herramienta 46 Gestión de la información

Ficha

Con el fin de proteger la seguridad y la privacidad de las víctimas y de mitigar los riesgos para la información de la organización, los casos de violaciones graves deben ser gestionados con estricto apego a las normas de confidencialidad. Esto implica adoptar precauciones especiales al recolectar, almacenar y compartir dicha información.

Seguridad y confidencialidad al recabar información
Evalúe su vulnerabilidad a situaciones que puedan poner en peligro su seguridad y la de su fuente y/o la confidencialidad de la información. Seleccione medidas de mitigación pertinentes, según el nivel de riesgo:

Riesgo	Nivel (alto/ medio/bajo)	Sugerencias
La información podría ser escuchada involuntariamente o transmitida a personas que no tienen *necesidad* de conocerla		☐ Elija un lugar adecuado si tiene previsto realizar entrevistas. ☐ No hable del caso con personas que no tengan necesidad de conocerlo ni tampoco cerca de ellas (por ejemplo, conductores de taxi o choferes de la oficina, personal de limpieza o de apoyo, colegas de otros proyectos u organizaciones, amigos personales, familiares, vecinos, etc.). ☐ Evite comunicar información confidencial por teléfono cuando haya riesgo de que su teléfono pueda estar interceptado, y tenga suma cautela cuando deba comunicarse por esta vía (por ejemplo, usando palabras en código). ☐ No deje información del caso a la vista ni en espacios compartidos. ☐ No envíe información del caso a través de otras personas, a menos que esté específicamente autorizado a hacerlo.
La información se puede perder		☐ Mantenga siempre la información del caso con usted hasta que pueda almacenarla. ☐ Guarde copias de la información del caso en un lugar seguro. ☐ Utilice códigos para la víctima, el monitor, la ubicación, la agresión y el agresor.
La información puede ser confiscada (detención, retén en carretera, punto de control)		☐ Utilice códigos para el caso, la víctima, la ubicación, el punto de enlace y el agresor. ☐ Si existe un riesgo inminente o probable de que la información pueda ser confiscada, no lleve con usted ningún tipo de formularios de recolección de datos. ☐ Anote únicamente información parcial o limítese a intercambios orales, y luego complete totalmente el informe tan pronto como sea posible en un lugar seguro. ☐ Asegúrese de saber qué decir y qué hacer en una situación en la cual existe el riesgo de que se confisque información delicada (allanamiento, detención, retén en carretera, punto de control).
Puede trascender que la fuente proporcionó información a su organización, y esto expone a la fuente y a usted a la posibilidad de acoso, represalias o estigmatización		☐ Elija una ubicación apropiada para realizar las entrevistas y confirme si la fuente se siente segura allí. ☐ Asegúrese de que la víctima o el padre/tutor preste su consentimiento informado antes de una entrevista y sepa de qué modo se va a gestionar la información. ☐ Mantenga un perfil bajo durante la realización de entrevistas. ☐ Mantenga una estrecha coordinación con la ONU para garantizar que las misiones de verificación no despierten atención en torno a la fuente. ☐ Identifique a las organizaciones asociadas o entidades que estén en condiciones de proporcionar protección física a una víctima/testigo en riesgo (p. ej., reubicación) y discuta esta opción con la víctima/el testigo.
Otros:		

Seguridad y confidencialidad al conservar información

Evalúe sus vulnerabilidades: ¿Qué tan altos son los siguientes riesgos para su oficina/organización? Seleccione las medidas de mitigación pertinentes de acuerdo con el nivel de riesgo:

Riesgo	Nivel (alto/ medio/bajo)	Sugerencias
Daños a las instalaciones (y documentos) debido a fenómenos/ desastres naturales		☐ Conserve copias de los archivos electrónicos y en papel en lugares diferentes. ☐ Reduzca la cantidad de información que almacena en ese lugar, por ejemplo archivando ficheros antiguos en otro lugar (otra oficina o en el extranjero) cada un cierto número de años. ☐ Considere la posibilidad de almacenar toda la información en otro lugar. ☐ Asegúrese de confeccionar una lista con todos los pasos relevantes para un plan de contingencia.
Allanamientos/ requisas		☐ Reduzca la cantidad de información que conserva en un solo lugar. Por ejemplo, traslade los archivos viejos a otro lugar (otra oficina o al extranjero) cada dos años. ☐ Guarde copias de los archivos electrónicos y en papel en un lugar diferente. ☐ Considere la posibilidad de almacenar toda la información en otro lugar. ☐ Conserve copias impresas en un lugar poco llamativo pero seguro, si considera que un armario cerrado con llave llamaría demasiado la atención durante un allanamiento/requisa. ☐ Asegúrese de confeccionar una lista con todos los pasos relevantes para un plan de contingencia.
Robo		☐ Conserve copias impresas en un armario cerrado con llave o en un lugar menos llamativo, si considera que un armario cerrado con llave llamaría demasiado la atención durante un robo. ☐ No guarde archivos en artículos de valor (computadores portátiles), o asegúrese de llevarse estos artículos cuando se retira de la oficina o el edificio al momento del cierre. ☐ Guarde los archivos electrónicos en un dispositivo móvil que pueda retirar de las instalaciones. ☐ Como último recurso, destruya todos los archivos (borrar, triturar o incinerar). ☐ Evalúe la seguridad de la oficina, y refuércela si es necesario. ☐ Conserve copias de los archivos electrónicos y en papel en distintos lugares.
Cierre repentino de las instalaciones debido a un ataque inminente		☐ Considere guardar toda la información en otro lugar. ☐ Guarde los archivos electrónicos en un dispositivo móvil que pueda llevarse fácilmente de las instalaciones. ☐ Llévese los archivos de las instalaciones, antes del cierre. ☐ Como último recurso, destruya todos los archivos (borrar, triturar o incinerar). ☐ Guarde copias de los archivos electrónicos y en papel en un lugar distinto. ☐ Asegúrese de de confeccionar una lista con todos los pasos relevantes para un plan de contingencia.
Vigilancia electrónica		☐ Proteja los archivos electrónicos con contraseñas o cifrado. ☐ Cambie las contraseñas periódicamente. ☐ Restrinja el número de personas que pueden acceder de manera directa a la información. ☐ Asegúrese de que su equipo tenga un *firewall* activo.
Otros:		

Seguridad y confidencialidad en el intercambio de información con puntos de enlace del MRM

☐ Aclare el formato y modo de comunicación: Evite el envío electrónico de información confidencial o tome precauciones si tiene que hacerlo (los *firewalls* no protegen los documentos enviados electrónicamente). Proteja con contraseña todos los documentos y/o utilice una plataforma segura de intercambio de archivos.

HERRAMIENTA 46

(cont.)

- ☐ Aclare qué información se puede compartir con el punto de enlace del MRM y si se utilizarán códigos o palabras de código.
- ☐ Aclare quiénes en su organización está autorizados a proporcionar información al punto de enlace del MRM.
- ☐ Aclare quién en la ONU es el punto de enlace del MRM que recibirá su información.
- ☐ Entable una relación basada en la confianza con su punto de enlace del MRM.
- ☐ Aclare de qué manera la ONU gestionará la información proporcionada por su organización (dónde va a ser almacenada y cómo será comunicada dentro del MRM).
- ☐ Considere adoptar un protocolo formal para el intercambio de información con la ONU que detalle todos los puntos mencionados.

Documentos y políticas institucionales que podrían tener que formular o adaptar según cómo sea su participación en el MRM

Documentos	Puntos clave
Código de conducta del personal (política/protocolo de aplicación)	• Comportamiento al recopilar información delicada. • Comportamiento al debatir sobre información delicada. • Acatamiento de protocolos y planes internos.
Protocolo interno de protección de datos (Ver recursos útiles del Sistema de Gestión de la Información sobre Protección Infantil más adelante)	• ¿Quiénes recogen la información? • ¿Cómo se transfiere la información desde el terreno a la oficina principal? • ¿Quiénes más pueden tener acceso a información dentro de la organización? • ¿Quiénes analizan la información? • ¿Quiénes comunican información a actores externos? • ¿Qué códigos y palabras clave se utilizan? • ¿Dónde se guarda y almacena la información (papel, formato electrónico)? • ¿Quiénes tienen acceso a las contraseñas y llaves? • Plan de contingencia para emergencias: ¿Cuáles son los pasos? ¿Quiénes son responsable?
Incluir a la gestión de la información en el plan de seguridad de la organización	• Incluir medidas preventivas para almacenar información delicada de forma segura. • Incluir un plan de contingencia para retirar o eliminar información delicada en caso de emergencia.
Formulario con información / consentimiento de clientes	• Dar opciones para el consentimiento acerca de cómo se puede utilizar la información y quiénes pueden acceder a ella.

herramientas relacionadas

- herramienta 45 – Modelo comentado de base de datos sobre casos
- herramienta 44 – Preguntas frecuentes "Usar una base de datos sobre casos"
- herramienta 29 – Lista de verificación "Confidencialidad"
- herramienta 30 – Lista de verificación "Consentimiento informado"
- herramienta 47 – Ejercicio grupal "Gestión de la confidencialidad y de la información"

otros recursos

- *Child Protection Information Management System, Training Manual* (Template data protection protocol and data protection checklist), disponible en **http://cpwg.net/resources/inter-agency-child-protection-information-management-system-training-manual-zip-13mb/.**
- *Minimum Standards for Child Protection in Humanitarian Action,* Global Child Protection Working Group, 2012 – Standard 5 "Information Management".
- *Security in a Box: Tools and Tactics for Your Digital Security,* Tactical Technology Collective and Front Line Defenders.
- *Workbook on Security: Practical Steps for Human Rights. Defenders at Risk*, Front Line Defenders, 2011.