación de la Dignidad y

Soberanía Cubanas, Ley No. 80 de 1996, el Gobierno de la República de Cuba, ha presentado a la

consideración de la Asamblea Nacional del Poder Popular, el proyecto correspondiente.

POR TANTO: La Asamblea Nacional del Poder Popular en uso de las atribuciones que le están conferidas en el artículo 75 inciso b) de la Constitución de la República, ha adoptado la siguiente:

LEY No. 88

DE PROTECCION DE LA INDEPENDENCIA NACIONAL Y LA ECONOMIA DE CUBA

CAPITULO I

Generalidades

Artículo 1. Esta Ley tiene como finalidad tipificar y sancionar aquellos hechos dirigidos a apoyar, facilitar o colaborar con los objetivos de la Ley "Helms-Burton", el bloqueo y la guerra económica contra nuestro pueblo, encaminados a quebrantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba.

Artículo 2. Dado el carácter especial de esta Ley, su aplicación será preferente a cualquier otra legislación penal que le preceda.

Artículo 3.1. A los delitos previstos en esta Ley le son aplicables, en lo atinente, las disposiciones contenidas en la Parte General del Código Penal.

2. En los delitos previstos en esta Ley el tribunal puede imponer como sanción accesoria la confiscación de bienes.

3. Los delitos previstos en esta Ley se sancionan con independencia de los que se cometan para su ejecución o en ocasión de ella.

CAPITULO II

De las Infracciones Penales

Artículo 4.1. El que suministre, directamente o mediante tercero, al Gobierno de Estados Unidos de América, sus agencias, dependencias, representantes o funcionarios, información para facilitar los objetivos de la Ley "Helms-Burton", el bloqueo y la guerra económica contra nuestro pueblo, encaminados a que-

brantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba, incurre en sanción de privación de libertad de siete a quince años.

2. La sanción es de privación de libertad de ocho a veinte años cuando concurra alguna de las circunstancias siguientes:

a) si el hecho se comete con el concurso de dos o más personas;

b) si el hecho se realiza con ánimo de lucro o mediante dádiva, remuneración, recompensa o promesa de cualquier ventaja o beneficio;

c) si el culpable llegó a conocer o poseer la información de manera subrepticia o empleando cualquier otro medio ilícito;

d) si el culpable conociera o poseyera la información por razón del cargo que desempeñe;

e) si, como consecuencia del hecho, se producen graves perjuicios a la economía nacional;

f) si, como consecuencia del hecho, el Gobierno de Estados Unidos de América, sus agencias o dependencias, adoptan medidas de represalias contra entidades industriales, comerciales, financieras o de otra naturaleza, cubanas o extranjeras, o contra alguno de sus dirigentes o familiares.

Artículo 5.1. El que, busque información clasificada para ser utilizada en la aplicación de la Ley“Helms-Burton”, el bloqueo y la guerra económica contra nuestro pueblo, encaminados a quebrantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba, incurre en sanción de privación de libertad de tres a ocho años o multa de tres mil a cinco mil cuotas, o ambas.

2. La sanción es de privación de libertad de cinco a doce años cuando concurra alguna de las circunstancias siguientes:

a) si el culpable llegó a conocer o poseer la información de manera subrepticia o empleando cualquier otro medio ilícito;

b) si el hecho se comete con el concurso de dos o más personas.

3. La sanción es de privación de libertad de siete a quince años si la información obtenida, por la índole de su contenido, produce graves perjuicios a la economía nacional.

Artículo 6.1. El que acumule, reproduzca o difunda, material de carácter subversivo del Gobierno de Estados Unidos de América, sus agencias, dependencias, representantes, funcionarios o de cualquier entidad extranjera, para apoyar los objetivos de la Ley Helms-Burton, el bloqueo y la guerra económica contra nuestro pueblo, encaminados a quebrantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba, incurre en sanción de privación de libertad de tres a ocho años o multa de tres mil a cinco mil cuotas, o ambas.

2. En la misma sanción incurre el que con iguales propósitos introduzca en el país los materiales a que se refiere el apartado anterior.

3. La sanción es de privación de libertad de cuatro a diez años cuando concurra en los hechos a que se refieren los apartados anteriores, alguna de las circunstancias siguientes:

a) si los hechos se cometen con el concurso de dos o más personas;

b) si los hechos se realizan con ánimo de lucro o mediante dá-

diva, remuneración, recompensa o promesa de cualquier ventaja o beneficio.

4. La sanción es de privación de libertad de siete a quince años si el material, por la índole de su

contenido, produce graves perjuicios a la economía nacional.

Artículo 7.1. El que, con el propósito de lograr los objetivos de la Ley "Helms-Burton", el bloqueo y la guerra económica contra nuestro pueblo, encaminados a quebrantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba, colabore por cualquier vía con emisoras de radio o televisión, periódicos, revistas u otros medios de difusión extranjeros, incurre en sanción de privación de libertad de dos a cinco años o multa de mil a tres mil cuotas, o ambas.

2. La responsabilidad penal en los casos previstos en el apartado que antecede será exigible a los que utilicen tales medios y no a los reporteros extranjeros legalmente acreditados en el país, si fuese esa la vía empleada.

3. La sanción es de privación de libertad de tres a ocho años o multa de tres mil a cinco mil cuotas, o ambas, si el hecho descrito en el apartado 1 se realiza con ánimo de lucro o mediante dádiva, remuneración, recompensa o promesa de cualquier ventaja o beneficio.

Artículo 8.1. El que perturbe el orden público con el propósito de cooperar con los objetivos de la Ley "Helms-Burton" , el bloqueo y la guerra económica contra nuestro pueblo, encaminados a quebrantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba, incurre en sanción de privación de libertad de dos a cinco años o multa de mil a tres mil cuotas, o ambas.

2. El que, promueva, organice o incite a realizar las perturbaciones del orden público a que se refiere el apartado anterior incurre en sanción de privación de libertad de tres a ocho años o multa de tres mil a cinco mil cuotas o ambas.

Artículo 9.1. El que, para favorecer los objetivos de la Ley "Helms-Burton" , el bloqueo y la guerra económica contra nuestro pueblo, encaminados a quebrantar el orden interno, desestabilizar el país y liquidar al Estado Socialista y la independencia de Cuba, realice cualquier acto dirigido a impedir o perjudicar las relaciones económicas del Estado cubano, o de entidades industriales, comerciales, financieras o de otra naturaleza, nacionales o extranjeras, tanto estatales como privadas, incurre en sanción de privación de libertad de siete a quince años o multa de tres mil a cinco mil cuotas o ambas.

2. La sanción es de privación de libertad de ocho a veinte años cuando concurra alguna de las circunstancias siguientes:

a) si en la realización del hecho se emplea violencia, intimidación, chantaje u otro medio ilícito;

b) si el hecho se realiza con ánimo de lucro o mediante dádiva, remuneración, recompensa o promesa de cualquier ventaja o beneficio;

c) si, como consecuencia del hecho, el Gobierno de Estados Unidos de América, sus agencias o dependencias, adoptan medidas de represalias contra entidades industriales, comerciales o financieras, cubanas o extranjeras, o contra alguno de sus dirigentes o familiares.

Artículo 10. Incurre en sanción de privación de libertad de dos a cinco años o multa de mil a tres mil cuotas o ambas, el que:

a) proponga o incite a otros, por cualquier medio o forma, a ejecutar alguno de los delitos previstos en esta Ley;

b) se concierte con otras personas para la ejecución de alguno de los delitos previstos en esta Ley.

Artículo 11. El que, para la realización de los hechos previstos en esta Ley, directamente o mediante tercero, reciba, distribuya o participe en la distribución de medios financieros, materiales o de otra índole, procedentes del Gobierno de Estados Unidos de América, sus agencias, dependencias, representantes, funcionarios o de entidades privadas, incurre en sanción de privación de libertad de tres a ocho años o multa de mil a tres mil cuotas, o ambas.

Artículo 12. El que incurra en cualquiera de los delitos previstos en los artículos anteriores con la cooperación de un tercer Estado que colabore a los fines señalados con el Gobierno de Estados Unidos de América, será acreedor a las sanciones establecidas.

DISPOSICIONES FINALES

PRIMERA: La Fiscalía General de la República, respecto a los delitos previstos y sancionados en la presente Ley, ejerce la acción penal pública en representación del Estado en correspondencia con el principio de oportunidad, conforme a los intereses de la Nación.

SEGUNDA: Los Tribunales Provinciales Populares son competentes para conocer de los delitos previstos en esta Ley.

TERCERA: Se derogan cuantas disposiciones legales o reglamentarias se opongan a lo establecido en esta ley, que comen-

zará a regir desde la fecha de su publicación en la Gaceta Oficial de la República.

DADA en la sala de sesiones de la Asamblea Nacional del Poder Popular, Palacio de las Convenciones, en la ciudad de La Habana a los dieciséis días del mes de febrero de mil novecientos noventa y nueve, "Año del 40 Aniversario del Triunfo de la Revolución".