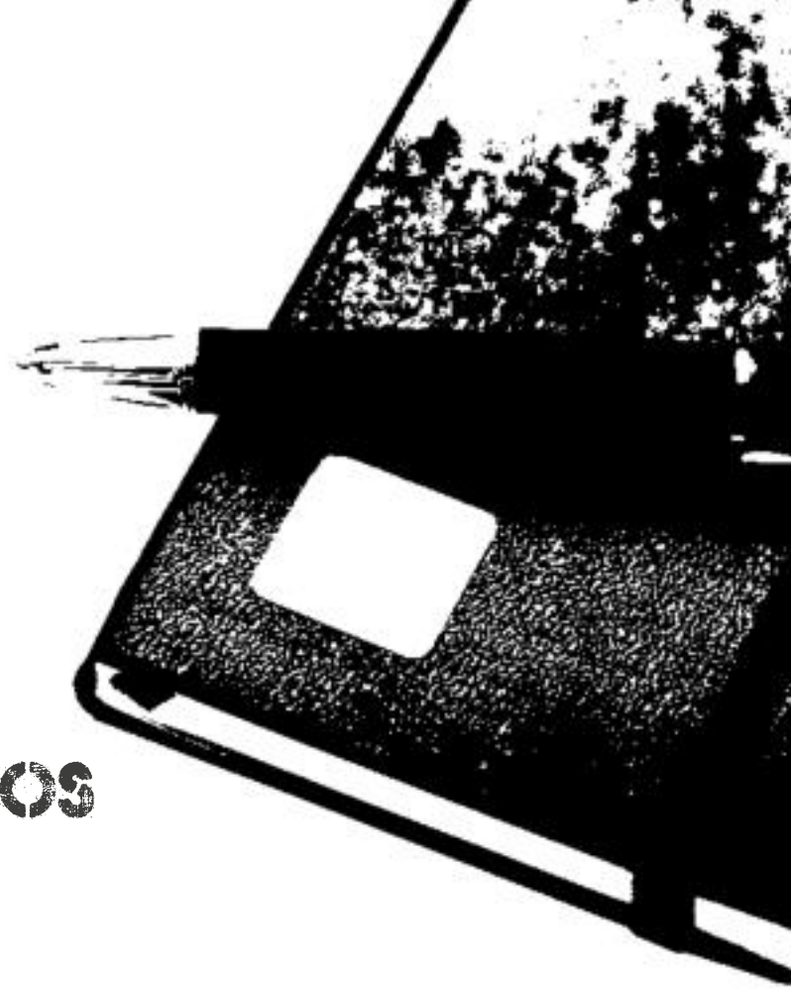
# PROTOCOLO DE SEGURIDAD PARA PERIODISTAS Y ACTIVISTAS DE DERECHOS HUMANOS

## CENTROAMÉRICA



Asdi

Hivos people unlimited

actores de cambio

La elaboración y reproducción de este material contó con el apoyo del **Programas Actores de Cambio,** financiado por la **Agencia Sueca de Desarrollo Internacional (ASDI).**

Todas las imágenes de esta publicación proceden de la modificacion de fotografías compartidas bajo licencias Creative Commons que permiten su reutilización con modificaciones, o son capturas de pantalla de la computadora. Sus autoras y autores son los siguientes: Portada: **Dave Lawler** (cámara fotográfica), y **Guy Sie** (libreta); página 6: **Roberto Ferrari**; página 8: **Climate Change, Agriculture and Food Security**; página 13: **MzNobody**; páginas 24 y 31: **Leslie**; página 26: **Eneas De Troya**; página 29: **Indi Samarajiva**; página 33: **Harumphy**; página 34: **HFG Project**; página 36: **The All-Nite Images;** página 39: **Francesco Michele**; y pagina 44: **ZepDonald.**

# ÍNDICE

# INTRODUCCIÓN

La práctica de la libertad de expresión y de información y la defensa de los derechos humanos están sujetas en Centroamérica a censuras y a presiones, a amenazas y a atentados sobre la libertad y la integridad física de las personas que las ejercen.

El programa Actores de Cambio, financiado por el Instituto Humanista para la Cooperación al Desarrollo, de la Agencia Sueca para el Desarrollo Internacional, impulsa el proyecto **PJ Shield** del Centro de Investigaciones para la Comunicación, cuyo objetivo es dotar a periodistas y defensores y defensoras de derechos humanos de mecanismos y herramientas, entre ellas, este protocolo, que aseguren su integridad física y el pleno ejercicio de la libertad de expresión en el desarrollo de sus actividades profesionales.

# PLAN DE SEGURIDAD

Toda persona que ejerza el periodismo o la defensa de los derechos humanos en un contexto hostil y de inseguridad puede reducir los riesgos que le amenazan mediante la elaboración de un Plan de seguridad, personal u organizacional.

Los pasos son 5:

**1** **Analizar el contexto**

**2** **Evaluar los riesgos, vulnerabilidades y capacidades**

**3** **Evaluar las amenazas;**

**4** **Clasificar y ordenar los riesgos**

**5** **Elaborar el Plan de seguridad**

Los riesgos, las amenazas, las vulnerabilidades y las capacidades cambian con el transcurso del tiempo, por lo que es recomendable **actualizar el plan de seguridad** periódicamente, cuando se den cambios sustanciales en el contexto social y político y cuando se vaya a enfrentar una situación de especial inseguridad.

A continuación, se detallan los pasos a seguir para la elaboración del Plan de seguridad.

Se incluyen **formularios** modelo para cada paso, preparados para su copia, impresión y cumplimentación.

## Análisis de contexto

Reflexionar sobre qué factores nos hacen sentir mayor inseguridad y los que, al contrario, nos brindan mayor seguridad.

En el análisis de contexto es importante saber:

**1.** Cuáles son los **índices de violencia y delincuencia** en el contexto en el que vivimos y trabajamos. Por un lado, el crimen también afecta a periodistas y activistas de derechos humanos, como a cualquier otra persona. Por otro, un acto violento, aparentemente casual, puede enmascarar una intencionalidad política.

**2.** Qué **incidentes o amenazas** contra del periodismo o la defensa de los derechos humanos son **habituales**, según los casos reportados por los medios de información o por colegas del gremio.

**3.** Cómo la **temática en la que trabajamos** influye en el contexto de seguridad. Por ejemplo, el periodismo deportivo, por regla general, presenta menor riesgo que la investigación de casos de corrupción.

**4.** Cómo las **circunstancias personales** (visibilidad pública, sexo, edad...) pueden influir en la seguridad. Por ejemplo, las mujeres son más susceptibles de una agresión sexual que los hombres.

**5.** Qué actores (políticos, policiales, militares, crimen organizado, pandillas, fuerzas paraestatales...) pueden representar una **amenaza**.

**6.** Qué organizaciones y personas (colegas, otros organismos o medios, entidades estatales e internacionales, redes formales e informales, autoridades, fuentes, vecinos y vecinas...) pueden ser consideradas **aliadas**.

**7.** Qué **ambientes o situaciones** presentan una mayor hostilidad y qué actividades profesionales son más seguras.

## Formulario 1
## ANÁLISIS DEL CONTEXTO

**1. ¿Qué factores me hacen sentir más segura/o?**

**2. ¿Qué factores me hacen sentir más insegura/o?**

## 2 Evaluación de riesgos, vulnerabilidades y capacidades

Para realizar esta evaluación puede utilizarse la llamada **fórmula del riesgo:**

$$\frac{\text{AMENAZAS} \times \text{VULNERABILIDADES}}{\text{CAPACIDADES}} = \text{RIESGO}$$

A mayores amenazas y vulnerabilidades, mayor riesgo. A menos capacidades, mayor riesgo. Y viceversa, si reducimos las amenazas y/o las vulnerabilidades, disminuye el riesgo; si aumentamos nuestras capacidades, el riesgo se reduce.

**Amenaza** es la intención o declaración de algún actor o actores de provocarnos un daño o un perjuicio.

**Vulnerabilidad** es todo factor que aumenta la probabilidad de sufrir un daño o que este sea mayor. Por ejemplo, no estar en buena forma física puede suponer una vulnerabilidad al no poder hacer frente o huir de un intento de agresión.

**Capacidad** es todo recurso o fortaleza de una persona u organización que mejora su seguridad y reduce las posibilidades de sufrir un daño. Por ejemplo, haber recibido formación sobre seguridad digital es una capacidad que hace que nuestras comunicaciones por correo electrónico sean más seguras y privadas.

**Riesgo** es la posibilidad de que se produzca algún daño físico o material.

El formulario de la siguiente página sirve para recoger los principales riesgos, vulnerabilidades y capacidades, a fin de analizarlos por separado y ver cómo disminuir los primeros y aumentar las últimas.

Se adjunta un pequeño ejemplo sobre riesgos, vulnerabilidades y capacidades en la asistencia o cobertura de una manifestación:

| Riesgo | Vulnerabilidad | Capacidad existente | Capacidad requerida |
|---|---|---|---|
| Arresto | Acudo sin compañía | Conozco mis derechos | Teléfono de abogada/o |
| | | Identificación de prensa | |
| Cámara de fotos requisada | | Conozco mis derechos | Teléfono de abogada/o |
| | | Identificación de prensa | Copias de seguridad |

## Formulario 2
# EVALUACIÓN DE RIESGOS, VULNERABILIDADES Y CAPACIDADES

| Riesgo | Vulnerabilidad | Capacidad existente | Capacidad requerida |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 3 Evaluación de amenazas

La amenaza se presenta cuando un actor tiene, o declara tener, la intención de infligir un daño contra una persona, su familia o contra la organización o medio de comunicación en el que trabaja.

Las **amenazas directas** se dirigen contra la persona que se quiere intimidar, mediante una llamada telefónica, correo electrónico, nota escrita, verbalmente (por la persona que amenaza o un intermediario) o cualquier otro medio.

Algunas agresiones, atentados y campañas de desprestigio pueden tener el objetivo de, además de dañar a una persona u organización concreta, enviar un mensaje, una **amenaza indirecta**, al conjunto de periodistas o activistas de derechos humanos. También pueden considerarse una amenaza indirecta la delincuencia común y todo acto de violencia contra las mujeres (en el caso de las defensoras de derechos humanos y periodistas mujeres).

Las amenazas no se convierten siempre en agresiones. Quien las profiere, lo hace para evitar que continuemos con un trabajo que supone un peligro para sus intereses. La persona que amenaza elije amenazar antes que agredir por que, o no tiene capacidad para agredir, o quiere evitar las repercusiones políticas de la agresión. Cree que la amenaza será suficiente para paralizar nuestra labor.

Sin embargo, la situación puede cambiar: la persona amenazante puede adquirir nuevas capacidades que hagan posible la agresión, o puede perder el miedo a las consecuencias, por un cambio en el contexto político, por ejemplo.

Por ello, **toda amenaza debe considerarse seriamente.**

Las personas respondemos de diferentes maneras al recibir una amenaza: nos paralizamos, la ignoramos, intentamos insensibilizarnos o analizamos la amenaza y tomamos medidas. Todas son respuestas son legítimas, humanas, pero **sólo el análisis y la adopción de medidas son respuestas constructivas** que pueden reducir el riesgo de sufrir el daño.

Analizar una amenaza consiste en **recopilar toda la información posible** sobre ella y **determinar, en lo posible, si se cumplirá.** Es recomendable realizar este análisis con colegas de confianza, cuyas opiniones serán más objetivas y pueden ayudar a no tomar decisiones precipitadas. Pero la última palabra en decidir qué medidas tomar será siempre de la persona amenazada.

Las siguientes 5 preguntas pueden ser útiles para esta labor:

**1 ¿Cuáles son los hechos y circunstancias de la amenaza?**

¿En qué consistió la amenaza? ¿Por qué medio llegó (teléfono, nota, verbal...)? Si fue telefónica, ¿qué se escuchaba de fondo? ¿Cuál fue el tono y el lenguaje? Conviene anotar por escrito toda la información relativa a la amenaza.

**2 ¿Cuál es el propósito de la amenaza?**

¿Qué quieren conseguir amenazándonos? Si la amenaza no lo dejó claro, puede deducirse: ¿qué acciones, investigaciones, publicaciones, denuncias acabamos de hacer o estamos preparando? ¿Puede ser la amenaza una respuesta a estas acciones?

**3 ¿Quién es responsable de la amenaza?**

¿Se ha identificado la persona que amenaza o no? ¿En nombre de quién se ha hecho la amenaza? ¿Qué seguridad tenemos que sea realmente el responsable de la amenaza?¿Es un actor con capacidad para cumplir su amenaza? ¿Es sospechoso o responsable de amenazas o agresiones a otras personas?

**4 ¿Es un hecho aislado o responde a un patrón?**

¿Se repiten las amenazas? ¿Se repiten las formas, momentos, lugares, tipo de mensajes...? ¿Se registran hechos que pueden estar relacionados, como incidentes de seguridad o estar bajo vigilancia?

### 5 ¿Cuál es la probabilidad de que la amenaza se cumpla?

Es, quizás la pregunta más difícil de responder. Se debe considerar:

**a)** cuáles son las capacidades de quien amenaza;

**b)** si la amenaza forma parte de un patrón, o, por si el contrario, es un hecho aislado;

**c)** si se han producido incidentes de seguridad o actos de vigilancia en el entorno de la persona amenazada, en el mismo periodo de tiempo.

Estos tres indicadores ayudarán a qué definamos si la persona que amenaza tiene una intención real de provocarnos un daño y, por lo tanto nos enfrentamos a un **nuevo riesgo**.

Ante la duda, es mejor imaginar el peor escenario posible buscando el equilibrio entre la prudencia y la paranoia.

El formulario de la siguiente página ayudará a realizar un análisis de las amenazas. Su resultado será útil para los pasos posteriores.

**Libro de incidencias**

**Se recomienda llevar un libro de incidencias para anotar por escrito los hechos y circunstancias de toda amenaza, incidente de seguridad o indicio de estar bajo vigilancia, con todo lujo de detalles, datos y descripciones (de vehículos y personas sospechosas, por ejemplo) posibles.**

**Todo el personal de la organización o del medio de comunicación debe colaborar para mantener actualizado el libro de incidencias.**

**Este documento servirá para detectar si el contexto de seguridad ha empeorado y si es necesario tomar medidas.**

### Incidentes de seguridad y vigilancia

La ocurrencia en un breve plazo de tiempo de varios **incidentes de seguridad** (robo de una computadora con información sensible, allanamiento o registro de la oficina o redacción, amenazas a otros colegas o familiares...) puede dar ideas sobre si existe un patrón.

Si se registra cualquier **indicio de que alguien nos está siguiendo o vigilando o que nuestras comunicaciones están interceptadas,** debe averiguarse cuál de los siguientes es su propósito:

**a)** recabar información sobre nuestra persona, nuestro entorno, nuestras actividades o nuestra organización o medio de comunicación;

**b)** intimidarnos para paralizar nuestras labores;

**c)** preparar una agresión, secuestro o detención.

Estos hechos suponen un cambio en el contexto de seguridad e implican la necesidad de tomar las medidas oportunas.

## Formulario 3
## EVALUACIÓN DE AMENAZAS (A)

**1 ¿Cuáles son los hechos y circunstancias de la amenaza?**

**2 ¿Cuál es el propósito de la amenaza?**

## Formulario 3
## EVALUACIÓN DE AMENAZAS (B)

**3 ¿Quién es responsable de la amenaza?**

**4 ¿Es un hecho aislado o responde a un patrón?**

**5 ¿Cuál es la probabilidad de que la amenaza se cumpla?**

## Formulario 3
## EVALUACIÓN DE AMENAZAS (C)

**Medidas a tomar (en función de las vulnerabilidades y capacidades)**

## 4 Clasificación del riesgo

Después de rellenar los formularios anteriores obtendremos como resultado un Plan de seguridad básico. Es posible que varios riesgos tengan vulnerabilidades y capacidades en común, que se repitan. Concentrándonos en disminuir las vulnerabilidades y en aumentar las capacidades que más se repiten estaremos reduciendo varias amenazas a la vez.

El siguiente paso será ordenar y clasificar los riesgos en una **Matriz de Riesgo**. Para ello debemos analizar cada riesgo del Formulario 2 y cada amenaza del Formulario 3 que sea un riesgo real y responder a dos preguntas:

**1. ¿Cuál es la probabilidad de que de que el riesgo se materialice, de que el daño ocurra?**

La respuesta siempre será subjetiva, dependerá del momento, de la persona, de sus vulnerabilidades y de sus capacidades. Siempre será útil conocer a fondo el contexto en el que nos movemos y el historial reciente de incidentes que han afectado a periodistas y activistas. Si sabemos que la Policía tiene órdenes de reprimir duramente los actos de protesta política, el riesgo durante una manifestación, la probabilidad de sufrir daños personales o en el equipo, será alto.

**2. ¿Cuál sería el impacto sobre mi persona, y sobre mi medio u organización, si el daño ocurre?**

La respuesta también será subjetiva y dependerá de nuestras vulnerabilidades y capacidades. El robo del archivo fotográfico tendrá un impacto alto en la organización o el medio, pero se reducirá al mínimo si contamos con copias de seguridad (capacidad).

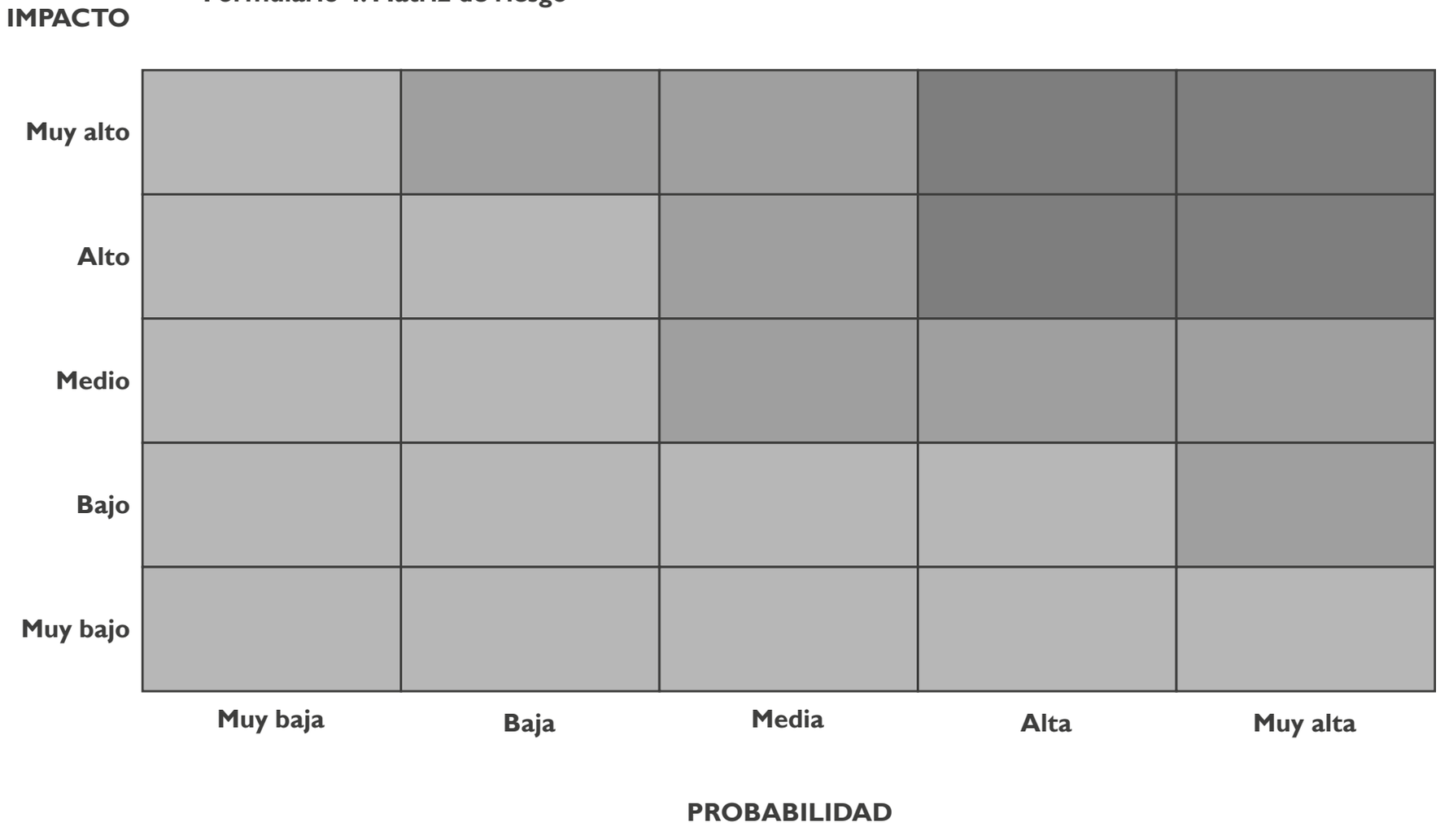
Después, clasificaremos todos los riesgos en la matriz, en función de su gravedad y su probabilidad, lo que nos ayudará a no perder tiempo preocupándonos de daños de poco impacto o poco probables.

Los riesgos ubicados en las celdas de color gris claro (de probabilidad muy baja; de probabilidad baja e impacto alto o menor; de probabilidad media e impacto bajo o menor; y de impacto muy bajo) pueden considerarse relativamente aceptables y requieren de **medidas de seguridad normales.**

Los riesgos ubicados en las celdas de color gris medio (de probabilidad baja, pero muy alto impacto; de probabilidad media e impacto medio o superior;  de probabilidad alta e impacto medio; y de probabilidad muy alta e impacto bajo o medio) requieren la elaboración de un **Plan de acción**.

Los riesgos más graves, celdas de color gris oscuro (impacto alto y muy alto y probabilidad alta y muy alta) requieren de un **Plan de acción** y un **Plan de contingencia** que establezca qué hacer si desgraciadamente el daño ocurre.

**Formulario 4. Matriz de riesgo**



# 5 Elaboración del Plan de seguridad

El último paso es la elaboración del Plan de seguridad, que, recordemos, se compone de:

## A) Plan de acción

Su propósito es el de establecer medidas que aumenten nuestras capacidades y reduzcan nuestras vulnerabilidades para disminuir la probabilidad de sufrir los riesgos que hemos identificado.

En la sección de **Medidas de seguridad** de este documento pueden encontrarse algunas ideas y consejos que pueden ayudar en la decisión de qué medidas tomar.

## B) Plan de contingencia

Tiene el objetivo de paliar los daños en caso de que los riesgos más graves y más probables ocurran. Sirve para prever qué hacer si se dan las perores situaciones. Entre otras, debe incluir medidas como:

**a)** contratar **seguros de salud y de vida** (ante un atentado o un asesinato);

**b)** contar con **asistencia psicológica** (en caso de agresión, violación, acoso, amenazas y otros hechos de gravedad);

**c)** disponer de un servicio de **asistencia legal** y de **apoyo nacional e internacional** (en los casos de detención o allanamiento policial, criminalización de nuestro trabajo,.. etc);

**d)** saber qué hacer **en caso de secuestro**;

**e)** contemplar la posibilidad de **reducir o cesar las actividades** que provocan la represalia.

## Formulario 5
# PLAN DE SEGURIDAD

**Riesgo o amenaza**

**Probabilidad** **Impacto**

**Vulnerabilidades**

**Capacidades**

**Medidas de acción**

**Medidas de contingencia**

## Plan organizacional

Toda organización de derechos humanos o medio de comunicación que enfrente riesgos en su labor debe contar con un Plan de seguridad. Los pasos anteriores ayudan a elaborar este documento.

Los riesgos menos graves y menos probables (según la **Matriz del riesgo**) puede paliarse mediante medidas sencillas, baratas y habituales. Los riesgos intermedios requieren de un **Plan de acción.** Los riesgos más graves ameritan, además, un **Plan de contingencia**.

Se recomienda centrarse, en un inicio, en los **dos o tres riesgos con mayor impacto y probabilidad**.

En la elaboración del Plan debe colaborar **todo el personal**, incluido el de apoyo (de limpieza, choferes...) que, si bien enfrentan riesgos menores, pueden aportar información y conocimientos muy válidos.

Discutido y elaborado el Plan, este debe **presentarse** al conjunto de la organización o medio de comunicación y **ponerse en práctica de inmediato**.

Una persona será la **responsable de monitorear su implementación y su revisión periódica**.

El Plan será **actualizado** cuando se produzca un cambio importante en el contexto, cuando aparezca un nuevo riesgo o se reciba una nueva amenaza.

También puede ser útil crear un **Semáforo de seguridad,** en el que:

**Verde** indica que la situación es normal y no es necesario tomar medidas de seguridad especiales.

**Amarillo** indica que el contexto se ha vuelto más inseguro y que es necesario implementar una serie de medidas específicas.

**Rojo** indica que la situación es grave y que se deben tomar las máximas medidas de seguridad.

## Plan personal

Si bien contar con diferentes experiencias y perspectivas facilitará la elaboración de un Plan de seguridad, también puede elaborarse un Plan individual, dado que el Plan organizacional puede no contemplar los riesgos de la vida fuera de la actividad laboral. Además, cada persona presenta características, vulnerabilidades y capacidades propias que pueden demandar medidas específicas.

Para elaborar el Plan individual pueden seguirse los pasos anteriormente descritos, centrándonos en dos o tres riesgos de impacto medio a muy alto, y medio a de muy alta probabilidad.

Se recomienda consultar también la sección de **Medidas de seguridad** de este documento.

# MEDIDAS DE SEGURIDAD

# MEDIDAS DE SEGURIDAD GENERALES

## 1 Preparación física y mental

Mantenerse en buena forma física y mental.

No caer en la paranoia.

Hacer caso de la intuición y utilizar el sentido común.

Formarse sobre protección personal y seguridad digital.

## 2 En el domicilio

Revisar la seguridad del hogar e instalar sistemas de seguridad (candados, verjas, cerrojos, alarmas, cámaras de vigilancia...) si es necesario.

Consensuar medidas de seguridad con la familia, como palabras clave, para entrar a la casa o para llamadas telefónicas y correos electrónicos.

La familia debe tener claro qué hacer y a quién llamar en caso de emergencia.

Las y los menores de edad deben ser capacitados para no dar información privada ni relacionarse con personas desconocidas.

Hacer simulacros de diversas situaciones de peligro.

Conocer el vecindario y detectar cambios en él (presencia de personas o vehículos sospechosos...).

En la vida vecinal y social, no granjearse enemigos de forma gratuita.

## 3 En el ejercicio de la profesión

Cumplir con la labor profesional de forma ética y honorable.

Las y los periodistas deben evitar competencia innecesaria en zonas de peligro. Los riesgos también afectan a las y los colegas.

Cumplir escrupulosamente con la ley, especialmente en relaciones con el Estado (declaración de impuestos, seguro y permisos del vehículo, trámites de diversa índole...).

Ser transparente en la vida diaria, no ocultar secretos que pueden ser utilizados en una campaña de desprestigio.

# MEDIDAS ESPECÍFICAS PARA MUJERES PERIODISTAS Y ACTIVISTAS

**Capacitarse** en protección personal y seguridad digital.

**Participar** en la elaboración del contexto de seguridad, evaluación de riesgos, vulnerabilidades y capacidades y en la adopción de medidas de seguridad del medio de comunicación o el organismo en el que se trabaja.

En contextos especiales de riesgo, **mantener el control de la situación**, evitar que su vida y las decisiones estén en manos de terceras personas.

En **estado de embarazo**, medir los riesgos físicos de acuerdo a la etapa de gestación.

Portar **elementos de defensa personal**, como aerosol irritante, alarma, silbato, linterna.

En coberturas o misiones arriesgadas, **vestir y calzar de forma cómoda** y que no dificulte la movilidad.

Ante una agresión, **llamar la atención**. Suelen ser más efectivos gritos que alerten a otras personas sobre su propia seguridad (por ejemplo:, "fuego, fuego", mejor que "me atacan").

En una entrevista con un hombre, **mantener una distancia prudente**, marcar los límites y evitar o cortar de manera tajante cualquier acercamiento verbal o físico.

No hay una respuesta adecuada, correcta, **frente a una agresión sexual**; depende de cada situación y es una decisión que competen únicamente la víctima. El objetivo primordial debe ser sobrevivir. Las reacciones pueden ser:

**a)** someterse a la agresión, si hay temor por la vida.

**b)** resistirse pasivamente, con insultos, decir que se tiene una infección de transmisión sexual, provocarse el vómito... distintas acciones que pueden disuadir al agresor.

**c)** resistirse activamente con gritos, golpes, patadas, arañazos..

Tras una agresión sexual se debe obtener de inmediato:

**a)** asistencia psicológica.

**b)** asistencia médica (análisis regulares de infecciones de transmisión sexual, dispositivos de prevención del embarazo o de impedimento posterior).

**c)** Asistencia jurídica.

Evaluar la pertinencia de denunciar cualquier agresión personal y/o discriminación. La decisión última es potestad de la víctima.

# GESTIÓN DE AMENAZAS TELEFÓNICAS

## 1 Prevención

Mantener en la privacidad los **números telefónicos de la vivienda familiar y del celular de uso personal**; su conocimiento debe estar restringido a personas de absoluta confianza. En relaciones por motivos laborales, dar únicamente el número de la redacción o la oficina.

Tratar de que el **mensaje del buzón de voz** (convencional o celular) sea corto, para no permitir reconocimiento de la voz, y que no dé nombre, apellidos ni el número telefónico.

Tener **varios celulares, o números,** cada uno para un uso específico (trabajo, familiares...).

Instalar un **identificador de llamadas** en los teléfonos convencionales.

Instalar un sistema o una aplicación de **grabación de llamadas** (consultar **Medidas de seguridad digital**).

Contar con un **sistema para escuchar**, desde fuera del domicilio, los **mensajes de voz** del teléfono de la casa.

## 2 Durante una amenaza telefónica

Al recibir una llamada, **evitar identificarse** si la persona que llama no lo hace y no se reconoce su número o su voz.

Si resulta obvio que la llamada es una amenaza, **no entrar en pánico**, no dialogar ni confrontar.

Si no se está grabando la llamada, **anotar todos los detalles** que sean posibles (hora, sexo y acento de la voz, palabras exactas...) durante la llamada o inmediatamente después.

## 3 Después de una amenaza telefónica

Analizar si se trata de un error técnico, una llamada a un número equivocado o un **verdadero intento de intimidación**.

Valorar si realmente se trata de una amenaza: **una llamada con insultos** no es lo mismo que una llamada con amenazas de muerte o que demuestra que conocen los movimientos y hábitos de la persona o familia.

**Registrar** el hecho **en el libro de incidencias**.

Recibida la amenaza, **descolgar o apagar** el teléfono convencional varias horas o incluso días.

Instalar en el celular una **aplicación de bloqueo de llamadas** (ver **Medidas de seguridad digital**).

Valorar la **pertinencia de denunciar las amenazas**. En ocasiones, lo único que se busca con las amenazas es amedrentar y la publicidad favorece los intereses de las personas responsables de las amenazas.

En caso de decidir **denunciar públicamente** las amenazas, acudir a los medios de comunicación, instancias judiciales y organismos nacionales e internacionales de derechos humanos y libertad de expresión.

En todo caso deben **ponerse en conocimiento de familiares y editores del medio o colegas del organismo** en el que se trabaja.

# DESPLAZAMIENTOS

## 1 Desplazamientos diarios

Mantener la adecuada **discreción** sobre hábitos, ubicación y desplazamientos.

**Cambiar** aleatoriamente horarios, rutinas y formas de transporte.

Tomar precauciones a la hora de **subir y bajar del carro**. Retrasar la llegada a destino si se detectan personas sospechosas o comportamientos extraños.

No usar **audífonos o el teléfono celular** en la calle, carro, taxi o transporte público; distraen de lo que ocurre en el entorno.

No frecuentar **lugares poco recomendables**.

Tener en cuenta que el lugar de residencia o trabajo son puntos donde pueden comenzar **acciones de vigilancia y seguimiento**.

## 2 Desplazamientos largos en vehículo privado

No emprender desplazamientos largos **en solitario ni en horas de la noche.**

Establecer y apegarse a un **horario** para saber cuándo se sale y cuándo se vuelve.

Dejar rastros; no hacer público el itinerario pero sí tener una **persona de confianza**, de la redacción o del organismo, que conozca dónde viajamos, por qué y a quién vamos a ver. Establecer con ella **tiempos y formas de contacto**.

Utilizar un vehículo en **óptimas condiciones y con combustible**. Asegurar que **se dispone libremente de él,** que no se depende de terceras personas.

Estudiar en un **mapa** el itinerario, la ubicación del destino y las posibles vías de salida rápida.

Revisar el equipo (consultar apartado **Equipo**).

Subir o bajar del carro **sin personas extrañas cerca**.

Mantener los **vidrios y las puertas cerradas** del carro, especialmente en ambientes urbanos.

En un **retén**, mantener el motor encendido y seguir instrucciones policiales.

Cumplir estrictamente las **normas de tránsito**.

Mantener la **suficiente distancia con otros vehículos** para que el nuestro no quede encajonado.

Evitar **lugares solitarios u oscuros**. Pasos angostos, como callejones, puentes o túneles, no son recomendables.

No transportar a **personas extrañas**.

## 3 En destino

Evitar encuentros con **fuentes poco confiables** en horas de la noche, sin compañía y en lugares desconocidos o en los que se dependa de terceras personas para salir (un departamento desconocido, un barrio conflictivo...).

Definir con la persona acompañante una **palabra clave** que sirva para alertar de un peligro e implique abandonar el lugar.

Gritar en caso de encontrarse en una **situación de riesgo sin posibilidad de escape**. Normalmente llaman más la atención los gritos de "fuego, fuego", que "me atacan".

**No hacer pactos** con la fuente que no está en nuestras manos cumplir.

## 4 En zonas rurales

Contar con una persona de **contacto con reconocimiento y liderazgo** en la comunidad o la población que se visita.

Contar con un **interprete** si en la zona se habla un idioma distinto al nuestro.

Evitar desplazamientos en **horas de la noche**.

Estudiar en un mapa la zona y las vías de llegada y salida.

Comprobar el **estado de las carreteras**.

Utilizar un vehículo en óptimas condiciones, adecuado a la **orografía del terreno** y con combustible. Asegurar que se dispone libremente de él, que no se depende de terceras personas.

Revisar el equipo (consultar apartado **Equipo**).

Contar con una **forma de comunicación** con la redacción o sede del organismo, como radio de largo alcance o teléfono satelital.

# ACTIVIDADES INFORMATIVA HOSTILES

Antes de acudir a una conferencia de prensa o actividad informativa con presencia de autoridades o poderes públicos, tratar de asegurar que **no se nos recibirá con hostilidad**.

Si se prevé un ambiente de hostilidad, enviar a una **persona joven, no reconocida por su labor, que pueda pasar por estudiante,** y que no porte identificación ni elemento que ayude a identificarlo (libreta del medio, camiseta de la organización...).

La **no asistencia a una conferencia o rueda de prensa** no implica que no se puede realizar la labor periodística Se recomienda:

**a)** buscar **fuentes alternativas** de la información brindada en la actividad (grabación televisiva o radial del acto, intercambio de información con otros medios..).

**b)** conseguir **información añadida**; la mera declaración de una autoridad no es la única información necesaria para una noticia: son útiles también datos de contexto, declaraciones anteriores de la misma fuente, otros puntos de vista...

En la actividad informativa, tomar el pulso de la situación antes de lanzar **preguntas o cuestionamientos críticos**.

En el caso de que alguien trate de a**rrebatar o requisar algún equipo** (cámara, grabadora) armar un escándalo para llamar la atención y que el hecho no pase desapercibido. Registrar el hecho y denunciarlo.

En el caso de **expulsión de la sala**, negarse sin llegar a un enfrentamiento físico. Tratar de registrar el hecho y denunciarlo.

# PUBLICACIONES O DENUNCIAS DE ESPECIAL GRAVEDAD

Si se prevén **represalias violentas** ante la publicación o denuncia pública de un tema de especial trascendencia y gravedad, se recomienda:

a) Dejar que el tiempo corra hasta que la denuncia puede realizarse en **un momento menos susceptible** de respuestas violentas.

a) Denunciar a través de **medios de comunicación u organismos extranjeros** y después retomar la denuncia en el país.

a) Acordar la **denuncia simultánea y conjunta** con otros medios y organismos.

a) Realizar la publicación o denuncia **sin firma ni autoría**, tomando las oportunas medidas de seguridad y prevención.

# ACTOS MULTITUDINARIOS DE CARÁCTER POLÍTICO

## 1 Antes del acto, se deben conocer:

Motivo y convocantes de la actividad.

Reacción del Gobierno y poderes fácticos ante la convocatoria.

Potenciales agresores y sus capacidades y otras posibles amenazas a la seguridad.

Autoridad responsable del despliegue policial para comunicarle la intención de asistir o cubrir la actividad.

Eventuales aliados presentes (otros periodistas, miembros de otras organizaciones de derechos humanos...).

Horario de la actividad (las horas nocturnas pueden ser más peligrosas).

## 2 Antes, situar en un mapa:

La zona donde se desarrollará la actividad.

Ruta de llegada y de evacuación.

Lugar de parqueo del vehículo que posibilite una rápida salida.

Medios alternativos de salida (transporte público).

Punto de reunión.

Punto de asistencia médica más cercano.

## 3 Decidir con antelación:

Necesidad y pertinencia de acudir a la actividad **en virtud del riesgo**.

Recursos humanos a desplazar a la actividad: a mayor riesgo, **mayor experiencia** necesaria del personal.

Responsables, tiempos y formas de **monitoreo y seguimiento** del equipo desplazado.

Revisar el equipo (consultar apartado **Equipo**).

## 4 Durante la cobertura o asistencia a la actividad

No acudir ni caminar en solitario, **rodearse de personas de confianza**.

Mantener el **control de los movimientos** sin depender de terceras personas; guardar consigo las llaves del vehículo o una copia.

Cumplir con la **ruta acordada**, desplazarse por la actividad según lo establecido.

Evitar estar en el centro de la actividad y procurar desplazarse por uno de los **costados**.

Ubicar y mantener **contacto visual con aliados** (otros periodistas, miembros de otras organizaciones de la sociedad civil...).

Prestar a**tención constante** a todo lo que está ocurriendo. En caso de fotoperiodistas o cámaras, saber **qué ocurre fuera del visor**.

Elegir cuidadosamente el **lugar y momento de aproximarse a las fuentes**: que una entrevista no se convierta en situación de riesgo.

Tomar medidas de seguridad digital para **guardar automáticamente una copia de seguridad** de los archivos (textos, imágenes, vídeos, audios), para evitar su sustracción.

**No responder** a amenazas o provocaciones verbales.

**Priorizar siempre la vida y la integridad física**, propias y de las demás personas, frente a la labor que se está desarrollando.

## 5 En caso de enfrentamientos

Evitar **quedar entre manifestantes y Policía**. Buscar un punto suficientemente alejado para evitar daños pero que permita observar y/o grabar lo que ocurre.

En caso de lanzamiento de objetos y/o artefactos por parte de manifestantes o Policía, **no ser blanco fácil**, buscar resguardo. **No tocar** ningún objeto o artefacto lanzado.

Ante una **agresión o acoso**, huir y armar escándalo para llamar la atención de las personas circundantes y de personas aliadas.

**Registrar cualquier agresión, amenaza o acto de represión** de la que se sea testigo o víctima.

Mostrar **apoyo y solidaridad** a colegas víctimas de una agresión.

En caso de **detención policial**, no resistirse ni confrontar a los agentes. Identificarse, si es necesario a gritos, con nombre, apellidos y medio u organización para la que se trabaja.

**Informar rápidamente de toda detención** a las entidades convocantes y al grupo de asistencia legal.

**Abandonar la zona** si la situación es muy tensa y se cree que se corre peligro.

# TRATO CON POLÍCIA Y EJÉRCITO

Evite llegar a un lugar donde ha ocurrido un hecho violento, **antes que la Policía** u otros cuerpos de seguridad.

Mantener una **actitud de respeto y distancia, nunca de confianza.**

Conocer y respetar los **cargos y la jerarquía** dentro del cuerpo.

Averiguar el **nombre y cargo de la autoridad responsable** y comunicarlos a la redacción o sede del organismo.

Identificarse ante el cargo policial o militar y **comunicar la cobertura periodística o misión de observación**.

En un retén, escenario del crimen o situación de tensión, **cumplir las indicaciones** de los miembros de las fuerzas policiales o militares, sin dejarse avasallar. Evitar **discusiones acaloradas o forcejeos**.

En un **retén**, mantener el motor encendido y seguir instrucciones.

Ante la **posibilidad de controles o cacheos**, no portar libretas de direcciones y teléfonos ni con información sensible o personal.

Llevar siempre al menos **una identificación** (cédula o pasaporte, acreditación o gafete del medio de comunicación u organismo) que pueda colocarse en un lugar visible pero que se pueda ocultar con facilidad.

Si la Policía lo requiere, **mostrar una única identificación**, nunca todas las que se portan.

Nunca portar **armas u objetos cortopunzantes**.

Si **nos están fotografiando o filmando**, hacer lo mismo: tomar imágenes de la persona o agente que nos fotografía o graba.

Ante un intento de **requisar equipo de grabación o filmación**, negarse dentro de lo posible, no hay razón legal para ello. En caso de que no se pueda impedir, mostrar inconformidad.

Portar siempre **tarjetas de memoria falsas, dañadas o vacías** ante la posibilidad de que sean requisadas.

En caso de sufrir **malos tratos o agresiones** por parte de miembros de la Policía o el Ejército, relatarlas en cuanto sea posible al grupo de asistencia legal; someterse de inmediato a una evaluación médica forense; documentar mediante fotografías las eventuales lesiones.

**Conocer y hacer respetar los derechos** recogidos en la Constitución Política y en las leyes.


POLICIA
POLICIA
POLICIA

# EQUIPO

# COMPROBACIÓN DE EQUIPO (A)

## Vehículo

- Óptimo estado ☐
- Adecuado a la orografía del terreno ☐
- Plenamente disponible ☐
- Varias copias de las llaves ☐
- Combustible ☐
- Documentación en regla ☐
- Accesorios y repuestos exigidos por ley ☐

## Mapa

- Itinerario ☐
- Localización de la actividad y su ruta ☐
- Vías rápidas de acceso y salida ☐
- Transporte alternativo ☐
- Asistencia sanitaria más cercana ☐
- Punto de parqueo ☐
- Punto de reunión ☐

## Documentación

- Identificación visible pero fácilmente ocultable ☐
- Dinero y documentos separados en ubicaciones distintas ☐
- Tarjeta de crédito o débito con saldo mínimo ☐

## Teléfonos de emergencia

- Persona del medio u organización responsable del monitoreo de la actividad ☐
- Organizaciones sociales convocantes y/o presentes ☐
- Responsable policial del acto al que se acude ☐
- Familiares del equipo de trabajo ☐
- Asistencia legal ☐

(Es recomendable aprender de memoria los números más importantes en previsión de algún problema con el teléfono: cobertura, saldo, batería, sustracción del celular...).

## Indumentaria

- Cómoda, no llamativa, difícilmente identificable, adecuada a las condiciones climáticas y de tejido no inflamable. ☐
- Indumentaria de repuesto, para pasar desapercibida/o en momentos de tensión ☐
- Calzado, apto para correr y con suela antideslizante ☐

**NO** portar prendas con escudos, emblemas o colores que puedan confundirse con los de un partido político, un equipo deportivo, una empresa, etc., que pueda motivar una agresión.

**NO** vestir prendas militares o de aspecto militar (verde olivo o de camuflaje).

# COMPROBACIÓN DE EQUIPO (B)

## Protección y prevención

- Kit de primeros auxilios ☐
- Pañuelo o mascarilla ☐
- Limón o algún otro cítrico para neutralizar químicos irritantes ☐
- Agua ☐
- Comida energética ☐
- Vacunas, en caso de ser necesarias ☐
- Cascos, chalecos, máscaras antigás ☐

(tener en cuenta que:
- restan movilidad y visibilidad
- ayudan a identificar a la persona que lo lleva
- su uso requiere de cierta práctica previa
- debe ser adecuado frente al tipo de proyectil o bomba de humo que puede esperarse.
- hay modelos específicos para mujeres)

**NO** portar armas ni objetos cortopunzantes.

## Comunicación

- Teléfono celular operativo con: ☐
  - Cámara ☐
  - Cobertura ☐
  - Conexión a Internet ☐
  - Batería cargada y de repuesto ☐
  - Saldo suficiente (varios chips) ☐
- En desplazamientos largos, equipo de comunicación seguro y de largo alcance con la redacción o sede, como radio o teléfono satelital ☐

## Fotografía, video, audio

- Correcto funcionamiento comprobado ☐
- Plan de protección del equipo poe si alguien pretende sustraerlo o dañarlo ☐
- Cables de conexión necesarios ☐
- Conexión para, durante la actividad, hacer copias de seguridad en Internet de los archivos (textos, fotos, videos, audios) ☐
- Tarjetas de memoria vacías o falsas para entregarlas en caso de que sean requisadas o robadas ☐

Valorar la posibilidad de sustituir el equipo habitual por otro más pequeño, discreto y manejable.

Tener en cuenta que accesorios como lentes, trípodes o flash pueden confundirse con un arma.

## Otros

_____ ☐
_____ ☐
_____ ☐
_____ ☐
_____ ☐
_____ ☐
_____ ☐
_____ ☐

# SEGURIDAD DIGITAL

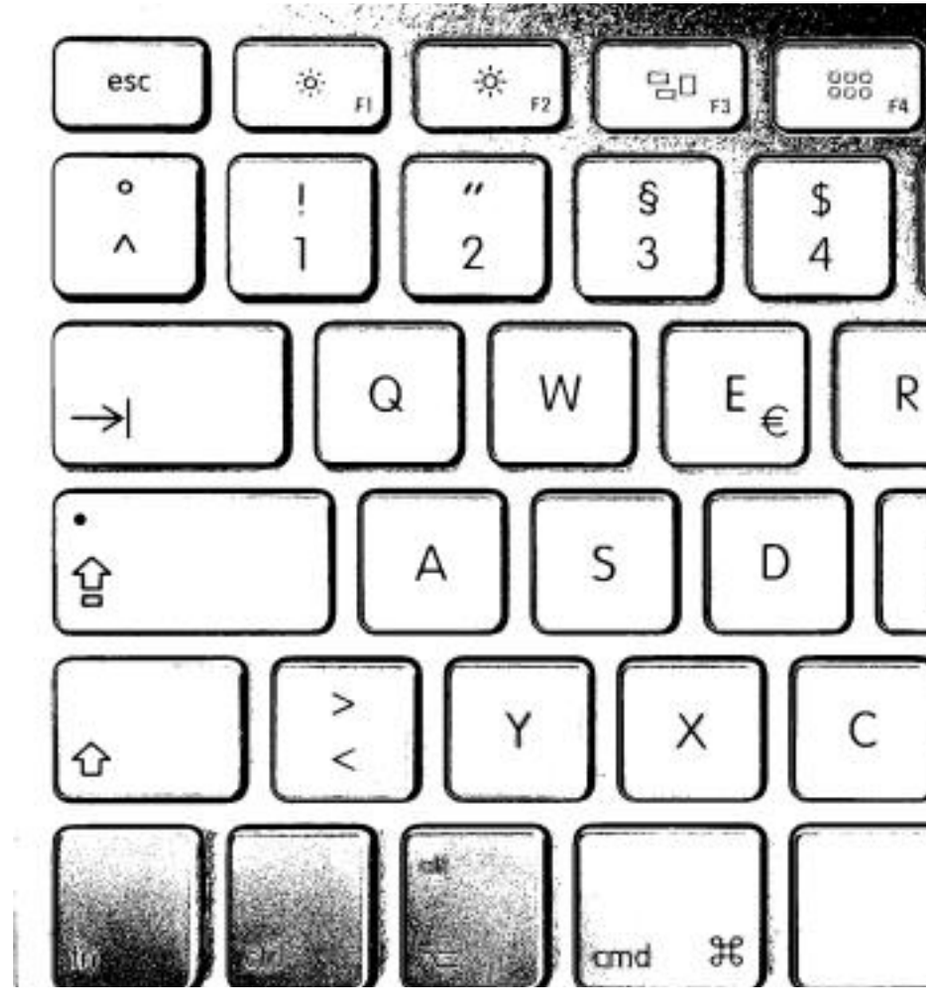
# SEGURIDAD FÍSICA DE LOS DISPOSITIVOS ELECTRÓNICOS

Prevenir cualquier daño físico que pueda sufrir el dispositivo electrónico: ubicarlo siempre en un lugar alejado de líquidos y de campos electromagnéticos; contar con un estabilizador de corriente eléctrica.

En zonas sísmicas, prever la posible caída de objetos o líquidos sobre el dispositivo durante un temblor.

Reducir el riesgo de robo del dispositivo, en especial de aparatos portátiles (celular, tableta...).

Valorar la posibilidad de guardar la información más sensible en USB, más fáciles transportar y ocultar, y no en computadoras, vulnerables a ataques físicos o informáticos. No usar estos USB en computadoras públicas o de otra persona.



# CONTRASEÑAS

## 1 Consejos generales

Establecer **contraseñas diferentes** para cada servicio, aplicación y dispositivo (una para el correo electrónico, otra para una red social; una para la computadora, otra para el bloqueo del celular...).

Aumentar la complejidad de la contraseña con un **programa para la generación de claves seguras**, como KeePass (keepass.info).

En caso de recibir un correo electrónico solicitando un cambio de contraseña para un servicio o aplicación, examinar la dirección de remite del correo. Puede tratarse de **intento de robo de contraseña**.

Limitar el uso de la opción de **Guardar contraseña** que ofrecen los programas de navegación por Internet; si alguien llega a acceder a la computadora o dispositivo, tendrá acceso a redes sociales, correo electrónico y otras aplicaciones.

**No revelar las contraseñas** por teléfono, ni a nadie cuya identidad no se pueda verificar.

**No guardar las contraseñas** en un lugar visible cerca del dispositivo.

## 2 Contraseñas robustas

Usar contraseñas de al menos 8 letra mayúsculas y minúsculas, números y símbolos (, . ; : + - / * = ! ¿ ?), pero fáciles de recordar. Una fórmula a seguir es la siguiente:

**1**. Elegir un refrán (mejor con acentos y la letra "ñ"), por ejemplo:
**Más vale pájaro en mano**

**2**. Definir letras mayúsculas mediante un criterio fácil de recordar, por ejemplo: las primeras letras de cada palabra:
**Más Vale Pájaro En Mano**

**3**. Sustituir algunas letras por números de apariencia similar, por ejemplo, la "a" por el 4; la "e" por el 3; la "i" por el 1...:
**Más V4l3 Páj4r0 3n M4n0**

**4** Incluir símbolos, por ejemplo: unir las palabras con los símbolos de suma, resta, multiplicación y división:
**Más+V4l3-Páj4r0*3n/M4n0**

**5** Comprobar la fortaleza de la contraseña con How secure is my password (howsecureismypassword.net).

## 3 Bloqueo de dispositivos

Proteger los dispositivos (computadora, teléfono celular, tableta...) con una contraseña, pin o patrón de bloqueo que impida que una persona no autorizada acceda a la información. Cada sistema tiene su propio proceso:

### Sistema operativo Android

Cómo poner un patrón de bloqueo en un celular Android:
mimovilandroid.com/tutoriales/seguridad-como-poner-un-patron-de-bloqueo-en-un-movil-android

### Sistema operativo iOS (Apple)

Cómo cambiar la contraseña de tu iPhone (e iPad, iPod...):
electronica.practicopedia.lainformacion.com/iphone/como-cambiar-la-contrasena-de-tu-iphone-20544

### Sistema operativo Windows (Microsoft)

Cambiar la contraseña de Windows (computadoras):
windows.microsoft.com/es-es/windows/change-windows-password#change-windows-password=windows-7

Preguntas más frecuentes sobre la pantalla de bloqueo en teléfonos celulares:
www.windowsphone.com/es-es/how-to/wp7/basics/lock-screens-faq

### Sistema operativo Ubuntu (Linux):

Cambiar/Recuperar contraseña de Ubuntu en caso de olvido:
ubuntudriver.blogspot.com/2012/07/cambiarrecuperar-contrasena-de-ubuntu.html

### Sistema operativo BlackBerry

Cómo instalar un código de seguridad en una BlackBerry:
www.utilidad.com/como-instalar-un-codigo-de-seguridad-en-una-blackberry_1530

## En caso de robo o pérdida del dispositivo

Instalar una aplicación para el bloqueo, borrado de datos y ubicación a distancia del aparato en caso de que se pierda o sea robado.

### En Android

Localizar, bloquear y borrar un dispositivo perdido o robado:
www.xatakandroid.com/tutoriales/como-localizar-bloquear-y-borrar-nuestro-dispositivo-android-en-caso-de-perdida-o-robo

### En Windows Phone

Encontrar un teléfono perdido:
www.windowsphone.com/es-ar/how-to/wp8/settings-and-personalization/find-a-lost-phone

### En iPhone

Buscar mi iPhone:
www.apple.com/es/icloud/find-my-iphone.html

### En BlackBerry

Encontrar y proteger un dispositivo perdido:
help.blackberry.com/es/blackberry-classic/10.3.2/help/als1339706385344.html

### Varios sistemas

Herramienta de Google que permite localizar el móvil a distancia y borrar datos:
www.hijosdigitales.es/2013/09/herramienta-de-google-que-permite-localizar-el-movil-a-distancia-y-borrar-datos/

# 2 Antivirus

Instalar un programa antivirus, que elimine virus, troyanos, gusanos y todo programa malicioso cuyo objetivo es dañar la memoria del dispositivo, alterar su funcionamiento o sustraer información y datos.

Algunos programas gratuitos recomendados:

**Computadoras:**

Avast
www.avast.com/es-ww/index

Avira
www.avira.com/es/avira-free-antivirus

Se recomienda instalar sólo un programa antivirus, en caso contrario podrían interferir uno con otro. Sin embargo, cualquiera de los mencionados anteriormente puede complementarse con Malwarebytes: es.malwarebytes.org

**Celulares, tabletas**

**Android**

AntiVirus FREE
play.google.com/store/apps/details?id=com.antivirus&hl=es

**iPhone**

Norton Mobile Security
itunes.apple.com/us/app/norton-mobile-security-lost/id520284590?mt=8

**Blackberry**

NQ Antivirus FREE
appworld.blackberry.com/webstore/content/32153/?lang=es&

## 3 Cifrado, borrado y copias de seguridad de archivos

**1. Cifrar** archivos específicos o discos duros completos, para impedir que personas extrañas accedan a la información. Algunos programas:

**BitLocker para Windows**
windows.microsoft.com/es-es/windows7/products/features/bitlocker

**FileVault para MacIntosh**
support.apple.com/kb/HT4790?viewlocale=es_ES

**2. Establecer un plan de copia de seguridad de datos e información** sensibles o importantes, que defina archivos a copiar, dónde y con qué periodicidad. A tomar en consideración:

Deben guardarse original y copia de seguridad en soportes distintos (disco duro extraíble, USB, DVD o la nube).

Debe identificarse cada copia con nombre y fecha para facilitar hallar la última versión.

La copia de seguridad puede hacerse de forma automática o manual; configurar el sistema en función del plan de copia de seguridad elaborado.

Especialmente útil puede resultar la copia de seguridad automática y en la nube para dispositivos portátiles conectados a Internet: permite guardar en remoto fotos y grabaciones de vídeo o sonido.

Si la cámara o teléfono es requisado, perdido o robado, al menos se contará con una copia de los archivos. Enlaces de ayuda:

Cómo crear una copia de seguridad automática con Google+
support.google.com/plus/answer/1647509?hl=es

Dropbox. ¿Cómo puedo subir archivos desde mi teléfono?
www.dropbox.com/help/84

One Drive, servicio en la nube de Windows
onedrive.live.com/about/es-mx

iCloud, servicio en la nube de Apple
www.apple.com/es/icloud/features

**3. Borrar archivos o informaciones sensibles** con un programa de borrado definitivo de archivos, como Eraser (eraser.heidi.ie); el vaciado de la papelera del escritorio no borra la información por completo y esta podría recuperarse.

**4. Borrar periódicamente los archivos temporales** (copias de seguridad que el propio sistema va realizando mientras se trabaja) con una herramienta de limpieza de datos, como CCleaner (www.piriform.com/ccleaner).

# METADATOS

Algunos archivos guardan metadatos, datos adicionales que no se ven a simple vista pero que pueden informar sobre la persona que creo el archivo, el lugar, la fecha, el modelo de cámara con el que se tomó la foto... etc.

Eliminar los metadatos cuando supongan un riesgo para la privacidad y la seguridad. Existen programas informáticos específicos para ello, pero puede realizarse en **Windows** de forma sencilla:

**1.** Localizar el **archivo** que se quiera "limpiar" de metadatos.

**2.** Pulsar sobre él con el **botón derecho** del ratón.

**3.** Seleccionar la opción **Propiedades**.

**4.** Seleccionar la pestaña **Detalles**; la ventana mostrará toda la información adjunta al archivo.

**5.** Seleccionar la opción **Quitar propiedades e información personal**, abajo.

**6.** Seleccionar **Quitar las siguientes propiedades**.

**7.** Seleccionar **todo**.

**8.** Pulsar en **Aceptar**.

# NAVEGACIÓN SEGURA Y ANÓNIMA

Internet y nuestra computadora guardan datos como la dirección y dispositivos desde los que nos conectamos, las páginas o sitios web que hemos visitado y todos los datos e información no cifrada que hayamos proporcionado. Para eliminar o cifrar esta información:

**Eliminar el caché, historial, cookies y demás datos de navegación,** periódicamente de la computadora personal, y siempre si ha utilizado una computadora pública (cibercafé, hotel...) o de otra persona.

Comprobar, **en páginas que deban asegurar intercambio de información cifrada** (páginas de cambio de contraseña, de correo electrónico, de transacciones de dinero...) que la dirección electrónica de la página empieza por "**https://**", con "s" y que aparece un **candado** en la barra de direcciones o en la barra de herramientas inferior, según el navegador.

En computadoras públicas o de otras personas, utilizar la **opción de navegación anónima**, que no dejará ninguna información en la computadora, **aunque los servidores sí guardarán información** sobre nuestra computadora y las páginas que hemos visitado.

Para navegación segura, seleccionar en el menú (según el programa):

**Firefox**
Archivo / Nueva ventana privada

**Chrome**
Archivo / Nueva ventana de incógnito

**Explorer**
Herramientas / Seguridad / Navegación InPrivate

**Safari**
+ / Nav. Privada

Utilizar redes de anonimato, como **Tor** (torproject.org), para una **navegación completamente anónima**, en la que no quede absolutamente ningún registro de la dirección de conexión de nuestra computadora ni de las páginas visitadas.

Considerar que el hecho de firmar comentarios o publicar desde un **perfil de redes sociales con seudónimo** no garantiza por si mismo el anonimato.

# COMUNICACIÓN SEGURA Y PRIVADA

## 1 Consideraciones generales

Actuar como si el teléfono convencional y celular y el correo electrónico **estuviesen intervenidos**. No transmitir información personal o confidencial por estos medios.

Buscar **alternativas "analógicas"** para transmitir información sensible o importante, como reuniones personales en la redacción, sede del organismo o lugares públicos.

Establecer **palabras clave o santo y seña** antes de establecer la comunicación por vía telefónica, correo electrónico u otros canales digitales.

Utilizar con mucha precaución las **redes wifi públicas y abiertas**.

Usar herramientas que envían **imágenes que se borran automáticamente** pocos segundos después de ser vistas, como Snapchat (www.snapchat.com). (Un mensaje privado puede escribirse dentro de una imagen y enviarlo con este tipo de aplicaciones).

Usar herramientas de **chat difrado**, como Telegram (www.telegram.org).

## 2 Correo electrónico

Manejar **varias cuentas de correo electrónico**, reservando el uso de algunas para determinados destinatarios o temáticas sensibles.

Utilizar servicios de correo electrónico que garanticen una **capa de seguridad** (la dirección empieza con https://), como Gmail (https://mail.google.com) o Riseup (https://help.riseup.net/).

Valorar la contratación de un **proveedor de correo electrónico encriptado radicado en un país sin vinculaciones económicas o políticas** con los eventuales agresores.

Valorar la posibilidad de usar un **sistema de cifrado de los correos electrónicos** especialmente sensibles, de modo que, aunque pueda interceptarse la comunicación, no se pueda acceder al contenido del mensaje, como Thunderbrid con GPG y Enigmail (https://support.mozilla.org/es/kb/firma-digital-y-cifrado-de-mensajes).

No abrir correos electrónicos de **remitentes desconocidos o sospechosos** (prestar atención a la dirección desde donde llega el correo), ni descargar **adjuntos que no sean de total confianza**.

## 3 Teléfono celular

Manejar **varios números de teléfono** celular, reservando el uso de algunos para determinas personas o temáticas sensibles.

Active el **servicio de identificación de llamada** (cada modelo y sistema operativo cuenta con un proceso distinto), para saber quién, o desde que número, se está llamando.

Instale una **aplicación para la grabación de llamadas**, en caso de recibir amenazas por esta vía.

### Para Android

Grabadora de llamadas
play.google.com/store/apps/details?id=com.appstar.callrecorder&hl=es

### Para iPhone

IntCall
itunes.apple.com/us/app/call-recorder-intcall/id521680097?mt=8

### Para Windows Phone

Call Recorder
www.windowsphone.com/es-es/store/app/call-recorder/0ae54c27-41f6-43eb-8b91-61a7f95e01a3

La aplicación para grabar llamadas Google Voice (play.google.com/store/apps/details?id=com.google.android.apps.googlevoice&hl=es) **advierte de que la llamada se va a grabar, con los eventuales efectos disuasorios** que puede tener para la persona que amenaza.

Instalar una **aplicación de bloqueo de números**, como Mr. Number (play.google.com/store/apps/details?id=com.mrnumber.blocker), para no recibir llamadas o mensajes de texto de un número previamente identificado.

Instalar una **aplicación que oculte o modifique el número propio**, como Spoofcard (www.spoofcard.com/apps), para que la persona a la que se llama no identifique nuestro número o mire uno falso.

Tener en cuenta que los dispositivos **BlackBerry** incluyen un **sistema de cifrado de mensajes de texto muy robusto.**

# UBICACIÓN

Algunos dispositivos y aplicaciones informáticas informan en tiempo real de nuestra localización geográfica, aunque no nos demos cuenta de ello. Por ello, se recomienda:

**Configurar** todas las aplicaciones para que no informen de nuestra ubicación.

> ¿Cómo cambio o elimino mi ubicación cuando actualizo mi estado en la aplicación de Facebook?
> www.facebook.com/help/297024380340522
>
> Preguntas frecuentes sobre la característica de ubicación geográfica del Tweet
> support.twitter.com/articles/20169204#

**Desinstalar** aplicaciones basadas en la geolocalización, como Foursquare o Facebook Places.

**Desactivar** la función Ubicación y/o GPS en teléfonos celulares inteligentes (el proceso varía según el modelo y el sistema operativo).


Aunque no esté conectado a Internet e incluso aunque no esté encendido, el celular sigue dando información sobre su ubicación. Para evitarlo:

**Sacar la batería**, teniendo en cuenta que **dificultaría hacer una llamada rápida** en caso de emergencia y que un teléfono apagado **puede interpretarse como una señal de peligro** por colegas o familiares.

# USO SEGURO DE REDES SOCIALES

Considerar las redes sociales **más como un medio de difusión del trabajo** que se desarrolla y **menos para usos personales o familiares.**

Valorar tener **dos perfiles**, uno personal y otro profesional.

Si se decide publicar información personal o familiar, **seleccionarla** muy cuidadosamente.

No anunciar **desplazamientos o viajes.**

No informar de **asistencia a actividades**.

**Configurar la privacidad**, quién puede ver, la información que se publica en **Facebook** (www.facebook. com/settings/?tab=privacy).

No aceptar "amigos" de forma indiscriminada. Organizar a los "amigos" de Facebook en listas, configurando qué información puede ver cada lista (www.facebook.com/bookmarks/lists).

**Monitorear** qué personas han comenzado a **seguirnos en Twitter**.

Moderar los **comentarios agresivos o insultantes** en redes sociales, tratando de establecer un diálogo argumentado. Si la actitud de la persona agresora se mantiene, ignorarla, bloquearla y borrar sus comentarios.

Si se reciben amenazas:

**1**. Tratar de **identificar** a la persona que amenaza.

**2**. Tomar **captura de pantalla** de los mensajes amenazantes.

**3**. **Denunciar** a la persona **en la propia red social**.

**4**. Valorar si se realiza **denuncia pública** ante autoridades judiciales, medios de comunicación y organismos de la sociedad civil.

**5**. Por último, **bloquear** a la persona:

**En Facebook**
www.facebook.com/settings?tab=blocking

**En Twitter**
support.twitter.com/articles/259218-como-bloquear-usuarios-en-twitter

# ACTUALIZACIONES

Instalar, de forma periódica y cuando sea necesario, las actualizaciones de:

Sistema operativo.

Programas antivirus.

Programas instalados.

Aplicaciones del celular o la tableta.

Gestor de contenidos (como Wordpress) de un blog o página web y sus plugins.

Asdi

Hivos
people unlimited

actores de cambio