OCHA centre for humdata

CENTRO PARA LOS DATOS HUMANITARIOS

SERIE DE NOTAS DE ORIENTACIÓN
RESPONSABILIDAD DE LOS DATOS EN LA ACCIÓN HUMANITARIA

GESTIÓN DE INCIDENTES CON DATOS

CONCLUSIONES FUNDAMENTALES:

- Los incidentes con datos del ámbito humanitario son sucesos que afectan a la gestión de los datos, que han causado o pueden causar perjuicio a las personas afectadas por crisis, a organizaciones y a sus operaciones, y a otras personas o grupos.
- Las rupturas físicas de infraestructuras, la revelación no autorizada de datos y el uso de datos de beneficiarios para fines no humanitarios, entre otros, son ejemplos de incidentes con datos del ámbito humanitario.
- Los incidentes con datos tienen cuatro aspectos: (I) una fuente de amenaza, (II) un suceso de amenaza, (III) una vulnerabilidad y (IV) unas consecuencias adversas.
- Hay cinco pasos para responder a los incidentes con datos: (I) comunicación, (II) clasificación, (III) tratamiento y (IV) cierre del incidente, y (V) aprendizaje.

QUÉ ES UN INCIDENTE CON DATOS EN UNA RESPUESTA HUMANITARIA

En el sector humanitario los incidentes con datos son sucesos que afectan a la gestión de los datos, que han causado o pueden causar perjuicio a poblaciones afectadas por crisis, a organizaciones humanitarias y a sus operaciones, y a otras personas o grupos. Estos sucesos pueden explotar o exacerbar vulnerabilidades existentes.[1] En algunos casos, también pueden crear vulnerabilidades nuevas que aumenten el riesgo de que se produzcan incidentes con datos en el futuro.

El personal humanitario no ha tenido una idea común de lo que constituye un incidente con datos, ni existe un estándar técnico mínimo para indicar cómo se deben evitar y gestionar este tipo de incidentes. La forma en que el sector humanitario diseña herramientas e implementa procedimientos para gestionar los incidentes con datos desempeñará una función importante en la evolución de la ética, los derechos humanos, la técnica y los estándares profesionales de las operaciones humanitarias.

> "Si los actores humanitarios digitalizan más proporción de sus datos y comunicaciones tienen que aumentar de forma inmediata sus esfuerzos en seguridad digital. Aunque algunos actores están diseñando herramientas de protección prometedoras, sería aconsejable que las organizaciones de ayuda en general escucharan algún comentario del mundo de la seguridad informática; "Hay dos tipos de organizaciones: las que han sufrido ataques informáticos y las que los sufrirán."
>
> - Rahel Dette, Do No Digital Harm: Mitigating Technology Risk in Humanitarian Contexts

[1] "Una *vulnerability* es una debilidad de un sistema de información, de los procedimientos de seguridad de un sistema, de los controles internos o una implementación que podría explotar una fuente de amenaza." **NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments**.

Las rupturas físicas de infraestructuras, la revelación no autorizada de datos y el uso de datos de beneficiarios 'anonimizados' para fines no humanitarios, entre otros, son incidentes con datos del ámbito humanitario. Los incidentes con datos también pueden ocurrir sin que la infraestructura técnica se vea comprometida en modo alguno. La recopilación, el uso y el intercambio legítimos de datos por parte del personal humanitario puede tener incluso implicaciones operativas que constituyan un incidente con datos en casos en los que haya rumores, sensibilidades culturales, dinámicas políticas y otros factores que conlleven efectos adversos vinculados a los datos.

DEFINICIONES Y MARCOS PARA COMPRENDER LOS INCIDENTES CON DATOS

Los gobiernos y el sector privado han creado definiciones y marcos para la comprensión de los incidentes con datos que sirven como referencias útiles para el sector humanitario.

- La Organización Internacional de Normalización (ISO) en la *Norma ISO 27000* define 'incidente crítico' como "un único o una serie de sucesos indeseados o imprevistos que afectan a la seguridad de la información con una importante probabilidad de comprometer operaciones empresariales y de amenazar la seguridad de la información."[2]

- El Departamento de Comercio del Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos define un acontecimiento adverso que supone una 'ciberamenaza' como "un acontecimiento o estado que tiene el potencial de causar una pérdida de activos y las consecuencias o el efecto indeseables de dicha pérdida."[3]

- Mahmood Sher-Jan, de la Asociación Internacional de Profesionales Privados (IAPP, por sus siglas en inglés), identifica tres categorías adicionales de sucesos que amplían la definición de acontecimientos adversos del NIST. Estas son, en orden de gravedad creciente: incidentes de seguridad, incidentes de privacidad y violación de datos.[4]

Ejemplos de posibles incidentes con datos del ámbito humanitario

Un incidente con datos tiene cuatro factores: una fuente de amenaza, un suceso de amenaza, una vulnerabilidad y unas consecuencias adversas.[5] A continuación se recogen dos tipos de incidentes con datos hipotéticos que podrían ocurrir en contextos humanitarios.

El primer escenario es un incidente de violación de datos típico situado en el contexto de un conflicto armado. El segundo es un ejemplo del tipo de vulnerabilidades que pueden iniciar incidentes con datos exclusivos del sector humanitario.

1. El acceso no autorizado a datos se produce **[consecuencias]** debido a la existencia de unos actores armados **[fuente]** que atacan un centro y se apoderan de discos duros con datos de beneficiarios **[suceso]**. Los discos duros no estaban encriptados **[vulnerabilidad]**.

2. La ausencia de orientaciones que limiten la recopilación de datos para una finalidad específica **[vulnerabilidad]** conlleva que el personal recopile datos sobre el estado civil de las mujeres embarazadas **[fuente]**. Después se produce una violación de datos **[suceso]** que da como resultado un aumento de las posibilidades de violencia física **[consecuencias]** hacia embarazadas solteras beneficiarias.

Estos escenarios muestran cómo pensar en identificar cadenas causales que pueden crear incidentes con datos específicos de contexto.

[2] Organización Internacional de Normalización, ISO/IEC 27000:2018.

[3] Glosario del Centro de Recursos de Seguridad Informática del NIST.

[4] IAPP, Is It an Incident or a Breach, How to Tell and Why It Matters, Mahmoud Sher-Jan (febrero de 2017).

[5] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

MODELOS DE RIESGO

En la figura que aparece a continuación se presenta un modelo de riesgo genérico con factores de riesgo que pueden utilizar las organizaciones para entender cómo pueden producirse los incidentes con datos. Un suceso de amenaza explota una vulnerabilidad existente que se magnifica por condiciones que lo predispongan o se mitiga mediante controles de seguridad que ya están en vigor. Esto provoca consecuencias adversas que producen un riesgo organizativo, en el que están incluidos riesgos para la organización y para las personas afectadas.

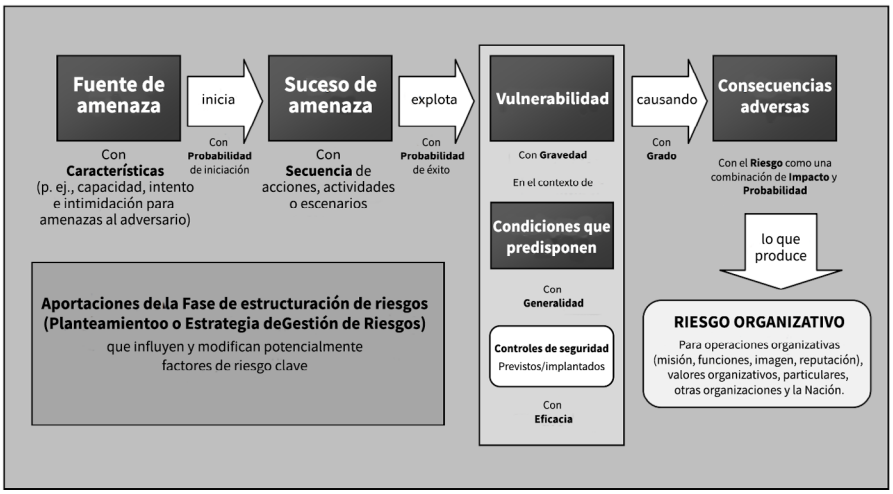

Figura 1. "Modelo de riesgo genérico con factores de riesgo clave". Fuente: NIST Special Publication 800-30 pg. 12[6]

En la figura que aparece a continuación se presenta un ejemplo de cómo se podría adaptar al sector humanitario este modelo de riesgo genérico.

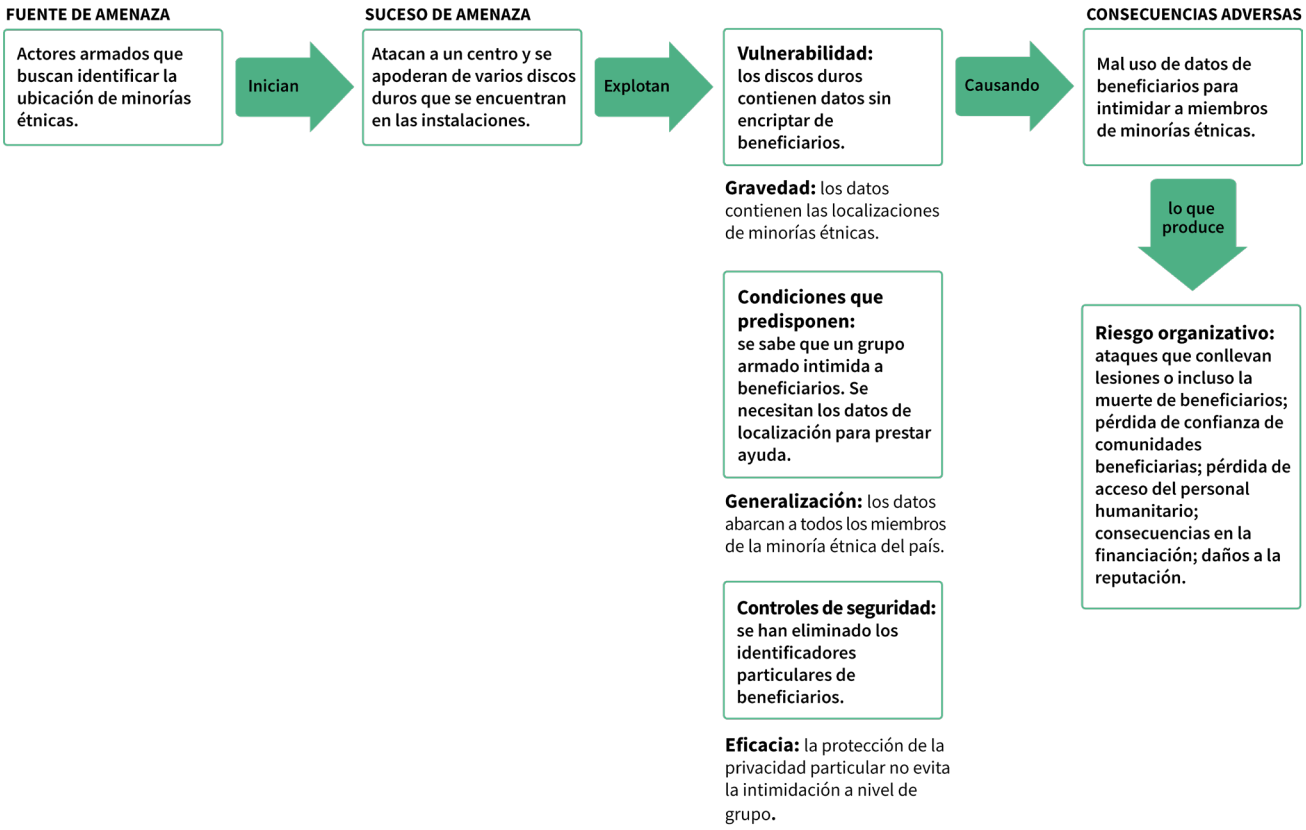

Figura 2. Modelo de riesgo con factores de riesgo clave adaptados a un contexto humanitario.

[6] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

Las organizaciones humanitarias pueden crear sus propios modelos de riesgo específicos para la gestión de los incidentes con datos que incorporen estos factores. La naturaleza de estos factores de riesgo y cómo contribuyen a constituir incidentes con datos variarán de una organización a otra y deberían adaptarse a las realidades operativas específicas.

PASOS PARA LA GESTIÓN DE INCIDENTES CON LOS DATOS

Después de definir con claridad lo que constituye un incidente con datos, las organizaciones pueden crear Procedimientos operativos estándares (POE) para la gestión de los incidentes con datos.

Los POE para la gestión de los incidentes con datos deberían contener los siguientes 5 pasos: 1) comunicación, 2) clasificación, 3) tratamiento, 4) cierre y 5) base de conocimientos.[7]

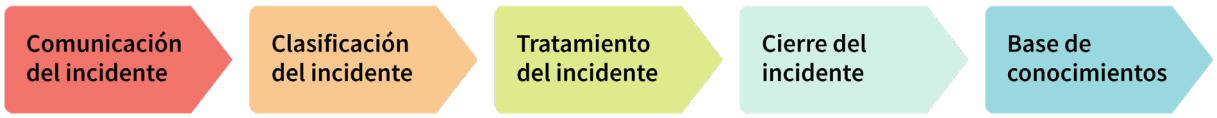

Figura 3: Cinco pasos para el tratamiento de los incidentes de seguridad (Fuente: *How to handle incidents according to ISO 27001 A.16, Antonio Jose Segovia*[8]

La aplicación de estos pasos en una organización puede quedar del siguiente modo:

1. **Comunicación del incidente**: alguien detecta un incidente y lo comunica a los compañeros pertinentes conforme a los procedimientos de comunicación de la organización (normalmente, por correo electrónico, llamada telefónica, herramienta de software, etc.). La comunicación debe contener, a ser posible, una descripción de los factores de riesgo clave que entraña el incidente: fuente, suceso, vulnerabilidad y consecuencias.

2. **Clasificación del incidente**: el receptor de la comunicación clasifica el incidente según sus consecuencias (de nivel alto, medio o bajo) y la urgencia del tratamiento (de nivel alto, medio o bajo).[9] La gestión del riesgo comienza con la clasificación de todos los incidentes, resulte de ellos un daño tangible realmente o no.[10]

3. **Tratamiento del incidente**: un técnico experto decide qué medidas son necesarias para tratar el incidente una vez que este se haya clasificado y se haya acordado el momento para llevar a cabo el tratamiento.

4. **Cierre del incidente**: se registra toda la información generada durante el tratamiento y se informa a la persona que envió la comunicación del incidente en primer lugar de que este se cierra.

5. **Base de conocimientos**: toda la información generada durante el tratamiento del incidente se usa para informar y formar a compañeros y como material de referencia para futuros incidentes similares.

Las organizaciones humanitarias pueden basar sus POE en este modelo de cinco pasos y detallar cómo se debe efectuar cada paso en su organización. Deberían incluirse aquí las funciones/ labores y los equipos de la organización responsables en cada paso del proceso. Los protocolos de respuesta ante incidentes existentes deben incorporar estos pasos o ampliarse con ellos (p. ej., la gestión de los incidentes de seguridad relacionados con el acceso del personal humanitario).

En un contexto de respuesta determinado, las organizaciones también deben trabajar para integrar procedimientos de gestión de incidentes conjuntos en las estructuras de coordinación existentes, como los grupos y los mecanismos para la coordinación intergrupal e intragrupal.

[7] El Centro de Datos Humanitarios ofrece varias fuentes de orientación que informan sobre la creación de POE de Gestión de incidentes con datos en la **página de Responsabilidad de datos**.

[8] **How to handle incidents according to ISO 27001 A.16**, Antonio Jose Segovia, (, (octubre de 2015.).

[9] Para las organizaciones humanitarias, un ejemplo de ello es la **Clasificación Internacional para la Seguridad del Paciente de la Organización Mundial de la Salud (OMS), Marco conceptual de la Clasificación Internacional para la Seguridad del Paciente**.

[10] OMS, **Marco conceptual de la Clasificación Internacional para la Seguridad del Paciente**.

RECOMENDACIONES PARA LA MEJORA DE LA GESTIÓN DE INCIDENTES CON DATOS EN ORGANIZACIONES HUMANITARIAS

Introducir o mejorar la gestión de incidentes con datos en operaciones humanitarias es fundamental para lograr una práctica con los datos más responsable en el sector. El Centro de Datos Humanitarios recomienda que las organizaciones se centren en las siguientes áreas:

1. **Establecer una idea común de la gestión de los incidentes con datos**
   Utilizar un modelo de riesgos para comprender la cadena causal que puede conducir a los incidentes con datos para sistemas y oficinas específicos. Identificar a los principales actores que suponen una amenaza y las vulnerabilidades de oficinas y sistemas, y comprender los controles de seguridad existentes y su eficacia. Por último, elaborar un mapa de la capacidad de gestión de los incidentes con datos existente y determinar si está posicionado de forma adecuada. Una vez articulados los procesos y definiciones de forma clara, invertir en la concienciación del personal y apoyar una cultura de diálogo abierto sobre los incidentes, en la que se incentive la comunicación proactiva y la gestión de estos, sin castigarse.

2. **Refuerzo de la capacidad de gestión de los incidentes con datos**
   Adoptar medidas para poner en marcha controles de seguridad que mitiguen el riesgo de que se produzcan incidentes con datos y compartir las mejores prácticas con colaboradores. Desarrollar el trabajo existente en el sector para cubrir carencias en materia de gobernanza que puedan crear vulnerabilidades para su organización. Comprometerse con las organizaciones colaboradoras a establecer canales de información en torno a los incidentes con datos. Compartir las vulnerabilidades que se conozcan de forma controlada con colegas en los que confíe para lograr un aprendizaje entre las organizaciones.

3. **Apoyo al aprendizaje continuo**
   Respaldar el aprendizaje y la creación de prácticas de gestión de incidentes con datos mejoradas mediante la organización de formaciones y simulacros basados en escenarios que es probable que ocurran en diferentes marcos operativos. Los ejercicios deberían realizarse de forma regular y en ellos incluso podrían integrarse simulacros y formaciones de varias organizaciones conjuntamente. Además, documentar los incidentes con datos reales como casos para crear conocimiento interno.

Animamos a las organizaciones a que compartan su experiencia en el desarrollo de la gestión de los incidentes con datos con el Centro de Datos Humanitarios a través de centrehumdata@un.org.

COLABORADORES: **UNIVERSIDAD DE YALE, JACKSON INSTITUTE OF GLOBAL AFFAIRS.**

El **Centre Para Los Datos Humanitarios** (‘El Centro’), junto con colaboradores principales, está publicando una serie de ocho notas orientativas sobre Responsabilidad con los Datos en la Acción Humanitaria durante el transcurso de 2019 y 2020. La serie de Notas orientativas aparece tras la publicación del **working draft OCHA Data Responsibility Guidelines (anteproyecto de directrices de responsabilidad sobre los datos de OCHA)** en marzo de 2019. Con la serie el Centro pretende ofrecer una orientación adicional sobre cuestiones, procesos y herramientas específicos para la responsabilidad con los datos en la práctica. Esta serie ha sido posible gracias el generoso apoyo de la Dirección General de Protección Civil y Ayuda Humanitaria de la Unión Europea (DG ECHO, por sus siglas en inglés).

Este documento abarca actividades de ayuda humanitaria implementadas con la ayuda económica de la Unión Europea. Las opiniones expresadas aquí en modo alguno deben entenderse como un reflejo de la opinión oficial de la Unión Europea y la Comisión Europea no se hace responsable del uso que pueda realizarse de la información que contiene.

Este proyecto está cofinanciado por la Unión Europea