Manual de Seguridad Organizativa

Protocolos de actuación

I. DECLARACIÓN ORGANIZATIVA SOBRE LA POLÍTICA DE SEGURIDAD

Los fines organizativos de NOVACT requieren desarrollar nuestras actividades en contextos operacionales con múltiples amenazas para nuestro equipo operativo y nuestras socias. La defensa de los derechos humanos, la justicia global y la noviolencia como estrategia de transformación social implica, en esencia, un cierto nivel de riesgo porque atentamos contra el status quo y contra los intereses políticos, económicos o militares de actores que se están beneficiando de estas desigualdades.

El presente documento aspira a establecer los protocolos mínimos para minimizar los riesgos, reducir nuestras vulnerabilidades y reforzar nuestra capacidades. Es, en síntesis, un marco de gestión de riesgos y un plan de seguridad organizativa. Esta estrategia de seguridad y protección pretende expandir y mantener los espacios de trabajo de la organización y garantizar el respeto de los derechos humanos tanto de nuestros miembros como las poblaciones locales con las que trabajamos.

NOVACT tiene el deber legal de proteger a su equipo y tomar las medidas prácticas para mitigar peligros previsibles en el lugar de trabajo. Una responsabilidad que tiene implicaciones adicionales cuando los empleados están destacados en el extranjero. Sin embargo, la prevención de los riesgos requiere un compromiso y trabajo de cada uno de los/las miembros del equipo, por ello el esfuerzo debe ser colectivo y participativo. Solo de esta manera será posible construir una cultura organizativa de la seguridad.

II. DEFINICIONES

Las siguientes definiciones nos permiten consensuar aspectos claves de la seguridad que posteriormente desarrollaremos en los protocolos. Estos términos deben formar parte de nuestra cultura organizativa entendiendo el significado y adaptándolo a nuestra necesidades propias y contexto. Es un proceso consciente, compartido y dinámico en el que todas y todos somos responsables.

- *Amenaza:* Un peligro en el entorno de las operaciones. La valoración de las amenazas nos será útil para saber que probabilidades que están se lleven a cabo. Una categorización inicial de las amenazas: a) Targeting: amenazas que surgen por la tarea que realizamos; b) Incidentales: emergen del contexto en el que trabajo en zonas de conflicto armado, ocupación, delincuencia, entre otros.

- *Riesgo:* La probabilidad y el impacto potencial de tener que enfrentar una amenaza. Es un concepto dinámico que varia a lo largo del tiempo y en función de las variaciones producidas en la naturaleza de las amenazas, la vulnerabilidad y la capacidad. Esto implica que los riesgos se deben evaluar periódicamente, en especial si se trabaja en un entorno de trabajo variable con múltiples amenazas o si nuestro puntos vulnerables o nuestras capacidades para responder cambian.

- *Riesgo residual:* El riesgo inevitable que permanece tras la reducción del riesgo y la aplicación de medidas de mitigación (ningún enfoque de seguridad puede eliminar todos los riesgos).

- *Vulnerabilidad:* hace referencia al grado en que la gente es sensible al impacto de la amenaza (sufrimiento, daño, presión). Varia de persona a persona y de

grupo a grupo, y varia en la persona y el grupo en el tiempo. La vulnerabilidad es relativa porque todas las personas y todos los grupos somos de una manera u otra vulnerable. No obstante, todos tenemos nuestro propio nivel y tipo de vulnerabilidades dependiendo de las circunstancias.

- *Capacidad:* de respuesta en la protección. Alude a los puntos fuertes y recursos que tiene el grupo o una persona para conseguir un grado razonable de seguridad.

- *Análisis/Evaluación del riesgo:* Análisis o estudio para considerar el riesgo de manera más sistemática en función de las amenazas en el entorno de una organización, de sus vulnerabilidades particulares y las medidas de seguridad existentes. Es un calculo basado en la reflexión: el resultado son nuestras necesidades en seguridad y protección.

$$\text{RISC} = \frac{\text{AMENACES} \times \text{VULNERABILITAT}}{\text{CAPACITAT}}$$

- *Gestión del riesgo:* Intento de reducir la exposición a los riesgos más serios (riesgos contextuales, programáticos e institucionales) mediante la identificación, la supervisión y el abordaje de factores clave de riesgo. También supone lograr un equilibrio entre los riesgos y las oportunidades, o una serie de riesgos contra los otros.

- Gestión de los riesgos de seguridad/Marco de gestión del riesgo (SRM): Una parte de la gestión del riesgo que acarrea una estructura para entender mejor la naturaleza y el nivel de los riesgos para la organización o el programa. Este riesgo deberá contrarrestarse con los beneficios del programa para la población afectada y deberán considerarse los medios para hacer frente y mitigar estos riesgos.

- Criticidad del programa: Enfoque que implica determinar qué programas son más críticos en una parte determinada del país (en términos de salvar vidas o que requieran una entrega inmediata) y que por ello justifica aceptar un nivel de riesgo mayor o una asignación mayor de los recursos para mitigar tales riesgos.

- Estrategia de seguridad: La filosofía global, aplicación de los enfoques y uso de los recursos que enmarcan la gestión de la seguridad de una organización.

- Incidente de seguridad: se puede definir como cualquier hecho o evento que pensamos que podría afectar nuestra seguridad personal o como organización. Un incidente de seguridad puede ser incidental, intencionada o no intencionada. Los incidentes de seguridad son "la unidad mínima" de las medidas de seguridad y son indicativos de la magnitud de la oposición a nuestro trabajo, o de la presión que soportamos. Hay que fijarse bien en ellos. Algunos ejemplos de incidentes serian: Lesión física, coche de policía vigilando nuestra oficina, robo de material de oficina (celular, ordenador, etc). Es importante destacar que todas las amenazas son incidentes de seguridad, pero no todos los incidentes de

seguridad son amenazas. Es decir, un robo de móvil no tiene porque suponer una amenaza, debemos valorar su intencionalidad y vulnerabilidad (acceso a los datos, contactos, etc). Cuanto más conscientes seamos del entorno y cuanto mejor entrenadas y entrenados estemos, menos incidentes escaparán a nuestra atención.

- Triangulación: Verificación de información o hechos comparando las opiniones las versiones provenientes de diferentes fuentes.

- Umbral de aceptación del riesgo: El punto a partir del cual se considera que el riesgo es demasiado alto para continuar operando; influenciado por la probabilidad de que ocurra un incidente y la gravedad de su impacto.

- La protección: conjunto de actividades que una organización lleva a cabo para garantizar la seguridad de otras personas y organizaciones con las que trabaja.

- Información sensible: es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico.

- Información confidencial: Es aquella información relativa al contenido esencial del derecho a la privacidad, del derecho a la intimidad, el derecho al honor, el derecho a la propia imagen, y aquella que expresamente la ley les otorgue dicho carácter, que se encuentra en poder del Estado y cuyo acceso se encuentra restringido de manera permanente, salvo que exista consentimiento del propio titular de la información.

III. ESTRUCTURA

A partir de las definiciones descritas, los protocolos que proponemos se estructuran en los categorías siguientes:

- **Protocolos de análisis:** destinados a evaluar los riesgos de las amenazas y nuestra vulnerabilidades. (1 a 5, y 20)
- **Protocolos preventivos:** destinados a prevenir los riesgos (6 a 14)
- **Protocolos reactivos:** destinados a reaccionar a las amenazas (15 a 19)

IV. PROTOCOLOS

Protocolos de análisis

Los riesgos surgen de nuestro entorno de trabajo y la criticidad de los programas implementados. Analizaremos los riesgos organizativos a dos niveles: a) Evaluación de riesgos comunes a todo el equipo; b) Evaluación de riesgos por contextos operacionales o países.

Paralelamente al proceso de evaluación de los riesgos organizativos, es necesario evaluar las vulnerabilidades y capacidades organizativas para analizar el impacto que

una amenaza puede ocasionar en un miembro del equipo o a su conjunto, así como nuestra capacidad de reacción. Este análisis nos permitirá crear nuevos protocolos o reforzar los ya existentes, para así reducir las vulnerabilidades y reforzar nuestra capacidades a nivel securitario. Analizaremos las vulnerabilidades y capacidades organizativas a dos niveles: a) Evaluación de vulnerabilidades y capacidades comunes al conjunto de la organización; b) Evaluación de vulnerabilidades y capacidades por contextos operaciones o países.

Será necesario realizar formaciones específicas para poder elaborar mejorar los documentos de análisis.

Protocolo 1. Evaluación de riesgos comunes

Supone la identificación y el análisis de las amenazas a las que nos enfrentamos la organización en su conjunto. A partir de este análisis determinaremos el riesgo que nos permitirá desplegar los protocolos de mitigación y emergencia.
La evaluación de los riesgos comunes es responsabilidad del equipo operativo a través de un taller de seguridad organizativa anual que producirá de forma colectiva y participativa la **"Ficha de Evaluación de Riesgos Comunes" (ANEXO 1).** El facilitador/a de la sesión formará parte del equipo operativo.

Protocolo 2. Evaluación de riesgos por contextos operacionales y/o países

Se trata de identificar y analizar las amenazas a las que estamos expuestos/as en los contextos operacionales o países en los que trabajamos. A partir de este análisis determinaremos el riesgo de esas amenazas por contexto/país.
Cada área y oficina tiene que rellenar su ficha de evaluación de riesgos comunes y de riesgos por contextos/países que tiene que servir para producir de forma colectiva y participativa un documento único.
Los/las miembros de cada área son los responsables de elaborar las **"Fichas de evaluación de riesgos por contextos o países" (ANEXO 2)** a través de una sesión de trabajo interna en cada área. Debido a la inestabilidad y cambiante situación de los contextos donde operamos, se deberá realizar producir fichas cada 6 meses como mínimo. El/la responsable determinará si se debe realizar evaluaciones en períodos inferiores. Una vez realizadas deberán ser compartidas con el resto del equipo operativo y archivas con la fecha de elaboración en la carpeta correspondiente.

Protocolo 3. Registro de incidentes

Para poder realizar análisis adecuados de amenazas y riesgos, es necesario llevar un registro de listado de incidentes de seguridad. Se deben producir listado de incidentes a dos niveles: a) para las amenazas comunes y b) para cada uno de los contextos operacionales o países donde trabajamos. El registro de incidentes nos permitirá determinar los patrones de las amenazas.

El registro de incidentes para las amenazas comunes debe ser realizado por el Responsable administrativo en cooperación con los responsables de áreas si es necesario. Mientras que el registro de incidentes en los contextos operacionales/países debe ser cumplimentado por el /la responsable de área.

En caso de incidente se debe:

- Primero, informar a codirección y responsable de área de forma inmediata
- Segundo, en las siguientes 24 hora rellenar la **Ficha de Registro de Incidentes (Annexo 3)**
- Tercero, compartir la ficha con el responsable administrativo y área
- Cuarto, compartir la ficha con el equipo operativo.

Protocolo 4. Evaluación de vulnerabilidades y capacidades comunes

Para poder determinar el impacto de una amenaza es necesario evaluar nuestra vulnerabilidades, a partir de este análisis podremos crear y reforzar determinados protocolos y reforzar nuestras capacidades para reaccionar, prevenir y hacer frente a la amenaza.

La evaluación de las vulnerabilidades y capacidades comunes es responsabilidad del equipo operativo a través de un taller de seguridad organizativa anual para producir de forma colectiva y participativa la **"Ficha de Evaluación de Vulnerabilidades y Capacidades Comunes" (ANEXO 4)**. El facilitador/a de la sesión formará parte del equipo operativo.

Protocolo 5. Evaluación de vulnerabilidades y capacidades por contexto operacional y/o país

A nivel de contexto operacional y/o país, las vulnerabilidad y capacidades pueden variar. Asimismo, la naturaleza cambiante y la inestabilidad de los países donde operamos requiere un análisis más constante de nuestra vulnerabilidades para poder reforzar nuestras capacidades de mitigación de amenazas y reacción en caso de consumación.
Con este objetivo, la evaluación de vulnerabilidades y capacidades se realizará cada 6 meses en el marco de los áreas de la organización, facilitado/a por el responsable del área. El producto final será la **"Ficha de Evaluación de Vulnerabilidades y Capacidades por Contexto Operacional y/o País" (ANEXO 5)**

Todos los documentos de análisis estarán en carpetas encriptadas para asegurar su confidencialidad.

Protocolos preventivos

Protocolo 6. Oficinas

La seguridad en la sede de la organización, oficinas y casas del equipo expatriado, de ahora en adelante utilizaremos oficinas para referirnos a estos tres tipos de espacios, es fundamental para la organización. Los puntos vulnerables de una oficina se deben determinar en función de las amenazas a las que nos enfrentamos. En este sentido los robos de información y material oficina, emergencias por incendio, agresiones, entre otros, son algunas de las amenazas comunes a las que nos podemos enfrentar. En el caso de casas de expatriado revisar el estatuto del cooperante.

6.1. Selección y emplazamiento de la oficina. El equipo operativo destinado en el país seleccionará la oficina y su emplazamiento y propondrá al responsable de área la opción

escogida para su validación final. Los aspectos a tener en cuenta en el emplazamiento de la oficina son:

- Condiciones del edificio: solidez de las estructuras, materiales de construcción, puertas, ventanas, barreras protectoras, entre otras.
- Barrio: Estadísticas del crimen; cercanía a objetivos potenciales de ataques armados, tales como instalaciones militares o edificios del gobierno; lugares seguros utilizables como refugio; otras organizaciones nacionales e internacionales con las que mantengamos contacto.
- Relaciones: Tipo de gente en el barrio; reputación de dueños, anteriores inquilinos; anteriores usos del edificio.
- Acceso: Una o varias buenas rutas de acceso (cuantas más, mejor, aunque es bueno recordar que el cualquier potencial agresor también tendría más donde elegir); acceso en transporte público y privado.
- Alumbrado público en la zona
- Propensión a accidentes humanos o naturales: Incendios, inundaciones importantes, deslizamientos de terreno, vertido de materiales peligrosos, fábricas con procesos industriales perjudiciales para la salud, etc
- En el caso de vehículos: Un garaje o al menos un patio o espacio cerrado con una barrera de paso.

6.2. Acceso personal externo a las oficinas. Se debe controlar el flujo de personas externas a la entidad a través de un procedimiento de admisión. Es clave evitar que personas no autorizadas accedan a nuestra oficina. El procedimiento de admisión, por tanto, será que:

a) Ninguna persona no autorizada no puede acceder a nuestras oficinas
b) Debe existir una persona responsable de admisión de grupos externos o personas, esta persona autorizará el acceso y uso de salas
c) La persona responsable de admisión debe estar presente durante el acceso y el tiempo que estén en la oficina. En el caso que se entregue llaves para ese uso específico, será la persona responsable la que haga la entrega.
d) En los casos en que la persona responsable de admisión no pueda dar acceso físicamente se delegará en otro/a miembro del equipo operativo.

El equipo operativo en cada oficina elijaran a una persona responsable de admisión a la oficina y podrá reforzar este procedimiento.

6.3. Llaves. No dejar a la vista de la visitas externas las llaves. Realizar copias de llaves para los/las miembros del equipo operativo. Si finaliza la relación de trabajo con la organización, las personas que dispongan de llaves deberán entregarlas. Es necesario disponer de inventario de copias de llaves y las personas que las poseen. De acuerdo a las amenazas que nos enfrentemos en cada oficina, el equipo operativo en el país decidirá si deja copias de llaves a las personas externas autorizadas. En el caso de tener llaves para los armarios y otras salas de la oficina es preferibles utilizar números en lugar de una descripción. En el caso de pérdida de llaves se deberá realizar cambio de cerradura, salvo consideremos que haya sido un accidente y no haya riesgos de amenazas.

6.4. Dispositivos de seguridad, extinción y detección de riesgos. Las oficinas deben disponer de forma obligatoria de los siguientes dispositivos:

- Extintores portátiles: cada 15 metros

- Alarmas de detección de intrusión e incendios
- Alumbrado de emergencia
- Señalización para evacuación: incluyendo plano de evacuación
- Linternas: con pilas adicionales

Es necesario mantener un mantenimiento de los dispositivos cada 6 meses, guardar los manuales de uso y tener en cuenta los cortes de electricidad para el funcionamiento de los dispositivos de seguridad. El Área de Administración o el responsable de la oficina debe asegurarse de que estén dispositivos estén instalados.

Cada equipo operativo en el país decidirá con su responsable de área y programa la necesidad de disponer de otros dispositivos de seguridad (cámaras de vídeo, barreras protectoras, etc) de acuerdo a los riesgos de amenazas a los que se exponen. En cualquier caso, es necesario tener en cuenta que la disposición y la cantidad de dispositivos de seguridad podría ser contraproducente y atraer el interés de delincuentes u otras potenciales hostilidades.

Los medios de seguridad (extintores, etc) deben de ser de acuerdo a la normativa del país de la oficina como mínimo

6.5. Teléfonos de emergencia. Las oficinas deben tener una lista de teléfonos de bomberos, médicos, hospitales, policía, miembros del equipo operativo de la oficina y de otras oficinas en un lugar fácil acceso. El Equipo operativo en el país es el responsable de redactar el listado.

6.6. Seguros de las oficinas. Las oficinas deben disponer de seguros para los posibles daños y robos que se puedan producir. Los responsables de áreas son responsables de gestionar esos seguros con el Área de Administración.

Protocolo 7. Salud y prevención de riesgos laborales

Se consideran daños laborales (Art. 4 de la Ley de PRL) los originados por:
- Accidentes de trabajo.
- Enfermedades profesionales.
- Otras patologías derivadas del trabajo (fatiga, estrés, insatisfacción laboral,…).

La prevención de los riesgos laborales de la organización se rige con la Ley de 54/2003 de 12 de diciembre que tiene por objetivos básicos los siguientes:
- Combatir la siniestralidad laboral.
- Fomentar una auténtica cultura de la prevención de riesgos en el trabajo, que asegure el cumplimiento efectivo y real de las obligaciones preventivas.
- Reforzar la necesidad de integrar la prevención de los riesgos laborales en los sistemas de gestión de la empresa.
- Mejorar el control del cumplimiento de la normativa de prevención de riesgos laborales.

7.1. Instrucciones para la prevención de riesgos laborales. El equipo operativo debe conocer sus derechos y obligaciones, para ello anexamos el documento de

“Instrucciones para la prevención de riesgos laborales” a los Protocolos de Seguridad Organizativos. **(ANEXO 6).**

7.2. Pantallas de visualización de datos. Debido a las características de nuestro trabajo pasamos muchas horas antes ordenadores. Largos períodos de trabajo antes las pantallas de visualización de datos (PVD) pueden ocasionar molestias, lesionas o incluso enfermedades profesionales. Para ello recomendamos la lectura del documento de **“Instrucciones para Prevención de riesgos laborales relacionado con las Pantallas de visualización de datos” (ANEXO 7).**

7.3. Accidentes laborales. El caso de accidente laboral en el lugar de trabajo o durante el trayecto hacia/desde el lugar de trabajo, la persona accidentada deberá comunicar el accidente al área de Administración que elaborará parte de accidente (volante) para poder visitar la Mutua de Accidentes Laborales contratada (Asepeyo). En el caso de no poder obtener parte de accidente y necesidad urgente de atención sanitaria, el accidentado/a puede ir directamente al centro asistencial más cercano (Red de Delegaciones Asepeyo) o llamando al teléfono gratuito de información permanente de Asepeyo (900 151 000) donde le indicarán el centro más cercano. Para más detalle como proceder en caso de accidente laboral ver el **Manual de actuación en caso de accidente de Asepeyo (ANEXO 15)**

7.4. Estrés. El estrés suele ser muy habitual en nuestro trabajo debido a las largas horas de trabajo y presión a la que estamos sometidas. Además el estrés prolongado y/o intenso puede ser causa de múltiples enfermedades y provocar problemas de comunicación inter-personal. Para ello se propone que la gestión del estrés de forma individual, a través de la práctica de ejercicios específicos a lo largo del día **(Consejos para Reducir el Estrés - ANEXO 8)**, y de forma colectiva a través de los talleres de cuidados emocionales una vez al mes.

Protocolo 8. Transporte interno y viajes de campo
Se refiere a los viajes a ubicación de trabajo de los expatriados/as, viajes de campo de los/las miembros a países diferentes donde residen (viajes puntuales) y transporte interno en los países de trabajo.

8.1. Seguros de viaje. Es necesario que todas las personas que trabajan en la entidad y viajan por motivos laborales estén cubiertas en sus viajes por un seguro que cubra salud y accidentes. Adquirir seguros de viaje para los miembros del equipo operativo siempre que sea necesario. En los casos que no sea posible adquirir un seguro de viaje debido a la situación de conflicto armado y aun cuando el/la miembro del equipo operativo dese viajar, será necesario firmar un acuerdo entre la organización y el/la miembro del equipo operativo para la exención de responsabilidad de la organización. Hay que distinguir estos cinco supuestos:

a) Seguro del expatriado/a: regulado por el Estatuto del Cooperante para asegurar al miembro del equipo operativo durante su estancia en el país para realizar las funciones asignadas. El responsable de área al que pertenezca el expatriado/a contratará los seguros correspondientes en cooperación con el área de Administración. A través del Seguro del Cooperante tenemos contratadas dos **pólizas: la de DKV (ANEXO 16)** cubre la asistencia sanitaria y la de Generali es un seguro de vida del expatriado/a.
b) Seguro de personal en sede para viaje de campo: Dos tipos de casos:

b.1) En el caso de países de la UE, CEE, EEE, Suiza y otros países con convenio internacional es necesario viajar con la Tarjeta Sanitaria Europea para cubrir la sanidad por enfermedad común y accidentes no considerados laborales.
Para accidentes laborales tenemos cobertura sanitaria, incluyendo repatriación, con la Mutua oficial de la organización (Asepeyo). Ver Anexo 9
El/la miembro del equipo operativo debe informar al Área de Administración que elaborará el formulario TA.300. Sin este trámite previo no existirá cobertura sanitaria. Se recomienda también la obtención de la Tarjeta Sanitaria Europea.
b.2) En los casos de países no cubiertos por el convenio de la SS y la Mutua oficial de la organización, será necesario contratar un seguro especial que pueda cubrir ese país específico. De no ser así se deberá renunciar la viaje o subscribir una exención de responsabilidad entre la organización y el/la miembro del equipo operativo.

c) Personal local. Hay que averiguar sobre la legislación local
d) Voluntariado. Siempre ha de viajar con un seguro privado contratado por Novact.
e) Profesionales asociados. Hemos de asegurarnos que el profesional ha contratado un seguro privado de viaje

8.2. Accidentes laborales en el extranjero (Tanto personal expatriado como viajes de campo): En los casos de accidente o enfermedad laboral en el extranjero, el/la miembro del equipo operativo debe ponerse en contacto con la Mutua de Seguros (+34 934 955 181) u otra Mutua especial adquirida. Es imprescindible que antes se haya contratado el Seguro del Cooperante o se haya cumplimentado el formulario TA.300 o se haya contratado un servicio especial para destino. Si no se posee la Tarjeta Sanitaria Europea, el trabajador deberá realizar el pago de los gastos de la asistencia sanitaria en el extranjero y posteriormente solicitar a Asepeyo la reintegración de esos gastos a través de la documentación justificativa correspondiente. El Área de Administración dará apoyo para este proceso. Para más información ver el **Documento de Asistencia Sanitaria con la Mutua oficial** para los primeros dos casos. **(ANEXO 9).**

8.3. Información a las autoridades españolas. En los casos de residencia en los países de destino o viajes de campo de duración larga, informar a la Embajada o Consulado español en el país de nuestra llegada y período. En el caso de residencia será necesario registrarse.

8.4. Transporte en el interior de los países. En el extranjero utilizar los medios de transporte más seguros. Para ello valorar con el equipo operativo destinado en el país los diferentes medios de transporte. Si es necesario consultar otras organizaciones expatriadas su procedimientos de viaje. En el caso de desplazamientos internos el miembro del equipo operativo que realice viaje debe elaborar una "Orden de Misión" que incluirá período del viaje, itinerario del desplazamiento, personas con las que se reunirá. La Orden debe ser aprobada por el responsable de área y programa.

8.5. Desplazamiento a zonas y países críticas. A parte de los trámites de seguro, será necesario activar mecanismos adiciones para mitigar riesgos de amenazas. Entendemos por desplazamiento a zonas y países críticas los viajes a zonas del mismo país (ej. Gaza) o países donde existe riesgos de denegación de entrada, interrogatorios, situación de conflicto armado, etc. (ej. Israel, Marruecos). En este caso, el/la miembro del equipo que realice el viaje deberá elaborar, en cooperación con el/la responsable de área, un **"Ficha de emergencias" (ANEXO 10)** al menos una semana antes del viaje. Por

normal general, los viajes de campo tienen que tener ficha de emergencia. El responsable de programa debe validar el Formulario de emergencias. En los casos de viaje a países muy sensibles se tratará colectivamente a través de una reunión de equipo operativo la decisión final del viaje.

En la medida de lo posible se recomienda:

- Realizar los viajes críticos en pareja.
- Adquirir una tarjeta SIM del país en el aeropuerto. Devolver la tarjeta a administración a la vuelta.
- Adquirir móviles liberados para comunicación durante los viajes fuera de España.
- Consultar con el equipo en terreno la ruta mas segura de viaje para llegar a la oficina y los medios mas seguros de transporte en el caso que no haya alguien que vaya a buscarlo.
- Consultar la cobertura sanitaria, seguros y protocolos de actuación en caso de accidente antes de realizar el viaje

Protocolo 9. Plan de prevención por oficinas

Con el objetivo de ajustar aun más las medidas preventivas de seguridad al contexto operacional, se realizará un plan de prevención adaptado para cada oficina que cubra los siguientes aspectos:

1. Análisis y localización de riesgos, incluyendo la ficha de Evaluación de Riesgos y protocolos de actuación (Protocolo 2 - Anexo 2)
2. Refuerzo de protocolos preventivos y reactivos identificados en Anexo 2
3. Seguridad en la oficina (Protocolo 6)
4. Riesgos laborales (Protocolo 7)
5. Seguridad en los transportes (Protocolo 8)
6. Plan de evacuación oficina y país (Protocolo 20)
7. Ficha de emergencias (Anexo 10)

El Equipo operativo de cada área elaborará el **Plan de Prevención por Áreas (ANEXO 11)** que será una adaptación al país y una profundización del Manual de Seguridad.

Protocolo 10. Manejo de dinero y objetos valiosos

Para evitar robos de dinero de proyecto deben realizarse transferencias directamente de un banco a otro, realizar los pagos con tarjetas o sacar dinero en efectivo en el país de destino. Los donantes establecen límites para pagos en efectivo de hasta 3.000 EUR. En caso de pago en efectivo siempre hacer recibos de entrega y justificantes de lo sobrante.

No se recomienda viajar con altas cantidades de dinero (existen restricciones de cantidades para poder entrar y salir de un país aprox. 10.000 USD). En caso de viaje con altas cantidades de dinero cumplimentar un “Ficha de emergencias” (ANEXO 10).

En caso de robo, registrar el incidente, informar de inmediato al responsable de área y realizar una denuncia de robo a las autoridades.

Protocolo 11. Documentación

Hace referencia a la gestión de documentación de carácter confidencial. La información confidencial son aquellos documentos, datos, objetos y asuntos cuya revelación no autorizada podría dañar la seguridad de la organización y de sus miembros, perjudicar nuestros intereses, dificultar el cumplimiento de nuestra misión o poner en peligro a nuestros socios/as. Por ello es necesario mantener este tipo de documentación archivada de forma segura.

11.1. Obtención y transferencia de la información. Si necesitamos recibir o capturamos información de carácter personal es necesario recibir autorizaciones expresas de la persona que aporta esta información de acuerdo a la Ley de Protección de Datos. Esto tiene especial relevancia para la base de datos de incidentes de derechos humanos o listas de contactos que guardamos para posteriormente enviar newsletter. En ambos casos se necesita autorizaciones expresas. Existe otro tipo de situaciones en los que el testimonio puede correr riesgos por la transferencia de la información, en estos casos es necesario crear canales seguros para la entrega/obtención de la información (comunicaciones encriptadas, entrega de información en espacios privados seguros, etc). En cualquier caso, es fundamental informar a la fuente que se va a hacer con esta información (objetivos, custodia, tratamiento, etc), asimismo debe informarse de los riesgos que pueden entrañar el traspaso de esa información. Si los documentos son impresos, se debe intentar en la medida de lo posible, pasa esta información a USB, nubes de información segura con códigos encriptados. Evitar viajar con documentos impresos y los soportes digitales cuando se atraviesan checkpoints, controles de aeropuerto, etc. Para ello enviar CD-ROM o USD encriptados, o subir la información directamente al Cloud.

11.2. Almacenamiento de la información. Los archivos impresos solo deberían ser almacenados cuando sea estrictamente necesario. En este caso, archivar esta información en armarios cerrados bajo llave. El método habitual para el almacenamiento de la información debería ser digital, aquella información confidencial debería estar en el Cloud organizativo con un sistema de protección alto (Firewall). En casos supuesto de información muy sensible se debe encriptar las carpetas y tener los códigos bien sistematizados (Keypass). Deben realizarse copias de seguridad de forma periódica. El registro de información de carácter personal supone la obligación de informar a la Agencia Española de Protección de Datos de los tipos de información que estamos recogiendo. De lo contrario podríamos estar realizando una captura y almacenado de información ilícita.

11.3. Tratamiento, distribución y visualización pública de la información. Las personas que accedan a la documentación sensible o confidencial deben firmar documentos de confidencialidad. La dirección debe establecer el grado de acceso a la información confidencial de la organización a voluntarios/as, colaboradores y personal externo a la entidad. La distribución de la información debería realizarse a través de medios seguros como comunicaciones encriptadas. En cuanto a la visualización siempre se debe preservar la información de la fuente, evitar información, cuidar el redactado de los

datos sensibles, etc. Siempre priorizando la protección de la fuente, socios/as, comunidades locales.
11.4 Información sensible en las oficinas expatriadas. Cada 3 meses se realizarán envíos de información sensible de la oficina a la sede central a través de servicio privado de correo.

11.5. Baja de miembro de equipo. En el caso de un miembro de equipo operativo finalice su relación contractual se permitirá se dará de baja su cuenta de correo electrónico de la organización, se redireccionarán los emails a otras cuentas del equipo y se hará un cambio de contraseñas de las nubes de información y otras herramientas tecnológicas a las que tenía acceso.

Protocolo 12. Seguridad digital

La seguridad digital es un elemento clave de la estrategia de seguridad de la organización. La mayoría de comunicaciones se produce a través de herramientas digitales (correo electrónico, skype, etc), así como el almacenamiento de información confidencial. Es clave incorporar en nuestro día a día técnicas y herramientas seguras para que esta componente no suponga una vulnerabilidad organizativa. La seguridad digital es por tanto, responsabilidad de cada uno de los/las miembros del equipo operativo y de las herramientas digitales corporativas. Hay que tener en cuenta que este sector es muy dinámico, una caja de herramientas actualizada es la producida por FrontLine Defenders: https://securityinabox.org/es. Algunas de las herramientas que proponemos a continuación están recogidas en este kit. Asimismo, anualmente se realizarán formaciones internas de seguridad digital para explorar nuevas herramientas, hábitos, entre otros.

12.1. Ordenadores. Deben quedar bajo llave al salir de la oficina. También debe tener una contraseña de acceso inicial. Las copias de seguridad se realizarán en el Cloud, por tanto, en la medida de lo posible, no almacenar documentos en nuestros ordenadores. Realizar limpiezas periódicas de historial web, cookies, archivos en la papelera a través de Ccleaner.

12.2. Contraseñas. Utilizar contraseñas de seguridad alta a través de la combinación de números, letras y mayúsculas/minúsculas. Una herramienta muy útil para genera contraseñas segura de forma periódica es Keepass. La carpeta donde se guardan las contraseñas oficiales de la organización debe estar encriptada. Es necesario realizar cambios de contraseña de forma periódica.

12.3. Internet. Nuestra salida a internet debe ser segura para que no puedan acceder a nuestro ordenadores y red de trabajo. Para ello se reforzaran los firewalls. Tener en cuenta que cuando nos conectamos a wifi fuera de la oficina estamos más expuestos, especialmente aquellos wifis abiertos que no tienen contraseña.

Recomendaciones para trabajar desde un ciber-café:

a) Utilizar un navegador seguro: Firefox
b) Encriptación de emails.
c) Si utilizamos un ordenador del ciber-café, es necesario comprobar que no contiene un virus. Si hay virus podrían acceder a nuestro lístin de direcciones/contactos de nuestra cuenta de correo. Así como acceder a los disco

duro externos que conectemos. Por tanto, es necesario tener un disco duro externo encriptado si lo vamos a utilizar en un ordenador ajeno.

12.4. Correo electrónico. Nuestra emails no van directos de nuestro correo a la cuenta de recepción sino que por el camino pasan por varios nodos del mismo país o incluso diferente. Al cabo del día enviamos numerosos correos electrónicos y muchas de estas comunicaciones pueden ser interceptadas, pero también recibimos muchos correos que pueden suponer una amenaza. A continuación establecemos las reglas mínimas de seguridad:

No encriptar mails como política general de la organización. Necesario establecer una definición de qué es información sensible y problemática y muy importante la formación constante en estos temas.

a) Encriptar los emails con información sensible o confidencial a través de enigmail (desde Thunderbird o Outlook) o correos electrónicos que permitan encriptar como Protonmail. Un correo no encriptado es como una postal, puede ser leído por cualquiera. Un correo encriptado es como una carta en un sobre y dentro de una caja fuerte.
b) NUNCA abrir un correo de alguien que no conozcamos.
c) NUNCA reenviar un correo de alguien que no conozcamos, incluso si éste nos ha sido a su vez reenviado por alguien que conocemos. También esos correos que circulan con "mensajes positivos" pueden contener virus. Al reenviarlos, podemos estar infectando los ordenadores de todo el mundo.
d) NUNCA descargar o abrir un documento adjunto a no ser que sepamos lo que contiene y que es seguro. Debemos desactivar la opción del programa de correo electrónico que hace las descargas automáticas. Muchos virus y troyanos se propagan como "gusanos" y los gusanos modernos a menudo resultan haber sido enviados por alguien que conocemos. Los gusanos replicantes escanean nuestro listín de direcciones, en especial si usamos el Microsoft Outlook o el Outlook Express, y luego se envían solos disfrazados de adjuntos normales procedentes de nuestros contactos. Si usamos el programa PGP al firmar nuestros correos, tanto en los que van con adjunto como en los que no, podríamos ayudar a quienes reciben nuestros correos a tener menos dudas respecto a si el adjunto está libre de virus (el PGP es un software que encripta la información.
e) NUNCA debemos enviar un mensaje a un grupo numeroso usando la línea del "Para" (destinataria/o(s)) o "CC" (con copia a). Cuando deseemos enviar algo a mucha gente, en la línea de "Para" copiaremos nuestra propia dirección y añadiremos las direcciones de los demás en la línea "CCO" (copia oculta a). (Para acceder a CCO es necesario ir a "Herramientas" y luego hacer clic en "Seleccionar destinatarios".) Esto no se hace sólo por cuestión de seguridad: es una cuestión de respeto a la privacidad: darle a otras personas la dirección de correo de alguien que no nos han autorizado a hacer tal cosa se considera una falta de educación, una falta de respeto y algo que nos puede dar un disgusto y poner en peligro.
f) NUNCA responder al spam, ni siquiera para pedir que nos borren de una lista. Los servidores de spam envían correos a listas interminables de direcciones y nunca saben cuáles están en uso. Cuando respondemos, el servidor nos reconoce como dirección válida y esto suele implicar que a partir de ese momento nos freirán a spam.

12.5. Cloud. La información debe ser almacenada en el cloud. Este cloud debe ser seguro con acceso restringido a nuestro usuarios y con cortafuegos (Firewall) sólidos. Deben realizarse copias de seguridad de nuestro cloud y servidor interno como mínimo cada semana. Por otra parte, es importante destacar que debe ser restringido el acceso a las personas que acaben su relación laboral con la organización al día siguiente de la finalización de su contrato o bien cambiar las contraseñas de acceso al cloud.

12.6. Software. Debería ser legal ya que el uso de software pirata puede suponer una vulnerabilidad para la organización y justificar redadas, sanciones o delitos de piratería, una forma de criminalizar a la organización a ojos de la opinión pública. Se pueden hacer excepciones en programas muy específicos como Indesign que no todo el equipo utiliza.

12.7. Teléfonos móviles. No es un medio seguro pero lo necesitamos a diario. Existen múltiples herramientas que pueden interceptar nuestras comunicaciones. Para comunicaciones sensibles utilizar mensajería encriptada. Cuando viajemos a zonas críticas y que no queremos ser localizados desconectar la geolocalización. Informar a la red de emergencia de forma periódica donde nos encontramos en las zonas críticas.

Protocolo 13. Tiempo libre

Las consumación de una amenaza suele producirse en los momentos más vulnerables y cuando la capacidad de reacción es menor (Por ej. Denegación de entrada en un país un domingo). Desde un punto de vista de seguridad, la amenaza no distingue entre horas de trabajo y horas de ocio, por esta razón es importante mantener también unos mínimos durante nuestras horas de descanso. El objetivo no es obsesionarnos con la seguridad a todo momento, sólo si existe un riesgo alto de amenaza entonces deberíamos también reforzar nuestra seguridad en el tiempo libre. Por tanto, si los riesgos son altos deberíamos tener en cuenta los siguientes criterios en nuestras horas de ocio, noche y vacaciones:

a) En la medida de lo posible, no realizar viajes a países o zonas que creemos críticos durante los días de descanso de la organización, ya que puede que nuestra red de emergencia no tenga la misma capacidad de reacción durante esos días.
b) Cuidar la ingesta de alcohol y/o drogas en lugares públicos y críticos.
c) Informar a una persona de la red de emergencia si vamos a realizar un viaje de ocio a una zona crítica dentro de nuestro país de destino.
d) Mantener la confidencialidad de aquella información sensible incluso en las relaciones informales en nuestro tiempo libre. Esta suele ser una forma de investigación bastante habitual de obtención de información.
e) Cuidar nuestra imagen en relación con valores sociales, culturales y/o religiosos en zonas críticas. Un comportamiento inadecuado desde un punto social en un zona crítica puede volverse en contra nuestra y ser utilizada para dañar los intereses de la organización.

La prioridad de nuestro tiempo libre es desconectar de los asuntos de trabajo para poder descansar y reducir nuestro nivel de estrés. Pero un equilibrio con los aspectos securitarios debería ser un conveniente cuando sea necesario.

Protocolo 14. Cuidados y gestión emocional

Se trata de desarrollar una cultura organizativa del cuidado que nos permita resolver problemas, identificar situaciones de estrés o agobio y reforzar el nivel de resilencia de los/las miembros del equipo operativo. Para ello se organiza una vez al mes una sesión para todo el equipo operativo para nuestra cura emocional. El taller se realizará en el espacio de una reunión de equipo, por un facilitador/a interno a la organización y siguiendo con las instrucciones del **Protocolo de las sesiones de cuidados y gestión emocional (ANEXO 14)**

Protocolo 15. Robo de información

La reacción ante un caso de robo de información debería incluir:

- Informar de inmediato a la dirección de la entidad
- Determinar cuánta información se ha perdido y cómo de sensible era.
- Valorar el tema de informar posteriormente a las personas e instituciones potencialmente afectadas.
- Valorar la posibilidad de informar a las autoridades y de hacer públicos los hechos. En caso positivo, realizar denuncia de robo.
- Dar cualquier otro paso necesario para evitar los daños que pueden producirse si usan la información perdida o robada.
- Cumplimentar el formulario de registro de incidentes (ANEXO 3)

Protocolo 16. Registro de oficina y/o casa

No podemos considerar que un registro de una oficina o casa por parte de las autoridades es un hecho inesperado. Existen incidentes previos que pueden llevar a indicarnos que un registro de este tipo puede suceder. De ahí la importancia de registrar los incidentes previos para poder reducir el riesgo de la amenaza de un registro y las vulnerabilidades. Los registros pueden suponer una serie de amenazas y peligros como que alguien salga herido o haya daños psicológicos, se pierda o destruya información confidencial, esa información sea utilizada contra nuestros intereses o el de nuestras socias, se roba dinero, se destruya ordenadores, etc. En estos casos, el equipo operativo destinado en el país en cooperación con el responsable de área deben ser capaces de identificar un potencial registro y reforzar sus capacidades para reaccionar. Algunos ejemplos de esa reacción puede ser mantener la calma, conocer la ley, tener identificados documentos oficiales de registro, actuar rápidamente después del registro, entre otros.

Para prevenir los registros en oficinas y robos de información sensible, se realizarán envíos de información cada 3 meses a la sede central en Barcelona y tener toda la información que podamos en la nube.

Protocolo 17. "Sin noticias", detención o retención.

En los casos que se desconozca el paradero de un miembro del equipo operativo, debemos tener en cuenta que puede producirse por diferentes causas (que la persona no quiera que se le contacte, este hospitalizada o tenga problemas técnicos para poder comunicarse). Es importante, comunicar los desplazamientos a zonas críticas a través de el "Formulario de Emergencias" (ANEXO 11) y detallar medios alternativos de comunicación. A través del formulario de emergencias se puede hacer un seguimiento más adecuado e intentar identificar a la persona.

Se pueden producir otras situaciones en que la persona este retenida por un grupo no estatal o detenida por las autoridades. Ambos casos son considerados situaciones de crisis y deben seguirse los protocolos establecidos. Para poder evitar una detención o retención es necesario identificar el riesgo de la amenaza a través del registro de incidentes y tomar las siguientes medidas:

a) En la medida de lo posible, no viajar sola/o.
b) Analizar la ley del país sobre visados, extranjería y otros aspectos relacionados con nuestro viaje.
c) Información adecuada sobre la zona y los actores que vamos a visitar, elaborar un programa de actividades, números de contacto de las personas que vamos a visitar.
d) Todas las personas que participen en la misión deben disponer de documentos de identidad válidos y llevarlos siempre consigo.
e) Avisar a los contactos de la red de emergencia de la organización a quienes corresponda estar alerta durante la misión (desde el momento de su salida hasta que esté de vuelta).
f) Planificar actualizaciones regulares sobre el estado de la misión (normalmente por teléfono, a horas que hayamos acordado previamente).
g) Valorar la seguridad del medio de transporte elegido (que podrá ser a veces un vehículo de la propia organización y otro transporte público, para poder estar rodeadas y rodeados de testigos potenciales).
h) Donde sea relevante, entregar información adecuada a autoridades civiles, militares y de la comunidad, y también a quienes sean responsables de la misión (para que asuman su responsabilidad en temas de seguridad de la misión y no digan que "no lo sabíamos").
i) Presentar una explicación bien preparada sobre los objetivos y el mandato de la organización, intentando que ésta pueda serle aceptable a grupos armados y fuerzas de seguridad (es mejor no adaptarla a un grupo armado con el que nos topemos, pues podría ser difícil identificar quiénes son y podríamos cometer un error).
j) Valorar cuál es la mejor hora para salir de viaje. No viajar de noche.
k) Nunca ir mostrando abiertamente objetos de valor (cámaras de foto o vídeo).
l) Comportarse adecuadamente en el viaje.
m) Conviene que la organización consiga algún tipo de permiso para su trabajo en la zona visita (incluido, allí donde sea posible, noticia de que nuestro trabajo será tolerado por los grupos armados)
n) Se debe llevar siempre el móvil encima, cargado y con saldo para llamar y también dinero en efectivo. Necesario también saber de memoria un número de teléfono del equipo encima y esa persona del equipo será la encargada de gestionar si hay problemas con el viaje.

Si se produce una detención o retención: i) Si se conoce la situación: se debe activar seguir el Formulario de Emergencias cumplimentado y poner en contacto con los primeros contactos identificados, normalmente el/la responsable de área y programa. ii) si se desconoce la situación, ponerse en contacto con autoridades locales y/o españolas siguiendo el "Formulario de Emergencias" (ANEXO 10) que se haya elaborado en casos de emergencias.

Protocolo 18. Acoso psicológico, sexual, por razón de sexo u orientación sexual y otras discriminaciones en el trabajo.

Conscientes de la violencia machistas y las relaciones de poder de la sociedad patriarcal en la que vivimos, la organización adopta un **"Protocolo de acoso en NOVACT" (ANEXO 12).** Este protocolo, que reúne en un solo documento las actuaciones para prevenir, detectar y solucionar las situaciones de acoso psicológico, sexual, por razón de sexo u orientación sexual y otras discriminaciones que se puedan producir en la organización, también representa un compromiso para la erradicación total de estas conductas y para garantizar la salud de las personas que han padecido estas situaciones. Este es un protocolo que aclara actuaciones y responsabilidades de los que han de intervenir en la resolución de estas situaciones y que asegura la pluralidad de intervenciones para garantizar un tratamiento técnico adecuado en la valoración de cada una de les actuaciones, respetando la metodología más apropiada en cada caso de acuerdo con los principios generales de este protocolo.

Los casos de acoso sexual deben tramitarse a través de la Grupo de Género (**gender@NOVACT.org**) que trabajaran de forma justa, profesional y responsable para proteger a la presunta víctima.

A parte de este protocolo es clave que la organización vaya transitando hacia una cultura libre de violencia machista a través del cuestionamiento de los papeles y actitudes del sistema de sexo-género, trabajar las presuposiciones erróneas y cambiar las actividades sexistas, así como desarrollar políticas de discriminación positiva para facilitar que se den estos cambios.

Éste tránsito también se realizará a nivel externo a través de nuestra relación con otras organizaciones socias. El equipo de género producirá un **acuerdos de mínimos entre las dos organizaciones para prevenir y actuar antes casos de acoso y la erradicación del machismo (ANEXO 13)**. Ese documento deberá ser subscrito antes de iniciar un proyecto conjunto. En el caso de incumplimiento, se informará al equipo de género que posteriormente informará a codirección para determinar la respuesta organizativa.

Protocolo 19. Gestión de crisis

En situaciones en las que se consuma una amenaza, se debe activar un protocolo de gestión de la crisis. Este protocolo esta directamente relacionado con el "Formulario de emergencias" que habremos redactado previamente entre el equipo operativo de un área, su responsable de área y la validación del responsable de programa. La gestión de la crisis significa reaccionar de forma inmediata, rápida o gradual.

18.1. Red de emergencia. La persona que ha sido víctima de la amenaza debe ponerse en contacto directo con las persona/s descritas en la red de emergencia. Normalmente el responsable de área y programa. La codirección debe estar informada de esta crisis e implicarse si es necesario. Sin embargo, mantener un único interlocutor facilita la comunicación y mantener la calma con la víctima.

18.2. Comunicación con los familiares. La "Ficha de emergencias" (ANEXO 10) debe incluir al menos el contacto de un familiar. Durante la comunicación del interlocutor/a con la víctima se decidirá quien se pone en contacto con el familiar. Normalmente, será recomendable que la propia víctima se ponga en contacto, pero si no fuera posible lo realizará un contacto de la red de emergencia.

18.3. Comunicación con las autoridades. Locales y españolas (Embajada, Consulado, AECID) para obtener más información y movilizar la acción diplomática. Después de hablar con el/la miembro afectado/a decidiremos si la comunicación con las autoridades es necesario. En el caso de no poder comunicarnos con el/la miembro del equipo deberemos inmediatamente comunicarnos con las autoridades.

18.4. Difusión pública. En el caso que se decida hacer público una amenaza (agresión, denegación de entrada, detención, etc) se elegirá a un portavoz. Es clave tener preparada una narrativa que explique nuestros objetivos y trabajamos que realizamos para desmontar la versión de la otra parte. Los medios utilizados para la difusión deben ser elegidos también de forma estratégica.

18.5. Acción política. La consumación de una crisis puede tener un coste político para el agresor/a. El/a responsable de área, programa y codirección decidirán si activan una campaña o acción política movilizando a los actores políticos estratégicos y consiguiendo su apoyo, condena de la amenaza o otras consecuencias políticas. Siempre tener en cuenta que consecuencias podría tener la difusión pública y la acción política para el resto del equipo destinado en un contexto operacional o país específico. Evaluar también los costes políticos organizativos será necesario.

18.6. Defensa legal. La "Ficha de emergencia" también incluirá información de abogados/as locales del país donde se produce la crisis. Después de valorar la situación con el/la miembro del equipo operativo afectado, obtener toda la información y comunicarse con las autoridades políticas. El responsable de área, programa y codirección podrían activar al acción legal para defender a la víctima. Para ello será necesario crear una caja de resistencia que nos permita cubrir los gastos de este tipo de acciones.

18.7. Emergencias médicas y psicológicas. Todo el equipo operativo dispone de una póliza de seguros o de un seguro especial para un país específico: **Asistencia Sanitaria (ANEXO 9)**. Esta mutua aportará la asistencia sanitaria necesaria en caso de emergencia médica. En cualquier caso, los costes de una emergencia médica durante el desarrollo de nuestro trabajo nunca será cubierto por el trabajador, incluyendo las situaciones de crisis. Por otra parte, si es necesario apoyo psicológico, el/la responsable de área y programa decidirán, después de haber consultado al miembro del equipo operativo que ha sufrido la amenaza, si es necesario apoyo psicológico desde la mutua sanitaria o bien a través de las sesiones de cura emocional de la organización.

18.8 Daños materiales. En el caso que se produzca daños materiales será necesario hacer un inventario de los mismos y hacer una valoración económica de los mismos para enviarlos a la póliza de seguros. Para ello es necesario que previamente tengamos un inventario de los equipos y materiales en nuestras oficinas, incluyendo casas de expatriados/as, con fotografías y facturas. De esta manera, podríamos recuperar parte de los gastos que se produzca.

Protocolo 19. Evacuación

En el caso de que el nivel de riesgo sea muy elevado y este relacionado con amenazas graves (detenciones, agresiones, etc). La codirección, responsable de programa y el equipo operativo en el país de destino tomarán la decisión de la evacuación del equipo en el país y sus pertenencias. Esta decisión deberá ser validada por el Consell de Govern de la organización.

Para el proceso de evacuación se realizará según consignas del las Autoridades españolas (Embajada, Consulado) e internacionales (OCHA, ONU) en el país de destino. A partir de ahí, se esperan consignas del Responsable de Área y Programa para desplazarse al aeropuerto. Cada destino debe incluir en sus planes de emergencia el proceso la forma de evacuación (terrestre, aérea, etc).

Protocolo 20. Planificación y Evaluación del Manual de Seguridad

El documento que hemos presentado es una herramienta dinámica que debe ser revisada de forma periódica. En términos de planificación para la preparación de los documentos:

1. Evaluación de riesgos y vulnerabilidades (anualmente en el caso de riesgos/vulnerabilidades comunes, y cada 6 meses en caso de riesgos/vulnerabilidades de contextos operaciones y país).
2. Elaboración del plan de emergencias (Elaboración anual con una revisión cada 6 meses en el caso de cada área).
3. Cumplimentación del listado de registro de incidentes (de forma constante)
4. Elaboración de fichas específicas como la de emergencia (cuando haya riesgo de emergencia)
5. Formaciones periódicas (seguridad digital, etc)
6. Curas emocionales (mensualmente)
7. Evaluación del Manual de Emergencia (anualmente).