El poder de la humanidad

Consejo de Delegados del Movimiento Internacional
de la Cruz Roja y de la Media Luna Roja
22 y 23 de junio de 2022, Ginebra

Salvaguardar los datos humanitarios

DOCUMENTO DE ANTECEDENTES

Mayo de 2022

ES

CD/22/16
Original: inglés
Para información

Documento elaborado por
el Comité Internacional de la Cruz Roja
con el apoyo de la Plataforma de directivos en materia de Restablecimiento del contacto entre familiares

RESUMEN

El ciberataque acometido en 2022 contra los servidores que alojaban datos del Comité Internacional de la Cruz Roja (CICR) y de más de 60 Sociedades Nacionales de la Cruz Roja y de la Media Luna Roja (Sociedades Nacionales)[1] puso de relieve el riesgo que plantean las ciberoperaciones y las violaciones de datos para las organizaciones humanitarias. Desde hace muchos años, el CICR y otros componentes del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (Movimiento) vienen alertando sobre la necesidad imperiosa y urgente de que los Estados y otros actores protejan los datos humanitarios y la infraestructura digital frente a ciberoperaciones, así como a intrusiones cibernéticas y al uso indebido de medios cibernéticos. Lamentablemente, la reciente violación de datos deja en evidencia que este riesgo es muy concreto.

Los ataques a los datos humanitarios desvirtúan la labor de las organizaciones humanitarias y pueden plantear riesgos considerables para la dignidad y la seguridad de las personas afectadas por conflictos armados, desastres y otras emergencias.

A la par de las medidas que adopta el Movimiento para proteger a las personas afectadas por el acceso indebido a los datos y de las actividades que ha emprendido para reconstruir la infraestructura informática comprometida, esta resolución del Consejo de Delegados tiene como objetivo fortalecer el marco jurídico y normativo que protege los datos y la infraestructura digital de las organizaciones humanitarias imparciales. Sienta las bases para la labor colectiva del Movimiento hacia un consenso firme –tanto en el discurso como en la acción– de que los datos humanitarios no deben ser atacados en ninguna circunstancia y de que las actividades humanitarias deben protegerse en el ámbito virtual de la misma manera que fuera de él.

1) INTRODUCCIÓN

A principios de 2022, el CICR descubrió que los servidores que contenían los datos personales de más de 500.000 personas que recibían servicios del Movimiento se habían visto comprometidos en un sofisticado ciberataque[2]. Si bien causó mucha conmoción, no se trata de un hecho aislado: refleja una tendencia en aumento de ciberoperaciones dirigidas contra organizaciones humanitarias.

Operaciones de este tipo pueden tener consecuencias graves para personas vulnerables. El ciberataque que sufrió el Movimiento, por ejemplo, comprometió datos personales (nombres, ubicaciones y datos de contacto, etc.) de personas desaparecidas y sus familiares, niños no acompañados y separados, personas detenidas y otras personas que recibían servicios humanitarios a causa de conflictos armados, desastres naturales o migraciones. Si caen en las manos equivocadas, los datos a los que se accedió podrían llegar a ser utilizados por algunos Estados, por grupos armados no estatales o por particulares para contactar o encontrar a personas con el fin de causarles un perjuicio, por ejemplo, para arrestar o atacar a opositores políticos o traficar niños no acompañados.

Asimismo, las ciberoperaciones que atacan datos humanitarios pueden llegar a perturbar las operaciones humanitarias y socavar la confianza depositada en su labor. Esa confianza en esencial para el desarrollo de las actividades de las organizaciones humanitarias, y una violación de datos podría poner en riesgo el acceso de esas organizaciones a las personas que las necesitan, así como la seguridad de su personal y de sus actividades, lo que, en última instancia, podría empeorar la situación humanitaria de personas afectadas por conflictos armados, desastres

[1] Más información en https://www.icrc.org/es/document/ciberataque-cicr-que-sabemos-hasta-ahora.
[2] *Ibíd*.

naturales y otras emergencias.

A la par de los avances del Movimiento en cuanto a medidas para proteger a las personas afectadas por este ciberataque y de sus esfuerzos por reconstruir la infraestructura informática comprometida, esta resolución tiene como objetivo fortalecer el marco jurídico y normativo que protege los datos y la infraestructura digital de las organizaciones humanitarias imparciales. Sienta las bases para la labor colectiva del Movimiento hacia un consenso firme –en el discurso y en la acción– de que los datos humanitarios no han de ser atacados en ninguna circunstancia y de que las actividades humanitarias han de protegerse en el plano virtual de la misma manera que fuera de él.

La resolución también constituye un paso más dentro de la labor jurídica, normativa y técnica del Movimiento en favor de la protección de los datos humanitarios y las actividades operacionales, sobre la base de la resolución 4 de la XXXIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja (Conferencia Internacional), y un puente hacia otra posible resolución en el marco de la próxima XXXIV Conferencia Internacional.

2) ANTECEDENTES

La resolución es el resultado de una iniciativa conjunta del CICR, la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (Federación Internacional) y algunas Sociedades Nacionales en respuesta al ciberataque de 2022. Envía un mensaje contundente a los Estados, a otros actores y a otras organizaciones humanitarias imparciales acerca de la importancia de salvaguardar los datos humanitarios.

Como la resolución se presenta en respuesta al acceso indebido a los datos ocurrido en 2022, se invitó y se alentó a todos los componentes del Movimiento a que participen en una serie de consultas en modalidad acelerada durante marzo y abril de 2022, en función del siguiente cronograma:

- Mediados de marzo de 2022: envío del anteproyecto de resolución a todos los componentes del Movimiento.
- Finales de marzo de 2022: consulta informal en línea abierta a todos los componentes del Movimiento
- 8 de abril de 2022: fecha límite para que los componentes del Movimiento enviaran sus comentarios por escrito sobre el anteproyecto de resolución.
- Principios de mayo de 2022: envío oficial de todos los documentos del Consejo de Delegados, incluido un proyecto de resolución definitivo sobre la salvaguarda de los datos humanitarios.

Si desean debatir acerca del proyecto de resolución, se alienta a los componentes del Movimiento a comunicarse con alguna de las siguientes personas:

- Tilman Rodenhäuser, asesor jurídico, CICR, trodenhauser@icrc.org.
- Mathilde Piret, asesora jurídica, CICR, mpiret@icrc.org.

3) ANÁLISIS

El ciberataque de 2022 puso de relieve el riesgo que plantean las operaciones cibernéticas, entre ellas, las violaciones de datos, a las organizaciones humanitarias, incluido el Movimiento. Desde hace muchos años, el CICR y otros componentes del Movimiento vienen alertando sobre la necesidad imperiosa y urgente de que los Estados y otros actores protejan los datos humanitarios y la infraestructura digital frente a ciberoperaciones, así como a intrusiones cibernéticas y al uso indebido de medios cibernéticos. Lamentablemente, la reciente violación de datos deja en evidencia que este riesgo es muy concreto.

Acceder de manera indebida a datos que hayan sido recopilados, almacenados o procesados de alguna otra manera por organizaciones humanitarias imparciales o extraerlos sin autorización desvirtúa la labor de esas organizaciones y puede generar riesgos considerables para la dignidad y la seguridad de las personas afectadas por conflictos armados, desastres y otras emergencias. Si bien las tecnologías digitales dependen de sistemas informáticos y funcionan en ellos, el énfasis del Movimiento debe estar siempre puesto en las personas, sobre todo las más vulnerables.

A los efectos de la resolución, recomendamos definir "datos humanitarios" como datos, entre los cuales se incluyen datos personales, que las organizaciones humanitarias procesan (es decir, recopilan, almacenan, transfieren o archivan, por ejemplo) con fines humanitarios. Pueden ser datos personales en relación con una necesidad de servicios humanitarios, así como datos no personales recogidos en el contexto de operaciones humanitarias, como informes de visitas a lugares de detención, informes sobre las necesidades de las poblaciones afectadas y datos necesarios para planificar la asistencia humanitaria.

Fortalecer la ciberseguridad, la seguridad de los datos y la protección de los datos personales dentro del Movimiento y en el sector humanitario en general es un objetivo a largo plazo que exige medidas jurídicas, normativas y técnicas. Para lograrlo, los componentes del Movimiento tienen a su disposición varias herramientas, como el programa de formación y certificación para encargados de protección de datos en actividades humanitarias que llevan adelante la Oficina de Protección de Datos del CICR y la Universidad de Maastricht. El proyecto de resolución titulado “Salvaguardar los datos humanitarios” es un elemento más dentro de la respuesta del Movimiento. Tiene varios objetivos interrelacionados:

- Llamar la atención respecto del riesgo creciente de las ciberoperaciones contra las organizaciones humanitarias y del impacto negativo que tienen las violaciones de datos, y subrayar el valor de los datos humanitarios y la necesidad de que se protejan.
- Comunicar un mensaje de que atacar los datos confiados a organizaciones humanitarias tiene las siguientes consecuencias:
    - Afecta la seguridad, la dignidad y la privacidad de las personas vulnerables y puede exponerlas a riesgos graves, incluso daños físicos y psicológicos.
    - Socava la confianza en estas organizaciones, así como en la acción humanitaria imparcial en general, con lo cual podría llegar a alterar sus operaciones y sus esfuerzos por aliviar el sufrimiento humano.
- Reafirmar el compromiso del Movimiento de poner en práctica normas de protección de datos y medidas de ciberseguridad, y de disponer prácticas eficaces y su cumplimiento.
- Facilitar la labor en todo el Movimiento para poner en común buenas prácticas, fortalecer las capacidades de todos los componentes del Movimiento y considerar el desarrollo conjunto de un Código de Conducta del Movimiento para la protección de datos, y establecer un grupo de trabajo informal a estos efectos.
- Hacer partícipe a todo el Movimiento en el tema y enviar un mensaje contundente de compromiso del Movimiento a los Estados, otros actores y otras organizaciones humanitarias imparciales en torno a los siguientes puntos:
    - la responsabilidad de las organizaciones humanitarias de adoptar medidas concretas y eficaces en favor de la seguridad de los datos y la protección de los datos personales confiados a ellas.
    - la responsabilidad de los Estados de respetar y proteger las organizaciones humanitarias y su personal, su información y sus activos, tanto dentro como fuera del espacio virtual.
    - la necesidad de que los componentes del Movimiento colaboren con otras organizaciones humanitarias y con entidades asociadas para fortalecer la ciberseguridad y formular o adquirir soluciones idóneas que fortalezcan los mecanismos de prevención contra esos ataques y mitiguen su impacto, en caso de que ocurran.

- Encaminar a todo el Movimiento hacia un interés común de investigar y formular medidas para proteger el espacio humanitario neutral, independiente e imparcial en el ámbito digital, por ejemplo, la investigación del CICR sobre el emblema digital[3].

4) RECURSOS NECESARIOS

Al aprobar esta resolución, los componentes del Movimiento se comprometen a adoptar las medidas necesarias, dentro del alcance de sus respectivas capacidades y necesidades operacionales, a fin de mejorar su capacidad de garantizar niveles adecuados y altos de seguridad al procesar datos (por ejemplo, en la recopilación, el almacenamiento o la transferencia) para la realización de sus actividades, cumplir el derecho vigente y los marcos de protección de datos personales, y aplicar normas y buenas prácticas pertinentes en el procesamiento de datos personales, teniendo en cuenta el *Manual sobre protección de datos en la acción humanitaria.*

También se invitará a los componentes del Movimiento a participar en un grupo de trabajo informal para intercambiar prácticas idóneas sobre seguridad de datos y protección de datos personales, a apoyarse mutuamente en el fortalecimiento de capacidades, a procurar que el personal y los voluntarios estén al tanto de la importancia de la seguridad de los datos y la protección de datos, así como de qué manera todos pueden y deben contribuir a ese objetivo, y a considerar la posibilidad de elaborar un código de conducta del Movimiento relativo a la protección de datos.

Asimismo, la resolución propuesta incentiva al CICR y a otros componentes del Movimiento a investigar y elaborar medidas para proteger el espacio humanitario neutral, independiente e imparcial en el ámbito digital. También incentiva al CICR a consultar y coordinar con los componentes del Movimiento en su investigación en torno a la factibilidad técnica de un emblema digital y a evaluar sus beneficios.

La implementación de estos compromisos puede conllevar una inversión de recursos por parte de los componentes del Movimiento de manera individual, en función del alcance de sus programas y actividades vigentes, así como del volumen de personal asignado al tema.

5) IMPLEMENTACIÓN Y SEGUIMIENTO

El éxito de la resolución dependerá de su implementación eficaz y su aplicación coherente por parte de los componentes del Movimiento. Se espera que todos ellos la implementen y apliquen como parte de su labor en el ámbito de la seguridad de los datos y la protección de datos personales, en la medida en que sea factible y adecuado.

Se invita a todos los componentes del Movimiento a informar ante el Consejo de Delegados que se reunirá en 2023 sobre los progresos alcanzados en la implementación de esta resolución.

[3] El concepto de emblema digital que figura aquí y en el proyecto de resolución se refiere a "un emblema, signo distintivo u otro medio digital para identificar los datos y la infraestructura digital de organizaciones y entidades autorizadas para exhibir los emblemas distintivos reconocidos por el derecho internacional humanitario e indicar, cuando corresponda, su protección jurídica". La idea es elaborar un emblema, señal u otro medio de identificación digital que cumpla las funciones protectora e indicativa de los emblemas distintivos, según lo definido en el derecho internacional humanitario.

Conclusión y recomendaciones

En vista del ataque a los datos humanitarios en poder del CICR y de más de 60 Sociedades Nacionales ocurrido en 2022, una resolución del Consejo de Delegados para salvaguardar los datos humanitarios es una pieza importante de la respuesta del Movimiento a esta amenaza nueva y de rápida evolución.

La resolución pone de relieve los riesgos que suponen las ciberoperaciones que afectan datos humanitarios para las personas a cuyos datos personales se acceda indebidamente y para las organizaciones humanitarias en lo que respecta a su capacidad de cumplir su cometido de brindar asistencia y protección a personas afectadas por conflictos armados, desastres naturales y otras emergencias. También afirma el compromiso del Movimiento de utilizar nuevas tecnologías de manera responsable haciendo lo posible por implementar normas relativas a la protección de datos y medidas de ciberseguridad, y envía un mensaje claro y contundente a los Estados para que respeten y protejan a las organizaciones humanitarias y a su personal, sus datos y sus recursos, tanto dentro como fuera del espacio virtual.