ACADEMIA HUMANITARIA · HUMANITAIRES JOBS

Mini MBA Seguridad y gestión de riesgos: proteger a los equipos y mantener el acceso

Material del curso · Semana 9 : Seguridad digital y protección de la información

Programa de exactamente 3 meses (12 semanas, 144 horas) para gestionar la seguridad y los riesgos de una organización humanitaria: deber de cuidado, análisis del contexto, evaluación de riesgos, planes y procedimientos, aceptación y negociación del acceso, incidentes, gestión de crisis y secuestro, salud y bienestar del personal, seguridad digital y protección de datos, riesgos de la organización y cumplimiento, reparto del riesgo con los socios, gobernanza y continuidad de las actividades. Ejercicios numéricos corregidos, tres exámenes mensuales con estudios de caso y un diploma verificable de la Academia Humanitaria.

https://humanitairejobs.org/es/academia/mini-mba-securite-risques/semaine-9/

Documento gratuito de la Academia Humanitaria. Puede imprimirse y compartirse libremente con fines de formación, sin modificaciones.

Semana 9 : Seguridad digital y protección de la información

Objetivos

- Identificar las amenazas digitales propias de las organizaciones humanitarias: phishing, fraude en transferencias, vigilancia, fuga de datos.
- Establecer medidas básicas proporcionadas: autenticación, copias de seguridad, cifrado, gestión de accesos, dispositivos.
- Proteger los datos de las personas asistidas y del personal, y reaccionar ante un incidente digital.

Por qué lo digital es un riesgo de seguridad

Las organizaciones humanitarias poseen información muy sensible: listas de beneficiarios (a veces con biometría y localización), testimonios de violaciones, datos médicos, información sobre el personal, análisis de seguridad, movimientos. Una fuga o un ataque informático puede poner en peligro **vidas**, no solo datos.

Varios ciberataques conocidos han tenido como objetivo a organizaciones humanitarias, incluido el robo de datos de cientos de miles de personas vulnerables. Las organizaciones también son blanco del fraude financiero en línea y de la **vigilancia** de las comunicaciones por parte de actores estatales o no estatales.

Principales amenazas:

- **Suplantación de identidad** (phishing): correos o mensajes falsos que roban credenciales o instalan programas maliciosos.
- **Fraude en transferencias**: falso proveedor, falso director que solicita un pago urgente, cambio fraudulento de datos bancarios.
- **Ransomware**: cifrado de los datos a cambio de un rescate.
- **Robo o incautación de dispositivos** (ordenadores, teléfonos) en los puestos de control o durante asaltos.
- **Vigilancia** de las comunicaciones y de las redes sociales.
- **Errores internos**: compartir por error, archivo enviado al destinatario equivocado, contraseña a la vista.

Las medidas básicas

Unas pocas medidas sencillas bloquean la gran mayoría de los ataques comunes:

- **Autenticación multifactor** (MFA) en el correo electrónico, el almacenamiento en línea, el banco y el programa de contabilidad.
- **Gestor de contraseñas** y contraseñas largas y únicas.
- **Actualizaciones** automáticas de los sistemas y las aplicaciones.

- **Copias de seguridad** periódicas, una de ellas sin conexión o aislada, y pruebas de restauración (regla 3-2-1: tres copias, dos soportes diferentes, una copia fuera de las instalaciones).
- **Cifrado** de los discos de los ordenadores portátiles y de los teléfonos.
- **Gestión de accesos**: cada persona solo accede a lo que necesita; retirada de los accesos el día de la salida de un empleado.
- **Formación** periódica, con ejercicios de phishing simulados.

Ejemplo de ejercicio. Se envía un correo de phishing falso a 120 empleados: 38 hacen clic en el enlace (31,7 %), 14 introducen sus credenciales (11,7 %), 9 notifican el correo al servicio informático (7,5 %). Tras una formación específica, un segundo ejercicio da 12 clics (10 %), 3 introducciones de credenciales (2,5 %) y 41 notificaciones (34,2 %). El aumento de las notificaciones es tan importante como el descenso de los clics: convierte al personal en un sistema de alerta.

Fraude en transferencias y procedimientos financieros

El **fraude del CEO** y el fraude de datos bancarios cuestan cada año sumas importantes a las organizaciones, incluidas las humanitarias. Los procedimientos financieros son la mejor defensa:

- Toda **modificación de los datos bancarios** de un proveedor o de un empleado se verifica mediante una llamada a un número ya conocido, nunca al indicado en la solicitud.
- Ningún pago urgente fuera de procedimiento, ni siquiera a petición aparente de un director: la doble validación sigue siendo obligatoria.
- Los accesos a la banca en línea utilizan dispositivos y cuentas dedicados, con doble firma electrónica.
- El personal sabe que contará con **respaldo** si rechaza un pago sospechoso, aunque lo pida un superior.

> La urgencia y la confidencialidad son las dos palancas favoritas de los estafadores: «Estoy en una reunión, haz esta transferencia ahora mismo y no se lo digas a nadie».

Dispositivos, puestos de control y vigilancia

Sobre el terreno, los riesgos digitales también son **físicos**:

- En los puestos de control, los teléfonos pueden ser registrados. Un teléfono que contiene fotos de posiciones militares, mensajes críticos con una parte o listas de beneficiarios puede dar lugar a una detención. Norma: llevar solo lo necesario, borrar los datos sensibles de los dispositivos de terreno, utilizar dispositivos dedicados al trabajo.
- Las **redes sociales** del personal revelan información aprovechable: localización en tiempo real, opiniones políticas, fotos de colegas, signos de riqueza. Una política sobre el uso de las redes sociales, explicada y no punitiva, reduce estos riesgos.

- Las **mensajerías** cifradas de extremo a extremo protegen el contenido, pero no el hecho de que se esté comunicando, ni el propio teléfono si se incauta desbloqueado.
- El uso de ciertas herramientas (satélites, VPN, drones) puede estar prohibido o resultar sospechoso: verificar la legislación y la aceptación.

Proteger los datos de las personas

La **protección de datos** de los beneficiarios y del personal se basa en principios reconocidos (en particular, el manual del CICR y del Brussels Privacy Hub sobre la protección de datos en la acción humanitaria):

- **Licitud y finalidad**: base legítima y finalidad precisa para cada recogida.
- **Minimización**: recoger solo lo necesario.
- **Consentimiento informado** cuando esa es la base elegida, teniendo en cuenta las relaciones de poder (un hogar que necesita ayuda no es libre de negarse).
- **Seguridad**: cifrado, accesos limitados, registro de actividad.
- **Conservación limitada** y supresión al término de la finalidad.
- **Intercambio regulado** mediante acuerdos de intercambio de datos, con un análisis de riesgos (incluidas las solicitudes de autoridades o de partes en el conflicto).
- **Evaluación de impacto** antes de todo nuevo sistema (biometría, pago móvil, plataforma compartida).

Ejemplo de minimización. Para una distribución de kits, hay que identificar el hogar y verificar que no haya recibido ya el kit. La pertenencia étnica o religiosa no es necesaria y no debe recogerse; la foto y la huella dactilar generalmente tampoco lo son.

Reaccionar ante un incidente digital

Un incidente digital (cuenta pirateada, ordenador robado, ransomware, archivo enviado por error) se trata como un incidente de seguridad:

- **Contener**: cambiar las contraseñas, revocar las sesiones, aislar el dispositivo infectado, borrar a distancia un dispositivo robado.
- **Evaluar**: ¿qué datos, qué personas, qué riesgo para ellas?
- **Informar**: dirección, responsable de protección de datos, personas afectadas si están expuestas a un riesgo, autoridades de control según el derecho aplicable, donantes según los contratos.
- **Restaurar** a partir de las copias de seguridad; no pagar un rescate sin decisión de la dirección y análisis jurídico.
- **Aprender**: análisis, correcciones, formación.

Ejemplo. Un ordenador portátil sin cifrar que contiene la lista de 3 200 hogares con sus números de teléfono y su localización es robado durante un asalto. El riesgo para las personas depende del contexto: si algunos hogares pertenecen a un grupo perseguido, es elevado. Acciones: evaluación inmediata, información a las comunidades afectadas por canales seguros

si están expuestas, cambio de las modalidades de contacto, cifrado obligatorio de todos los ordenadores portátiles.

Ejercicio: un correo urgente del director

Situación. Un viernes a las 17 h, la contable recibe un correo aparentemente del director de país, que está de viaje: «Confidencial. Tenemos que pagar hoy el anticipo de 48 000 USD al nuevo proveedor de combustible o perderemos el contrato. Datos bancarios adjuntos. No estoy localizable, reunión con el ministro». La dirección de envío difiere en una letra de la dirección habitual. El mismo día, un proveedor habitual ha pedido por correo cambiar sus datos bancarios. El correo de la organización no tiene autenticación de dos factores.

Trabajo solicitado. 1) Señales de alerta. 2) Conducta inmediata. 3) Medidas duraderas.

Solución. 1) Urgencia, confidencialidad, indisponibilidad del solicitante, nuevo proveedor sin expediente de compra, dirección de envío ligeramente diferente, solicitud paralela de cambio de datos bancarios. 2) No pagar; llamar al director a su número conocido (o a su adjunto); no modificar los datos del proveedor habitual sin una llamada de verificación a un número ya conocido; informar al responsable informático y a finanzas; conservar los correos como pruebas. 3) Autenticación de dos factores en todo el correo; norma escrita: ningún pago fuera de procedimiento, doble validación, verificación telefónica de toda modificación bancaria; formación y ejercicios de phishing; filtrado de los dominios parecidos; mensaje claro de la dirección: rechazar un pago sospechoso siempre contará con respaldo.

Para recordar

- Los datos humanitarios son sensibles: una fuga puede poner vidas en peligro.
- MFA, contraseñas únicas, actualizaciones, copias de seguridad 3-2-1, cifrado, accesos mínimos, formación.
- Fraude en transferencias: verificación a través de un número conocido, doble validación, respaldo a quien se niega.
- Terreno: dispositivos con lo mínimo en los puestos de control, política sobre las redes sociales.
- Protección de datos: finalidad, minimización, seguridad, conservación limitada, evaluación de impacto.

Cuestionario

1. 150 empleados reciben un correo falso; 24 hacen clic. Tasa de clics:
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. La regla de copias de seguridad 3-2-1 significa:
   A. 3 copias, 2 soportes diferentes, 1 copia fuera de las instalaciones
   B. 3 contraseñas, 2 factores, 1 cuenta
   C. 3 días, 2 semanas, 1 mes
   D. 3 servidores, 2 países, 1 nube

3. Un proveedor pide por correo cambiar sus datos bancarios. Usted:
   A. Los cambia inmediatamente
   B. Paga en efectivo
   C. Responde al correo
   D. Lo verifica con una llamada al número ya conocido

4. Para una distribución de kits, recoger la pertenencia étnica de los hogares es:
   A. Obligatorio
   B. Recomendable
   C. Contrario al principio de minimización si no es necesario
   D. Inocuo

5. Roban un ordenador sin cifrar que contiene listas de beneficiarios. Primer paso:
   A. Comprar otro ordenador
   B. Evaluar los datos expuestos y el riesgo para las personas, y después informar
   C. No decir nada
   D. Publicar un comunicado

Respuestas del cuestionario : 1. B · 2. A · 3. D · 4. C · 5. B