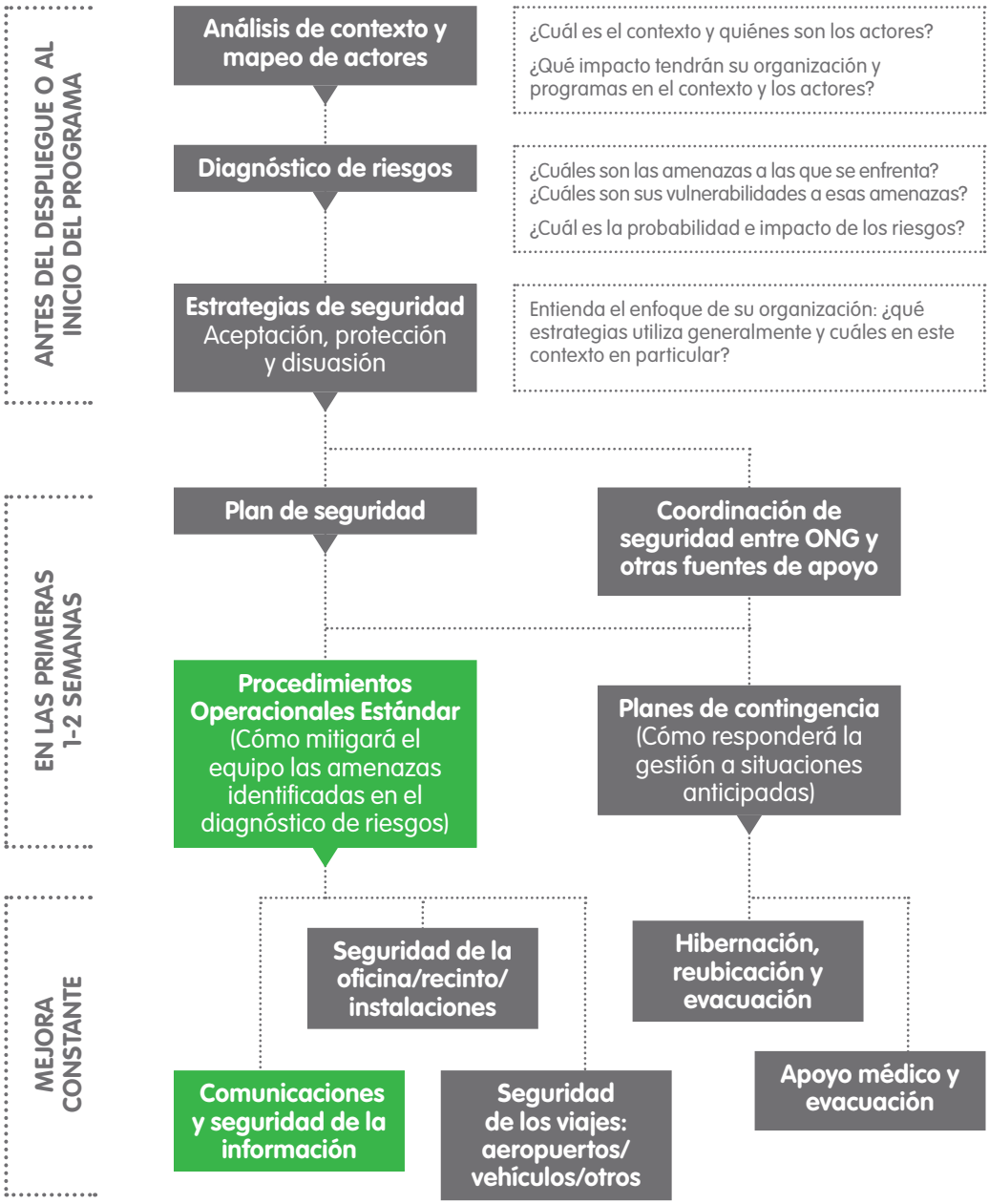
8 Comunicaciones y seguridad de la información



Al establecer un nuevo despliegue, proyecto o misión, hay que tomar el tiempo para analizar los tipos de comunicaciones que se tendrá a disposición (teléfono fijo, redes de telefonía móvil, teléfonos satelitales, Internet, correo postal, mensajería, etc.) y qué tan confiables se espera que sean. En el mundo moderno, las comunicaciones son una necesidad clave para la "supervivencia", tanto como los alimentos, el agua y el albergue.

Presupuestar fondos con suficiente antelación para contar con sistemas de comunicaciones fiables -incluyendo sistemas de respaldo y alternativos para reemplazar el equipamiento dañado, perdido o robado- es un componente clave tanto de la seguridad del personal como del éxito del programa. Además, es posible que hagan falta licencias para utilizar algunos métodos de comunicación, tales como las radios o los sistemas satelitales. Las Naciones Unidas tal vez puedan ayudar a obtener dichas licencias. La organización debe incluir en el presupuesto el tiempo de uso o la adquisición de las licencias cuando sea necesario.

Sea consciente de las nuevas tecnologías que pueden mejorar sus comunicaciones eficientemente como las tarifas satelitales para teléfonos inteligentes o sistemas de mensajería por satélite frente a teléfonos de voz tradicionales.

Compre lo mejor que se puede permitir finacieramente.

No obstante, las organizaciones tienen que considerar la imagen que da su equipamiento de comunicaciones. Si tener un perfil bajo es parte de la estrategia de seguridad, colocar radios y antenas de alta frecuencia a los vehículos, los hará resaltar tanto como si llevaran un logo.

En las regiones donde hay conflicto o disturbios civiles o donde acaba de ocurrir un desastre natural, nunca asuma que el Internet y las redes móviles funcionarán adecuadamente. Cuando hay emergencias de seguridad o desastres naturales, los gobiernos suelen tomar control de las redes (o incluso cerrarlas), cuando más las necesita. Es importante no depender de un solo sistema, ya sean líneas terrestres, redes de telefonía móvil, teléfonos satelitales, Internet u otros.

Sea creativo. En situaciones de emergencia, las ONG han utilizado repetidores de taxistas para mantener las comunicaciones con el personal cuando los teléfonos o el Internet no han estado operativos, o empleado camellos para llevar mensajes y mantener el contacto con comunidades alejadas.

Procedimientos y seguridad de las comunicaciones

Establecer y mantener una red de comunicaciones amplia es clave para la seguridad y el éxito de las operaciones. Si su organización tiene redes de radio o teléfonos satelitales, enseñe al personal a utilizarlos en el proceso de orientación inicial e indíque dónde pueden usar el equipo de comunicaciones instalado (por ejemplo, ¿hay que estar en el exterior? ¿hay puntos donde el equipamiento no funciona?). Asegúrese de que el personal pueda comunicarse con su familia y amigos durante los despliegues y especialmente en emergencias.

Cada vez son más las organizaciones y los organismos de coordinación que utilizan WhatsApp y otras aplicaciones sociales similares para intercambiar información directamente entre el personal. Esto puede ser muy ventajoso a la hora de compartir información en tiempo real, aunque la información que se transfiere en estas redes no está verificada. Debe haber directrices claras sobre qué información se puede y no se puede compartir y sobre los procedimientos que indiquen cómo actuar al recibir información.

Por lo general, todos los procedimientos y las directrices de comunicación deben ser discutidos con el personal. Los procedimientos escritos, así como la información esencial de contacto en casos de emergencia, incluyendo los números de teléfono, frecuencias y señales de llamada, deben estar publicados en la oficina, en cada vehículo y en una tarjeta que cada empleado lleve consigo.

Es importante comprobar los sistemas regularmente y tener una fuente de energía de respaldo para la radio y para cargar los teléfonos móviles/satelitales.

Buenas prácticas:

- El personal nunca transmite información sensible, por ejemplo, sobre transferencias de efectivo o itinerarios de viaje, en lenguaje claro por radio o redes telefónicas.
- El equipamiento de comunicaciones, que incluye radios, teléfonos móviles y teléfonos satelitales, está aprobado por el gobierno del país anfitrión y tiene las licencias correspondientes previas a su uso.
- Cuando se utilizan las radios, se han obtenido múltiples frecuencias VHF y HF para cada oficina (cuando sea posible).
- Se ha coordinado el uso de redes de radio de otras organizaciones -como las de las Naciones Unidas.
- Se hacen controles periódicos por mensaje de texto, llamadas por teléfono satelital o radio con las oficinas alejadas y el personal en viaje por la zona, según sea necesario. Hay una política vigente en caso de que un miembro del personal o un equipo no pueda responder y no pueda ser contactado. Todo el personal está familiarizado con esta política y se implementa sistemáticamente.
- Se han establecido palabras o frases en código para casos de emergencia comunes como secuestros o intrusiones. Su uso se ha discutido con el personal.
- Las radios y los teléfonos de emergencia se monitorean 24 horas al día, según corresponda.

Seguridad de la información

Independientemente de cómo nos percibamos a nosotros mismos, a menudo, las organizaciones de ayuda internacional ya no son percibidos por actores externos como agencias neutrales o independientes. Estas organizaciones intervienen, obligan a otros rendir cuentas, hacen incidencia política y a veces asumen actividades asociadas normalmente con los gobiernos (como la atención médica, el agua, el saneamiento y el socorro de emergencia) y en muchas ocasiones realizan estas actividades con financiación de gobiernos "occidentales" que tienen sus propias agendas políticas. Esto hace que todo lo que hacen las ONG humanitarias parezca sospechoso a los ojos de mucha gente.

▶ *Consulte el documento informativo del EISF "The future of humanitarian security in fragile contexts: an analysis of transformational factors affecting humanitarian action in the coming decade".*

Por lo general, los gobiernos tienen los medios para monitorear las llamadas telefónicas, la actividad en Internet, las cuentas de Facebook y Twitter y el contenido RSS de las organizaciones, así como de hackear el disco duro de sus computadoras. Las organizaciones criminales también percibirán a las ONG como adineradas, a causa de los vehículos, las computadoras portátiles y los teléfonos satelitales que suelen utilizar, además de los niveles de financiación de los donantes que se anuncian públicamente. Todo esto hace que las organizaciones de ayuda sean vulnerables a los riesgos en materia de seguridad de la información. Sea consciente de que los delincuentes o agentes gubernamentales pueden leer cualquier cosa que usted escriba en un correo electrónico.

▶ *Consulte el documento informativo del EISF "Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management".*

Tenga cuidado con lo que guarda en los discos compartidos. El personal de respuesta de emergencia suele traer sus propias computadoras y copiar todo en un disco compartido cuando se va, para la continuidad. Esto puede incluir fotos inadecuadas, información personal y análisis de contexto que otros actores o miembros del personal pueden considerar ofensivos. Es importante tener presente también qué información -tanto profesional como personal- se guarda en dispositivos móviles tales como teléfonos inteligentes, ya que se puede perder o sustraer con facilidad.

Evalúe el impacto que la información pueda tener si cae en las manos equivocadas -acoso del personal, diseminación de fotos inapropiadas, acceso a correos electrónicos o a la red privada virtual/servidor de la oficina, y así sucesivamente.

Buenas prácticas:

- Periódicamente haga una copia de seguridad de todos los archivos y guarde las copias de seguridad de todos los documentos y registros clave (acuerdos con el gobierno, documentos legales, estados bancarios, registros de recursos humanos) en otro lugar por si ocurre un incendio, una inundación, un robo u otro hecho que destruya los originales.
- Los documentos en papel pueden dar lugar a que se filtre información cuando se dejan en papeleras o se dejan sobre un escritorio, al alcance del personal de limpieza o de otros empleados o visitantes, que pueden verlos/copiarlos/llevárselos. Utilice una trituradora de papel para deshacerse de los archivos que no se guarden en un lugar seguro.
- Mantenga un buen sistema de firewall (sistema de protección) en todos los servidores y reduzca al mínimo el acceso del personal a las redes con

computadoras, tabletas o teléfonos ajenos a la organización para prevenir la propagación de virus.

- Recuerde que Skype no es más seguro al hackeo que cualquier otro método de comunicación.
- Nunca dé la impresión de estar recopilando "inteligencia" ni de estar pasando información militar o de seguridad a gobiernos extranjeros (ni a sus donantes, ni siquiera a la sede de su organización). Asimismo, el hecho de encriptar información puede mandar un mensaje equivocado. Particularmente si su ONG dice ser abierta y rendir cuentas, es posible que le cuestionen por qué es necesario encriptar la documentación.
- De ser posible, no utilice computadoras de escritorio. Aunque las computadoras portátiles son más fáciles de robar, también son más sencillas de trasladar si hay que llevar la oficina o el proyecto a otro lugar.
- Considere la posibilidad de emplear procesos de verificación de la información recibida por WhatsApp y otras aplicaciones sociales que simplifican la transferencia de información directamente entre el personal. También debe haber orientaciones claras sobre lo que se debe y lo que no se debe compartir.
- Asegúrese de contar con una política sobre las redes sociales que deje claro al personal lo que puede y no puede publicar en las redes sociales.

▶ *Consulte la guía del EISF titulada "Managing the Message: Communication and Media Management in a Crisis".*

Para las herramientas técnicas y las directrices, *"Front Line Defenders"* y *"Tactical Technology Collective"* han diseñado una guía sobre la seguridad digital para activistas y defensores de los derechos humanos titulada *"Security in-a-Box"* (Caja de herramientas para la seguridad). La guía cubre los principios básicos, incluyendo consejos sobre cómo utilizar las plataformas de redes sociales y los teléfonos móviles de manera más segura, además de ofrecer instrucciones paso a paso para instalar y utilizar los servicios y programas de seguridad digital más esenciales.

Contenido

Introducción 02

Módulos 04

Planificación y preparación

Módulo 1 04
Proceso de planificación de la gestión de riesgos de seguridad

Módulo 2 09
Mapeo de actores y análisis de contexto

Módulo 3 14
Herramienta de diagnóstico de riesgos

Módulo 4 22
Estrategias de seguridad: aceptación, protección y disuasión

Módulo 5 26
Coordinación de seguridad entre ONG y otras fuentes de apoyo

Módulo 6 30
Plan de seguridad

Módulo 7 34
Seguridad de las instalaciones

Módulo 8 42
Comunicaciones y seguridad de la información

Módulo 9 48
Seguridad de los viajes: aeropuertos, vehículos y otros medios de transporte

Respuesta

Módulo 10 55
Hibernación, reubicación y evacuación

Módulo 11 61
Apoyo médico y evacuación

Servicios de apoyo

Módulo 12 67
Gestión de personal

Glosario 85

Otras publicaciones de EISF 86

El Foro Europeo Interinstitucional para la Seguridad (EISF)

EISF es una plataforma independiente de referentes de seguridad que actualmente representan 90 ONG humanitarias con base en Europa que operan a nivel internacional. El EISF está comprometido a mejorar la seguridad de las operaciones y del personal humanitario. Tiene como objetivo incrementar el acceso seguro por parte de organizaciones humanitarias a personas afectadas por emergencias. Es clave para su trabajo el desarrollo de investigaciones y herramientas que promueven la concientización, la preparación y las buenas prácticas.

EISF se creó para establecer un rol más destacado de la gestión de riesgos de seguridad en operaciones humanitarias internacionales. Facilita el intercambio entre las organizaciones miembro y otros organismos como la ONU, los donantes institucionales, las instituciones académicas y de investigación, el sector privado y un amplio rango de ONG internacionales. La visión de EISF es convertirse en un punto de referencia global para una práctica aplicada y un conocimiento colectivo, siendo esencial para su trabajo el desarrollo de una investigación práctica para la gestión de riesgos de seguridad en el sector humanitario.

EISF es una entidad independiente actualmente financiada por la Oficina Estadounidense de Asistencia para Desastres (US Office of Foreign Disaster Assistance, OFDA), la Agencia Suiza para el Desarrollo y la Cooperación (COSUDE) (Swiss Agency for Development and Cooperation, SDC), el Departamento para el Desarrollo Internacional del Reino Unido (Department for International Development, DFID) y las contribuciones de los miembros de EISF.

www.eisf.eu

Agradecimientos

La primera edición de esta guía, publicada en el 2015, fue desarrollada en conjunto por James Davis (Act Alliance) y Lisa Reilly, Directora Ejecutiva de EISF. La Gerente de Proyecto fue Raquel Vázquez Llorente, Investigadora en el EISF.

El Módulo 12 – Gestión de personal fue desarrollado por Christine Williamson. La Gerente de Proyecto fue Adelicia Fairbanks, Investigadora en el EISF.

EISF y los autores desean expresar su agradecimiento a los siguientes individuos por compartir su experiencia con nosotros: Marko Szilveszter Macskovich (Oficina de la ONU para la Coordinación de Asuntos Humanitarios), Michelle Betz (Betz Media Consulting), Veronica Kenny-Macpherson (Cosantóir Group), Jean Michel Emeryk, Peter Wood, Shaun Bickley, William Carter, Rebekka Meissner y Christine Newton.

Traducción y editación por: Translators without Borders, Megan Caine y Susana Carrera (monkeyproof.co.uk), y Yelena Torres López.

Agradecemos especialmente a Gonzalo de Palacios (Humanitarian Access), quien nos apoyó con la revisión de esta edición en español.

Sugerencia para citas

Davis, J. et al. (2017) *Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria*. European Interagency Security Forum (EISF).

Aviso Legal

EISF es una agrupación dirigida por sus miembros y no posee una identidad legal independiente bajo la Ley de Inglaterra y Gales o cualquier otra jurisdicción. Las referenceias a "EISF" en este aviso legal incluirán a las organizaciones miembros, observadores y secretaría de EISF.

El contenido de este documento no pretende constituir un asesoramiento en el que debe confiar. Debe obtener asesoramiento profesional o especializado antes de tomar, o abstenerse de, cualquier acción tomada en base al contenido de este documento.

Aunque EISF trata de asegurar la veracidad de la información de este documento, no garantiza su exactitud ni su exhaustividad. La información de este documento es proporcionada 'tal cual' sin condiciones, garantías u otros términos, y la confianza depositada en la información contenida en el presente documento será responsabilidad total del lector. Por consiguiente, y hasta donde permita la ley, EISF excluye todas las representaciones, garantías, condiciones y otros términos que de no ser por este aviso legal podrían tener efecto en relación con la información del presente documento. EISF no será responsable de ninun tipo de perdida o daño de cualquier tipo causado al lector o a una tercera parte derivado de la confianza depositada en la información de este documento.

© 2017 European Interagency Security Forum

Diseño e ilustraciones: www.wave.coop