# Red de Vínculos Familiares del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja

# Código de Conducta sobre protección de datos

**Versión 2.0**

**2024**

# Prefacio

El presente Código de Conducta (en adelante, el Código) fue redactado por un grupo de trabajo compuesto por representantes de la Cruz Roja Alemana (Jutta Hermanns), la Cruz Roja Austríaca (Claire Schocher-Döring), la Cruz Roja de Bélgica (Flandes) (Axel Vande Veegaete y Nadia Terweduwe), la Cruz Roja Británica (Mark Baynham y Emily Knox), la Oficina de la Cruz Roja para la Unión Europea (Olivier Jenard), el Comité Internacional de la Cruz Roja (Romain Bircher, Massimo Marelli y Katja Gysin) y la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (Christopher Rassi). Varios representantes más de esas instituciones también ayudaron a redactarlo, participaron en los debates y las reuniones, e hicieron aportes importantes. El grupo de trabajo comenzó a debatir este proyecto a fines de 2013 y, a lo largo de dos años, ha mantenido varias reuniones en distintos lugares de Europa: Mechelen (abril de 2014), Bruselas (julio de 2014), Viena (septiembre de 2014), Sofía (noviembre de 2014) y Londres (enero de 2015). Además, los miembros se han comunicado muchas veces por teleconferencia y correo electrónico. El grupo de trabajo adoptó el Código por consenso, incorporando los comentarios recibidos de numerosas Sociedades Nacionales.

El Código fue revisado en 2024 por miembros del grupo de aplicación y por otros representantes de la Oficina de Protección de Datos y la Unidad de Protección de Vínculos Familiares (PVF) del CICR. El grupo de aplicación adoptó por consenso la versión revisada del Código de Conducta, habiendo incorporado los comentarios recibidos de sus miembros.

Se consideró necesario el Código de Conducta, en primer lugar, por las numerosas personas y grupos del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja que trabajan en la Red de Vínculos Familiares, así como la necesidad de transferir datos en el seno del Movimiento, y a otras personas y grupos externos a él, y en segundo lugar, por el cambiante entorno normativo en Europa y en todo el mundo en lo que respecta a la legislación y las normas sobre protección de datos. El Código establece los principios, compromisos y procedimientos mínimos que deben cumplir los miembros del Movimiento al procesar datos de la Red de Vínculos Familiares. El objetivo es cumplir con las normas más estrictas en materia de protección de datos, especialmente la legislación de la Unión Europea. Al utilizar este Código, las Sociedades Nacionales deben asegurarse también de cumplir su propia legislación nacional, que prevalecerá en caso de conflictos con el Código de Conducta. El Código es un documento de referencia integrado en el conjunto principal de materiales del Movimiento para dar orientación sobre Restablecimiento del contacto entre familiares (RCF). Cada miembro del Movimiento deberá adoptarlo e incorporarlo en sus propios procedimientos estándar.

Este Código es una herramienta que pueden usar todos los miembros del Movimiento para proteger los derechos y las libertades fundamentales de las personas que participan en actividades de RCF, en particular el derecho a la privacidad y a la protección de datos personales. La intención es que el Código dé confianza tanto a las personas como a los entes reguladores en relación con el trabajo del Movimiento, y también a los miembros del Movimiento que necesiten transferirse datos sobre casos de RCF.

# Índice

# Definiciones

## Movimiento Internacional de la Cruz Roja y de la Media Luna Roja

El Movimiento es un movimiento humanitario mundial cuya misión es prevenir y aliviar, en todas las circunstancias, el sufrimiento humano; proteger la vida y la salud, y hacer respetar a la persona humana, en particular en tiempo de conflicto armado y en otras situaciones de urgencia; tratar de prevenir las enfermedades y promover la salud y el bienestar social; fomentar el trabajo voluntario y la disponibilidad de los miembros del Movimiento, así como un sentimiento universal de solidaridad para con todos los que tengan necesidad de su protección y de su asistencia".

El Movimiento se compone del Comité Internacional de la Cruz Roja (CICR), las Sociedades Nacionales de la Cruz Roja y de la Media Luna Roja (las Sociedades Nacionales), y la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (FICR).

## Agencia Central de Búsquedas

La Agencia Central de Búsquedas (ACB) es un servicio permanente del CICR, en virtud de las disposiciones de los cuatro Convenios de Ginebra y sus Protocolos adicionales, así como de los Estatutos del Movimiento. En colaboración con otros componentes del Movimiento, la ACB lleva a cabo actividades de RCF para ayudar a las personas afectadas por conflictos armados y otras situaciones de violencia, desastres naturales y otras circunstancias que requieran una respuesta humanitaria. Según el Acuerdo de Sevilla de 1997 y sus Medidas complementarias de 2005, así como la Estrategia del Movimiento relativa al RCF para el período 2008-2018, la ACB tiene la función directiva, dentro del Movimiento, en todo lo relativo a RCF; coordina las operaciones y actúa como asesora técnica de las Sociedades Nacionales.

## Controlador de datos

El controlador de datos es cualquier componente del Movimiento que, de manera individual o en conjunto con otros[1], establece los fines y los métodos del procesamiento de datos personales.

## Procesador de datos

[1] Puede encontrarse una breve explicación de la contraloría y la contraloría conjunta entre el CICR y las Sociedades Nacionales en el anexo 5.

Un procesador es una persona, una autoridad pública, un organismo u otra entidad que procesa datos personales en nombre de un controlador de datos y de acuerdo con sus instrucciones (por ejemplo, un prestador de servicios informáticos).

## Referente de protección de los datos de RCF

Un referente de protección de los datos de RCF es una persona o unidad responsable de sensibilizar sobre la protección de datos y de que los miembros del Movimiento cumplan con el Código de Conducta. Debe tener una sólida experiencia en RCF, y conocer los principios y obligaciones en materia de protección de datos.

## Titular de los datos

Un titular de datos es una persona física (es decir, un particular) que puede identificarse directa o indirectamente sobre la base de sus datos personales[2].

Para determinar si una persona es identificable, hay que contemplar todos los medios que sea razonable prever que utilice el controlador u otros para identificarla directa o indirectamente. Eso implica considerar todos los factores objetivos, como el costo de la identificación y el tiempo que lleva, tomando en cuenta tanto la tecnología disponible en el momento del procesamiento como el desarrollo tecnológico futuro. Por ello, no se considera datos personales a la información anónima, sin relación con personas físicas no identificadas o identificables, ni a los datos que se hayan anonimizado de manera que impida identificar a su titular. En vista de las capacidades de las nuevas tecnologías, es difícil tener la seguridad de que la información anónima o anonimizada no pueda utilizarse para identificar a su titular. Por lo tanto, este Código no se refiere al procesamiento de información anónima, con fines estadísticos y de investigación, por ejemplo.

Cuando las personas utilizan servicios en línea, se las puede vincular con los identificadores que facilitan sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de IP o las cookies. Es posible que queden rastros que, al combinarse con identificadores únicos y con otros datos recibidos por los servidores, puedan utilizarse para crear perfiles de las personas en cuestión e identificarlas. Si la información —números, datos de ubicación o identificadores en línea (como direcciones de IP o cookies)— no permiten identificar a una persona, se la considera anónima, y no entra en la categoría de datos personales.

## Familiares

Puede clasificarse como familiares a las siguientes personas:

- hijos (nacidos dentro y fuera del matrimonio, hijos adoptados e hijastros);
- parejas (casadas o no);
- padres y madres (biológicos o adoptivos), suegros y suegras;
- hermanos y hermanas (nacidos de los mismos padres o de padres distintos o adoptivos);

[2] Por ejemplo, la persona que presenta una solicitud de búsqueda ante un componente del Movimiento.

- familiares cercanos[3];
- cualquier otra persona con quien exista un vínculo afectivo fuerte, aunque no haya consanguinidad.

También es importante considerar cómo se definen los lazos de parentesco en la legislación nacional.

## Menores

Todos los seres humanos menores de 18 años, a menos que obtengan la mayoría de edad antes según la legislación vigente.

## Otras personas

Además de las quienes presentan solicitudes de búsqueda y de las personas desaparecidas, las actividades de RCF pueden concernir a otros familiares, testigos, vecinos, líderes comunitarios, otras personas desaparecidas, etc.

## Datos personales

Toda información relativa a una persona identificada o identificable. Una persona física identificable es alguien que puede identificarse, directa o indirectamente, mediante un identificador, como un nombre, un número, material audiovisual, datos de ubicación, identificadores en línea, o por uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona.

Los datos personales no incluyen la información anónima, es decir: a) la información no relacionada con una persona física identificada o identificable; o b) la información que se haya anonimizado de manera que impida identificar a su titular.

## Datos sensibles

Datos personales especialmente sensibles en relación con una situación específica atravesada por su titular y que podría causar daños graves (por ejemplo, discriminación o represión) en caso de que se dé a conocer o no se gestione correctamente. Por ese motivo, los datos sensibles deben manejarse con un grado mayor de atención y protección. Para determinar la sensibilidad de los datos, hay que realizar una evaluación de riesgos sobre la situación en la que se llevan adelante las actividades de RCF y afines.

Los datos biométricos y genéticos, así como los que se relacionan con la salud de su titular, se consideran datos sensibles independientemente de la situación. En el caso de otros tipos de datos, la

[3] En muchos contextos socioculturales, la familia incluye a todas las personas que viven bajo el mismo techo o que mantienen lazos cercanos entre sí. Por lo tanto, el concepto de familia debe entenderse en función de la interpretación y las prácticas sociales.

sensibilidad se determina caso por caso y según la situación. Por regla general, pueden ser sensibles los datos que revelan el origen étnico o racial, las opiniones políticas, las creencias religiosas o filosóficas, o detalles sobre la vida o la orientación sexual del titular.

Para las Sociedades Nacionales, el alcance de los datos sensibles puede variar en función de la legislación nacional.

## Ataque a datos personales

Vulneración accidental o ilícita de la seguridad que conduce o puede conducir a la destrucción, pérdida, robo, alteración o divulgación no autorizada de datos personales, o al acceso a ellos, mientras se los transmite, almacena o procesa en cualquier otra forma.

## Procesamiento

Toda operación o conjunto de operaciones que se realicen con datos personales o conjuntos de datos personales, ya sea con medios automatizados o no, como su obtención, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, distribución del tipo que sea o eliminación. Toda transferencia de datos dentro o fuera del Movimiento constituye una operación de procesamiento.

## Destinatario

Toda persona, autoridad pública, servicio o cualquier otro organismo, diferente del titular, el controlador o el procesador de los datos, que recibe datos personales.

## Derivación

Proceso que consiste en vincular a una persona con un servicio que necesite. Puede implicar compartir datos personales de una persona desaparecida, así como los datos de la persona que presentó la solicitud de búsqueda.

## Actividades de Restablecimiento del contacto entre familiares y actividades afines

“Restablecimiento del contacto entre familiares” (RCF) es un término genérico que describe un conjunto de actividades destinadas a evitar la separación entre familiares, a restablecer y mantener el contacto, y a esclarecer el destino y el paradero de las personas desaparecidas.

Estas actividades pueden vincularse con otros servicios de apoyo a los que puede derivarse a las personas afectadas, como asistencia médica, psicológica, psicosocial, jurídica y administrativa. Los familiares también pueden acceder a asistencia material, programas de reubicación y reintegración, y servicios de bienestar social (para más detalles, ver el anexo 1).

## Servicios de RCF

Las Sociedades Nacionales y las delegaciones del CICR en todo el mundo tienen en sus estructuras personal especializado responsable de desarrollar e implementar actividades de RCF y afines.

## Red de Vínculos Familiares

Cuando las familias se separan y hay personas que quedan desaparecidas a causa de conflictos armados, otras situaciones de violencia, desastres naturales, migraciones u otras crisis humanitarias, debemos hacer todo lo que esté a nuestro alcance para determinar qué les ha ocurrido, restablecer el contacto con sus familiares y, si es posible, reunirlos.

Los servicios de RCF de las Sociedades Nacionales y el CICR forman una única red mundial denominada **Red de Vínculos Familiares**. La ACB actúa como asesora técnica y coordinadora de esta red, que moviliza a empleados y voluntarios a escala mundial, y hace que la labor de RCF se lleve adelante conforme a una metodología y principios comunes en todas partes del mundo.

En el sitio web sobre RCF, http://familylinks.icrc.orghttps://familylinks.icrc.org/es/pagina-de-inicio, hay más información sobre la Red de Vínculos Familiares.

## Persona vulnerable

En el contexto de este Código, llamamos persona vulnerable a toda persona que a) haya sufrido particularmente el impacto emocional y psicológico de la separación familiar y las condiciones humanitarias que haya tenido que experimentar o que b) no esté en condiciones de entender los riesgos y oportunidades que trae consigo el procesamiento de datos, a causa de su complejidad.

# 1. Introducción

## *1.1 Propósito de este Código de Conducta*

Este Código establece los principios, compromisos y procedimientos mínimos que debe cumplir el personal de RCF del CICR, las Sociedades Nacionales y la Federación Internacional al procesar datos en el marco de las actividades de RCF, para: 1) cumplir las normas y la legislación correspondientes en materia de protección de datos; 2) permitir el libre flujo de los datos personales que requieran las actividades de RCF, y 3) proteger los derechos y las libertades fundamentales de los solicitantes, las personas desaparecidas y otras personas, como testigos u otros familiares, relacionadas con las actividades de RCF según el derecho internacional humanitario (DIH), el derecho internacional de los derechos humanos y otras normas internacionales, en particular el derecho a la privacidad y a la protección de los datos personales.

## *1.2 Alcance de este Código de Conducta*

### 1.2.1 Restablecimiento del contacto entre familiares

Este Código es aplicable a las actividades de RCF y a las actividades relacionadas con RCF de los controladores de datos (ver anexo 1).

### 1.2.2 Datos personales

Este Código de Conducta rige la tarea de los controladores de datos en el procesamiento de los datos personales de quienes presentan solicitudes de búsqueda, de las personas desaparecidas y de otras personas relacionadas con actividades de RCF (entre ellas, personas fallecidas).

## *1.3 Red de Vínculos Familiares*

Los Convenios de Ginebra de 1949, sus Protocolos adicionales de 1977, los Estatutos del Movimiento, las resoluciones aprobadas por el Consejo de Delegados y las aprobadas por la Conferencia Internacional de la Cruz Roja y de la Media Luna Roja encomiendan a los controladores de datos el cometido de llevar a cabo actividades de RCF.

Las Sociedades Nacionales ejecutan ese cometido junto a sus autoridades públicas respectivas en el ámbito humanitario y desempeñan una función única en materia de RCF en todo el mundo. En coordinación con las autoridades públicas, organizan distintos servicios para ayudar a las víctimas de conflictos armados, desastres naturales y otras emergencias.

## *1.4 Principios y directrices del Movimiento*

### 1.4.1 Principios Fundamentales

Los controladores de datos llevan a cabo sus actividades según los Principios Fundamentales que guían al Movimiento: humanidad, imparcialidad, neutralidad, independencia, voluntariado, unidad y universalidad. Cualquier procesamiento de datos personales que se lleve a cabo en el marco de los servicios de RCF de los controladores de datos debe ser compatible con estos principios.

### 1.4.2. Principio de no causar daño

Al llevar adelante los servicios de RCF de los controladores de datos, se hace todo lo posible por evitar causar daños a personas en el procesamiento de sus datos personales.

### 1.4.3 Confidencialidad o normas para la divulgación de información

Cuando los titulares de los datos compartan información con los controladores de datos de manera confidencial, los controladores de datos deberán respetar y garantizar esa confidencialidad. Los controladores de datos deben cumplir todas las obligaciones jurídicas nacionales, regionales e internacionales que correspondan, y están sujetos a las restricciones que se resumen en esta sección (1.4). Para determinar la aplicabilidad de esas obligaciones, deberá considerarse: 1) cualquier privilegio, inmunidad o exención de obligaciones con los que cuenten los controladores de datos en el país o la región en cuestión; y 2) cualquier protección jurídica que establezcan el derecho internacional, incluido el DIH, y el cometido asignado por los Estatutos del Movimiento.

### 1.4.4 Directrices operacionales vigentes

El procesamiento de datos personales se lleva a cabo según las directrices de la Red de Vínculos Familiares, como la guía para Sociedades Nacionales sobre restablecimiento del contacto entre familiares[4], el manual para las Sociedades Nacionales y el CICR sobre evaluación de las necesidades en materia de RCF, y el manual para el terreno y la normativa profesional relativa a la labor de protección de RCF en casos de catástrofe[5].

## 2. Principios básicos de procesamiento de datos y compromisos del controlador de datos

### *2.1 Propósito*

En el momento de la obtención de datos, los controladores de datos deben establecer los fines específicos, explícitos y legítimos con los que se los procesa.

Los datos se procesan principalmente para restablecer el contacto entre familiares separados como consecuencia de conflictos armados y otras situaciones de violencia, desastres naturales, migraciones u otras situaciones que requieran una respuesta humanitaria.

En ciertos casos, puede ser necesario un procesamiento adicional para las actividades relacionadas con RCF, como el archivado, investigaciones científicas o históricas, o análisis estadísticos. Por lo tanto, se pueden procesar los datos con fines distintos de los que se especificaron inicialmente en el

[4] https://www.icrc.org/en/publication/0784-restoring-family-links-guide-national-red-cross-and-red-crescent-societies

[5] Pueden encontrarse documentos de orientación pertinentes en Restoring Family Links Extranet.

momento de su obtención, siempre que el procesamiento respete toda la legislación pertinente sobre protección de datos (para más información, ver anexo 1)[6].

## *2.2 Procesamiento legítimo y justo*

Todo procesamiento de datos personales por parte del controlador de datos debe realizarse en función de uno o varios de los siguientes fundamentos jurídicos:

- el interés público;
- el interés vital del titular de los datos o de otras personas;
- el consentimiento del titular de los datos;
- el interés legítimo de los controladores de datos;
- el cumplimiento de una obligación jurídica.

Al iniciar una operación de procesamiento de datos, el controlador debe determinar el fundamento jurídico que la legitima. De todas formas, incluso cuando se identifica un fundamento jurídico pertinente, el titular de los datos puede ejercer sus derechos[7].

### 2.2.1 Interés público

Este fundamento jurídico se activa cuando los datos se procesan en el marco del cometido humanitario de alguno de los miembros de la Red de Vínculos Familiares, en virtud del derecho nacional o internacional, o para otra actividad que se considere de interés público de acuerdo con la legislación vigente. Si bien es un fundamento esencial para las actividades de la Red, no siempre se lo reconoce en la legislación de los países; por ese motivo, antes de utilizarlo para justificar el procesamiento de datos, las Sociedades Nacionales deben verificar si el derecho nacional lo permite.

Las actividades relacionadas con la Red de Vínculos Familiares que llevan adelante controladores de datos son de interés público, porque son de índole exclusivamente humanitaria, como se establece en la sección 1.3 (ver ejemplos en el anexo 2).

### 2.2.2 Interés vital

Se considera que el procesamiento de datos personales es de interés vital cuando es necesario para proteger la vida, la integridad, la salud, la dignidad o la seguridad de los beneficiarios; por ejemplo, si los titulares de los datos están en una situación tan vulnerable que los servicios de la Red de Vínculos Familiares pueden salvar su vida.

[6] Para determinar si el o los fines del procesamiento adicional son compatibles con el o los fines establecidos inicialmente, el controlador de datos deberá considerar la conexión entre los fines iniciales y los del procesamiento adicional, el contexto en el que se obtuvieron los datos personales —que incluye las expectativas razonables de su titular— y los posibles efectos sobre el titular de los datos.
[7] V. capítulo 3 de este documento.

### 2.2.3 Consentimiento del titular de datos

Desde el punto de vista de la protección, el consentimiento es esencial para que los servicios de la Red de Vínculos Familiares sean transparentes y los beneficiarios tengan una participación directa en ellos. En el contexto de este Código de Conducta, es uno de los fundamentos jurídicos necesarios para una actividad de procesamiento de datos. El consentimiento de que sus datos se procesen debe darse sin ambigüedades y por un medio apropiado para indicar los deseos del titular en forma voluntaria, específica e informada, ya sea por escrito, mediante una declaración verbal o a través de cualquier otra acción positiva.

El consentimiento constituye un fundamento jurídico para todas las actividades de procesamiento que se realizan con el propósito original o con otros propósitos compatibles. Si los controladores de datos desean iniciar otras operaciones de procesamiento para propósitos nuevos e incompatibles, deben buscar un fundamento jurídico distinto o volver a solicitar el consentimiento de los titulares.

El consentimiento puede darse con limitaciones, y los titulares de los datos tienen derecho a retirarlo en cualquier momento. Los pormenores del consentimiento prestado, el grado de confidencialidad requerido y cualquier limitación que corresponda se registran y conservan junto con los datos personales durante todo el proceso.

### 2.2.4 Interés legítimo

También se procesan datos personales en circunstancias en que ello redunda en interés legítimo del controlador de datos, siempre y cuando ni los intereses ni los derechos y libertades fundamentales del titular de los datos invaliden ese interés legítimo (ver ejemplos en el anexo 3).

### 2.2.5 Cumplimiento de una obligación jurídica

Los controladores de datos también deben respetar toda la legislación pertinente al procesar datos personales: por ejemplo, deben respetar la legislación nacional y regional, las órdenes judiciales y los Principios Fundamentales del Movimiento. Las obligaciones legales pueden variar según la situación y el país de que se trate.

## *2.3 Compromisos de procesamiento*

### 2.3.1 Responsabilidad y rendición de cuentas

Los controladores de datos deben asegurarse de que cualquier persona o entidad que procese datos —es decir, que tenga acceso a datos personales y siga instrucciones de los controladores— lo haga en cumplimiento de este Código. Además, los controladores de datos deben constatar que las responsabilidades de cada una de las entidades que participen en el procesamiento de datos personales se asignen claramente y se especifiquen en cláusulas contractuales adecuadas.

En ocasiones, el procesador de datos necesita contratar a un tercero (subprocesador) para que realice determinadas actividades de procesamiento en nombre del controlador de datos. Cuando eso ocurre, el procesador debe informar de antemano al controlador de datos, que decidirá si autoriza o no la operación. En caso de que la apruebe, el subprocesador estará sujeto a las mismas responsabilidades y obligaciones contractuales que el procesador.

En la sección 4 puede encontrarse más información sobre la transferencia de datos a terceros, que pueden no procesar los datos exclusivamente según las instrucciones del controlador de datos.

### 2.3.2 Procesamiento de datos adecuados, pertinentes y actualizados

**Datos adecuados**: los datos personales procesados por los servicios de RCF de los controladores de datos se revisarán para garantizar que sean adecuados y pertinentes, y que no sean excesivos en relación con el fin para el cual se obtienen y procesan. Los datos personales archivados no estarán sujetos a esa revisión, ya que sirven propósitos científicos, históricos y estadísticos.

**Precisión de los datos**: los datos personales deberán ser suficientemente precisos y completos, y estar suficientemente actualizados para el fin con el que se obtienen y procesan.

### 2.3.3 Protección intencional y por defecto

Al diseñar sistemas de gestión de datos y establecer procedimientos para la obtención de datos personales, se adoptarán medidas técnicas y organizativas adecuadas a fin de cumplir los requisitos de este Código.

### 2.3.4 Evaluación de impacto relativa a la protección de datos

Cuando sea probable que el procesamiento de datos conlleve riesgos considerables para los derechos y las libertades de los titulares, como las transferencias, la publicación y la divulgación de los datos, el controlador llevará a cabo una evaluación de impacto relativa a la protección de los datos antes de procesarlos. Si es posible, el controlador de datos consultará previamente al referente de protección de los datos de RCF y a otras partes interesadas en el proyecto de procesamiento[8] para establecer y evaluar lo siguiente:

- los beneficios de procesar los datos;
- el origen, la índole, y la gravedad de los riesgos, así como la probabilidad de que se materialicen;
- las medidas adecuadas que se deben adoptar para demostrar que se minimizan los riesgos, y que los datos personales se procesan en cumplimiento de este Código y de cualquier legislación correspondiente.

El nivel de riesgo y, por consiguiente, la necesidad de realizar una evaluación de impacto relativa a la protección de los datos, se determinan en función de una serie de factores como la magnitud, el alcance y el contexto de las actividades de procesamiento, los métodos empleados para procesar los datos, el carácter y la sensibilidad de los datos personales procesados, y la vulnerabilidad de los titulares.

La finalidad de la evaluación es minimizar el riesgo de daños para los titulares de los datos, así como el de posibles violaciones de sus derechos y libertades. El controlador de datos documentará el resultado y su fundamentación. También deberá garantizar que las medidas que se tomen como

[8] Se debe incluir a todas las funciones que participen en la formulación del proyecto: por ejemplo, las de servicios informáticos, jurídicos, de protección, de archivo y gestión de la información, etc.

consecuencia de la evaluación de impacto relativa a la protección de los datos se implementen adecuadamente y tengan los efectos deseados.

Ante una emergencia, no siempre será posible realizar una evaluación de impacto antes de iniciar el procesamiento de los datos. En esos casos, la evaluación se llevará a cabo después del procesamiento, lo más pronto posible.

### 2.3.5 Retención de los datos

Cuando ya no se necesiten con el fin para el que se obtuvieron, para un procesamiento adicional o para su procesamiento sobre otra base legítima o lícita, los datos personales se archivarán o eliminarán según la política de retención de datos del controlador de datos (ver también la sección 3.3).

El controlador de datos incorporará la gestión de datos personales en los procedimientos internos, incluido el almacenamiento de datos con fines de archivo.

### 2.3.6 Seguridad de los datos

En función de su disponibilidad, en todo momento del procesamiento de los datos, se adoptarán medidas de seguridad técnicas, físicas y organizativas razonables para proteger los datos personales contra la destrucción o pérdida accidental o ilícita, el robo, el acceso y la divulgación no autorizados o ilegales. Solo se permitirá acceder a los datos personales a los controladores de datos que necesiten ese acceso para realizar una tarea o proveer un servicio específico, con medidas de seguridad y restricciones de acceso (para más detalles, ver anexo 3).

### 2.3.7 Ataques a datos personales

El controlador de datos deberá notificar sin demoras al titular en caso de acceso indebido a sus datos personales, si es probable que el episodio ponga en riesgo considerable sus derechos y libertades.

Si el controlador de datos está sujeto a obligaciones jurídicas internas específicas sobre ataques a datos personales, deberá evaluar si tiene la obligación de notificar a las autoridades estatales ante un episodio de ese tipo.

Si un episodio de acceso indebido a datos personales repercute en casos compartidos con otros miembros de la Red de Vínculos Familiares, la ACB debe informar a las Sociedades Nacionales pertinentes y al CICR sin demoras, para que la Red pueda coordinar una respuesta adecuada y notificar a los titulares afectados.

El objetivo de notificar al titular de los datos sobre el acceso indebido a sus datos personales es minimizar los riesgos para esa persona. El controlador de datos realizará una evaluación antes del procesamiento para determinar la magnitud del riesgo para el titular de los datos, así como la necesidad de notificarlo en caso de ataque.

El controlador de datos puede decidir que no es necesario notificar al titular de los datos si se verifica una o más de las siguientes situaciones:

- El controlador de datos ha implementado medidas de protección organizativas, tecnológicas o físicas adecuadas, que se han aplicado a los datos personales afectados por el acceso indebido.
- El controlador de datos ha adoptado medidas posteriores que garantizan que ya no es probable que los derechos y libertades del titular de los datos se vean gravemente afectados.
- Informar al titular supondría un esfuerzo desproporcionado, en particular por las condiciones logísticas o de seguridad imperantes o por el número de casos. En esas circunstancias, el controlador de datos se planteará, en cambio, si conviene emitir una comunicación pública o tomar alguna medida similar para informar con la misma eficacia a los titulares de los datos.
- Informar al titular afectaría un interés público sustancial y socavaría la viabilidad de las operaciones del controlador de datos.
- Dadas las condiciones de seguridad imperantes, ponerse en contacto con el titular de los datos podría ponerlo en peligro o causarle un sufrimiento grave.

Si el controlador de datos considera necesario notificar al titular de los datos, deberá seleccionar y utilizar el mejor canal de comunicación para que el titular reciba la información de la manera más adecuada para la situación.

# 3. Derechos de los titulares de los datos

### *3.1 Información y acceso*

**Información:** el controlador de los datos está obligado a proporcionar información transparente a su titular. Ese es un principio básico que se aplicará independientemente del fundamento jurídico del procesamiento de los datos. En virtud de dicho principio, al obtener datos personales o lo antes posible después de hacerlo, el controlador deberá brindar al titular, si las restricciones logísticas y de seguridad lo permiten, información sobre el procesamiento de esos datos, verbalmente o por escrito.

El titular de los datos debe recibir explicaciones en un lenguaje fácil de entender, ya sea en forma verbal o por otro medio adecuado, como una notificación por escrito. Como mínimo, se le debe proporcionar la siguiente información:

- la identidad y los datos de contacto del controlador o los controladores de los datos;
- el propósito específico con el que se procesan los datos;
- el hecho de que el controlador de datos puede procesar los datos personales con fines distintos de los que se especificaron en el momento de su obtención, siempre que sean compatibles con el fin específico mencionado;
- el derecho del titular de los datos a acceder a ellos, corregirlos o eliminarlos, así como a retirar su consentimiento, objetar el procesamiento o insistir en determinadas limitaciones;
- una estimación del período durante el que se conservarán los registros (el período de retención de los datos) y los criterios que se usarán para determinarlo;
- el hecho de que los datos personales pueden transmitirse a terceros, como otras organizaciones (por ejemplo, otros componentes del Movimiento) o las autoridades estatales del país donde se obtienen los datos o de otros países, o bien divulgarse públicamente, para todo lo cual se requiere autorización del titular.

Debe respetarse la legislación nacional aplicable, que puede exigir a las Sociedades Nacionales incluir información adicional para el titular de los datos.

**Acceso:** los titulares de los datos tienen derecho a que se les confirme, en cualquier momento en que lo soliciten, si en ese momento se están procesando sus datos personales. Cuando así sea, podrán acceder a ellos y a información sobre los fines de ese procesamiento, las personas que tienen acceso a sus datos personales y las medidas de seguridad adoptadas.

Si lo solicitan y es técnicamente factible, se les facilitará una copia de los documentos que contengan sus datos personales.

Antes de otorgar acceso, el controlador de datos deberá evaluar la viabilidad de la solicitud de acceso y la identidad de la persona que lo solicita. Los siguientes son motivos para restringir el acceso a los datos:

- un interés público superior, como la confidencialidad;
- los intereses de protección de los datos, y los derechos y libertades de otras personas;
- los documentos en cuestión no pueden sufrir modificaciones significativas por razones de seguridad y situaciones de emergencia;
- la solicitud es manifiestamente infundada o excesiva.

El controlador de datos mantendrá un registro de las solicitudes de acceso y del resultado de cada una de ellas, incluidas las categorías de los datos personales a los que se haya accedido y las negativas de acceso a la información.

### *3.2 Divulgación a familiares o tutores*

Un familiar o tutor de un niño, niña u otro titular de datos en situación de vulnerabilidad puede solicitar acceso a sus datos personales. Por lo general, se presume que la solicitud se realiza en favor de los intereses del titular y, por lo tanto, debe aceptarse, salvo que haya razones suficientes para suponer lo contrario. Deberá consultarse siempre que sea posible al titular de los datos, para establecer si tiene alguna objeción a esa divulgación.

### *3.3 Rectificación y eliminación*

**Rectificación**: cuando se solicita rectificar datos personales, antes que nada, el controlador de datos debe identificar a la persona que presenta la solicitud y determinar la viabilidad de aceptarla. Luego, responderá a la solicitud, en particular cuando los datos sean incorrectos o estén incompletos, incluso si se trata de datos archivados. El controlador comunicará las rectificaciones realizadas a los destinatarios de esos datos personales, a menos que la rectificación no sea significativa o que su comunicación requiera un esfuerzo desproporcionado.

**Eliminación**: el titular de los datos tiene derecho a que se eliminen sus datos personales de las bases de datos activas del controlador de datos en cualquiera de los casos siguientes:

- cuando ya no se necesiten para el fin con el cual se obtuvieron ni para un procesamiento adicional;

- cuando el titular de los datos haya retirado su consentimiento para el procesamiento y no haya ningún otro fundamento para procesar sus datos personales;
- cuando el titular objete el procesamiento de sus datos personales;
- cuando el procesamiento de los datos personales del titular incumpla en algún otro sentido este Código o la legislación nacional aplicable a las Sociedades Nacionales.

Si los datos personales se han publicado, el controlador debe tomar medidas razonables —por ejemplo, de orden técnico— para eliminarlos del dominio público, tanto en su versión original como de cualquier enlace o copia que pudiera existir.

Sin embargo, pueden conservarse los datos personales de un titular cuando eso resulte necesario o justificado, como en las siguientes circunstancias:

- con fines históricos, estadísticos y científicos; por ejemplo, para documentar las medidas adoptadas por un controlador de datos en cumplimiento del cometido encomendado por los Convenios de Ginebra de 1949, sus Protocolos adicionales o los Estatutos del Movimiento;
- por razones de interés público;
- con fines humanitarios a largo plazo;
- para plantear, ejercer o defender un reclamo jurídico;
- con miras a la publicación por parte de cualquier persona de material periodístico, literario o artístico, en ejercicio del derecho a la libertad de expresión y de información.

También se permitirá conservar los datos personales de un titular cuando la ley la requiera. El controlador de datos documentará todas las solicitudes, y se notificará a los titulares de los datos correspondientes la decisión adoptada en cada caso.

Cuando los controladores de datos reciban una solicitud de eliminar datos personales, deberán explicar al titular las consecuencias de esa eliminación para la prestación de servicios de RCF. El controlador de datos se reserva el derecho a rechazar una solicitud de rectificación o eliminación por parte del titular de los datos si considera que esa solicitud puede haberse hecho bajo presión ilegítima o en el caso de que una eliminación pueda ser perjudicial para los intereses vitales del titular de los datos.

En caso de que los datos personales eliminados se hayan transmitido a otras entidades, el controlador de datos les comunicará la eliminación y les pedirá que supriman cualquier enlace a ellos o copia de los que dispongan, a menos que los datos eliminados no sean significativos o que esa comunicación requiera un esfuerzo desproporcionado. Si los destinatarios son miembros de la Red de Vínculos Familiares, informarán lo antes posible al controlador de datos de la decisión tomada sobre la eliminación de los datos.

### *3.4 Objeción al procesamiento*

El titular de los datos tiene derecho a objetar, en cualquier momento, el procesamiento de sus datos personales si el fundamento jurídico de dicho procesamiento es el interés público o el interés legítimo del controlador de datos. Los datos personales en cuestión dejarán de procesarse, a menos que el controlador de datos demuestre razones legítimas superiores para que continúe el procesamiento.

El controlador de datos informará a los destinatarios, de haberlos, de la objeción.

### *3.5 Derecho a retirar el consentimiento*

Cuando el fundamento jurídico para procesar los datos personales es el consentimiento, el titular de los datos tiene derecho a retirar su consentimiento cuando lo desee. Si eso ocurre, el controlador de datos debe tomar todas las medidas razonables para detener el procesamiento y eliminar los datos en cuestión. Si los datos se transfirieron a terceros, el controlador de datos debe informar a esas entidades que el titular de los datos ha retirado su consentimiento, para que estas puedan también proceder a la eliminación correspondiente.

### *3.6 Reparaciones*

El titular de los datos deberá enviar su solicitud al controlador de datos, que deberá responderla en un plazo razonable y, en todo caso, en el plazo que establezca la ley.

La persona que reciba una solicitud de un titular de datos corroborará la identidad de este por medio de cualquier método razonable y tomará una de las siguientes medidas:

- aprobar la solicitud, y notificar al solicitante cómo se ha cumplido o va a cumplirse;
- informar al solicitante por qué no puede cumplirse o no va a cumplirse la solicitud, así como que dispone de la posibilidad de presentar un reclamo contra el controlador de datos.

## 4. Disposiciones especiales sobre transferencias de datos

### *4.1 Principios generales*

#### 4.1.1 Antecedentes

En el marco de las actividades de RCF y afines, suelen realizarse transferencias transfronterizas de datos personales entre distintos controladores de datos.

En ocasiones, los controladores de datos también precisan transferir datos personales a entidades como organizaciones no gubernamentales (ONG), organizaciones internacionales, autoridades públicas y otras terceras partes cuyos servicios son necesarios para llevar adelante actividades de RCF y afines.

Esas transferencias se realizan de acuerdo con las actividades de la Red de Vínculos Familiares, según se explica en la Sección 1.3: hay que informar debidamente al titular de los datos cuando se lleva a cabo una transferencia, y esta debe tener un fundamento jurídico, es decir, ser de interés público, proteger los intereses vitales del titular de los datos u otras personas, o contar con el consentimiento del titular. Además, las transferencias deben respetar los principios y las directrices del Movimiento expuestas en la sección 1.4.

### 4.1.2 Principios generales aplicables a las transferencias de datos

Toda transferencia de datos dentro o fuera del Movimiento constituye una operación de procesamiento. Por lo tanto, las transferencias están sujetas a los principios básicos expuestos en el capítulo 2 y a los derechos de los titulares de los datos expuestos en el capítulo 3. Sin embargo, las transferencias son una operación de procesamiento especialmente delicada, por lo que algunos de los requisitos revisten particular importancia, como las evaluaciones de impacto relativas a la protección de los datos, la información que se brinda al titular de los datos y la seguridad de los datos.

Como se menciona en la sección 3.1, debe informarse al titular de toda transferencia previsible de sus datos personales a terceros antes de su obtención o en el momento de obtenerlos.

Para transferir datos personales a personas o instituciones, deben adoptarse protecciones adecuadas y proporcionales, entre ellas las mencionadas en las secciones 4.1.4 y 4.1.6, así como medidas de seguridad técnicas y organizacionales, entre ellas las enumeradas en el anexo 3. Debe tomarse en cuenta la sensibilidad de los datos, la urgencia de la acción humanitaria, y las restricciones logísticas y de seguridad, como detalla este Código, y siempre debe respetarse el principio de no causar daño.

### 4.1.3 Evaluación del impacto de la protección de datos para las transferencias de datos

El requisito de llevar a cabo una evaluación de impacto relativa a la protección de los datos es especialmente importante en el contexto de las transferencias de datos. Por ello, cuando sea probable que la transferencia de datos presente riesgos considerables para los derechos y las libertades de sus titulares, el controlador llevará a cabo una evaluación de este tipo (ver orientaciones en el anexo 6) antes de realizar la transferencia, según se establece en la sección 2.3.4. La evaluación de impacto tomará en consideración los siguientes elementos:

- la legislación y normativa nacionales sobre protección de datos que rigen la transferencia de datos;
- la situación de seguridad, el respeto de los derechos humanos y el DIH, y la protección de los titulares de los datos en el país;
- si bastará con datos anónimos o agregados, o si es necesario transferir datos que permitan al controlador de datos identificar a su titular;
- los medios y condiciones de la transferencia de datos;
- la posibilidad de implementar una obligación contractual para evitar que un tercero transfiera posteriormente los datos a otros terceros (transferencias ulteriores);
- el grado de vulnerabilidad del titular de los datos, ya que puede ser necesario adoptar protecciones adicionales para preservar la confidencialidad y el anonimato.

En cualquier caso, el controlador de datos no debe proceder con una transferencia de datos cuando es probable que esta perjudique de alguna manera al titular.

### 4.1.4 Condiciones

Las transferencias de datos están sujetas a las siguientes condiciones acumulativas:

- Se debe realizar una evaluación de impacto relativa a la protección de los datos con antelación a la transferencia, si es probable que esta implique riesgos considerables para el titular de los datos.
- El destinatario de la transferencia debe procesar los datos de acuerdo con los motivos especificados para el procesamiento y cualquier propósito compatible.
- El destinatario recibirá únicamente los datos del tipo y en la cantidad necesarios para los propósitos especificados o a efectos del procesamiento adicional previsto.
- La transferencia debe ser compatible con las expectativas razonables del titular de los datos.

El controlador de datos evaluará los riesgos que implica transferir ciertos datos personales a determinadas organizaciones para asegurar que se respete el principio de no causar daño.

#### 4.1.5 Documentación de las transferencias de datos

El controlador de datos deberá mantener registros de las transferencias, los métodos de transferencia y los destinatarios de datos personales.

#### 4.1.6 Acuerdos de intercambio de datos

Como se establece en la Sección 4.1.2, pueden transferirse datos personales si el controlador de datos considera que las medidas de seguridad garantizan la protección de los datos personales por parte del destinatario. Esas medidas de seguridad adecuadas pueden establecerse mediante acuerdos de intercambio de datos entre controladores de datos y terceros cuando se contemple realizar transferencias periódicas. Los acuerdos deben disponer con toda claridad que los datos personales se transferirán únicamente con los propósitos contemplados y a los efectos de cualquier otro propósito adicional compatible. También deben disponer las medidas técnicas y organizacionales que han de adoptarse para proteger los datos durante el procesamiento.

Las transferencias de datos personales dentro del Movimiento no requieren un acuerdo de intercambio de datos, porque los componentes del Movimiento se atendrán a lo estipulado en este Código.

El/la referente de protección de los datos de RCF debe participar en la redacción de esos acuerdos o de instrumentos jurídicos equivalentes.

Incluso cuando las partes firmen un acuerdo, el contexto operacional puede sufrir cambios a raíz de los que deje de considerarse seguro transferir determinadas categorías de datos a ciertos destinatarios. En ese caso, se realizará una evaluación previa sobre la base del principio de no causar daño.

### *4.2 Métodos de transmisión*

En caso de que se produzca una transferencia de datos personales a terceros, se adoptarán medidas adecuadas para garantizar la seguridad. El nivel de seguridad establecido y el método de transmisión deberán ser proporcionales a la naturaleza y la sensibilidad de los datos personales, así como a los riesgos que señale la evaluación de impacto.

# 5. Disposiciones especiales sobre la publicación de datos

## *5.1 Principios generales*

La publicación de datos personales por parte del controlador constituye una operación de procesamiento. Como tal, está sujeta a los principios generales expuestos en el capítulo 2 y a los derechos de los titulares de los datos expuestos en el capítulo 3. Sin embargo, la publicación es una operación de procesamiento especialmente delicada. Una vez que se publican datos personales, el controlador de los datos y el titular pierden en gran medida la capacidad de controlar cómo se procesan. Por ello, deben seguirse también los principios adicionales que se establecen en este capítulo.

En función de los resultados de la evaluación de impacto relativa a la protección de los datos, así como los de las obligaciones jurídicas aplicables, los servicios de RCF del controlador de datos pueden publicar datos personales para restablecer el contacto entre familiares separados por conflictos armados y otras situaciones de violencia, desastres naturales y migración. Los datos pueden ser nombres, fotografías, situaciones (que alguien está con vida, herido, fallecido, desaparecido o desplazado), etc., y publicarse en internet, en los medios de comunicación, en afiches, en folletos o por otras vías.

Como se explica en la sección 2.2.1, el interés público es el fundamento jurídico más utilizado para la publicación de datos personales.

## *5.2 Evaluación de impacto relativa a la protección de datos con miras a su publicación*

El requisito de realizar una evaluación de impacto relativa a la protección de los datos, como se establece en la sección 2.3.4 y en el anexo 6, es de particular importancia en el contexto de la publicación de datos.

Además de los puntos mencionados en la sección 2.3.4, en el contexto de la publicación, las evaluaciones de impacto relativas a la protección de los datos deben tomar en cuenta los siguientes elementos:

- la legislación y normativa nacionales sobre protección de datos que rigen la publicación de datos;
- la situación de seguridad, el respeto de los derechos humanos y el DIH, y la protección de los titulares de los datos en el país;
- si bastará con datos anónimos o agregados, o si es necesario publicar datos que permitan al controlador de datos identificar a su titular, y, en ese caso, si otros medios de protección de la identidad del titular de los datos (como no asociar una fotografía con ningún nombre, característica distintiva, ubicación precisa, etc.) facilitarán u obstaculizarán el propósito con el que se los publica;
- el método y las condiciones de publicación;
- la posibilidad de implementar un requisito para impedir que los datos que se publiquen sean utilizados por terceros;

- la posibilidad de especificar el período durante el cual pueden quedar publicados ciertos datos en una plataforma determinada y el método de destrucción que debe utilizarse una vez cumplido el propósito de su publicación;
- cuán útil y adecuada es la publicación, por medio de evaluaciones periódicas del controlador de datos;
- la importancia de proteger a las personas vulnerables de la curiosidad del público en el contexto de la comunicación pública.

Si el titular de los datos es una persona en situación de vulnerabilidad, cuando corresponda, deberán tenerse en cuenta consideraciones adicionales, como medidas de protección suplementarias para proteger la confidencialidad y el anonimato. Respetar el principio de no causar daño es la mejor manera de proteger a los titulares de datos.

### *5.3 Publicación de datos para RCF*

Si van a publicarse datos, la publicación debe seguir las pautas establecidas para cada contexto concreto, y puede haber orientación más específica en relación con ciertas categorías de titulares de datos. En función de los resultados de la evaluación de impacto, pueden tomarse, entre otras, las siguientes medidas de mitigación específicas:

- adoptar el enfoque de no causar daño;
- limitar la publicación a los datos imprescindibles para que los familiares identifiquen a la persona cuyo nombre o fotografía se publica, y puedan ponerse en contacto con ella nuevamente;
- prohibir que se publiquen fotografías de personas vulnerables junto con otros datos personales (por ejemplo, su nombre), así como la dirección de una persona menor de edad.

### *5.4 Publicación de datos para archivos públicos*

Los datos personales archivados pueden hacerse públicos en cumplimiento de la legislación correspondiente.

### *5.5 Publicación de datos para comunicación pública*

Pueden publicarse datos personales con el fin de promocionar las actividades de RCF o de sensibilizar a la población sobre situaciones preocupantes, siempre y cuando se cumpla la legislación pertinente. Cuando se publican datos con ese propósito, antes que nada, el controlador de datos debe obtener el consentimiento de la persona que presenta la solicitud de búsqueda. La comunicación pública también está vinculada con la libertad de información y de expresión, así como con la rendición de cuentas pública. Sin embargo, como ocurre con cualquier publicación, hay que respetar los principios que se establecen en este Código y realizar una evaluación de impacto relativa a la protección de los datos.

# 6. Aplicación del Código de Conducta

Un grupo de aplicación del Código de Conducta ayudará a poner en práctica este Código en todo el mundo promoviendo el aprendizaje y el desarrollo continuos.

Además de estar sujetos a la legislación nacional, todos los controladores de datos deberán aplicar el presente Código por las siguientes vías:

- corroborar que el Código se refleje en las políticas, directrices y programas de RCF;
- procurar que el Código se incorpore en la gestión de personal de RCF y se utilice como herramienta de formación de todos los controladores de datos;
- designar un referente de protección de los datos de RCF en cada una de las organizaciones que formen parte de la Red de Vínculos Familiares, y difundir sus datos de contacto para conformar una red de protección de los datos;
- participar en encuestas periódicas sobre la puesta en práctica de este Código;
- cooperar con el grupo de aplicación del Código;
- realizar autoevaluaciones, participar en diálogos, practicar la revisión por pares y de otros tipos de revisión voluntaria con miras a la mejora y el aprendizaje continuos en el Movimiento.

El grupo de aplicación del Código revisará y actualizará el texto cuando sea necesario.

# 7. Referencias

### *7.1 Orientación e instrumentos jurídicos*

Asamblea General de las Naciones Unidas, *Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales*, 14 de diciembre de 1990.

*Pacto Internacional de Derechos Civiles y Políticos*, art. 17.

Rallo Lombarte, A., *Estándares internacionales sobre protección de datos personales y privacidad*: *Resolución de Madrid: Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*, *5 de noviembre de 2009*, Agencia Española de Protección de Datos, Madrid, 2009.

Consejo de Europa, *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal*, 108, 28 de enero de 1981, BRON.

Parlamento Europeo y Consejo de Europa, *Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, 24 de octubre de 1995, OJ L 281 23 de noviembre de 1995, pp. 31-50.

Unión Europea, *Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales*, art. 8.

Unión Europea, *Tratado de Funcionamiento de la Unión Europea*, art. 16.

Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento Europeo, *Carta de los Derechos Fundamentales de la Unión Europea*, art. 7 y 8.

Organización para la Cooperación y el Desarrollo Económico (OCDE), *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales,* Publicaciones OCDE, París, 2002.

OCDE, *Directrices para la protección de los consumidores en el contexto del comercio electrónico*, Publicaciones OCDE, París, 2000.

Foro de Cooperación Económica Asia-Pacífico (APEC), *Marco de Privacidad*, Secretaría del APEC, Singapur, 2005.

Estatutos del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, en su versión enmendada de 2006.

CICR, *resolución 4 del Consejo de Delegados celebrado en 2007 sobre la Estrategia para el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja relativa al Restablecimiento del Contacto entre Familiares*, CICR, Ginebra, 2007.

37.° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, *resolución sobre privacidad y acción internacional humanitaria*, Ámsterdam, 2015.

XXXIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, resolución 4, *Restablecimiento del contacto entre familiares en un marco de respeto de la privacidad, incluso en materia de protección de los datos personales,* 33IC/19/R4, CICR, Ginebra, 2019.

Consejo de Delegados del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, resolución 12, *Salvaguardar los datos humanitarios*, CD/22/R12, CICR, Ginebra, 2022.

### *7.2 Doctrina*

*CICR, El restablecimiento del contacto entre familiares en casos de catástrofe: Manual para el terreno*, CICR, Ginebra, 2009.

CICR, *Evaluación de las necesidades en materia de restablecimiento del contacto entre familiares: Manual para las Sociedades Nacionales y el CICR*, CICR, Ginebra, 2010.

ICRC, *Directrices sobre la prestación de servicios de restablecimiento del contacto entre familiares a personas separadas como consecuencia de la migración: Documento interno para el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja*, CICR, Ginebra, 2010.

CICR, *Restablecimiento del contacto entre familiares: Estrategia para el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (2020-2025) y base jurídica*, CICR, Ginebra, 2009.

Morgan, O., Tidball-binz, M., van Alphen, D. (ed.), *La gestión de cadáveres en situaciones de desastre:* guía práctica para equipos de respuesta, Organización Panamericana de la Salud, Washington, D.C., 2009.

# Anexos

## *Anexo 1: actividades de RCF y afines*

**Actividades de RCF**. Según la situación y el contexto, pueden realizarse distintos tipos de actividades:

- organización de intercambios de noticias entre familiares;
- búsqueda de personas;
- registro de datos de personas (niños o adultos) y seguimiento de sus casos para evitar su desaparición e informar a sus familiares de su paradero;
- reunión de familiares y repatriación de personas;
- obtención, gestión y envío de información sobre los fallecidos;
- transmisión de documentos oficiales, como partidas de nacimiento, documentos de identidad u otros certificados emitidos por las autoridades;
- emisión de certificados de detención y otros documentos que informen sobre la situación de personas incluidas en un registro;
- emisión de documentos de viaje del CICR;
- seguimiento de las personas reunidas con sus familiares para verificar que estén readaptándose bien;
- promoción y apoyo de mecanismos para averiguar lo sucedido a las personas desaparecidas.

**Actividades asociadas a RCF.** Otros servicios humanitarios relacionados con las actividades de Restablecimiento del contacto entre familiares, que lleva adelante el equipo de RCF, como las siguientes:

- prestación de apoyo material, psicológico y psicosocial para los familiares de personas desaparecidas y otras personas afectadas por conflictos armados, otras situaciones de violencia, desastres naturales, migraciones y otras crisis humanitarias;
- apoyo a las autoridades pertinentes para la gestión de restos humanos y las tareas de identificación forense;
- acompañamiento para familiares de personas desaparecidas, menores no acompañados y personas en situación de vulnerabilidad (ya sea directamente desde la Red de Vínculos Familiares o a través de la derivación a terceros);
- prestación de servicios de restablecimiento o (derivación a) servicios de apoyo para la reinserción de grupos de personas en situación de vulnerabilidad;
- archivo para diversas necesidades, como memorias individuales o familiares; memorias colectivas de la humanidad; necesidades administrativas individuales, rendición de cuentas de las partes en los conflictos, investigación histórica, estadística y médica;
- gestión de las relaciones públicas para promover las actividades de RCF y las actividades asociadas.

## *Anexo 2: fundamentos jurídicos*

**a. Interés público**

Se toma el interés público como fundamento jurídico en los siguientes casos:

- Crisis a gran escala que requieren acción inmediata, cuando el titular de los datos está en condiciones de entender la información que se le proporciona y reaccionar al intercambio o publicación de sus datos personales.
- Cuando las operaciones de procesamiento son muy complejas y requieren tecnologías complejas y la participación de procesadores externos, lo que dificulta a los titulares de los datos entender cabalmente los riesgos y los beneficios de las medidas de procesamiento necesarias. Si no se pueden establecer los intereses vitales del titular de los datos o de otra persona (por falta de urgencia), el procesamiento puede producirse sobre la base del cometido encomendado al controlador de datos, siempre y cuando se lleve a cabo una evaluación de impacto satisfactoria sobre la protección de los datos.
- Cuando se distribuye asistencia y no es posible obtener el consentimiento de todos los beneficiarios, y es poco probable que esté en juego la vida y la integridad del titular de los datos (en cuyo caso, el fundamento más adecuado para el procesamiento sería el interés vital).
- Cuando se procesan los datos personales de un titular en detención: por ejemplo, cuando una persona se ve privada de libertad a raíz de un conflicto armado u otra situación de violencia, y el CICR (o una Sociedad Nacional) aún no ha conseguido visitarla para obtener su consentimiento, y las condiciones de detención en el caso en cuestión podrían impedir el uso del interés vital como fundamento jurídico.
- Cuando se procesan los datos personales de menores no acompañados que carecen de la capacidad jurídica de otorgar un consentimiento válido, y cuando no se cumplen las condiciones que darían lugar al uso del interés vital como fundamento jurídico.

**b. Interés vital**

Se toma el interés vital como fundamento jurídico en los siguientes casos:

- En situaciones de emergencia en las que la persona que busca a un ser querido desaparecido no está en condiciones físicas o psicológicas de indicar su parecer sobre el uso de sus datos personales por parte del CICR o la Sociedad Nacional.
- Cuando la prestación de servicios de RCF es necesaria para proteger la vida, la integridad, la salud o la dignidad de los beneficiarios.

**c. Interés legítimo**

Se toma el interés legítimo como fundamento jurídico cuando es necesario procesar datos personales para los siguientes fines:

- Preservar la seguridad de los sistemas informáticos y los servicios asociados que se ofrecen o a los que se accede por medio de ellos, las autoridades públicas, los equipos de respuesta ante emergencias informáticas, los equipos de respuesta ante incidentes de seguridad informática, los prestadores de redes y servicios electrónicos de comunicación, y los prestadores de tecnologías y servicios de seguridad. Por ejemplo, evitar el acceso no autorizado a redes electrónicas de comunicación, ataques y daños a equipos informáticos y

sistemas electrónicos de comunicación mediante el uso de códigos maliciosos y denegación de servicios, o bien procesar los datos al mismo tiempo que se analizan los sistemas informáticos en busca de virus.
- Prevenir y brindar pruebas de las situaciones de fraude o robo, por ejemplo, verificando la identidad de los beneficiarios cuando solicitan ejercer sus derechos.
- Anonimizar o pseudoanonimizar los datos.
- Plantear, ejercer o defender demandas jurídicas, más allá de si se trata de un procedimiento judicial, administrativo o que no requiere acudir a los tribunales, o una campaña de marketing directo o de relaciones públicas. Un ejemplo sería la necesidad de defender la demanda jurídica de un beneficiario.
- Realizar un seguimiento interno de las capacidades de RCF, evaluando la eficacia de las respuestas y el apoyo que proporcionan los equipos, y llevando a cabo ejercicios de "lecciones aprendidas".

**d. Cumplimiento de una obligación jurídica**

Según las circunstancias del controlador de datos, el cumplimiento de una obligación jurídica puede incluir:

- el cumplimiento de la legislación nacional o regional: por ejemplo, en el ámbito del derecho laboral, los informes financieros, el fraude, el lavado de dinero, etc.;
- las órdenes judiciales.

## *Anexo 3: seguridad de los datos*

Los datos personales se deben procesar de manera que mantenga su confidencialidad, integridad y disponibilidad. Eso incluye la prevención del acceso o uso no autorizados de los datos y de los equipos que se emplean para procesarlos.

Quienquiera que actúe bajo la autoridad del controlador de datos y que tenga acceso a datos personales deberá procesarlos en cumplimiento de este Código y de la política aplicable en materia de seguridad de los datos, como se explica con más detalle en este anexo.

Para proteger los datos e impedir procesamientos que violen este Código, el controlador deberá evaluar los riesgos específicos inherentes a su procesamiento y adoptar medidas para mitigarlos. Esa evaluación debe llevarse a cabo en estrecha colaboración con el equipo de seguridad o tecnología de la información, de haberlo, o con consultores externos, de ser posible. Las medidas deben garantizar un grado suficiente de seguridad —en función de la tecnología disponible, las condiciones logísticas y de seguridad imperantes, y los costos de implementarlas— en relación con los riesgos y la índole de los datos personales que se busca proteger. Por ejemplo:

- formación;
- gestión de derechos de acceso a bases de datos que contienen datos personales;
- seguridad física de las bases de datos;
- seguridad informática;
- clasificación de datos;

- cláusulas de discreción;
- métodos de destrucción de datos personales;
- cualquier otra medida pertinente.

El objetivo de estas medidas es garantizar la seguridad de los datos personales en los planos tanto técnico como organizativo, y su protección contra toda modificación, copia o manipulación no autorizada, destrucción ilegal, pérdida accidental, divulgación o transferencia indebida.

Las medidas relacionadas con la seguridad de los datos pueden variar en función de diversos factores, entre ellos:

- el tipo de operación;
- el carácter y el grado de sensibilidad de los datos personales en cuestión;
- la forma o el formato en los que se almacenen los datos;
- el entorno o lugar donde se encuentren los datos personales;
- las condiciones logísticas y de seguridad imperantes.

Las medidas de seguridad adoptadas deben revisarse y mejorarse periódicamente para que el nivel de protección sea congruente con el grado de sensibilidad de los datos personales.

El controlador de datos es responsable de lo siguiente:

- Implementar un sistema de gestión de la seguridad informática. Para eso, deberá establecer y actualizar periódicamente una política de seguridad de los datos basada en normas que cuenten con aceptación internacional, así como en una evaluación de riesgos. Esa política deberá consistir, por ejemplo, en pautas de seguridad física, una política de seguridad informática y pautas para el uso del correo electrónico, pautas de uso de los equipos de tecnología de gestión de la información, la tipología de gestión de la información, un plan de contingencia y pautas para la destrucción de documentos.
- Utilizar procedimientos y las herramientas digitales que ofrece la ACB para el intercambio de datos personales dentro de la Red en la mayor medida posible.
- Establecer una infraestructura de comunicación y de bases de datos para preservar la integridad y la confidencialidad de los datos, en cumplimiento de la política de seguridad.
- Tomar, de acuerdo con el presente Código, todas las medidas adecuadas para proteger la seguridad de los datos procesados en el sistema de información del controlador de datos.

**1. Derechos de acceso a bases de datos**

El controlador de datos es responsable de lo siguiente:

- otorgar acceso a bases de datos que contengan datos personales;
- preservar la seguridad de las herramientas que permiten al personal autorizado acceder a las bases de datos;
- respetar las normas de seguridad expuestas en este anexo;
- verificar que el personal autorizado a acceder a los datos esté en condiciones de cumplir con este Código, lo que incluye ofrecer formación y corroborar que haya una cláusula de confidencialidad en su contrato de trabajo, así como que este se haya firmado;
- otorgar acceso solo en caso de necesidad;

- llevar un registro de los miembros del personal que tienen acceso a cada base de datos y actualizarlo cuando corresponda, por ejemplo, cuando una persona cambia de función y deja de necesitar acceso;
- si es factible, llevar un registro histórico del personal que haya tenido acceso a cada una de las bases de datos mientras permanezcan allí los datos procesados por esos miembros del personal, a efectos de la rendición de cuentas.

Cada miembro del personal deberá procesar los datos dentro de los límites de los derechos de procesamiento que se le hayan otorgado.

Los empleados con derechos de acceso más amplios o encargados de gestionar derechos de acceso pueden estar sujetos a obligaciones contractuales adicionales en lo que respecta a la confidencialidad.

**2. Seguridad física**

El controlador de datos es responsable de lo siguiente:

- establecer normas de seguridad que impongan controles técnicos, administrativos y de procedimiento para mantener la confidencialidad, la integridad y la disponibilidad de las bases de datos (ya sean físicas o informáticas)[9];
- verificar que el personal conozca y respete estas normas de seguridad;
- corroborar que el personal no autorizado no pueda acceder a los lugares de almacenamiento;
- adoptar mecanismos de control adecuados para salvaguardar los datos;
- verificar que se implementen estándares adecuados de seguridad eléctrica y contra incendios en los lugares de almacenamiento;
- procurar que los volúmenes almacenados sean los mínimos necesarios.

**3. Seguridad informática**

El controlador de datos es responsable de lo siguiente:

- establecer normas de seguridad que impongan controles técnicos, administrativos y de procedimiento para mantener la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos utilizados;
- adoptar mecanismos de control adecuados para salvaguardar los datos;
- de considerarse necesario, establecer normas de seguridad específicas para cierta parte de la infraestructura de comunicación informática, cierta base de datos o un departamento específico.

Toda correspondencia por correo electrónico, interna o externa, que contenga datos personales deberá procesarse solo en la medida en que sea necesario. Los destinatarios de los correos electrónicos deberán seleccionarse cuidadosamente para evitar una divulgación innecesaria de datos

[9] Por ejemplo, bloquear la computadora antes de alejarse del escritorio, no dejar documentos sensibles en la impresora por mucho tiempo, no dejar contraseñas a la vista.

personales. No deben utilizarse cuentas de correo electrónico privadas para transferir datos personales a menos que sean el único medio disponible en una situación de emergencia.

Cuando se acceda en forma remota a los servidores y se haga un uso laboral de dispositivos personales, debe ser en cumplimiento de los estándares de seguridad que se establecen en la política de seguridad informática del controlador de datos. A menos que sea absolutamente necesario por razones operacionales, debe evitarse el uso de tomas coaxiales y conexiones inalámbricas no seguras para obtener, intercambiar, transmitir o transferir datos personales.

El personal encargado de la gestión de datos personales debe adoptar las precauciones necesarias al establecer conexiones remotas con los servidores del controlador de datos. Las contraseñas deben estar siempre protegidas, y los empleados deben verificar que hayan finalizado correctamente la sesión en los sistemas informáticos y cerrado todos sus navegadores.

Las computadoras portátiles, los teléfonos inteligentes y demás equipos portátiles requieren precauciones de seguridad especiales, sobre todo cuando se trabaja en entornos difíciles. Los equipos portátiles deben guardarse en todo momento en lugares seguros y protegidos.

No deben guardarse datos personales relacionados con los beneficiarios en el almacenamiento local de los dispositivos a menos que no haya alternativa (por ejemplo, si no es posible acceder a las plataformas autorizadas de gestión y almacenamiento de documentos[10]) o que se trate de una situación de emergencia. En esos casos, la información debe eliminarse del dispositivo en cuanto haya cumplido su propósito.

No deben utilizarse dispositivos portátiles o extraíbles para almacenar documentos que contengan datos personales clasificados como especialmente sensibles. Si fuera inevitable hacerlo, los datos personales deberán transferirse cuanto antes a sistemas informáticos y aplicaciones de bases de datos adecuados. Si se utilizan dispositivos como memorias USB y tarjetas de memoria para almacenar temporalmente datos personales, esos dispositivos deben estar protegidos y sus registros electrónicos deben cifrarse. Asimismo, debe eliminarse la información del dispositivo portátil o extraíble en cuanto se haya almacenado correctamente y haya dejado de ser necesario conservarla en el dispositivo en cuestión.

Se deben implementar procedimientos eficaces de recuperación y respaldo para todos los registros electrónicos, y el responsable de tecnología de la información y las comunicaciones (TIC) que corresponda debe corroborar que se hagan copias de respaldo periódicamente. Cuando se trate de datos sensibles, las copias de respaldo deben realizarse con más frecuencia. En situaciones en las que sea difícil aplicar procedimientos de respaldo —por ejemplo, allí donde sean habituales los cortes de energía, las fallas del sistema o los desastres naturales—, se deben automatizar los registros electrónicos para facilitar la recuperación.

Cuando los registros electrónicos y las aplicaciones de bases de datos dejan de ser necesarios, el controlador de datos debe coordinar su eliminación definitiva con el responsable pertinente de TIC.

**4. Deber de confidencialidad y conducta del personal**

El deber de confidencialidad es un elemento central de la seguridad de los datos personales que incluye las siguientes condiciones:

[10] Por ejemplo, la herramienta Family Links Answers.

- Todo el personal y los consultores externos deben firmar acuerdos de confidencialidad[11] en el marco de su contrato laboral o de servicios de consultoría. Este requisito se suma al de que los empleados procesen datos únicamente de acuerdo con las instrucciones del controlador de datos.
- Todos los procesadores externos deben firmar contratos que contengan cláusulas de confidencialidad. Este requisito se suma al de que solo se procesen datos de acuerdo con las instrucciones del controlador de datos.
- Todos los empleados y procesadores externos deben aplicar correctamente la tipología de gestión de la información de acuerdo con su estatus de confidencialidad.
- Toda solicitud que haga un titular con respecto al modo de procesar sus datos personales debe quedar correctamente registrada en el expediente del titular de los datos, más aún si la persona desea que sus datos sean confidenciales y no se compartan con terceros.

A fin de limitar el riesgo de que se vulneren los datos, solo el personal autorizado se encargará de obtener y gestionar los datos de fuentes confidenciales, así como de acceder a la documentación según la tipología de gestión de la información, que clasifica toda la información en términos de su grado de confidencialidad (pública, interna, confidencial o estrictamente confidencial).

Los empleados deben aplicar la tipología de gestión de la información para atribuir grados de confidencialidad a los datos que procesan, y consultar, transmitir y usar los datos en función del grado de confidencialidad correspondiente.

El grado de confidencialidad atribuido puede modificarse en cualquier momento; por ejemplo, puede reducirse si se considera que los datos ya no requieren tanta protección como en un principio.

**5. Planificación de contingencia**

El controlador de datos es responsable de formular y poner en práctica un plan de evacuación de los registros en caso de emergencia.

**6. Métodos de destrucción de datos**

Cuando se determina que deja de ser necesario tener almacenados ciertos datos personales, deben destruirse o anonimizarse todos sus registros y copias de respaldo.

El método de destrucción que se utilice dependerá principalmente de los siguientes factores:

- la índole de los datos personales y su grado de sensibilidad;
- el formato y el medio en los que se los almacena;
- el volumen de registros electrónicos o en papel.

El controlador deberá evaluar la sensibilidad de los datos antes de destruirlos, a fin de utilizar técnicas adecuadas para su eliminación.

a. Destrucción de registros en papel

Los registros en papel deben destruirse por métodos como la trituración o la incineración, de modo que no puedan reconstruirse ni volverse a usar.

[11] Por ejemplo, un acuerdo de no divulgación.

Puede tomarse la decisión de digitalizar los registros en papel. En ese caso, una vez que se realiza la conversión, debe destruirse todo rastro de los registros en papel, a menos que la legislación nacional aplicable exija que estos se mantengan o que sea necesario conservar copias físicas con fines de archivo.

b. Destrucción de registros electrónicos

La destrucción de registros electrónicos debe quedar en manos del personal de TIC, porque las funciones comunes de los sistemas informáticos para eliminar archivos no necesariamente garantizan su destrucción total.

Si así se le solicita, el personal de TIC debe ocuparse de eliminar todo rastro de los datos personales de los sistemas informáticos y otros programas, como cualquier copia de respaldo que pudiera existir.

Deben limpiarse las unidades de disco y las aplicaciones de bases de datos, así como todos los medios reescribibles, como CD, DVD, microfichas, cintas de vídeo y cintas de audio que se utilicen para almacenar datos personales, antes de su reutilización. Asimismo, debe realizarse un seguimiento estricto de los medios físicos para destruir registros electrónicos, como el reciclaje, la pulverización o la incineración.

c. Registros de eliminación

El controlador de datos debe corroborar que todo contrato de servicios, memorando de entendimiento, acuerdo o contrato escrito de transferencia o procesamiento indique un período de conservación, es decir, durante cuánto tiempo se almacenarán los datos antes de su destrucción. Las terceras partes deberán devolver los datos personales al controlador de datos y certificar que se han destruido todas sus copias, incluidos los datos personales que hayan compartido con agentes autorizados y subcontratistas. Por otra parte, han de mantenerse y adjuntarse a los informes de proyecto o de evaluación registros de eliminación que indiquen el momento y el método de destrucción, así como la índole de los registros destruidos.

La destrucción de grandes volúmenes de registros en papel puede delegarse en empresas especializadas. En ese caso, el controlador de datos debe verificar que los terceros que participen en el proceso firmen acuerdos de confidencialidad, y tengan la obligación contractual de presentar registros de eliminación y certificados de destrucción de los datos.

**7. Otras medidas**

La seguridad de los datos exige también la adopción interna de medidas organizacionales adecuadas, como la distribución periódica de las normas de seguridad de los datos entre todos los empleados y la información de sus obligaciones en virtud de la legislación sobre protección de datos, en especial en lo que respecta a la confidencialidad.

Cada controlador de datos debe asignar a uno o más de sus empleados (puede ser alguien que trabaje en administración o TI) la función de responsable de seguridad de los datos, cuyas tareas principales serán:

- corroborar que el personal respete los procedimientos de seguridad que establece este Código y sus normas de seguridad aplicables;
- actualizar esos procedimientos cuando sea necesario;

- ofrecer al personal formación adicional sobre seguridad de los datos.

### *Anexo 4: breve guía sobre la evaluación de impacto relativa a la protección de datos*

El propósito de la evaluación de impacto relativa a la protección de datos es detectar, evaluar y atender los riesgos específicos para los datos personales que surjan de ciertas actividades de RCF. La evaluación de impacto debe servir de base para adoptar medidas que permitan evitar, minimizar o mitigar esos riesgos. Esta guía está pensada para ayudar al personal de RCF a realizar ese tipo de evaluación. Las organizaciones de la Red de Vínculos Familiares también pueden acceder a una plantilla de evaluación de impacto relativa a la protección de datos, que se adjunta como documento independiente.

A modo de ejemplo, estas son algunas situaciones hipotéticas en las que se debería considerar realizar una evaluación de impacto sobre la protección de los datos:

- Su organización en el terreno almacena archivos en CD y en papel. Ahora usted quiere adoptar un sistema de almacenamiento de archivos en la nube. ¿Cómo determinar cuál es el mejor método para almacenar cada tipo de información?
- Un tsunami destruye decenas de ciudades costeras. Miles de personas son dadas por desaparecidas. ¿Cuánta información personal se debe solicitar a sus familiares? ¿Mucha o poca? ¿La información debe incluir datos sensibles, como ADN, religión o filiación política?
- El Gobierno adopta un sistema para centralizar toda la información sobre las personas que quedaron desaparecidas tras el tsunami, y solicita que su organización le brinde toda la información de la que dispone sobre esas personas. ¿Cuánta información personal se le debe suministrar para ayudar en la búsqueda? ¿Con qué condiciones debería compartirse la información personal con el Gobierno?
- Otra organización humanitaria le pide que comparta con ella datos sobre personas que viven en un campamento de refugiados. ¿Debe aceptar el pedido? ¿Con qué condiciones? ¿Cuáles serían las consecuencias? ¿La organización en cuestión tendrá los mismos cuidados que la organización a la que pertenece usted en el manejo de los datos personales?
- Su organización está pensando en obtener datos biométricos a gran escala usando nuevas tecnologías de análisis de huella dactilar y reconocimiento facial. ¿Qué protecciones técnicas se deben adoptar? ¿Qué condiciones debe imponer el contrato con el prestador de servicios? ¿Los beneficiarios aceptarán de buen grado proporcionar esa información?
- ¿Se pueden publicar fotografías de niños no acompañados que buscan a sus familiares? ¿Se pueden imprimir carteles con fotografías de niños desaparecidos? De ser así, ¿en qué circunstancias y con qué condiciones?
- Una red social ofrece ayudar a restablecer el contacto entre familiares separados tras un desastre. ¿Cómo se podría cooperar con la plataforma sin poner en riesgo a las personas afectadas ni sus datos personales?
- Mañana, el CICR visitará un lugar de detención donde se cree que está detenida una persona desaparecida. Dada la urgencia de la situación, ¿se puede enviar una solicitud de búsqueda o un mensaje de Cruz Roja por correo electrónico al CICR?

En algunos casos, puede no haber tiempo para llevar a cabo una evaluación de impacto completa; también es posible que la complejidad, la sensibilidad o la escala del procesamiento de datos no requieran una evaluación de impacto de carácter formal. Sin embargo, el personal de RCF siempre debe hacer algún tipo de evaluación de riesgos (y registrarla, si es posible) respecto de la protección de los datos al tomar decisiones sobre su transferencia. Por lo tanto, los empleados y voluntarios de RCF tienen que conocer el proceso de la evaluación de impacto relativa a la protección de datos y considerar las preguntas planteadas.

El proceso de una evaluación de impacto relativa a la protección de datos consta de los siguientes pasos, que deben volcarse en un informe:

**A. Análisis preliminar**

1. Determinar, sobre la base de la complejidad, la sensibilidad y la escala de la actividad de procesamiento:

- si es necesario realizar la evaluación;
- quién la realizará;
- quién la revisará y validará.

2. Establecer cómo se obtendrán, usarán, almacenarán y divulgarán los datos en el contexto de la actividad de RCF en cuestión, trazando un mapa de las partes interesadas y describiendo el flujo de datos. Se deben considerar los siguientes puntos:

- cuál es el objetivo del proyecto;
- qué tipos de datos personales se obtendrán, de quiénes, y quiénes se encargarán de obtenerlos;
- cómo se obtendrá y procesará la información;
- cómo se almacenará, dónde y durante cuánto tiempo;
- qué medidas de seguridad se adoptarán; si habrá algún proceso de pseudoanonimización, depuración o anonimización de los datos para proteger la información sensible, y si se eliminarán los datos que no sean estrictamente necesarios;
- en caso de que se recurra a procesadores externos, quiénes tendrán acceso a la información.

3. Identificar a las partes interesadas que podrían ser de ayuda, ya sean internas, como especialistas en TI, asesores jurídicos, psicólogos, programadores, etc., o externas, como otras organizaciones, organismos gubernamentales, trabajadores sociales, dirigentes comunitarios, tutores, etc. a los que podría concernir o afectar el procesamiento de datos analizado.

**B. Evaluación**

4. Identificar los riesgos que puedan entrañar para las personas la actividad de procesamiento y cualquier incumplimiento de este Código. Si se han identificado partes interesadas internas o externas, convine conversar sobre este punto con ellas. Una manera de detectar los riesgos es determinar las amenazas y vulnerabilidades en torno a todos los principios del Código de Conducta y, a continuación, los riesgos que emanan de ellas.

5. Evaluar los riesgos en términos de probabilidad y gravedad de su impacto.

6. Formular medidas para evitar, minimizar o mitigar los riesgos.

7. Formular recomendaciones, como modificaciones técnicas y organizacionales, o cambios en la estrategia de protección de datos.

**C. Aprobación e implementación**

8. Pedir a especialistas en protección de datos[12] que revisen la evaluación y obtener la aprobación del personal a cargo[13].

9. Poner en práctica las recomendaciones acordadas.

10. Actualizar la evaluación de impacto en caso de que haya modificaciones en la actividad.

Si se realiza una evaluación de impacto relativa a la protección de datos, eso debe constar en un informe, con un detalle de las etapas A, B y C mencionadas. El informe de la evaluación de impacto (es decir, las conclusiones del proceso de evaluación) puede ser muy breve, o más extenso y detallado, de acuerdo con la complejidad, la sensibilidad y la escala de la actividad de procesamiento, y puede incorporar la plantilla que se ofrece adjunta.

## *Anexo 5: contraloría y contraloría conjunta*

Un miembro de la Red de Vínculos Familiares, ya sea el CICR o una Sociedad Nacional, actuará como controlador de los datos si se cumplen los siguientes criterios:

- Es la única organización de la Red de Vínculos Familiares que presta un servicio de RCF; por ejemplo, la apertura de un caso de búsqueda determinado, la obtención y envío de mensajes de Cruz Roja o la facilitación de llamadas telefónicas.
- El CICR y las Sociedades Nacionales (sea una, dos o más) no comparten casos de búsqueda ni llevan adelante otras asociaciones, iniciativas ni servicios colectivos.

Dos o más miembros de la Red de Vínculos Familiares —el CICR y/o las Sociedades Nacionales— se desempeñarán como controladores conjuntos cuando colaboren para establecer los propósitos y los medios con los que se procesan los datos. Un criterio importante es que el procesamiento no sería posible sin la participación de ambas partes. Es decir, se aplicará la contraloría conjunta cuando dos o más miembros de la Red de Vínculos Familiares presten a los beneficiarios un servicio de RCF determinado para el que necesiten obtener y usar datos personales: por ejemplo, cuando manejen juntos un mismo conjunto de casos de búsqueda.

[12] Asesores jurídicos o consultores externos en materia de protección de datos.
[13] Por ejemplo, el/la referente de protección de los datos de RCF, en caso de haberlo/a. De lo contrario, la persona responsable de las actividades de RCF debe aprobar la evaluación de impacto relativa a la protección de datos.