

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES Y SENSIBLES DE LA SOCIEDAD NACIONAL DE LA CRUZ ROJA COLOMBIANA**A. OBJETO, FINALIDAD, INSTRUMENTOS Y MARCO NORMATIVO****Objeto**

La Sociedad Nacional de la Cruz Roja Colombiana, adopta la presente Política de Tratamiento de Datos Personales y Sensibles, que brinda la orientación legal y técnica para la garantía de los derechos de los Titulares de la Información en ellos contenida; la autenticidad, confidencialidad, uso adecuado e integral del tratamiento, en todas y cada una las actividades que involucre, de manera total o parcial: la recolección, almacenamiento, organización, uso, circulación, transmisión, transferencia, actualización, rectificación, supresión y eliminación de esa información.

Finalidad

El presente documento consagra la política de tratamiento de los datos personales y sensibles de las personas naturales a quienes dirige y desarrolla sus actividades de carácter humanitario, de quienes recibe apoyo, ayuda y beneficios; de sus clientes, proveedores, empleados, voluntarios y de terceros que en algún momento y en el contexto de las actividades y de la gestión propia de la institución, participan del cumplimiento de nuestra Misión Humanitaria, de obligatorio y estricto cumplimiento para la Sociedad Nacional de la Cruz Roja Colombiana en su condición de Responsable de Tratamiento, así como para todos los terceros que obran en nombre de la institución, o que sin actuar en su nombre tratan datos personales por disposición de ésta como encargados.

Instrumentos

Para la implementación de la Política de Tratamiento de Datos Personales y Sensibles en la Sociedad Nacional de la Cruz Roja Colombiana, se integrarán: el Manual de la Política de Tratamiento de datos Personales y Sensibles; los Manuales de Seguridad de Información y de Gestión de Archivos de la Información, así como los procedimientos adoptados por la institución para la Gestión del Riesgo.

Marco Normativo Aplicable

- El Artículo 15 de la Constitución de la República de Colombia establece que cualquier persona tiene derecho a conocer, actualizar y rectificar los datos personales que existan sobre ella en banco de datos o archivos de entidades públicas o privadas. Igualmente, ordena a quienes tienen datos personales de terceros respetar los derechos y garantía previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.
- La Ley 23 de 1981. ÉTICA MÉDICA. Tratamiento de datos de la Historia Clínica.
- La Ley 852 del 20 noviembre de 2003, por medio de la cual se protege y regula la misión y las actividades humanitarias de la Sociedad Nacional de la Cruz Roja Colombiana, se le brindan garantías para su ejercicio y se dictan otras disposiciones.
- La Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- La Ley 1448 de 2011. Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno, en especial la referida a la confidencialidad de información sobre víctimas.

- Decreto 4800 de 2011. Por el cual se reglamenta la Ley 1448 de 2011 sobre información compartida y armonizada sobre víctimas.
- La Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la Protección de Datos personales.
- Decreto Reglamentario No. 1727 de 2009 y Decreto Reglamentario parcial No. 1377 de 2013, por el cual se regula de manera parcial la Ley 1581 de 2012.
- La Sentencia C 1011 de 2008, por la que define la exequibilidad del proyecto de Ley estatutaria del Habeas Data.
- La Sentencia C-748 de 2011, por la que se define la constitucionalidad del proyecto de Ley Estatutaria de Protección de Datos Personales.
- Las Sentencias T- 729 de 2002 y T- 414 de 2010. Tipologías de Información en el marco del derecho a la intimidad de las personas naturales.
- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio
- Circular Externa 008 de 2017 de la Superintendencia de Industria y Comercio

B. INFORMACIÓN SOBRE LA INSTITUCIÓN

La Sociedad Nacional de la Cruz Roja Colombiana es una persona jurídica de derecho privado que por su naturaleza jurídica y objetivos es una especial Institución de utilidad común, sin ánimo de lucro, con patrimonio propio e independiente. Está organizada mediante un sistema Federal, y constituida de acuerdo con las leyes de la República de Colombia, y con fundamento en los tratados Internacionales que reconocen al Movimiento Internacional de la Cruz Roja y de la Media Luna Roja como entidad de Derecho Internacional, a los cuales ha adherido el Estado Colombiano.

Es auxiliar de los poderes públicos en sus actividades humanitarias, sin perjuicio de la observancia de sus Principios Fundamentales, su Doctrina y sus Estatutos. De conformidad con lo dispuesto en la Ley 852 de 2003 por la cual se protege y regula la Misión y las actividades humanitarias de la Sociedad Nacional, las autoridades públicas reconocen la adhesión de la Sociedad Nacional de la Cruz Roja Colombiana a los Principios del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja.

Domicilio: De acuerdo con el Artículo 3° de los Estatutos Nacionales, la Sociedad Nacional de la Cruz Roja Colombiana tiene su domicilio principal en la ciudad de Bogotá, Distrito Capital.

Dirección: Avenida Carrera 68 No. 68B-31 Bloque Sur

Teléfono: 6017946566

Correo electrónico: protecciondedatos@cruzrojacolombiana.org

C. DEFINICIONES Y PRINCIPIOS

La Política de Tratamiento de Información personal de la Sociedad Nacional de la Cruz Roja Colombiana, observará las siguientes:

1. Definiciones

- a) **Autorización:** Es el consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
- b) **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las

políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

- c) **Base de Datos:** Es el conjunto organizado de datos personales que sea objeto de Tratamiento;
- d) **Datos Biométricos:** Son aquellos datos personales, ya sean fisiológicos, físicos o conductuales que posibilitan la identificación de una persona.
- e) **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
- f) **Dato Público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- g) **Dato semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.
- h) **Dato Sensible:** Cualquier información que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.
- i) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
- j) **Incidente de seguridad:** Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del Tratamiento o por su Encargado.
- k) **Información Semi-privada:** Aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales;
- l) **Información Privada:** Aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones;
- m) **Información Reservada,** que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones
- n) **Menor de edad:** Según lo establecido en el artículo 34 del Código Civil, los menores de edad son niños o adolescentes, entendiendo por niño o niña las personas entre los 0 y los 12 años, y por adolescente las personas entre 12 y 18 años.
- o) **Referente de protección de datos:** es la persona dentro de la Sociedad Nacional de la Cruz Roja Colombiana, que tiene como función la vigilancia y control de la aplicación de la Política de Protección de Datos Personales, bajo la orientación y lineamientos del Comité de Protección de Datos Personales designado por la Dirección Nacional.

- p) **Reclamación:** Su objetivo es la protección de un derecho fundamental corregir, actualizar, eliminar o suprimir sus datos personales o la revocatoria de la autorización que otorgó.
- q) **Rectificación o actualización de datos:** La Cruz Roja Colombiana tiene la obligación de rectificar y actualizar a solicitud del titular, la información de éste que resulte ser incompleta o inexacta.
- r) **Registro Nacional de Base de Datos – RNBD:** Es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.
- s) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;
- t) **Revocatoria:** Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual.
- u) **Supresión:** Implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por la Universidad de los Andes.
- v) **Titular:** persona natural cuyos datos personales sean objeto de Tratamiento³. Podrán ejercer los derechos del titular:
 - **El propio titular**, quien deberá acreditar su identidad mediante los medios dispuestos por el responsable del tratamiento.
 - **Sus causahabientes**, quienes deberán demostrar dicha calidad.
 - **Su representante y/o apoderado**, previa acreditación de la representación o poder otorgado.
 - **Terceros por estipulación a favor de otro o para otro**, conforme a lo establecido en la ley.
- w) **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país;
- x) **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable de Tratamiento
- y) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

2. Principios

La aplicación de la Política de Tratamiento de Datos Personales y Sensibles de la Sociedad Nacional de la Cruz Roja Colombiana, se orientará y guiará con observancia estricta a integral de los Principios Fundamentales del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, proclamados en Viena en 1965 y por los siguientes principios de orden constitucional y legal:

- a) **Principio de libertad:** El tratamiento de datos sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;
- b) **Principio de legalidad:** El Tratamiento es una actividad reglada por la normatividad aplicable que debe sujetarse a lo establecido en ella;
- c) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;
- d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible con el fin de no inducir a errores en la ejecución de

tratamiento para el cual fueron capturados.. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

- e) **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;
- f) **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Constitución y de la ley. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la normatividad aplicable; los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a autorización legal;
- g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento, se deberá manejar con las medidas operativas, técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- h) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la ley y en los términos de la misma.

D. ÁMBITO DE APLICACIÓN Y FINALIDAD

Los datos personales son recolectados, almacenados, organizados, usados, circulados, transmitidos, transferidos, actualizados, rectificados, suprimidos, eliminados y en general gestionados de acuerdo y en proporción a la finalidad o finalidades que tenga cada tratamiento; para su tratamiento, la Sociedad Nacional de la Cruz Roja Colombiana, adopta las siguientes directrices.

1. Salvo las excepciones señaladas en el presente documento, la Política de Tratamiento de Información Personal y Sensible, se aplica a toda información registrada en cualquier base de datos generadas en:
 - a) Las actividades administrativas, organizacionales, de gestión y de control;
 - b) Los actos consensuales regidos por el derecho público o privado que ésta celebra;
 - c) Eventos sociales, académicos, administrativos, institucionales;
 - d) En las actividades públicas de asistencia y apoyo a la comunidad que brinda, sean éstas de carácter de nacional o internacional.
2. **Finalidad:**
 - a) La efectiva gestión en la comunicación, registro, acreditación, consolidación, organización, actualización, aseguramiento, procesamiento, investigación, capacitación, autorización, reporte, estadística, planeación, mejora, análisis, tramitación, auditaje, defensa jurídica, y de las actuaciones, informaciones y actividades en las cuales se relacionan o vinculan los funcionarios, contratistas prestadores de servicios, proveedores ex-trabajadores, ex-contratistas prestadores de servicios, pensionados y/o beneficiarios de la Sociedad Nacional de la Cruz Roja Colombiana.
 - b) El pertinente ejercicio de planeación, comunicación, registro, acreditación, actualización de datos, auditaje control del riesgo técnico y jurídico y reportes históricos, legales e institucionales,

en el desarrollo de los actos consensuales de naturaleza pública o privada, de carácter nacional o internacional que celebre la Sociedad de la Cruz Roja Colombiana;

- c) La consolidación de procesos, seguimiento e identificación de alternativas de solución de necesidades de las comunidades atendidas y beneficiadas con la intervención de la Sociedad Nacional de la Cruz Roja Colombiana. Esto incluye la comunicación, el registro, la actualización, la consolidación y la difusión de información y actividades necesarias para garantizar la correcta identificación, registro y seguimiento de los beneficiarios; asegurar la entrega oportuna y adecuada de la ayuda humanitaria; facilitar la trazabilidad de los recursos destinados a dicha asistencia o a la implementación de proyectos; garantizar el uso adecuado de los fondos; evaluar el impacto de la asistencia prestada; mejorar la eficiencia de los programas y proyectos; transferir información a los donantes y/o financiadores; generar reportes y estadísticas.
- d) La continuidad, fidelización y referenciación de actuales y nuevos benefactores, voluntarios y donantes de la Sociedad Nacional de la Cruz Roja Colombiana mediante la obtención de bases de datos relacionadas e información autorizada, actualización, de estrategias, y actividades de comunicación, registro, consolidación y organización;
- e) La oportuna y efectiva colaboración, asesoría y apoyo entre los agentes, organismos o entidades del Estado con la Sociedad Nacional de la Cruz Roja Colombiana Relaciónamiento, en sus actividades humanitarias, mediante la comunicación directa, la interacción, colaboración, registro, acreditación, actualización, consolidación, organización, aseguramiento, atención, tramitación, y gestión de las actuaciones, informaciones y actividades en las cuales se relacionan.
- f) La gestión de la participación de los jugadores, verificación del cumplimiento de requisitos, asignación y entrega de premios, prevención de fraudes, cumplimiento de obligaciones legales y regulatorias, así como llevar a cabo actividades de contacto, fidelización y promoción.
- g) Garantizar la trazabilidad y seguridad de las donaciones, gestionar la disponibilidad de componentes sanguíneos, realizar estudios epidemiológicos, cumplir con normativas sanitarias y regulatorias, y facilitar la comunicación con donantes para futuras campañas de donación o en caso de ser necesario un seguimiento médico.
- h) La gestión administrativa y académica de los programas de formación, el seguimiento del impacto de las capacitaciones, la certificación de participantes, la mejora continua de los procesos educativos y el cumplimiento de las normativas aplicables en materia de protección de datos personales.
- i) El registro, gestión y respuesta a las peticiones, quejas, reclamos y sugerencias presentadas; mejorar la calidad de los servicios ofrecidos; generar reportes internos de gestión; cumplir con obligaciones legales y regulatorias; y, en caso de ser necesario, contactar al solicitante para obtener información adicional o brindar seguimiento a su requerimiento.

3. Datos Sensibles

De conformidad con las disposiciones contenidas en el Artículos 5° de la Ley 1581 de 2012 y en el Artículo 6° del Decreto Reglamentario 1377 de 2013, salvo las excepciones allí contemplados y sin perjuicio del derecho de confidencialidad y demás derechos consagrados en la Ley 852 de 2003, la Sociedad Nacional de la Cruz Roja Colombiana garantiza el tratamiento adecuado y con medidas reforzadas de protección para los datos sensibles recolectados en el marco de sus actividades humanitarias.

En tal sentido, no se realizará tratamiento de datos sensibles sin el consentimiento previo, expreso e informado del titular, salvo en los casos en que la ley lo permita sin dicho consentimiento, y únicamente

cuando sea estrictamente necesario para cumplir con su mandato humanitario y misional. Esto aplica, entre otros, a los datos que puedan generarse en las siguientes actividades:

- a) Procesos, intervenciones y acciones humanitarias de atención, recuperación, apoyo psicológico, resiliencia. Rehabilitación, protección y seguridad brindados a víctimas, a niñas, niños y adolescentes, a personas en situación de riesgo, en las áreas de salud, asistencia a la comunidad, gestión en materia de riesgos, reducción, respuesta y recuperación en desastres, programas de educación y formación, bienestar y desarrollo comunitario y, organizaciones y programas especiales para el fortalecimiento económico de comunidades;
- b) Toda intervención, actividad y acciones que por conexidad pueda ser clasificada como información sensible, privada, reservada o confidencial¹ protegida por las normas internas, leyes especiales y por los tratados y acuerdos internacionales;
- c) Las actividades propias del Banco Nacional de Sangre de la Cruz Roja Colombiana.
- d) El Tratamiento de las bases de datos personales, generadas en el ejercicio de la actividad financiera, comercial y bancaria de la Sociedad Nacional de la Cruz Roja Colombiana, incluida la Lotería de la Cruz Roja Colombiana y que contiene información calificada como confidencial o reservada, se sujetará a las disposiciones de la Ley 1266 de 2008 y demás normas que regula o modifican expedidas por las entidades competentes.

E. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN

El Titular de Datos Personales tendrá los siguientes derechos:

- 1. Autorizar o no de manera previa, expresa, informada e inequívoca, a la Sociedad Nacional de la Cruz Roja Colombiana, para la obtención recolección, uso, almacenamiento, circulación, transferencia, transmisión, actualización, rectificación, supresión o eliminación de sus datos personales.
- 2. Acceder y consultar en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento: (i) al menos una vez cada mes calendario, y (ii) cada vez que existan modificaciones sustanciales de las directrices de tratamiento de la información que lo motiven a hacer nuevas consultas.
- 3. Conocer, actualizar y rectificar sus datos personales ante a la Sociedad Nacional de la Cruz Roja Colombiana, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
- 4. Solicitar prueba de la autorización otorgada a la Sociedad Nacional de la Cruz Roja Colombiana, en su condición de Responsable del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, es decir cuando no se requiera la autorización.
- 5. Ser informado por la Sociedad Nacional de la Cruz Roja Colombiana en su condición de el Responsable del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;
- 6. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento la Sociedad Nacional de la Cruz Roja Colombiana haya incurrido en conductas contrarias a la Ley y a la Constitución;

¹Información confidencial. Atendiendo lo dispuesto en el artículo 15 de la Constitución Política de Colombia, La información confidencial se refiere a datos que no están disponibles públicamente y cuyo conocimiento o divulgación podría causar un daño o perjuicio a la persona, empresa o entidad a la que pertenece.

F. OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO DE TRATAMIENTO DE INFORMACIÓN PERSONAL Y SENSIBLE

1. En su condición de Responsable de Tratamiento de Información Personal y Sensible, la Sociedad Nacional de la Cruz Roja Colombiana está obligada a:
 - a) Cumplir y hacer cumplir a directivos, voluntarios, funcionarios, contratistas y terceros que participan de su gestión y aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole, sin perjuicio del deber de confidencialidad, las directrices adoptadas en la presente Política de Tratamiento de Datos Personales y Sensibles tratados por la Sociedad Nacional de la Cruz Roja Colombiana.
 - b) Garantizar al Titular de la Información Personal y Sensible, en todo tiempo, el pleno y efectivo ejercicio del derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en los archivos de la Sociedad Nacional de la Cruz Roja Colombiana.
 - c) Solicitar y conservar, copia de la respectiva autorización otorgada por el Titular, para la obtención recolección, uso, almacenamiento, circulación, transferencia, transmisión, actualización, rectificación, supresión o eliminación de sus datos personales;
 - d) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
 - e) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
 - f) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
 - g) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
 - h) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
 - i) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en esta norma
 - j) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
 - k) Tramitar las consultas y reclamos formulados dentro de los quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.
 - l) Adoptar un manual interno de políticas y procedimientos para garantizar la adecuada atención de consultas y reclamos;
 - m) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
 - n) Informar a solicitud del Titular sobre el uso dado a sus datos;
 - o) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
 - p) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

2. Corresponde al **Encargado del Tratamiento** de Información Personal y Sensible definido por la Sociedad Nacional de la Cruz Roja Colombiana:
- a) Cumplir de manera estricta las directrices de la Sociedad Nacional de la Cruz Roja Colombiana, como Responsable de Tratamiento, sobre la obtención recolección, uso, almacenamiento, circulación, transferencia, transmisión, actualización, rectificación, supresión o eliminación de sus datos personales.
 - b) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en los archivos de la Sociedad Nacional de la Cruz Roja Colombiana.
 - c) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
 - d) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos señalados por la Ley 1581 de 2012
 - e) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
 - f) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente política.
 - g) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Política de Tratamiento de Información Personal y Sensible, en especial, para la atención de consultas y reclamos por parte de los Titulares;
 - h) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley 1581 de 2012 y en el Decreto 1377 de 2013
 - i) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
 - j) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
 - k) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
 - l) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
 - m) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Cualquier incumplimiento de las obligaciones y en general de las directrices contenidas en esta Política y en demás manuales que lo complementen, debe ser reportado a: protecciondedatos@cruzrojacolombiana.org.

G. PROCEDIMIENTO PARA EL TRATAMIENTO DE INFORMACIÓN PERSONAL Y SENSIBLE.

1. Manual de Procedimiento para el Tratamiento de Información

La Sociedad Nacional de la Cruz Roja Colombiana, adoptará el Manual de la Política de Tratamiento de datos Personales y Sensibles que integre con mínimo:

- a) Mecanismos, requisitos y procedimientos para que el Titular de la Información o sus causahabientes, pueda acceder, actualizar, rectificar y solicitar la supresión de la información contenida en las bases de datos de la Sociedad Nacional de la Cruz Roja Colombiana;

- b) Mecanismos, indicación de personas legitimadas y requisitos para el suministro de información, solicitada: i) Titular o sus Causahabientes; ii) Orden Judicial; iii) Entidades Públicas; iv) Terceros autorizados por el Titular y, v) Representantes de niñas, niños y adolescentes;
- c) Procedimiento para la obtención de la autorización previa, expresa, informada e inequívoca del Titular, o sus causahabientes para que la Sociedad Nacional de la Cruz Roja recolecte, almacene, organice, use, circule, transmita, transfiera, actualice, rectifique, suprima o elimine información en sus bases de datos;
- d) Deberes del Encargado de Tratamiento de conformidad con los señalados en la Política de Tratamiento de Información.
- e) Procedimientos, requisitos (legitimidad en la causa y causal admisible) y responsables de la atención de solicitudes, quejas y reclamos que presente el Titular o sus causahabientes sobre información, personal y sensible contenida en las bases de datos de la Sociedad Nacional de la Cruz Roja Colombiana.

Para la atención de las peticiones, consultas, quejas y reclamos de los Titulares de Información ante la Sociedad Nacional de la Cruz Roja Colombiana, se designará(n) uno o varios Referentes de Protección de Datos Personales, quienes contará con el apoyo de la Dirección o las direcciones, Áreas o Programas involucrados en el tratamiento de datos.

2. Procedimiento para el Tratamiento de información o datos Sensibles

Los datos e información clasificada como sensible por disposición de la ley y de la presente Política de Tratamiento de Información Personal y Sensible de la Sociedad Nacional de la Cruz Roja, solo podrán ser tratados de conformidad con los lineamientos que se generen por el Comité de Protección de Datos Personales que para el efecto se integre y conforme a la verificación de los siguientes eventos:

- a) Cuando el Titular de la Información o sus Causahabientes autoricen de manera previa, expresa, informada e inequívoca a tal tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- b) Cuando el Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- c) Cuando en Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
- d) Cuando el Tratamiento de la Información se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- e) Cuando el Tratamiento de Información tenga una finalidad histórica, estadística o científica. En este evento la Sociedad Nacional de la Cruz Roja Colombiana, adoptará las medidas conducentes a la supresión de identidad de los titulares

3. Procedimiento para el Tratamiento de Información o datos personales de niñas, niños y adolescentes

La Sociedad Nacional de la Cruz Roja Colombiana, sólo autoriza el Tratamiento de Información Personal y Sensible de niñas, niños y adolescentes que no sean de naturaleza pública, de conformidad con los lineamientos que para el efecto genere el Comité de Protección de Datos Personales y con el cumplimiento de los siguientes requisitos:

- a) Que responda y respete el interés superior de las niñas, de los niños y de los (as) adolescentes.
- b) Que se asegure el respeto de sus derechos fundamentales.
- c) Que se obtenga la opinión y autorización del menor cuando este cuente con la madurez, autonomía y capacidad para entender el asunto.

Cumplidos los anteriores requisitos, La Sociedad Nacional de la Cruz Roja Colombiana solicitará autorización al representante legal y/o tutor para el tratamiento de datos de la niña, el niño o el/la adolescente.

4. Procedimiento para la Transmisión y Transferencia Internacional de Datos Personales y Sensibles

La Sociedad Nacional de la Cruz Roja Colombiana podrá transmitir o transferir información sobre datos personales a entidades, organismos e instituciones públicas o privadas de carácter internacional, en el marco de actos de cooperación, contratos, convenios o alianzas estratégicas, para el desarrollo de programas, acciones y actividades en cumplimiento de su misión humanitaria.

Estas operaciones se llevarán a cabo previo concepto favorable del Comité de Protección de Datos Personales, cuando sea requerido, y con observancia de los siguientes requisitos:

- a) Verificación del marco normativo aplicable en el país receptor: Se debe verificar la existencia y vigencia de normas sobre protección de datos personales en el país sede del receptor de la información, especialmente si se trata de una transferencia internacional. Esta verificación debe quedar documentada.
- b) Obtención de la autorización del titular: Se deberá contar con la autorización previa, expresa, informada e inequívoca del titular de los datos, salvo en los casos de excepción establecidos en la Ley 1581 de 2012.
- c) Justificación documentada de la necesidad de transferencia: En particular, cuando se solicite o efectúe intercambio de datos de carácter médico o relacionados con la salud del titular, deberá documentarse la necesidad del tratamiento por razones de salud pública o interés vital.
- d) Transferencias con fundamento en tratados internacionales: Se permitirá la transferencia de datos personales cuando esta se realice en el marco de tratados internacionales ratificados por Colombia, o con base en el principio de reciprocidad internacional.
- e) Transferencias para la ejecución contractual: Se permitirá la transferencia de datos personales cuando esta sea necesaria para la ejecución de un contrato suscrito entre el titular y el responsable del tratamiento, o para la implementación de medidas precontractuales a solicitud del titular, siempre que exista autorización para ello.
- f) Transferencias requeridas por interés público o procesos judiciales: Se podrá realizar la transferencia de información cuando sea exigida legalmente para salvaguardar el interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- g) Transferencias financieras o bursátiles: Cuando se trate de datos financieros o bancarios, se observará la legislación especial aplicable, incluyendo la Ley 1266 de 2008.

- h) Contratos de transmisión internacional de datos:
En caso de que la información sea transmitida (no transferida), se deberá celebrar un contrato con el encargado del tratamiento, en los términos del artículo 25 del Decreto 1377 de 2013, en el que se establezcan las obligaciones del encargado y se asegure el cumplimiento de los principios y garantías previstos en la ley colombiana.

H. SEGURIDAD DE LA INFORMACIÓN

La Sociedad Nacional de la Cruz Roja Colombiana, integrará en un Sistema de Seguridad de la Información, las bases de datos que por la presente Política de Tratamiento de Información Personal y Sensibles se regula, asegurando las condiciones técnicas, tecnológicas, administrativas y de competencias humanas para su protección contra todo acto de adulteración, pérdida, acceso, uso, consulta no autorizado o fraudulento.

La adopción de mecanismos, instrumentos y protocolos de seguridad serán reglados en el Manual de Procedimientos para el Tratamiento de Información Personal y Sensible Manual de Procedimientos para el Tratamiento de Información Personal y Sensible que se ordena adoptar.

I. VIGENCIA DE LAS BASES DE DATOS

Las bases de datos generadas en la gestión de la Sociedad Nacional de la Cruz Roja Colombiana tendrán una vigencia igual al periodo en que se mantenga la finalidad o finalidades del tratamiento en cada base de datos, o el periodo de vigencia que señale una causa legal, contractual o jurisprudencial de manera específica.



Cruz Roja Colombiana

MANUAL DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES Y SENSIBLES

BOGOTÁ - COLOMBIA

2025

PREÁMBULO

La Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los principios y disposiciones contenidas en la mencionada ley son aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por parte de la Sociedad Nacional de la Cruz Roja Colombiana siendo estos de naturaleza pública o privada.

Por lo tanto, el tratamiento de datos realizado por la Sociedad Nacional de la Cruz Roja Colombiana (en lo siguiente denominada "Sociedad Nacional de la Cruz Roja Colombiana") se debe regir por el régimen de protección de datos personales establecido por esta ley, sus decretos reglamentarios y demás normatividad que la complemente, modifique o derogue así como por las especiales disposiciones contenidas en la Política de Tratamiento de Datos Personales y Sensibles, adoptada mediante Acuerdo No 115 de 2016 de la Junta Directiva Nacional.

Junta Directiva Nacional
Dirección Ejecutiva Nacional

INTRODUCCIÓN

La Sociedad Nacional de la Cruz Roja Colombiana es una entidad privada sin ánimo de lucro, constituida como persona jurídica de carácter especial como una institución de utilidad común, organizada mediante un sistema Federal, constituida de acuerdo con las Leyes de la República de Colombia, con fundamento en los tratados Internacionales que reconocen al Movimiento Internacional de la Cruz Roja y de la Media Luna Roja como entidad de Derecho Internacional, a los cuales se ha adherido el Estado Colombiano. Es auxiliar de los poderes públicos en sus actividades humanitarias sin perjuicio de la observancia de sus Principios Fundamentales, su Doctrina y sus Estatutos de conformidad con lo dispuesto en la Ley 852 de 2003 por la cual se protege y regula la Misión y las actividades humanitarias de la Sociedad Nacional de la Cruz Roja Colombiana a los Principios del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja.

La Sociedad Nacional de la Cruz Roja Colombiana ha decidido adoptar de forma voluntaria el presente Manual, el cual establece las condiciones de organización, obligaciones de los implicados e intervinientes en el tratamiento y uso de la información de carácter personal, régimen de funcionamiento, y procedimientos aplicables al tratamiento de datos personales que en el desarrollo de todas y cada una las actividades que involucre, de manera total o parcial la recolección, almacenamiento, organización, uso, circulación, transmisión, transferencia, actualización, rectificación, supresión y eliminación de esa información.

Lo anterior ha sido resuelto, con el fin de dar pleno cumplimiento a lo dispuesto por la Constitución Política de Colombia y la Ley 1581 de 2012, así como las demás normas que reglamentan y complementan el tratamiento para la Protección de Datos Personales en Colombia.

La Sociedad Nacional de la Cruz Roja Colombiana es la Responsable del tratamiento de Datos Personales y en cumplimiento a lo establecido en el artículo 13 del Decreto Reglamentario 1377 de 2013, adopta y hace público a todos los interesados el presente Manual que contiene todos los elementos esenciales, sencillos y seguros para el cumplimiento con la legislación correspondiente a la Protección de Datos Personales.

El presente documento consagra los procedimientos para la aplicación de la política de tratamiento de los datos personales y sensibles de las personas naturales a quienes dirige y desarrolla sus actividades de carácter humanitario, de quienes recibe apoyo, ayuda y beneficios; de sus clientes, proveedores, empleados, voluntarios y de terceros que en algún momento y en el contexto de las actividades y de la gestión propia de la institución, participan del cumplimiento de nuestra Misión Humanitaria, de obligatorio y estricto cumplimiento para la Sociedad Nacional de la Cruz Roja Colombiana en su condición de Responsable y/o Encargado del Tratamiento, así como para todos los terceros que obran en nombre de la institución, o que sin actuar en su nombre tratan datos personales por disposición de ésta como encargados.

CAPITULO I.

GENERALIDADES

1.1 ÁMBITO DE APLICACIÓN

Los procedimientos consagrados en este manual se aplicarán a la Sociedad Nacional de la Cruz Roja Colombiana.

Los presentes términos y condiciones aplican para cualquier registro de datos personales realizado en forma presencial, no presencial y/o virtual para la vinculación a cualquier actividad, servicio o beneficio de la Sociedad Nacional de la Cruz Roja Colombiana.

La Sociedad Nacional de la Cruz Roja Colombiana se encarga directamente del tratamiento de los datos Personales; sin embargo, se reserva el derecho a delegar en un tercero tal tratamiento exigiendo así mismo al encargado, la atención e implementación de los lineamientos y procedimientos idóneos para la protección de los datos personales y la estricta confidencialidad de los mismos.

1.2 DEFINICIONES

Las siguientes definiciones, permiten una correcta y apropiada interpretación de la Ley 1581 de 2012 y sus decretos reglamentarios, y son indispensables para la protección del *habeas data*, lo que contribuye a determinar las responsabilidades de los involucrados en el tratamiento de datos personales.

Aviso de privacidad: comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de

acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Autorización: consentimiento previo, expreso e informado del titular de los datos personales para llevar a cabo el tratamiento de datos personales.

Base de datos: conjunto organizado de datos personales, incluidos los archivos¹ y que sean objeto de Tratamiento.

Datos Biométricos: Son aquellos datos personales, ya sean fisiológicos, físicos o conductuales que posibilitan la identificación de una persona.

Dato personal: cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).

Dato público: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato personal público: toda información personal que es de conocimiento libre y abierto para el público en general.

¹ Sentencia C- 748 de 2011

Dato personal privado: toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.

Dato semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.

Dato sensible: aquel dato que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.

Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

Incidente de seguridad: Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del Tratamiento o por su Encargado.

Menor de edad: Según lo establecido en el artículo 34 del Código Civil, los menores de edad son niños o adolescentes, entendiendo por niño o niña las personas entre los 0 y los 12 años, y por adolescente las personas entre 12 y 18 años.

Referente de protección de datos: es la persona dentro de la Sociedad Nacional de la Cruz Roja Colombiana, que tiene como función la vigilancia y control de la aplicación de la Política de Protección de Datos Personales, bajo la orientación y lineamientos del Comité de Protección de Datos Personales designado por la Dirección Nacional.

Reclamación: Su objetivo es la protección de un derecho fundamental corregir, actualizar, eliminar o suprimir sus datos personales o la revocatoria de la autorización que otorgó.

Rectificación o actualización de datos: La Cruz Roja Colombiana tiene la obligación de rectificar y actualizar a solicitud del titular, la información de éste que resulte ser incompleta o inexacta.

Registro Nacional de Base de Datos – RNBD: Es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

Responsable del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el Tratamiento de los datos.

Revocatoria: Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual.

Supresión: Implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por la Universidad de los Andes.

Titular: persona natural cuyos datos personales sean objeto de Tratamiento². Podrán ejercer los derechos del titular:

- **El propio titular**, quien deberá acreditar su identidad mediante los medios dispuestos por el responsable del tratamiento.
- **Sus causahabientes**, quienes deberán demostrar dicha calidad.
- **Su representante y/o apoderado**, previa acreditación de la representación o poder otorgado.
- **Terceros por estipulación a favor de otro o para otro**, conforme a lo establecido en la ley.

Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

1.3 PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

La Cruz Roja Colombiana, comprometida con el adecuado tratamiento de los datos personales,

se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones contenidas en la Constitución Política, en las leyes y normas reglamentarias; en la Política de Tratamiento de Datos Personales y Sensibles adoptado por la Sociedad Nacional de la Cruz Roja Colombiana, y en las que se establecen en el presente Manual que las cuales constituyen las reglas a seguir en la recolección, almacenamiento, organización, uso, circulación, transmisión, transferencia, actualización, rectificación, supresión y eliminación

1.3.1 Principio de confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales, que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo suministrar o comunicar los datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley y en los términos de la misma.

En consecuencia, se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros, la información personal, contable, técnica, comercial o de cualquier otro tipo suministrada en la ejecución y ejercicio de las funciones diferentes a las registra les. Todas las personas que trabajen actualmente o sean vinculadas a futuro para tal efecto, en la administración y manejo de bases de datos, deberán suscribir un documento adicional u otrosí a su contrato laboral o de prestación de servicios para efectos de asegurar tal compromiso. Esta obligación persiste y se mantiene inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

² La Sentencia C- 748 de 2011

1.3.2 Principio de seguridad

La Sociedad Nacional de la Cruz Roja Colombiana como responsable y/o encargada del tratamiento de datos de carácter personal, proporciona las medidas operativas, técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad de los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

1.3.3 Principio de acceso y circulación restringida.

El Tratamiento de Datos Personales sólo podrá realizarse por personas autorizadas por el Titular y/o por quienes autorice la ley.

Los datos personales, excepto aquellos de naturaleza pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los Titulares o terceros autorizados. Para estos propósitos, la obligación de la Sociedad Nacional de la Cruz Roja Colombiana será de medio y no de resultado.

1.3.4 Principio de libertad

La Sociedad Nacional de la Cruz Roja Colombiana, garantiza que el tratamiento de datos sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Se podrán tratar y ceder los datos personales que se encuentren almacenados en sus bases de datos, sin el previo consentimiento del titular, siempre y cuando, estos provengan de los registros públicos, o que, si bien no están contenidos en ellos, sean de naturaleza pública o

se encuentran en bases de datos excluidas por la Ley (p.ej. periodísticas, estadísticas y para la investigación). En los demás casos, la Sociedad Nacional de la Cruz Roja Colombiana deberá obtener el consentimiento, previo, expreso e informado del Titular al momento de tratar sus datos personales.

1.3.5. Principio de Transparencia

La Sociedad Nacional de la Cruz Roja Colombiana garantiza a los titulares de datos personales, el derecho de acceso y conocimiento de la información de carácter personal que le concierna y que estén siendo tratados por la Institución.

1.3.6. Principio de Veracidad o Calidad.

La Información Tratada por la Sociedad Nacional de la Cruz Roja Colombiana, debe ser veraz, completa, exacta, actualizada, comprobable y comprensible con el fin de no inducir a errores en la ejecución de tratamiento para el cual fueron capturados. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

1.3.7. Principio de finalidad

El Tratamiento de datos personales que la Sociedad Nacional de la Cruz Roja Colombiana realiza, obedece a la finalidad legítima señalada en las normas nacionales y en el literal D de la Política de Tratamiento de Datos Personales y Sensibles, adoptadas por la Institución. La finalidad del tratamiento debe ser informada a los titulares con el propósito que éstos conozcan las actividades que desarrollará La Cruz Roja Colombiana con los datos personales que está entregando.

1.3.8. Principio de legalidad

El Tratamiento es una actividad reglada que se rige por la Ley Estatutaria 1581 de 2012, el

Decreto 1377 de 2013 y demás normatividad que las complementen, modifiquen o deroguen.

CAPITULO II.

TRATAMIENTO DE DATOS PERSONALES

2.1 TRATAMIENTO

2.1.1 Datos Públicos

La Sociedad Nacional de la Cruz Roja Colombiana advierte que, trata sin previa autorización del Titular los datos personales de naturaleza pública y los contenidos en los registros públicos, estos últimos por tratarse de una función pública reglada reconocida por la Ley. Esta situación no implica que no se adopten las medidas necesarias que garanticen el cumplimiento de los otros principios y obligaciones contempladas en la Ley 1581 de 2012 y demás normas que regulen esta materia.

2.1.2 Datos sensibles

Salvo las excepciones legales y sin perjuicio del derecho de confidencialidad y demás derechos consagrados en la Ley 852 de 2003, la Sociedad Nacional de la Cruz Roja Colombiana no autoriza la obtención, recolección, almacenamiento, uso, circulación o supresión de Datos Sensibles que se generen en:

a. Procesos, intervenciones y acciones humanitarias de atención, recuperación, apoyo psicológico, resiliencia, rehabilitación, protección y seguridad brindados a víctimas, a niñas, niños y adolescentes, a personas en situación de riesgo, en las áreas de salud y asistencia a la comunidad; gestión en materia de riesgos, reducción, respuesta y recuperación en desastres; programas de educación y formación, bienestar y desarrollo comunitario;

organizaciones y programas especiales para el fortalecimiento económico de comunidades;

b. Toda intervención, actividad y acciones que por conexidad pueda ser clasificada como información sensible, privada, reservada o confidencial³ protegida por las normas internas y por los tratados y acuerdos internacionales;

c. Las actividades propias del Banco Nacional de Sangre de la Cruz Roja Colombiana.

d. El ejercicio de la actividad financiera, comercial y bancaria de la Sociedad Nacional de la Cruz Roja Colombiana, incluida la Lotería de la Cruz Roja Colombiana y que contenga información calificada como confidencial o reservada, la cual se sujetará a las disposiciones de la Ley 1266 de 2008 y demás normas que regula o modifican expedidas por las entidades competentes.

2.1.2.1. La Sociedad Nacional de la Cruz Roja Colombiana restringirá el tratamiento de datos personales sensibles a lo estrictamente indispensable y solicitará consentimiento previo y expreso a los titulares (representantes legales, apoderados, causahabientes) informando sobre la finalidad exclusiva de su tratamiento.

La Sociedad Nacional de la Cruz Roja Colombiana utiliza y trata datos catalogados como sensibles, cuando:

- a) El tratamiento haya sido autorizado expresamente por el Titular de los datos sensibles, salvo en los casos que por Ley, no se requiera el otorgamiento de dicha autorización.
- b) El Tratamiento sea necesario para salvaguardar el interés vital del titular y

³ Información confidencial. Atendiendo lo dispuesto en el artículo 15 de la Constitución Política de Colombia, La información confidencial se refiere a datos que no están disponibles públicamente y cuyo

conocimiento o divulgación podría causar un daño o perjuicio a la persona, empresa o entidad a la que pertenece.

éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar la autorización.

- c) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- d) El Tratamiento tenga una finalidad histórica, estadística o científica o, dentro del marco de procesos de mejoramiento; este último, siempre y cuando se adopten las medidas conducentes a la supresión de identidad de los Titulares o el dato este disociado, es decir, el dato sensible sea separado de la identidad del titular y no sea identificable o no se logre identificar a la persona Titular del dato o datos sensibles.

Así mismo, la Sociedad Nacional de la Cruz Roja Colombiana cumple con las siguientes obligaciones:

- a) Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su tratamiento.
- b) Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles datos objeto de Tratamiento son de carácter sensible y la finalidad del tratamiento, y obtener el consentimiento expreso.
- c) No condicionar ninguna actividad a que el titular suministre datos personales sensibles (salvo que exista una causa legal o contractual para hacerlo).

En todo caso, la Sociedad Nacional de la Cruz Roja Colombiana, observa la regla general según la cual el Tratamiento de datos sensibles está

prohibido por la Ley, salvo en los siguientes casos:

- a) Cuando el Titular ha autorizado expresamente el Tratamiento.
- b) Cuando por Ley no sea requerido el arrogamiento de dicha autorización.
- c) Cuando el Tratamiento sea necesario para salvaguardar el interés vital del Titular.
- d) Cuando el Tratamiento sea efectuado por una fundación, ONG, asociación o cualquier organismo sin ánimo de lucro, cuya finalidad sea filosófica, religiosa.
- e) El Tratamiento sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- f) El Tratamiento obedezca a una finalidad histórica, estadística o científica. En este caso, se deben suprimir las identidades de los Titulares.

2.1.3 Tratamiento de datos de menores

De acuerdo con lo previsto en la Constitución Política de Colombia en sus artículos 44 y 45 Y en concordancia con el Código de la Infancia y la Adolescencia, los derechos de los menores deben ser interpretados y aplicados de manera prevalente y, por lo tanto, deben ser observados con especial cuidado

En tal sentido, el Tratamiento de datos personales de niños niñas y adolescentes está proscrito excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la ley 1581 de 2012, y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

- a) Que responda y respete el interés superior de los niños, niñas y adolescentes.

- b) Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal o tutor del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto⁴.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012, en el Decreto 1377 de 2013 y en la Política de Tratamiento de Datos Personales y Sensibles adoptado por la Sociedad Nacional de la Cruz Roja Colombiana.

La familia y la sociedad podrán intervenir ante la Sociedad Nacional de la Cruz Roja, para velar porque los responsables y encargados del tratamiento de los datos personales de los menores de edad cumplan las obligaciones establecidas en la Ley 1581 de 2012, en el Decreto 1377 de 2013 y en la Política de Tratamiento de Datos Personales y Sensibles adoptado por la Institución

2.2 LINEAMIENTOS MINIMOS PARA ADMINISTRACIÓN DE BASES DE DATOS Y TIPOS DE BASES DE DATOS

2.2.1. LINEAMIENTOS MINIMOS PARA ADMINISTRACIÓN DE BASES DE DATOS

La Sociedad Nacional de la Cruz Roja Colombiana ha clasificado sus Bases de Datos de la siguiente manera:

Cada área de la Cruz Roja Colombiana que maneje datos personales tiene la responsabilidad de implementar y utilizar bases de datos que sean seguras, organizadas y actualizadas, en línea con la naturaleza de los datos que se manejan y los propósitos específicos para los que fueron recolectados. Estas bases de datos pueden ser tanto físicas como digitales, y deben seguir ciertos lineamientos mínimos:

Clasificación de la Base de Datos: Es fundamental que los departamentos mantengan una clasificación clara entre las bases de datos que contengan información pública, privada, semiprivada, sensible o relacionada con menores de edad, de acuerdo con la legislación vigente.

Accesibilidad y Control: Se deben establecer mecanismos de control de acceso que aseguren que solo el personal autorizado pueda acceder a la base de datos, según su rol y funciones. Las bases digitales deben contar con credenciales seguras y sistemas de autenticación.

Integridad y Actualización: Las bases de datos deben estar siempre actualizadas, completas y libres de duplicados, con procedimientos claros para la actualización, corrección o eliminación de datos cuando lo requiera el titular.

Seguridad y Respaldo: Las bases de datos digitales deben estar alojadas en entornos tecnológicos seguros, con copias de seguridad periódicas de la información y protocolos de recuperación en caso de pérdida o corrupción de datos. En el caso de las bases físicas, es esencial garantizar su almacenamiento en lugares de acceso restringido y en condiciones adecuadas de conservación.

⁴ Sentencia C 748 de 2011.

Registro y Auditoría: Cada departamento debe llevar un registro de las bases de datos que tiene bajo su responsabilidad, que incluya su propósito, el tipo de datos almacenados, el número aproximado de registros, los responsables de su gestión y las medidas de seguridad implementadas. Este registro debe estar disponible para auditorías internas y controles institucionales.

2.2.2. TIPOS DE BASES DE DATOS

2.2.2.1. Según su estructura

- **Estáticas**

Con este tipo de bases de datos se persigue almacenar y registrar datos con el objetivo de realizar estudios históricos y comparativos de su comportamiento en el tiempo. Son bases de datos cuyo diseño está enfocado en la lectura de datos y lo suelen utilizar empresas, instituciones y profesionales para mejorar la toma de decisiones en el mundo de los negocios.

- **Dinámicas**

En este tipo de bases de datos la información cambia a lo largo del tiempo. A diferencia de las bases de datos estáticas, en las dinámicas la información no solamente se almacena, sino que se va modificando cuando es necesario.

2.2.2.2. Según su contenido

- **Bibliográficas**

Son bases de datos donde se registran una serie de datos para clasificar un evento, lugar, personas, etc. Son bases de datos que consultamos a diario y que incluyen datos sobre un determinado tema. Por ejemplo, nombre, edad de nacimiento, nacionalidad y profesión, entre otros datos.

- **Directorio**

Son bases de datos para guardar elementos básicos con una organización en forma de directorio. Este tipo de bases de datos son las que se consulta de manera habitual en el día a día en el ámbito empresarial, por ejemplo, una base de datos con la información sobre los clientes.

- **Texto Completo**

Se trata de bases de datos bibliográficas, pero que permiten búsquedas avanzadas de palabras clave. Se utilizan, por ejemplo, en el ámbito científico para hacer búsquedas sobre investigaciones académicas, entre otras.

2.2.2.3. Según como administran los datos

- **Jerárquicas**

Son bases de datos donde la información se clasifica siguiendo una estructura jerárquica. Este tipo de estructura en forma de árbol comienza por una raíz de la que surgen distintos nodos llamados padres, y desde cada uno de ellos surgen nuevos nodos llamados hijos, y así sucesivamente.

- **De red**

Se trata de un tipo especial de base de datos jerárquica donde cada nodo puede tener distintos padres. No se suele utilizar actualmente debido a la dificultad de modificar su estructura.

- **Relacionales**

Las bases de datos relacionales son las más comunes y con las que trabajamos a diario. En ellas la información se guarda en registros dentro de tablas, estableciendo relaciones entre estas tablas para poder procesar búsquedas y consultas fácilmente.

- **Transaccionales**

Con este tipo de bases de datos se persigue el envío y recepción de la información a una gran

velocidad. Se utilizan a nivel industrial o empresarial cuando se necesita que la información se transfiera de forma muy rápida, como por ejemplo en el sector bancario.

- **Multidimensionales**

Se trata de bases de datos relacionales que se utilizan para funciones específicas, pudiendo representarse dimensiones dentro de una tabla de datos.

- **Orientadas a objetos**

En este tipo de bases de datos, no se almacenan datos sobre un objeto, sino que se almacena el objeto en sí. Admiten mayor contenido que otros tipos de bases de datos y facilitan al usuario el acceso a información actualizada y completa.

- **Documentales**

Las bases de datos documentales tienen como objetivo el manejo de grandes volúmenes de datos en espacios cortos de tiempo. Se construyen con lenguaje NoSQL más comúnmente, dotándolas de gran flexibilidad y potencia.

- **Deductivas**

Las bases de datos lógicas o deductivas se fundamentan en la lógica matemática y vienen a resolver el problema que presentan las bases de datos relacionales cuando hay que realizar consultas recursivas o tener en cuenta las relaciones indirectas que se generan entre los registros almacenados.

CAPITULO III.

PRERROGATIVAS Y DERECHOS DE LOS TITULARES

La Sociedad Nacional de la Cruz Roja Colombiana reconoce y garantiza a los titulares de los datos personales los siguientes derechos fundamentales

- a) Acceder, conocer, actualizar y rectificar, sus datos personales frente a la Sociedad Nacional de la Cruz Roja Colombiana en su condición de responsable del Tratamiento.
- b) Solicitar prueba de la existencia de la autorización otorgada a la Sociedad Nacional de la Cruz Roja Colombiana, salvo los casos en los que la Ley exceptúa la autorización.
- c) Recibir información por parte de la Sociedad Nacional de la Cruz Roja Colombiana, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- d) Modificar y revocar la autorización y/o solicitar la supresión o eliminación de los datos personales, cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales vigentes.
- e) Tener conocimiento y acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.
- f) Previa presentación o reclamo y obtención de información ante la Sociedad Nacional de la Cruz Roja Colombiana, presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a las disposiciones aplicables.

Nota: Estos derechos solamente se reconocen y garantizan sobre los datos de carácter personal de las personas naturales que se encuentren almacenados en bases de datos diferentes a la de los registros públicos

En el presente documento, en secciones posteriores, define los procedimientos implementados para garantizar estos derechos.

CAPITULO IV.

DEBERES DE LA SOCIEDAD NACIONAL DE LA CRUZ ROJA COLOMBIANA CON RELACIÓN AL TRATAMIENTO DE LOS DATOS PERSONALES

La Sociedad Nacional de la Cruz Roja Colombiana tiene presente que los Datos Personales son de propiedad de las personas a las que les concierne y solamente ellas pueden decidir sobre los mismos. Así mismo, la Sociedad Nacional de la Cruz Roja Colombiana hará uso de dichos datos solamente para las finalidades para las que se encuentra debidamente facultada y respetando, en todo caso, la normatividad vigente sobre la Protección de Datos Personales.

La Sociedad Nacional dará estricto cumplimiento a los deberes previstos para los Responsables y Encargados del Tratamiento, contenidos en el artículo 17 y 18 de la Ley 1581 de 2012, o normas que la reglamenten o modifiquen, a saber:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- e) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás

medidas necesarias para que la información suministrada a este se mantenga actualizada;

- f) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
- g) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
- h) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
- i) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;
- j) Informar a solicitud del Titular sobre el uso dado a sus datos;
- k) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

CAPITULO V.

PROCEDIMIENTOS DEL TRATAMIENTO DE LA INFORMACIÓN

5.1 GENERALIDADES SOBRE LA AUTORIZACIÓN

Cuando se trate de datos diferentes a los de naturaleza pública, definidos en el numeral 2 del artículo 3 del Decreto Reglamentario 1377 de 2013 y en la Política de Tratamiento de Datos Personales y Sensibles adoptado por la Institución la Sociedad Nacional de la Cruz Roja Colombiana solicitará previamente la

autorización para el tratamiento de datos personales por cualquier medio legal que permita ser utilizado como prueba. Según el caso, dicha autorización puede ser parte de un documento más amplio como, por ejemplo, de un contrato, o de un documento específico (formato, formulario, otrosí, etc.).

En caso de tratarse de datos de carácter personal privados correspondientes a personas naturales, la descripción de la finalidad del tratamiento de los datos se informará mediante el mismo documento específico o adjunto. La Sociedad Nacional - informará al titular de los datos lo siguiente:

- a) El tratamiento al que serán sometidos sus datos personales y la finalidad específica del mismo.
- b) Los derechos que le asisten como titular.
- c) La página web, correo electrónico, dirección física y demás canales de comunicación en por los cuales podrá formular consultas y/o reclamos ante el Responsable o Encargado del tratamiento.

Autorización en formatos físicos y/o digitales: Las áreas que realicen iniciativas que impliquen la recolección de datos personales mediante formularios físicos y/o digitales deberán cumplir con los siguientes requisitos:

- a) Solicitar únicamente los datos personales estrictamente necesarios, de acuerdo con la finalidad de la recolección.
- b) Incluir en el formulario un aviso de privacidad que incorpore la autorización para el tratamiento de los datos.
- c) Asegurar que la institución solo pueda tratar los datos recopilados si el titular ha otorgado su autorización. En caso de que el titular no la haya concedido, se deberá

analizar la situación de manera individual.

- d) Verificar que el aviso de privacidad especifique claramente todas las finalidades del tratamiento de los datos recopilados.
- e) Garantizar la adecuada custodia y conservación de los formularios, asegurando la confidencialidad y seguridad de la información contenida en ellos.

5.1.1 Casos en que no se requiere la autorización

La autorización del Titular no será necesaria cuando se trate de:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus
- b) funciones legales o por orden judicial.
- c) Datos de naturaleza pública.
- d) Casos de urgencia médica o sanitaria
- e) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- f) Datos relacionados con el Registro Civil de las Personas.

5.2 DERECHOS DE LOS TITULARES

5.2.1 Del derecho de acceso

La Sociedad Nacional - garantiza el derecho de acceso conforme a la Ley 1581 de 2012, solamente a los Titulares de datos personales privados que correspondan a personas naturales, previa acreditación de la identidad del titular, legitimidad, o personalidad de su representante, poniendo a disposición de éste, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales tratados, a través de cualquier medio de comunicación, incluyendo los electrónicos que permitan el acceso directo del titular.

5.2.2 Del derecho de consulta

Los titulares de los datos personales podrán consultar la información de carácter personal que repose en cualquier base de datos de la Sociedad Nacional, excepto por lo establecido en la Ley 852 de 2003 y las demás normas que regulen sobre esta materia.

La Sociedad Nacional establecerá los mecanismos de autenticación que permitan identificar de manera segura al titular de los datos personales que realiza la consulta o petición. Esta obligación no aplica para las bases de datos de los registros públicos administradas por la Sociedad Nacional.

De manera independiente al mecanismo implementado para la atención de solicitudes de consulta, éstas serán tramitadas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. En el evento en el que una solicitud de consulta no pueda ser atendida dentro del término antes señalado, se informará al interesado antes del vencimiento del plazo las razones por las cuales no se ha dado respuesta a su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

5.2.3 Del derecho a reclamar

El Titular de datos personales privados que correspondan a una persona natural y considere que la información contenida o almacenada en una base de datos que no corresponda a los registros públicos de la Sociedad Nacional de la Cruz Roja Colombiana, puede ser objeto de corrección, actualización o supresión o eliminación o, cuando adviertan el presunto incumplimiento de cualquiera de los deberes y principios contenidos en la normatividad sobre Protección de Datos Personales. En tal sentido, podrán presentar reclamación ante el

Responsable o Encargado del tratamiento de la Sociedad Nacional.

La Sociedad Nacional cuenta con las medidas de autenticación necesarias que permiten identificar de manera segura al titular de los datos personales que realiza el reclamo. El reclamo lo podrá presentar el titular, sus causahabientes, el (los) representante (s) legal(es) debidamente reconocido(s) y demás personas o entidades autorizada por la Ley; el reclamo deberá contener como mínimo:

- a) La identificación del Titular.
- b) La descripción de los hechos que dan lugar al reclamo,
- c) La dirección geográfica o electrónica.
- d) Los documentos que se quiera hacer valer.

Si el reclamo estuviese incompleto, el titular lo podrá completar dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo, para que subsane las fallas o errores.

Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información solicitada, se entenderá que ha desistido del reclamo.

En caso de recibido reclamo que no sea competencia de la institución para resolverlo, se dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

Una vez la Sociedad Nacional haya recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda se mantendrá hasta que el reclamo sea decidido. El término máximo para resolver la reclamación es de quince (15) días hábiles, contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho

término, la Sociedad Nacional informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

5.2.4 Del derecho a la rectificación y actualización de datos

La Sociedad Nacional se obliga a rectificar y actualizar a solicitud del Titular, la información de carácter personal que corresponda a personas naturales, que resulte incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados. Lo anterior, siempre y cuando, no se trate de datos contenidos en los registros públicos, los cuales se regirán por la normativa especial. Al respecto, la Sociedad Nacional tendrá en cuenta lo siguiente:

- a) En las solicitudes de rectificación y actualización de datos personales, el Titular debe indicar las correcciones a realizar y aportar la documentación que avale su petición.
- b) La Sociedad Nacional, tiene plena libertad de habilitar mecanismos que le faciliten el ejercicio de este derecho, siempre y cuando beneficien al Titular de los datos personales.
- c) La Sociedad Nacional, podrá establecer formularios, formatos, sistemas y otros métodos, que serán informados en el Aviso de Privacidad y que se pondrán a disposición de los interesados en la página web u oficinas de la Sociedad Nacional.

5.2.5 Del derecho a la supresión de datos

El Titular de datos personales, tiene el derecho en todo momento, a solicitar a la Sociedad Nacional, la supresión (eliminación) de sus datos personales, siempre y cuando, no se trate de datos contenidos en los registros públicos, los cuales se regirán por la normativa especial. Para

el resto de datos, se tendrá en cuenta los siguientes supuestos:

- a) Que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la normatividad vigente sobre Protección de Datos Personales.
- b) Que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
- c) Que se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recogidos.

Esta supresión implica la eliminación o borrado seguro, total o parcial, de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por la Sociedad Nacional.

El derecho de supresión no es un derecho absoluto, y la Sociedad Nacional como responsable del tratamiento de datos personales, puede negar o limitar el ejercicio del mismo cuando:

- a) El titular de los datos tenga el deber legal o contractual de permanecer en la base de datos.
- b) La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- c) Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.

- d) Los datos sean datos de naturaleza pública y correspondan a los registros públicos, los cuales tienen como finalidad su publicidad.

5.2.6 Del derecho a revocar la autorización

Todo titular de datos personales que correspondan a personas naturales puede revocar en cualquier momento, el consentimiento al tratamiento de éstos, siempre y cuando, no lo impida una disposición legal o contractual. Para ello, la Sociedad Nacional ha establecido mecanismos sencillos y gratuitos que le permiten al titular revocar su consentimiento.

5.2.7 Protección de datos en los contratos

En los contratos laborales, la Sociedad Nacional ha incluido cláusulas con el fin de autorizar de manera previa y general el tratamiento de datos personales relacionados con la ejecución del contrato, lo que incluye la autorización de recolectar, modificar o corregir, en momentos futuros, datos personales del Titular correspondientes a personas naturales. También ha incluido la autorización para que algunos de los datos personales, en caso dado, puedan ser entregados o cedidos a terceros con los cuales la Sociedad Nacional tenga contratos de prestación de servicios, para la realización de tareas tercerizadas. En estas cláusulas, se hace mención del presente Manual y de su ubicación en el sitio web institucional, para su debida consulta.

En los contratos de prestación de servicios externos, cuando el contratista requiera de datos personales, la Sociedad Nacional le suministrará dicha información siempre y cuando exista una autorización previa y expresa del Titular de los datos personales para esta transferencia, quedando excluida de esta autorización, los datos personales de naturaleza pública definidos

en el numeral 2° del artículo 3° del Decreto Reglamentario 1377 de 2013 y los contenidos en los registros públicos. Dado que en estos casos, los terceros son Encargados del tratamiento de datos y sus contratos incluirán cláusulas que precisan los fines y los tratamientos autorizados por la Sociedad Nacional y delimitan de manera precisa el uso que estos terceros le pueden dar a aquellos, así como las obligaciones y deberes establecidos en la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, incluyendo las medidas de seguridad necesarias que garanticen en todo momento la confidencialidad, integridad y disponibilidad de la información de carácter personal encargada para su tratamiento.

Por su parte, la Sociedad Nacional al momento de recibir datos de terceros y actuar como Encargada del tratamiento de datos de carácter personal, verifica que la finalidad, o finalidades, de los tratamientos autorizados por el titular o permitidos por causas legales, contractuales o jurisprudencia les se encuentran vigentes y que el contenido de la finalidad esté relacionada con la causa por la cual se va a recibir dicha información personal de parte del tercero, pues solo de este modo estará facultado para recibir y tratar dichos datos personales.

5.2.8 Transferencia de datos personales a terceros países

La Sociedad Nacional de la Cruz Roja Colombiana podrá transmitir o transferir información sobre datos personales a entidades, organismos e instituciones públicas o privadas de carácter internacional, en el marco de actos de cooperación, contratos, convenios o alianzas estratégicas, para el desarrollo de programas, acciones y actividades en cumplimiento de su misión humanitaria.

Estas operaciones se llevarán a cabo previo concepto favorable del Comité de Protección de

Datos Personales, cuando sea requerido, y con observancia de los siguientes requisitos:

- a. Verificación del marco normativo aplicable en el país receptor: Se debe verificar la existencia y vigencia de normas sobre protección de datos personales en el país sede del receptor de la información, especialmente si se trata de una transferencia internacional. Esta verificación debe quedar documentada.
- b. Obtención de la autorización del titular: Se deberá contar con la autorización previa, expresa, informada e inequívoca del titular de los datos, salvo en los casos de excepción establecidos en la Ley 1581 de 2012.
- c. Justificación documentada de la necesidad de transferencia: En particular, cuando se solicite o efectúe intercambio de datos de carácter médico o relacionados con la salud del titular, deberá documentarse la necesidad del tratamiento por razones de salud pública o interés vital.
- d. Transferencias con fundamento en tratados internacionales: Se permitirá la transferencia de datos personales cuando esta se realice en el marco de tratados internacionales ratificados por Colombia, o con base en el principio de reciprocidad internacional.
- e. Transferencias para la ejecución contractual: Se permitirá la transferencia de datos personales cuando esta sea necesaria para la ejecución de un contrato suscrito entre el titular y el responsable del tratamiento, o para la implementación de medidas precontractuales a solicitud del titular, siempre que exista autorización para ello.

- f. Transferencias requeridas por interés público o procesos judiciales: Se podrá realizar la transferencia de información cuando sea exigida legalmente para salvaguardar el interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- g. Transferencias financieras o bursátiles: Cuando se trate de datos financieros o bancarios, se observará la legislación especial aplicable, incluyendo la Ley 1266 de 2008.
- h. Contratos de transmisión internacional de datos: En caso de que la información sea transmitida (no transferida), se deberá celebrar un contrato con el encargado del tratamiento, en los términos del artículo 25 del Decreto 1377 de 2013, en el que se establezcan las obligaciones del encargado y se asegure el cumplimiento de los principios y garantías previstos en la ley colombiana.

5.2.9 Reglas generales aplicables

La Sociedad Nacional ha establecido las siguientes reglas generales para la protección de datos personales, sensibles y de menores, como es el cuidado de bases de datos, archivos, ficheros electrónicos e información personal.

- a) La Sociedad Nacional de la Cruz Roja Colombiana obtendrá y utilizará los datos personales que en efecto se requieran para el desarrollo de su objeto, para cumplir con sus deberes legales y para atender en debida forma la relación que establezca con el titular del dato; de forma tal que evitará solicitar información ajena a dichos propósitos.
- b) La Sociedad Nacional de la Cruz Roja Colombiana utilizará los datos personales conforme a las finalidades con las que tales datos sean obtenidos.

c) Tales datos personales corresponderán a los de sus clientes, colaboradores, proveedores, administradores, aliados y en general a los de todas aquellas personas naturales con las que la Sociedad Nacional de la Cruz Roja Colombiana se relaciona para el cumplimiento pleno de su objeto.

d) La Sociedad Nacional de la Cruz Roja Colombiana obtendrá y utilizará datos personales siempre que se encuentre facultada para ello, bien porque la ley así lo dispone, bien porque ello se deriva de la naturaleza de la relación que tiene con el titular de los datos o bien por que el titular del dato la autoriza expresamente para el efecto.

e) Cuando quiera que se precise autorización del titular para el tratamiento de sus datos personales:

- La Sociedad Nacional de la Cruz Roja Colombiana informará al titular sobre la finalidad de tal tratamiento y obtendrá de él su consentimiento expreso e informado.
- La autorización se obtendrá en forma previa al tratamiento de los datos personales y, en todo caso, a más tardar al momento de la recolección inicial de tal información.
- La autorización podrá darse a través de cualquier medio que permita su adecuada conservación, así como su consulta posterior.

f) En los eventos en que la Sociedad Nacional de la Cruz Roja Colombiana requiera utilizar datos personales para una finalidad distinta a la inicialmente

informada a su titular y autorizada por éste o diferente a la señalada en la Ley o ajena a la naturaleza de la relación que lo vincula con la Sociedad Nacional de la Cruz Roja Colombiana, se deberá obtener del titular de los datos una nueva autorización.

g) La Sociedad Nacional de la Cruz Roja Colombiana ha previsto que siempre que los datos personales sean suministrados por un tercero, ese tercero debe contar con la autorización del titular que le permita compartir la información con la Sociedad Nacional de la Cruz Roja Colombiana o estar amparado en la ley para ello.

h) En el tratamiento de datos de menores de edad, la Sociedad Nacional de la Cruz Roja Colombiana tendrá en cuenta el interés superior de los mismos, así como la prevalencia de sus derechos. Adicionalmente, en los eventos en que los derechos de tales menores sean ejercidos por un tercero, la Sociedad Nacional de la Cruz Roja Colombiana verificará que ese tercero esté autorizado conforme a la ley para ello.

i) En el evento en que la información recopilada corresponda a Datos Sensibles, entendidos éstos como aquellos que afectan derechos prevalentes, la intimidad o cuyo uso indebido puede generar discriminación, la Sociedad Nacional de la Cruz Roja Colombiana debe informar al titular de la misma acerca del carácter de sensible de los datos que suministra y acerca de la posibilidad que tiene de suministrar o no dicha información.

j) La Sociedad Nacional de la Cruz Roja Colombiana velará porque los datos personales que se encuentran en sus

archivos y bases de datos sean almacenados y administrados en razonables condiciones de seguridad y confidencialidad.

- k) Son confidenciales los datos personales, excepto aquellos que tienen el carácter de públicos. La información clasificada como confidencial debe ser conocida y manejada exclusivamente por los colaboradores autorizados por la Sociedad Nacional de la Cruz Roja Colombiana para ello.
- l) La Sociedad Nacional de la Cruz Roja Colombiana velará porque se registren en los términos de la normatividad vigente, las bases de datos que contengan datos personales objeto de tratamiento por su parte.
- m) De manera adicional, en los procedimientos internos la Sociedad Nacional de la Cruz Roja Colombiana adoptará medidas de seguridad con el fin de: (i) evitar el daño, pérdida, alteración, hurto o destrucción de los datos personales, lo cual implica velar por la correcta operación de los procesos operativos y tecnológicos relacionados con esta materia; (ii) prevenir el uso, acceso o tratamiento no autorizado de los mismos, para lo cual se preverán niveles de acceso y circulación restringida de dicha información; (iii) incorporar los criterios de seguridad de los datos personales como parte integral de la adquisición, desarrollo y mantenimiento de los sistemas de información.

CAPITULO VI.

PROCEDIMIENTO PARA QUE LOS TITULARES PUEDAN EJERCER SUS DERECHOS A CONOCER, RECLAMAR (ACTUALIZAR, RECTIFICAR, SUPRIMIR) Y REVOCAR LA AUTORIZACIÓN

6.1 GENERALIDADES

Cualquier consulta o reclamo frente a derechos inherentes de los titulares sobre datos de carácter personal se debe realizar mediante un escrito dirigido a protecciondedatos@cruzrojacolombiana.org de la Sociedad Nacional - adjuntando fotocopia del documento de identidad del Titular interesado o cualquier otro documento equivalente que acredite su identidad y titularidad, relación parental, representación legal o competencia legal conforme a Derecho y los documentos que pretenda hacer valer.

Los derechos de acceso, actualización, rectificación, supresión y revocación de la autorización de datos personales son personalísimos y podrán ser ejercidos únicamente por el Titular, No obstante, el Titular podrá actuar a través de representante legal o apoderado cuando aquel se encuentre en situación de imposibilidad del ejercicio personal por sí mismo, por incapacidad o minoría de edad, en cuyo caso será necesario que sus causahabientes, representante legal o apoderado acrediten tal condición.

No se exigirá ningún valor o tasa alguna por el ejercicio de los derechos de acceso, actualización, rectificación, supresión o revocación de la autorización cuando se trate de datos personales de personas naturales que no hagan parte de los registros públicos. (Se tendrá en cuenta lo establecido en el artículo 21 del Decreto Reglamentario 1377 de 2013)

Con el objeto de facilitar el ejercicio de estos derechos, la Sociedad Nacional pondrá a disposición de los interesados, los formatos físicos o electrónicos adecuados a esta finalidad.

Una vez cumplidos y agotados los términos señalados por la Ley 1581 de 2012 y las demás

normas que la reglamenten o complementen, el Titular al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, actualización, rectificación, supresión y revocación, por parte de la Sociedad Nacional -, podrá poner en conocimiento ante la Autoridad Nacional de Protección de Datos Personales (Superintendencia de Industria y Comercio - Delegatura de Protección de Datos Personales) la negación o inconformidad frente al derecho ejercido.

6.2 PROCEDIMIENTOS

6.2.1 Consultas

Requisitos para la atención de Consultas.

- a) Se debe enviar una comunicación sea física o electrónica, esta debe contener como mínimo fecha de solicitud, fotocopia del documento de identificación, dirección de contacto (Física o Electrónica) y teléfono para efectos de notificación; para el representante del titular, documento autenticado que acredite la representación, si es el caso.
- b) Para ejercer este derecho por medio electrónico, el titular, su causahabiente, tercero autorizado o apoderado podrá formular la consulta por medio del correo electrónico destinado por la Sociedad Nacional de la Cruz Roja Colombiana. protecciondedatos@cruzrojacolombiana.org adjuntando la información anteriormente relacionada.
- c) Para ejercer este derecho por medio físico, su causahabiente, tercero autorizado o apoderado podrá radicar la consulta en cualquiera de las sedes de la Sociedad Nacional de la Cruz Roja Colombiana, adjuntando la información anteriormente relacionada.

Términos para la atención de consultas.

Independientemente del mecanismo que se implemente para la atención de solicitudes de consulta, éstas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. En el evento en el que una solicitud de consulta no pueda ser atendida dentro del término antes señalado, se informará al interesado antes del vencimiento del plazo las razones por las cuales no se ha dado respuesta a su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

6.2.2 Reclamos

El Titular, sus causahabientes, representantes legales o terceros interesados autorizados por la ley que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la normatividad sobre Protección de Datos Personales, podrán presentar un reclamo ante el responsable del tratamiento.

El reclamo lo podrá presentar el titular teniendo en cuenta la información señalada en el artículo 15 de la Ley 1581 de 2012 y las presentes reglas:

- a) Si el reclamo estuviese incompleto, el titular lo puede completar dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que se subsanen las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- b) En el caso de que quien reciba el reclamo no sea competente para resolverlo, se dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

- c) Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles

Requisitos para la atención de Reclamos, Rectificaciones, Actualización o Supresión de datos.

- a) El reclamo se formulara mediante solicitud escrita dirigida a la Sociedad Nacional de la Cruz Roja Colombiana y la comunicación debe contener como mínimo fecha de solicitud, descripción clara y detallada de los hechos que dan lugar al reclamo, fotocopia del documento de identificación, dirección de contacto (Física o Electrónica) y teléfono para efectos de notificación, así mismo debe venir acompañada del formato de reclamación de tratamiento de datos personales; para el representante del titular, documento autenticado que acredite la representación, si es el caso y copia de los documentos que pretenda hacer valer
- b) Para ejercer este derecho por medio electrónico, el titular, su causahabiente, representante legal, tercero autorizado o apoderado podrá formular la reclamación por medio del correo electrónico destinado por la Sociedad Nacional de la Cruz Roja Colombiana. protecciondedatos@cruzrojacolombiana.org adjuntando la información anteriormente relacionada.
- c) La persona interesada en ejercer este derecho deberá en todo caso, utilizar un medio que permita acreditar el envío y la recepción de la solicitud. Cualquiera que sea el medio utilizado para ejercer este derecho; la Sociedad Nacional de la Cruz Roja Colombiana atenderá la solicitud

siempre y cuando se cumpla con los requisitos indicados para la reclamación.

Términos para la atención de Reclamos.

El término máximo para atenderlo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

6.2.3 Revocar autorización

Todo titular de datos personales, sus causahabientes, representantes legales o terceros interesados autorizados por la Ley puede revocar, en cualquier momento, el consentimiento al tratamiento de éstos siempre y cuando no lo impida una disposición legal o contractual. Para ello, la Sociedad Nacional de la Cruz Roja Colombiana deberá establecer mecanismos sencillos y gratuitos que le permitan al titular revocar su consentimiento, al menos por el mismo medio por el que lo otorgó.

Requisitos para la atención de revocatoria de autorizaciones.

- a) La comunicación sea física o electrónica debe contener como mínimo fecha de solicitud, fotocopia del documento de identificación, dirección de contacto (Física o Electrónica) y teléfono para efectos de notificación; para el representante del titular, documento autenticado que acredite la representación, si es el caso.
- b) Para ejercer este derecho por medio electrónico, el titular, su causahabiente, tercero autorizado o apoderado podrá

formular la consulta por medio del correo electrónico destinado por la Sociedad Nacional de la Cruz Roja Colombiana. protecciondedatos@cruzrojacolombiana.org adjuntando la información anteriormente relacionada.

- c) La persona interesada en ejercer este derecho deberá en todo caso, utilizar un medio que permita acreditar el envío y la recepción de la solicitud. Cualquiera que sea el medio utilizado para ejercer este derecho; la Sociedad Nacional de la Cruz Roja Colombiana atenderá la solicitud siempre y cuando se cumpla con los siguientes establecidos en el presente Manual.

Términos para la atención de Revocatorias.

El término máximo para atenderlo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

CAPITULO VII.

FUNCIÓN DE PROTECCIÓN DE DATOS PERSONALES AL INTERIOR DE LA SOCIEDAD NACIONAL DE LA CRUZ ROJA COLOMBIANA

7.1 RESPONSABLES

La Sociedad Nacional designará como responsable del tratamiento de datos personales uno o varios referentes de Protección de Datos Personales, quienes se encargarán de recibir, procesar y canalizar las distintas solicitudes que se reciban, y las harán llegar a la respectiva dependencia encargadas del tratamiento, dependencias que una vez reciban estas

comunicaciones, entraran a cumplir con la función de protección de datos personales, y deberán dar trámite a las solicitudes de los titulares, en los términos, plazos y condiciones establecido por la normatividad vigente, para el ejercicio de los derechos de acceso, consulta, rectificación, actualización, supresión y revocatoria a que se refiere la normatividad vigente sobre protección de datos personales

En el evento en que se considere que la Sociedad Nacional de la Cruz Roja Colombiana dio un uso contrario al autorizado y a las leyes aplicables, el Titular de los Datos podrá enviar una comunicación dirigida al (los) Referentes de Protección de Datos Personales de la Sociedad Nacional de la Cruz Roja Colombiana. Dirección: Avenida carrera 68 # 68 B-31- bloque sur, Protección de Datos Personales, Correo electrónico:

protecciondedatos@cruzrojacolombiana.org

7.2 ENCARGADOS

La Sociedad Nacional de la Cruz Roja Colombiana como organización, y en los términos establecidos en la normatividad vigente, actuara como RESPONSABLE DEL TRATAMIENTO de Datos Personales; y las distintas dependencias actuaran como ENCARGADOS DEL TRATAMIENTO de datos personales.

7.3. COMITÉ DE PROTECCIÓN DE DATOS PERSONALES

El **Comité de Protección de Datos Personales** es el órgano encargado de definir, implementar, generar lineamientos y supervisar las políticas y estrategias de protección de datos dentro de la institución, garantizando el cumplimiento de la normativa vigente en materia de privacidad, protección y seguridad de la información.

7.3.1. Composición del Comité

El comité estará integrado por los siguientes miembros:

- **Dirección Ejecutiva Nacional:** Responsable de liderar y respaldar estratégicamente la política de protección de datos, asegurando su alineación con los objetivos institucionales.
- **Oficina Jurídica:** Encargada de interpretar y garantizar el cumplimiento de la normativa en materia de protección de datos, así como de asesorar en la gestión de riesgos legales relacionados.
- **Oficina de Riesgos:** Responsable de identificar, evaluar y mitigar los riesgos asociados al tratamiento de datos personales en la institución.
- **Oficina de Tecnologías de la Información y Comunicaciones (TICs):** Encargada de implementar y supervisar las medidas técnicas y de seguridad necesarias para la protección de la información y la prevención de incidentes de seguridad.

7.3.2. Actividades a cargo del Comité

Las siguientes atribuciones se presentan como orientadoras y podrán ampliarse, modificarse o ajustarse según las necesidades de la institución y las disposiciones normativas vigentes:

1. Proponer la actualización de la política de protección de datos personales en concordancia con la normativa vigente.
2. Generar los lineamientos para garantizar la protección de datos dentro de la Institución, asegurando el cumplimiento de la normativa vigente y promoviendo buenas prácticas en la gestión de la información confidencial.
3. Supervisar la implementación de medidas técnicas, organizativas y legales

para garantizar la seguridad y confidencialidad de los datos personales.

4. Evaluar y mitigar riesgos asociados al tratamiento de datos personales dentro de la institución.
5. Atender y resolver incidentes de seguridad de la información relacionados con la protección de datos personales.
6. Brindar capacitación y sensibilización al personal sobre buenas prácticas en la gestión de datos personales.
7. Revisar y aprobar contratos, acuerdos y o cualquier otro documento a suscribir a terceros que impliquen el tratamiento de datos personales, asegurando el cumplimiento de las normativas de protección de datos.
8. Garantizar el cumplimiento de derechos de los titulares de los datos, tales como acceso, rectificación, actualización, supresión y revocatoria de la autorización.
9. Atender auditorías y requerimientos de las autoridades de protección de datos, asegurando la trazabilidad y cumplimiento normativo.
10. Y las demás actividades que le sean asignadas por la Dirección Ejecutiva Nacional en el marco de sus competencias.

7.4. REFERENTE DE PROTECCIÓN DE DATOS PERSONALES

El/los **Referentes de Protección de Datos Personales** tendrá un rol clave en la implementación, supervisión y fortalecimiento de la estrategia de protección de datos, en línea con las obligaciones legales y buenas prácticas en la materia.

7.4.1 Actividades a cargo del/los Referentes de Protección de Datos Personales

Las siguientes actividades se presentan como orientadoras y podrán ampliarse, modificarse o ajustarse según las necesidades de la institución y las disposiciones normativas vigentes:

- Coordinar la aplicación de la política de protección de datos dentro de la institución.
- Actuar como enlace con la autoridad de control en materia de protección de datos personales.
- Asesorar a las distintas áreas de la organización sobre el cumplimiento normativo en la recolección, almacenamiento, uso y transferencia de datos personales.
- Gestionar solicitudes, quejas y reclamaciones de los titulares de datos personales.
- Monitorear y evaluar el cumplimiento de medidas de seguridad en la protección de datos personales.
- Reportar incidentes de seguridad y coordinar acciones correctivas y preventivas con el comité de protección de datos personales
- Liderar auditorías y revisiones internas para verificar el cumplimiento de la normativa de protección de datos.
- Y las demás actividades que le sean asignadas por la Dirección Ejecutiva Nacional en el marco de sus competencias.

CAPITULO VIII.

GESTIÓN DE INFORMACIÓN CONFIDENCIAL

8.1 DEFINICIÓN - INFORMACIÓN CONFIDENCIAL

Se entiende por **información confidencial** cualquier tipo de información, dato o

documento, en cualquier formato, cuyo acceso, divulgación o uso no autorizado pueda comprometer la seguridad, integridad o cumplimiento de la misión institucional.

Esta información puede incluir, entre otros:

- Datos personales de beneficiarios, voluntarios colaboradores, donantes entre otros.
- Información financiera de la Institución y de sus donantes.
- Estrategias operativas y planes de respuesta humanitaria.
- Acuerdos y alianzas con terceros.
- Cualquier otro documento clasificado como confidencial por la Institución.

8.2. PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL

Las medidas de protección de la información confidencial serán definidas por el Comité de Protección de Datos Personales, con el fin de garantizar la confidencialidad y seguridad de la información.

8.3. DEBER DE SECRETO Y CONFIDENCIALIDAD

El uso indebido, divulgación no autorizada o apropiación de información confidencial, así como la inobservancia del Principio de Confidencialidad y el incumplimiento de los deberes allí descritos, serán sancionados de conformidad con lo previsto en el Reglamento Interno de Trabajo y la legislación vigente.

CAPITULO IX

LEGISLACIÓN APLICABLE Y VIGENCIA

9.1. MARCO LEGAL

El presente Manual Políticas y Procedimientos de protección de datos personales ha sido

elaborado en concordancia con las siguientes normas y documentos:

- Constitución Política, artículo 15.
- Ley 852 de 2003
- Ley 1266 de 2008
- Ley 1273 de 2009
- Ley 1581 de 2012
- Decreto Reglamentario No. 1727 de 2009 y Decreto Reglamentario parcial No. 1377 de 2013
- Decreto Único No. 1074 de 2015
- Sentencias de la Corte Constitucional C-1011 de 2008 y C-748 del 2011
- Sentencias de la Corte Constitucional T-729 de 2002 y T-414 de 2010
- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio
- Circular Externa 008 de 2017 de la Superintendencia de Industria y Comercio
- Reglamento Interno de Trabajo.

9.2. VIGENCIA

El presente Manual rige a partir del **27 de junio de 2025**.

Actualizaciones del Manual: La Sociedad Nacional de la Cruz Roja Colombiana podrá modificar los términos y condiciones del presente documento de procedimientos como parte del esfuerzo por cumplir con las obligaciones establecidas por la Ley 1581 de 2012, los decretos reglamentarios y demás normas que complementen, modifiquen o deroguen lo contenido en este documento, con el fin de reflejar cualquier cambio. En los casos que esto ocurra se publicará el nuevo documento de políticas y procedimientos en la página de la Institución.



Cruz Roja Colombiana

ANEXO TÉCNICO

Al Manual de la Política de Protección de Datos Personales y
Sensibles

Sociedad Nacional de la Cruz Roja Colombiana

2025

TABLA DE CONTENIDO

1.	OBJETIVO.....	4
2.	ALCANCE	4
3.	DEFINICIONES TÉCNICAS.....	4
4.	ROLES Y RESPONSABILIDADES TÉCNICAS	5
	a) Comité de Protección de Datos Personales	5
	b) Referente de Protección de Datos Personales	6
	c) Administradores de Sistemas y Bases de Datos.....	6
	d) Usuarios Autorizados.....	7
	e) Proveedores y Terceros con Acceso a Información Personal.....	7
5.	ESQUEMA OPERATIVO DEL CICLO DEL DATO	8
	a) Identificación y clasificación de bases de datos	8
	i. Identificación y Análisis de Datos Existentes	8
	ii. Definición de Criterios para la Criticidad	8
	iii. Clasificación y Priorización de Bases de Datos.....	8
	iv. Asignación de Responsables	8
	v. Documentación y Formalización.....	9
	vi. Implementación de Controles iniciales	9
	b) Esquema para la recolección de datos	9
	c) Esquema para el uso y almacenamiento de datos.....	9
	d) Esquema para la transmisión y transferencia de datos	10
	e) Esquema para la anonimización y/o seudonimización de datos.....	10
	f) Esquema para la eliminación y destrucción segura de datos.....	10
	g) Esquema para la supresión o actualización de datos personales a solicitud del titular	
	11	
	i. Recepción de la Solicitud	11
	ii. Verificación de Identidad y Revisión de Requisitos.....	11
	iii. Análisis de Procedencia	11
	iv. Ejecución de la Supresión o Actualización.....	12
	v. Comunicación al Titular	12

vi.	Registro y Conservación de Evidencias.....	12
vii.	Notificación a Terceros.....	13
h)	Esquema para la gestión de incidentes y brechas de seguridad	13
i.	Detección y Reporte:	13
ii.	Clasificación y Evaluación:	13
iii.	Contención y Mitigación:.....	13
iv.	Notificación:	13
v.	Registro y Mejora:	13
6.	MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN	13
7.	PROGRAMA DE CAPACITACIÓN	14
8.	ANEXOS	14
9.	ACTUALIZACIÓN	14

1. OBJETIVO

El presente Anexo Técnico tiene por objeto complementar el Manual de la Política de Protección de Datos Personales y Sensibles de la Sociedad Nacional de la Cruz Roja Colombiana, detallando los aspectos técnicos, operativos y procedimentales necesarios para garantizar la protección integral de la información personal tratada por la Institución.

Su propósito es servir como guía práctica para la implementación, control y mejora continua de las medidas de seguridad de la información, fortaleciendo la confidencialidad, integridad y disponibilidad de los datos personales administrados.

2. ALCANCE

Este Anexo aplica a todos los procesos, sistemas, áreas y dependencias de la Sociedad Nacional de la Cruz Roja Colombiana que recolecten, almacenen, usen, circulen, transmitan o eliminen datos personales en el marco de sus actividades humanitarias, administrativas, comerciales o contractuales.

Incluye el tratamiento de datos personales en medios físicos y electrónicos, sin distinción del tipo de dato (público, privado, semiprivado o sensible), abarcando tanto información de titulares nacionales como internacionales.

3. DEFINICIONES TÉCNICAS

Seguridad de la Información: Conjunto de políticas, procesos, controles y medidas preventivas y reactivas orientadas a proteger la información contra su alteración, pérdida, destrucción, divulgación o acceso no autorizado. Su propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales y de toda información institucional, asegurando que solo las personas autorizadas accedan a ellos y que su uso se limite a las finalidades definidas.

Cifrado: Técnica criptográfica mediante la cual los datos se transforman en un formato ilegible o codificado, con el fin de impedir el acceso o comprensión de su contenido por parte de personas no autorizadas.

El cifrado puede aplicarse en tránsito (cuando los datos se transmiten por redes de comunicación) y en reposo (cuando están almacenados en sistemas o dispositivos). Solo quienes poseen las claves o certificados de descifrado pueden acceder al contenido original. Es una medida esencial para proteger información sensible y garantizar su confidencialidad.

Autenticación: Proceso mediante el cual se verifica la identidad de un usuario, sistema o dispositivo antes de permitirle el acceso a información o recursos institucionales.

La autenticación puede realizarse a través de distintos mecanismos, como contraseñas, tokens, biometría o autenticación multifactor (MFA). Su objetivo es confirmar que quien accede a los sistemas de información es realmente quien dice ser, reduciendo el riesgo de accesos indebidos o suplantaciones.

Seudonimización: ESQUEMA técnico que consiste en sustituir los datos personales que permiten identificar directamente a una persona por identificadores ficticios o códigos, de modo que no sea posible atribuir la información a un titular sin información adicional.

La seudonimización permite el tratamiento de datos con menor riesgo de exposición, facilitando su uso en investigaciones, estadísticas o análisis internos, siempre que las claves de correspondencia se mantengan bajo medidas de seguridad estrictas y separadas del conjunto principal de datos.

Anonimización: Proceso irreversible mediante el cual se eliminan o modifican los datos personales de manera que resulte imposible identificar, directa o indirectamente, a la persona titular.

La anonimización se aplica principalmente a fines estadísticos, científicos o históricos, cuando la identificación del titular no es necesaria. A diferencia de la seudonimización, la anonimización no permite revertir el proceso para conocer la identidad del titular, garantizando plenamente su privacidad.

Incidente de Seguridad: Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del Tratamiento o por su Encargado.

Todo incidente debe ser reportado inmediatamente al Referente de Protección de Datos Personales y al Comité de Protección de Datos para su análisis, registro, mitigación y eventual notificación a la autoridad competente.

Trazabilidad: Capacidad de registrar y reconstruir el historial, uso, modificaciones y flujo de los datos personales a lo largo de su ciclo de vida dentro de los sistemas de información.

La trazabilidad permite identificar quién accedió, cuándo, desde dónde y qué acciones realizó sobre la información, constituyéndose en un elemento esencial para la auditoría, el control interno y la detección de incidentes o usos indebidos de datos.

Respaldo (Backup): Copia de seguridad de los datos personales y de la información institucional, realizada con el propósito de permitir su recuperación ante pérdidas, daños, ataques cibernéticos o desastres.

Los respaldos deben efectuarse de manera periódica, segura y verificable, almacenándose en entornos protegidos y, cuando sea posible, fuera del sitio principal (off-site). Su gestión debe formar parte del plan de continuidad del negocio y del plan de recuperación ante desastres de la institución.

4. ROLES Y RESPONSABILIDADES TÉCNICAS

Con el fin de garantizar la adecuada implementación y cumplimiento de las medidas técnicas, organizativas y de seguridad establecidas en la Política y el presente Anexo, la Sociedad Nacional de la Cruz Roja Colombiana define los siguientes roles y responsabilidades:

a) Comité de Protección de Datos Personales

El **Comité de Protección de Datos Personales** es el órgano técnico–estratégico encargado de dirigir, coordinar y supervisar la gestión integral de la protección de datos en la Institución.

Responsabilidades:

1. Proponer la actualización de la política de protección de datos personales en concordancia con la normativa vigente.

2. Generar los lineamientos para garantizar la protección de datos dentro de la Institución, asegurando el cumplimiento de la normativa vigente y promoviendo buenas prácticas en la gestión de la información confidencial.
3. Supervisar la implementación de medidas técnicas, organizativas y legales para garantizar la seguridad y confidencialidad de los datos personales.
4. Evaluar y mitigar riesgos asociados al tratamiento de datos personales dentro de la institución.
5. Atender y resolver incidentes de seguridad de la información relacionados con la protección de datos personales.
6. Brindar capacitación y sensibilización al personal sobre buenas prácticas en la gestión de datos personales.
7. Revisar y aprobar contratos, acuerdos y o cualquier otro documento a suscribir a terceros que impliquen el tratamiento de datos personales, asegurando el cumplimiento de las normativas de protección de datos.
8. Garantizar el cumplimiento de derechos de los titulares de los datos, tales como acceso, rectificación, actualización, supresión y revocatoria de la autorización.
9. Atender auditorías y requerimientos de las autoridades de protección de datos, asegurando la trazabilidad y cumplimiento normativo.

b) Referente de Protección de Datos Personales

El **Referente de Protección de Datos Personales** es la figura operativa responsable de coordinar la aplicación del manual, las políticas y este anexo técnico.

Responsabilidades:

- Coordinar la aplicación de la política de protección de datos dentro de la institución.
- Actuar como enlace con la autoridad de control en materia de protección de datos personales.
- Asesorar a las distintas áreas de la organización sobre el cumplimiento normativo en la recolección, almacenamiento, uso y transferencia de datos personales.
- Gestionar solicitudes, quejas y reclamaciones de los titulares de datos personales.
- Monitorear y evaluar el cumplimiento de medidas de seguridad en la protección de datos personales.
- Reportar incidentes de seguridad y coordinar acciones correctivas y preventivas con el comité de protección de datos personales
- Liderar auditorías y revisiones internas para verificar el cumplimiento de la normativa de protección de datos.

c) Administradores de Sistemas y Bases de Datos

Los **Administradores de Sistemas y Bases de Datos** son responsables de garantizar la seguridad tecnológica e infraestructura que soporta el tratamiento de los datos personales.

Responsabilidades:

- Implementar y mantener las medidas técnicas de seguridad (firewalls, cifrado, antivirus, autenticación multifactor, registros de auditoría, etc.).
- Controlar y auditar los accesos a los sistemas y bases de datos que contengan información personal.

- Gestionar los mecanismos de respaldo y recuperación de la información (copias de seguridad, planes de contingencia, continuidad del negocio).
- Documentar y mantener actualizados los inventarios de activos tecnológicos relacionados con el tratamiento de datos personales.
- Reportar de inmediato cualquier incidente o vulnerabilidad detectada al Referente de Protección de Datos Personales y al Comité.
- Garantizar que las actualizaciones, parches y configuraciones de seguridad se apliquen de forma oportuna.
- Asegurar que la eliminación o transferencia de datos se realice conforme a los esquemas operativos seguros establecidos.

d) Usuarios Autorizados

Los **Usuarios Autorizados** son los funcionarios, contratistas o voluntarios que, por razón de sus funciones, tienen acceso a sistemas, archivos o bases de datos que contienen información personal.

Responsabilidades:

- Utilizar los sistemas informáticos y la información únicamente para los fines autorizados y en el marco de sus funciones.
- Mantener la confidencialidad de la información y de sus credenciales de acceso.
- Cumplir las políticas institucionales sobre contraseñas, seguridad de dispositivos y uso responsable de la información.
- No compartir, copiar o divulgar información personal sin autorización expresa.
- Reportar inmediatamente cualquier incidente, pérdida o acceso no autorizado al Referente de Protección de Datos o al Comité.
- Participar en las capacitaciones sobre protección de datos personales y seguridad de la información.

e) Proveedores y Terceros con Acceso a Información Personal

Los **Proveedores y Terceros** que, en virtud de un contrato, convenio o alianza, tengan acceso a datos personales, son considerados encargados del tratamiento y deberán cumplir con los mismos estándares de seguridad exigidos por la Institución.

Responsabilidades:

- Suscribir acuerdos de confidencialidad y cláusulas de tratamiento de datos personales conforme a la Ley 1581 de 2012 y al Decreto 1377 de 2013.
- Implementar medidas técnicas, organizativas y físicas equivalentes a las de la Sociedad Nacional de la Cruz Roja Colombiana.
- Garantizar la protección de los datos personales contra accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.
- Permitir y colaborar en las auditorías de cumplimiento que realice la Institución.
- Notificar inmediatamente cualquier incidente de seguridad que involucre información de la Cruz Roja Colombiana.
- Eliminar o devolver de manera segura la información una vez finalizada la relación contractual o cumplida la finalidad del tratamiento.

5. ESQUEMA OPERATIVO DEL CICLO DEL DATO

La Sociedad Nacional de la Cruz Roja Colombiana establece los siguientes esquemas operativos para asegurar la correcta gestión del ciclo de vida de los datos personales y sensibles —desde su recolección hasta su eliminación o anonimización— y para garantizar una respuesta eficaz ante incidentes de seguridad que puedan comprometer la información.

Cada esquema deberá documentarse, ejecutarse y mantenerse conforme a los principios de confidencialidad, integridad, disponibilidad, legalidad y finalidad, así como a las disposiciones de la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas aplicables.

a) Identificación y clasificación de bases de datos

Objetivo: Reconocer las Bases de Datos críticas y definir responsables en cada una de las áreas.

Lineamientos:

i. Identificación y Análisis de Datos Existentes

- Realizar un inventario exhaustivo de todas las bases de datos que maneja la organización.
- Analizar los tipos de datos almacenados en cada base, enfocándose en datos personales, sensibles y operativos que tienen relevancia para la misión institucional.
- Evaluar el propósito y la función de cada base de datos, considerando el impacto que tendría su pérdida, alteración o indisponibilidad en la organización.

ii. Definición de Criterios para la Criticidad

- Establecer criterios claros para determinar qué bases de datos son críticas, tales como:
 - Contiene información personal o sensible de alta confidencialidad.
 - Son esenciales para la continuidad operativa o para la atención de beneficiarios.
 - Están sujetas a regulaciones legales estrictas (por ejemplo, la Ley de Protección de Datos Personales en Colombia).
 - Impacto económico, reputacional y operativo en caso de falla o divulgación no autorizada.

iii. Clasificación y Priorización de Bases de Datos

- Clasificar las bases de datos según su nivel de criticidad con categorías (Críticas, semiprivadas, sensibles y públicas).
- Priorizarlas para asignar niveles diferenciados de protección y controles de seguridad.

iv. Asignación de Responsables

- Designar responsables para cada base de datos crítica:
 - Definir roles claros con funciones específicas, como custodios de la base de datos, administradores técnicos y delegados de protección de datos.
 - Responsables deben tener autoridad y competencia para gestionar la seguridad, integridad y uso adecuado de la información.

v. Documentación y Formalización

- Documentar formalmente la identificación, clasificación y responsables asignados.
- Establecer un registro actualizado que incluya descripción del contenido, nivel de criticidad, ubicación y responsable.
- Comunicar y formar a los responsables sobre sus obligaciones y protocolos de protección de datos.

vi. Implementación de Controles iniciales

- Verificar accesos y sistemas de seguridad iniciales con el involucramiento de responsables.
- Coordinar con el Oficial de Protección de Datos Personales para la supervisión y seguimiento.

Estas acciones aseguran un reconocimiento adecuado de las bases críticas y una responsabilidad clara que permita proteger eficazmente los datos personales en la organización, acorde a estándares legales y mejores prácticas.

Controles y Seguimiento:

- Registro obligatorio en el RNBD (Superintendencia de Industria y Comercio).
- Validación anual del inventario y responsables.

b) Esquema para la recolección de datos

Objetivo: Garantizar que la recolección de datos personales se realice de manera lícita, transparente y proporcional a la finalidad informada al titular.

Lineamientos:

- La recolección se efectuará únicamente cuando sea necesaria para el cumplimiento de las funciones institucionales o contractuales.
- Previamente, se informará al titular sobre las finalidades del tratamiento y los derechos que le asisten, mediante el **aviso de privacidad** o **formato de autorización**.
- Se verificará que la información recolectada sea pertinente, exacta y actualizada.
- Los formularios físicos o electrónicos deberán incluir la autorización expresa para el tratamiento de los datos.
- En el caso de menores de edad, se solicitará autorización al representante legal, respetando el principio del interés superior del niño o adolescente.

c) Esquema para el uso y almacenamiento de datos

Objetivo: Regular el tratamiento interno de los datos personales garantizando que su uso esté limitado a los fines autorizados por el titular y la ley.

Lineamientos:

- El acceso y uso de los datos se restringirá a los usuarios y áreas autorizadas según su rol institucional.
- Los sistemas y bases de datos deberán estar protegidos mediante controles de acceso, autenticación y trazabilidad.

- Toda operación sobre los datos (modificación, consulta, copia o traslado) deberá registrarse en los logs del sistema.
- Los datos sensibles serán objeto de un nivel de protección reforzado mediante cifrado y restricciones de acceso.
- Se prohíbe la reproducción o divulgación de información personal sin autorización expresa del titular o del Comité de Protección de Datos.
- Los datos deben ser almacenados en servidores seguros y segmentados
- Deben realizarse copias de seguridad cifradas y planes de recuperación (DRP).
- El equipo de Tic's realizada revisiones periódicas de seguridad

d) Esquema para la **transmisión y transferencia** de datos

Objetivo: Asegurar que toda transmisión o transferencia nacional o internacional de datos personales se realice con las debidas garantías de seguridad y legalidad.

Lineamientos:

- Toda transmisión o transferencia deberá estar soportada en un contrato o acuerdo de confidencialidad que incluya las cláusulas de protección de datos personales.
- Se deberá verificar que el receptor de la información cuente con niveles adecuados de protección, conforme a la legislación vigente.
- Los datos se transmitirán utilizando canales cifrados y protocolos seguros (como HTTPS, VPN o SFTP).
- En el caso de transferencias internacionales, se requerirá concepto favorable del Comité de Protección de Datos y, cuando aplique, la autorización del titular.
- Se llevará un registro de las transferencias y transmisiones efectuadas, indicando fecha, destinatario, propósito y nivel de riesgo.

e) Esquema para la **anonimización y/o seudonimización** de datos

Objetivo: Proteger la identidad de los titulares cuando los datos sean utilizados con fines estadísticos, investigativos o de análisis institucional.

Lineamientos:

- La anonimización se aplicará cuando sea posible eliminar toda referencia que permita identificar directa o indirectamente al titular.
- La seudonimización se empleará en aquellos casos en que sea necesario conservar un identificador reversible, bajo custodia segura y separada de los datos principales.
- Se utilizarán técnicas como enmascaramiento, agregación o sustitución de identificadores.
- El proceso deberá ser documentado, asegurando que las claves o equivalencias se almacenen bajo controles de acceso estrictos.
- Una vez anonimizada la información, se considerará fuera del ámbito de aplicación de la Ley 1581 de 2012.

f) Esquema para la **eliminación y destrucción** segura de datos

Objetivo: Asegurar que la supresión de datos personales se realice de manera definitiva, evitando su recuperación o acceso no autorizado.

Lineamientos:

- La eliminación de datos se efectuará una vez cumplida la finalidad del tratamiento o vencido el periodo legal o contractual de conservación.

- Para medios electrónicos, se aplicarán técnicas de **borrado seguro** o **sobrescritura** certificadas.
- Para archivos físicos, se utilizarán métodos de **triturado, incineración o destrucción certificada** mediante proveedores autorizados.
- Se deberá generar un acta o registro que documente la eliminación o destrucción efectuada, con la fecha, responsable y método utilizado.
- La eliminación será aprobada por el Referente de Protección de Datos Personales y registrada para efectos de auditoría.

g) Esquema para la **supresión o actualización** de datos personales a solicitud del titular

Objetivo: Establecer las directrices y pasos que debe seguir la Sociedad Nacional de la Cruz Roja Colombiana para atender de manera oportuna, segura y conforme a la ley, las solicitudes de supresión o actualización de datos personales realizadas por los titulares o sus representantes autorizados.

Lineamientos:

i. Recepción de la Solicitud

El titular o su representante deberá presentar la solicitud de supresión o actualización mediante los canales oficiales:

- Correo electrónico institucional: protecciondedatos@cruzrojacolombiana.org
- Formulario físico o electrónico habilitado para el ejercicio de derechos (Acceso, Rectificación, Cancelación y Oposición).
- Correspondencia escrita dirigida al Referente de Protección de Datos Personales.
- La solicitud deberá contener:
 1. Nombre completo y documento de identificación del titular.
 2. Descripción precisa de la solicitud (supresión, corrección o actualización).
 3. Copia del documento de identidad o poder si actúa por representación.
 4. Datos de contacto para notificaciones.

ii. Verificación de Identidad y Revisión de Requisitos

- El Referente de protección de datos verificará la autenticidad de la identidad del solicitante y la integridad de la documentación aportada.
- Si la información es incompleta, se requerirá al titular dentro de los **cinco (5) días hábiles** siguientes a la recepción, para que subsane la solicitud.
- Si no se completa la información en el término de **dos (2) meses**, se entenderá desistida la petición.

iii. Análisis de Procedencia

- El Referente de protección de datos evaluará si la solicitud de supresión o actualización procede conforme a la ley.
- No procederá la supresión cuando:
 - Exista un deber legal o contractual de conservar la información.
 - La información sea necesaria para cumplir una obligación legal o contractual vigente.

- La información deba conservarse por motivos de interés público, histórico o estadístico.
- En caso de actualización, se verificará la consistencia y validez de los nuevos datos aportados por el titular.
- iv. Ejecución de la Supresión o Actualización
 - Si la solicitud es procedente, el área responsable del tratamiento deberá ejecutar la acción ordenada por el Referente de protección de datos dentro de los **quince (15) días hábiles** siguientes.
 - **En caso de actualización:** se registrarán los nuevos datos en los sistemas correspondientes y se dejará trazabilidad de la modificación.
 - **En caso de supresión:**
 - Los datos serán eliminados o bloqueados de todas las bases de datos y respaldos activos.
 - Si no es posible su eliminación inmediata por razones técnicas o legales, se procederá a su **bloqueo temporal**, evitando su tratamiento posterior.
 - Se documentará la acción realizada en el **Registro de Actividades de Tratamiento** y en el expediente del titular.
- v. Comunicación al Titular
 - Una vez ejecutada la supresión o actualización, el Referente de protección de datos informará por escrito al titular, indicando:
 - Resultado de la solicitud.
 - Fecha de la acción.
 - Área responsable que la ejecutó.
 - Fundamentos legales en caso de negativa.
 - Si la solicitud fue improcedente, se comunicará al titular en un término no mayor a **diez (10) días hábiles**, exponiendo los motivos de la decisión.
- vi. Registro y Conservación de Evidencias
 - Toda solicitud deberá quedar registrada y documentada por los Referentes de Protección de datos Personales de la Institución, utilizando los medios institucionales disponibles (como correo electrónico o archivo físico/digital), e incluyendo:
 - Copia de la solicitud y respuesta.
 - Evidencia de la actualización o eliminación realizada.
 - Acta de validación del Referente de protección de datos.
 - La evidencia del trámite se conservará por un periodo mínimo de **cinco (5) años** para fines de auditoría y control.

vii. Notificación a Terceros

Si los datos personales hubiesen sido transmitidos o compartidos con terceros encargados del tratamiento, el Referente de protección de datos notificará a dichos terceros sobre la supresión o actualización realizada, para que adopten la misma acción en sus registros.

h) Esquema para la **gestión de incidentes y brechas de seguridad**

Objetivo: Detectar, analizar, responder y notificar oportunamente los incidentes que afecten o puedan afectar la seguridad de la información personal o institucional.

Lineamientos:

i. Detección y Reporte:

- Todo colaborador, contratista o proveedor deberá reportar inmediatamente cualquier incidente a los **Referentes de Protección de Datos Personales** mediante el canal designado (protecciondedatos@cruzrojacolombiana.org).

ii. Clasificación y Evaluación:

- Los Referentes de Protección de Datos y el Comité de Protección de Datos evaluarán la gravedad del incidente, determinando su impacto en la confidencialidad, integridad o disponibilidad de los datos.

iii. Contención y Mitigación:

- Se implementarán medidas inmediatas para contener la brecha, proteger los sistemas afectados y evitar la propagación del daño.

iv. Notificación:

- En caso de que el incidente represente un riesgo significativo para los derechos de los titulares, se notificará a la **Superintendencia de Industria y Comercio** dentro de los plazos legales, e informará al titular afectado cuando corresponda.

v. Registro y Mejora:

- Todo incidente deberá documentarse en el formato de registro de incidentes, con detalle de causas, medidas adoptadas y lecciones aprendidas.
- El Comité realizará seguimiento al cierre del incidente y propondrá acciones de mejora preventiva.

6. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información tratada en el marco del ciclo del dato, se establecen las siguientes medidas de seguridad:

- **Medidas Organizativas:** Definición de roles y responsabilidades en el tratamiento de la información, control de usuarios y gestión de accesos, implementación de políticas de contraseñas seguras, realización periódica de copias de seguridad y adopción de un plan de continuidad de la operación.
- **Medidas Técnicas:** Aplicación de mecanismos de cifrado para la protección de la información, uso de firewalls y sistemas antivirus actualizados, implementación de autenticación

multifactor y establecimiento de registros de trazabilidad para el seguimiento de actividades sobre los datos.

- **Medidas Físicas:** Control de acceso a las instalaciones donde se almacenan o tratan los datos, custodia segura de archivos físicos y dispositivos, y procedimientos para el transporte y destrucción certificada de soportes o documentos que contengan información.

7. PROGRAMA DE CAPACITACIÓN

Con el propósito de garantizar el conocimiento y la aplicación adecuada de las disposiciones en materia de protección de datos personales, se implementa un programa anual de formación dirigido a colaboradores, contratistas y voluntarios, orientado al fortalecimiento de las competencias y responsabilidades relacionadas con el tratamiento de la información.

De manera complementaria, se desarrollan campañas periódicas de sensibilización encaminadas a fomentar la cultura de la confidencialidad, la protección de datos y las buenas prácticas en ciberseguridad dentro de la Institución.

8. ANEXOS

1. Formato de autorización de datos
2. Formatos de registro de incidentes
3. Matriz de riesgos de datos personales
4. Formulario físico o electrónico habilitado para el ejercicio de derechos por parte de los titulares

9. ACTUALIZACIÓN

El presente anexo será revisado y actualizado cada dos años o antes si hay cambios normativos, tecnológicos o institucionales.