

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA
MONTSERRAT

NIT: 8600074005
2596000
CL 134 17 71
Bogotá, Distrito Capital - Colombia
atencionalusuario@icsn.co y comunicaciones@icsn.co

Manual de políticas web

1. Base legal y ámbito de aplicación

La política de tratamiento de la información se desarrolla en cumplimiento de los artículos 15 y 20 de la Constitución Política; de los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD); y del artículo 13 del Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

2. Definiciones establecidas en el artículo 3 de la LEPD y el artículo 3 del Decreto 1377 de 2013

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **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.
- **Datos sensibles:** Se entiende por datos sensible aquellos 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.

- **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.
- **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.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **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.
- **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.

3. Autorización de la política de tratamiento

De acuerdo al artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

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

4. Responsable del tratamiento

El responsable del tratamiento de las bases de datos objeto de esta política es **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, cuyos datos de contacto son los siguientes:

Dirección:

CL 134 17 71 Bogotá, Distrito Capital - Colombia

Correo electrónico:

atencionalusuario@icsn.co y comunicaciones@icsn.co

Teléfono:

2596000

5. Tratamiento y finalidades de las bases de datos

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

La siguiente tabla (Tabla I) presenta las distintas bases de datos que manejan la empresa y las finalidades asignadas a cada una de ellas.

Tabla 1. Bases de datos y finalidades

Finalidad:

6. Datos de navegación

El sistema de navegación y el software necesario para el funcionamiento de esta página web recogen algunos datos personales, cuya transmisión se haya implícita en el uso los protocolos de comunicación de Internet.

Por su propia naturaleza, la información recogida podría permitir la identificación de usuarios a través de su asociación con datos de terceros aunque no se obtenga para ese fin. En esta categoría de datos se encuentran, la dirección IP o el nombre de dominio del equipo utilizado por el usuario para acceder a la página web, la dirección URL, la fecha y hora y otros parámetros relativos al sistema operativo del usuario.

Estos datos se utilizan con la finalidad exclusiva de obtener información estadística anónima sobre el uso de la página web o controlar su correcto funcionamiento técnico, y se cancelan inmediatamente después de ser verificados.

7. Cookies o web bugs

Este sitio web no utiliza cookies o web bugs para recabar datos personales del usuario, sino que su utilización se limita a facilitar al usuario el acceso a la página web. El uso de cookies de sesión, no memorizadas de forma permanente en el equipo del usuario y que desaparecen cuando cierra el navegador, únicamente se limitan a recoger información técnica para identificar la sesión con la finalidad de facilitar el acceso seguro y eficiente de la página web. Si no desea permitir el uso de cookies puede rechazarlas o eliminar las ya existentes configurando su navegador, e inhabilitando el código Java Script del navegador en la configuración de seguridad.

8. Derechos de los titulares

De acuerdo con el artículo 8 de la LEPD y a los artículos 21 y 22 del Decreto 1377 de 2013, los Titulares de los datos pueden ejercer una serie de derechos en relación al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

1. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
2. Por sus causahabientes, quienes deberán acreditar tal calidad.
3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus datos personales.
- **Derechos de quejas y reclamos:** La Ley distingue cuatro tipos de reclamos:
 - **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.
- **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.
- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

9. Atención a los Titulares de datos

AURA VICTORIA CARRASCAL MARQUEZ identificado(a) con CC número **51624869** de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos. Teléfono: 2596000, Correo electrónico: atencionalusuario@icsn.co y comunicaciones@icsn.co.

10. Procedimientos para ejercer los derechos del Titular

10.1. Derecho de acceso a consulta

Según el artículo 21 del Decreto 1377 de 2013, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, solamente podrá cobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal

efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, enviado, mediante correo electrónico a **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a **CL 134 17 71 Bogotá, Distrito Capital - Colombia**. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Telecopia.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

Una vez recibida la solicitud, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

10.2. Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA**

NERVIOSO - CLINICA MONTSERRAT, enviado, mediante correo electrónico a **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a **CL 134 17 71 Bogotá, Distrito Capital - Colombia**, la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane 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.

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. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

11. Medidas de seguridad

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación se exponen las medidas de seguridad implantadas por el NOMBRE DE LA INSTITUCIÓN O EMPRESA, que están recogidas y desarrolladas en su Manual Interno de Seguridad (Tablas II, III, IV y V).

Tabla 2. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)

Gestión de documentos y soportes

1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.
2. Acceso restringido al lugar donde se almacenan los datos.
3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.
4. Sistema de etiquetado o identificación del tipo de información.
5. Inventario de soportes.

Control de acceso

1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones.
2. Lista actualizada de usuarios y accesos autorizados.
3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados.
4. Concesión, alteración o anulación de permisos por el personal autorizado.

Incidencias

1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.
2. Procedimiento de notificación y gestión de incidencias.

Personal

1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos.

2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.
3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.

Manual interno de seguridad

1. Elaboración e implementación del Manual de obligado cumplimiento para el personal.
2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

Tabla 3. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos

Bases de datos no automatizadas: Archivo

1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.

Bases de datos no automatizadas: Almacenamiento de documentos

1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.

Bases de datos no automatizadas: Custodia de documentos

1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.

Bases de datos automatizadas: Identificación y autenticación

1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.
2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.

Bases de datos automatizadas: Telecomunicaciones

1. Acceso a datos mediante redes seguras.

Tabla 4. Medidas de seguridad para datos privados según el tipo de bases de datos

Bases de datos automatizadas y no automatizadas: Auditoría

1. Auditoría ordinaria (interna o externa) cada dos meses.
2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información.
3. Informe de detección de deficiencias y propuesta de correcciones.
4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
5. Conservación del Informe a disposición de la autoridad.

Bases de datos automatizadas y no automatizadas: Responsable de seguridad

1. Designación de uno o varios responsable de seguridad.
2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad.
3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.

Bases de datos automatizadas y no automatizadas: Manual Interno de Seguridad

1. Controles periódicos de cumplimiento.

Bases de datos no automatizadas: Gestión de documentos y soportes

1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Bases de datos no automatizadas: Control de acceso

1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.

Bases de datos no automatizadas: Identificación y autenticación

1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.

Bases de datos no automatizadas: Incidencias

1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.

2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Tabla 5. Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas: Control de acceso

1. Acceso solo para personal autorizado.
2. Mecanismo de identificación de acceso.
3. Registro de accesos de usuarios no autorizados.

Bases de datos no automatizadas: Almacenamiento de documentos

1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.

Bases de datos no automatizadas: Copia o reproducción

1. Sólo por usuarios autorizados.
2. Destrucción que impida el acceso o recuperación de los datos.

Bases de datos no automatizadas: Traslado de documentación

1. Medidas que impidan el acceso o manipulación de documentos.

Bases de datos automatizadas: Gestión de documentos y soportes

1. Sistema de etiquetado confidencial.
2. Cifrado de datos.
3. Cifrado de dispositivos portátiles cuando salgan fuera.

Bases de datos automatizadas: Control de acceso

1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.
2. Control del registro de accesos por el responsable de seguridad. Informe mensual.
3. Conservación de los datos: 2 años.

Bases de datos automatizadas: Telecomunicaciones

1. Transmisión de datos mediante redes electrónicas cifradas.

12. Transferencia de datos a terceros países

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

13. Vigencia

Las bases de datos responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual

que requiera su conservación. Por todo ello, dicha base de datos ha sido creada sin un periodo de vigencia definido.

Firma:

Representante legal:

AURA VICTORIA CARRASCAL MARQUEZ

Documento de identidad:

51624869

Manual interno de políticas de seguridad de base de datos

Índice

1. Base legal y ámbito de aplicación
2. Definiciones
3. Cumplimiento y actualización
4. Medidas de seguridad
 1. Medidas de seguridad comunes
 2. Medidas de seguridad para bases de datos no automatizadas
 3. Medidas de seguridad para bases de datos automatizadas
5. Funciones y obligaciones del personal
6. Bases de datos y sistemas de información
7. Procedimiento de notificación, gestión y respuesta ante incidencias
8. Medidas para el transporte, destrucción y reutilización de documentos y soportes
9. Vigencia

1. Base legal y ámbito de aplicación

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, con objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y del Decreto 1377 de 2013, adopta este Manual Interno de Seguridad donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en el artículo 4 literal g) de la LEPD.

El presente manual pertenece a: **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

Dirección: CL 134 17 71 Bogotá, Distrito Capital - Colombia
Correo electrónico: atencionalusuario@icsn.co y comunicaciones@icsn.co
Teléfono: 2596000

Las disposiciones de este documento se aplican a las bases de datos objeto de responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, así como a los sistemas de información, soportes y

equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, a las personas que participan en el tratamiento y a los locales donde se ubican dichas bases de datos.

2. Definiciones de conceptos en materias de seguridad

- **Acceso autorizado:** Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autenticación correcta, generalmente mediante el ingreso de usuario y contraseña.
- **Autenticación:** Procedimiento de verificación de la identidad de un usuario.
- **Contraseña:** Señal secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autenticación de usuarios que permite el acceso autorizado.
- **Control de acceso:** Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autenticación.
- **Copia de respaldo:** Copia de los datos de una base de datos en un soporte que permita su recuperación.
- **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.
- **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.
- **Perfil de usuario:** Grupo de usuarios a los que se da acceso.
- **Recurso protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.
- **Responsable de seguridad:** Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.
- **Sistema de información:** Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.
- **Soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
- **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

3. Cumplimiento y actualización

El Manual Interno de Seguridad es un documento interno de la empresa de obligatorio cumplimiento para todo el personal de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, con acceso a los sistemas de información que contengan datos personales.

Este manual debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

4. Medidas de seguridad

Las bases de datos son accesibles únicamente por las personas designadas por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, y referidas en el numeral 6 de este documento.

Los responsables de seguridad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, señalados en numeral 6 del presente manual, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación se enumeran y detallan las medidas de seguridad implementadas por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

4.1. Medidas de seguridad comunes

4.1.1. Gestión de documentos y soportes

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados están referidos en el numeral 6 sobre bases de datos y sistemas de información del presente manual.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en el Manual Interno de Seguridad.

La identificación de los documentos y soportes de contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con

significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

El inventario de documentos y soportes de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** debe incluirse como anexo del presente manual.

4.1.2 Control de acceso

El personal de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento en este manual.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Los usuarios autorizados para el acceso a las bases de datos se establecen en el numeral 6 de este manual.

4.1.3 Ejecución del tratamiento fuera de los locales

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de los locales requiere una autorización previa por parte de **INSTITUTO COLOMBIANO**

DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

4.1.4 Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado en el numeral 6 puede realizar copias o reproducir los documentos.

4.1.5 Responsable de seguridad

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

4.1.6 Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, clasificadas con nivel de seguridad sensible o privado, se han de someter, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

Las auditorías concluirán con un informe de auditoría que contendrá:

- El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- La identificación de las deficiencias halladas y la sugerencia de medidas correctoras o complementarias necesarias.
- La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

El responsable de seguridad que corresponda estudiará el informe y trasladará las conclusiones al responsable del tratamiento para que implemente las medidas correctoras. Los informes de auditoría serán adjuntados al Manual Interno de Seguridad y quedarán a disposición de la Autoridad de Control.

4.2 Medidas de seguridad para bases de datos no automatizadas

4.2.1 Archivo de documentos

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en el numeral 6 de este manual.

Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Los dispositivos se identifican y describen en el numeral 6 del presente manual.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente manual.

La descripción de las medidas de seguridad de almacenamiento de encuentran recogidas en el numeral 6 de este documento.

4.2.2 Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el numeral 6 del manual, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad en cuestión de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

4.3 Medidas de seguridad para bases de datos automatizadas

4.3.1. Identificación y autenticación

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc. La nomenclatura utilizada para la asignación de nombres de usuario para acceder al sistema de información y el sistema de autenticación de los usuarios se recogen en el numeral 6 de este documento.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y letras. La política de contraseñas de **INSTITUTO**

COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, se encuentra en el numeral 6 del presente manual.

Por otra parte, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días. El periodo de vigencia de las contraseñas se recoge en el ya referido numeral 6.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados, también detallado en el numeral 6 del manual.

4.3.2 Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío.

El sistema de registro de entrada y salida debe ser anexado en el presente documento.

4.3.3 Control de acceso físico

Los locales que son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; así mismo, han de cumplir con las medidas de seguridad físicas correspondientes al documento o soporte donde incluyen los datos.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en el presente manual. Los locales e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes se señalan en el numeral 6 del presente documento.

Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.

4.3.4 Copias de respaldo y recuperación de datos

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez a la semana, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello en este manual.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses.

Los procedimientos de copia y respaldo se recogen en numeral 6 de este manual.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

4.3.5 Registro de acceso

De los intentos de acceso a los sistemas de información de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, deberá guarda, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los responsables de seguridad de las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la

manipulación o desactivación de los mecanismos que permiten el registro de acceso.

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente en el presente documento.

4.3.6 Redes de comunicaciones

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

5. Funciones y obligaciones del personal

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de , deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, tablón de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente manual para que puedan conocer la normativa de seguridad de la empresa y sus obligaciones en esta materia en función del cargo que ocupan.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el numeral 6 sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, se definen, con carácter general,

según el tipo de actividad que desarrollan dentro de la empresa y, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el numeral 6 sobre bases de datos y sistemas de información. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este manual por parte del personal al servicio de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la empresa.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la empresa u organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.
- **Funciones de control y autorizaciones delegadas:** El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos, estos se anexarán en el presente manual.
- **Obligaciones relacionadas con las medidas de seguridad implantadas:**
 - Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
 - No revelar información a terceras personas ni a usuarios no autorizados.
 - Observar las normas de seguridad y trabajar para mejorarlas.
 - No realizar acciones que supongan un peligro para la seguridad de la información.
 - No sacar información de las instalaciones de la organización sin la debida autorización.
- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.
- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

- **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.
- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.
- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la empresa.
- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.
- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el numeral 4 del presente manual.

6. Bases de datos y sistemas de información

Las bases de datos almacenadas y tratadas por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

Tabla I. Bases de datos y nivel de seguridad

Base de datos
Seguridad
Sistema de tratamiento

Compuconta.
Privados
Informático (digital)

La siguiente tabla (Tabla II) recoge la estructura de las bases de datos de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

Tabla II. Estructura de las Bases de datos

Nombre de la base de datos:

Compuconta.

Responsable del tratamiento:

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT

NIT: 8600074005

Dirección: CL 134 17 71. Bogotá, Colombia

Teléfono: 2596000

Correo electrónico: atencionalusuario@icsn.co y comunicaciones@icsn.co

Encargado de consultas y reclamos:

AURA VICTORIA CARRASCAL MARQUEZ

CC: 51624869

Tipos de datos:

Privados

Sistema de tratamiento:

Informático (digital)

Origen y procedencia de los datos:

Personal asistencial, administrativos, autorizados para ingresar datos.

Colectivo o categoría de titulares:

Usuarios activos del sistema.

El nombramiento de los responsables de seguridad no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

Tabla III. Responsables de seguridad y medidas de seguridad de las bases de datos

Nombre de la base de datos:

Compuconta.

Responsable de seguridad:

Proceso de Tecnologías de Información y Comunicaciones.

Control de acceso físico:

Usuarios registrados con usuarios y contraseña

Gestión documental:

Sistema de copias de respaldo. Archivos físicos en carpetas con identificación del usuario.

Control de acceso lógico:

Usuario y contraseña

Copias de respaldo y procedimiento de recuperación:

Respaldo con 3 copias diarias y una copia redundante la última hora.

Sistema de identificación y autenticación:

Contraseña de mínimo 8 caracteres.

Registro de acceso a los documentos:

Usuarios autorizados por el sistema

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT identifica en este manual, a los encargados del tratamiento así como las condiciones del encargo. Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente manual.

7. Procedimiento de notificación, gestión y respuesta ante incidencias

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

- Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa deberá comunicarlo, de manera inmediata, a los responsables de seguridad, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la

persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

- Una vez comunicada la incidencia ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos y debe incluirse como anexo en el presente manual.

Asimismo, debe implementar los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

8. Medidas para el transporte, destrucción y reutilización de documentos y soportes

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Antes de iniciar la destrucción se realizara un acata o se llevara el registro en un libro o agenda, en dicha a notación se describirá el documento objeto de destrucción, la fecha, hora y firma de las dos personas que evidencian la destrucción.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**. Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en el presente manual.

9. Vigencia

El presente manual ha sido aprobado por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** aceptando su contenido, ordenando su ejecución y cumplimiento, con carácter general por todo el personal, y en particular, por aquellos a los referidos en este documento.

El presente Manual de Políticas de Seguridad permanece vigente desde **lunes, 1 de abril de 2019**.

Firma:

Representante legal:

AURA VICTORIA CARRASCAL MARQUEZ

Documento de identidad:

51624869



INSTITUTO COLOMBIANO
DEL SISTEMA NERVIOSO

ATENCIÓN Y SERVICIO CON CALIDAD HUMANA

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT

NIT: 8600074005

2596000

CL 134 17 71

Bogotá, Distrito Capital - Colombia

atencionalusuario@icsn.co y comunicaciones@icsn.co

Manual interno de políticas y procedimientos de tratamiento de datos

Índice

1. Base legal y ámbito de aplicación
2. Definiciones
3. Autorización para la política de tratamiento
4. Responsable del tratamiento
5. Tratamiento y finalidades de las bases de datos
6. Derechos de los titulares
7. Atención a los titulares de las bases de datos
8. Procedimientos para ejercer los derechos del titular
 1. Derecho de acceso o consulta
 2. Derechos de quejas y reclamos
9. Medidas de seguridad
10. Transferencia de datos a terceros países
11. Vigencia

1. Base legal y ámbito de aplicación

La política de tratamiento de la información se desarrolla en cumplimiento de los artículos 15 y 20 de la Constitución Política; de los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD); y del artículo 13 del Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

2. Definiciones establecidas en el artículo 3 de LEPD y el artículo 3 del Decreto 1377 de 2013

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **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.
- **Datos sensibles:** Se entiende por datos sensible aquellos 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.
- **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.
- **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.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **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.
- **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.

3. Autorización de la política de tratamiento

De acuerdo al artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de **INSTITUTO**

COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

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

4. Responsable del tratamiento

El responsable del tratamiento de las bases de datos objeto de esta política es **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, cuyos datos de contacto son los siguientes:

- **Dirección:** CL 134 17 71 Bogotá, Distrito Capital - Colombia
- **Correo electrónico:** atencionalusuario@icsn.co y comunicaciones@icsn.co
- **Teléfono:** 2596000

5. Tratamiento y finalidades de las bases de datos

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

La siguiente tabla (Tabla I) presenta las distintas bases de datos que manejan la empresa y las finalidades asignadas a cada una de ellas.

Tabla I. Bases de datos y finalidades

	Finalidad

6. Derechos de los titulares

De acuerdo con el artículo 8 de la LEPD y a los artículos 21 y 22 del Decreto 1377 de 2013, los Titulares de los datos pueden ejercer una serie de derechos en relación

al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

1. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
2. Por sus causahabientes, quienes deberán acreditar tal calidad.
3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus datos personales.
- **Derechos de quejas y reclamos:** La Ley distingue cuatro tipos de reclamos:
 - **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
 - **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
 - **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
 - **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.
- **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.
- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

7. Atención a los titulares de datos

Instituto Colombiano del sistema Nervioso- Clinica Montserrat identificado(a) con CC **860007400-5** será el encargado(a) de la atención de peticiones, consultas y reclamos ante el cual el titular de los datos puede ejercer sus derechos.

- **Teléfono:** 2596000
- **Correo electrónico:** tics@icsn.co

8. Procedimientos para ejercer los derechos del Titular

8.1 Derecho de acceso o consulta

Según el artículo 21 del Decreto 1377 de 2013, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, enviado, mediante correo electrónico a **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el asunto "ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a la dirección: **CL 134 17 71 Bogotá, Distrito Capital - Colombia**, la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.

- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por nombre de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

Una vez recibida la solicitud, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

8.2 Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, enviado, mediante correo electrónico a **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el asunto "ejercicio del derecho queja o reclamo", o a través de correo postal remitido a la dirección: **CL 134 17 71 Bogotá, Distrito Capital - Colombia**. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane 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.

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. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

9. Medidas de seguridad

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación se exponen las medidas de seguridad implantadas por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, que están recogidas y desarrolladas en su Manual Interno de Seguridad (Tablas II, III, IV y V).

Tabla II. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)

Auditoría

1. Auditoría ordinaria (interna o externa) cada año.
2. Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.
3. Informe de detección de deficiencias y propuesta de correcciones.
4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
5. Conservación del Informe a disposición de la autoridad.

Gestión de documentos y soportes

1. Medidas tales como, destructora de papel que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.
2. Acceso restringido al lugar donde se almacenan los datos.
3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.
4. Sistema de etiquetado o identificación del tipo de información.
5. Inventario de los soportes en los que se almacenan bases de datos.

Control de acceso

1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo al rol que desempeña.
2. Lista actualizada de usuarios y accesos autorizados.
3. Autorización escrita del titular de la información para la entrega de sus datos a terceras persona, para evitar el acceso a datos con derechos distintos de los autorizados.
4. Concesión, alteración o anulación de permisos por el personal autorizado.

Incidencias

1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.
2. Procedimiento de notificación y gestión de incidencias.

Personal

1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos.
2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.
3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.

Manual interno de seguridad

1. Elaboración e implementación del Manual de obligado cumplimiento para el personal.
2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

Tabla III. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos

Bases de datos no automatizadas: Archivo

1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.

Bases de datos no automatizadas: Almacenamiento de documentos

1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.

Bases de datos no automatizadas: Custodia de documentos

1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.

Bases de datos automatizadas: Identificación y autenticación

1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.
2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.

Bases de datos automatizadas: Telecomunicaciones

1. Acceso a datos mediante redes seguras.

Tabla IV. Medidas de seguridad para datos privados según el tipo de bases de datos

Bases de datos automatizadas y no automatizadas: Auditoría

1. Auditoría ordinaria (interna o externa) cada dos meses.
2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información.
3. Informe de detección de deficiencias y propuesta de correcciones.
4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
5. Conservación del Informe a disposición de la autoridad.

Bases de datos automatizadas y no automatizadas: Responsable de seguridad

1. Designación de uno o varios responsable de seguridad.
2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad.
3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.

Bases de datos automatizadas y no automatizadas: Manual Interno de Seguridad

1. Controles periódicos de cumplimiento.

Bases de datos no automatizadas: Gestión de documentos y soportes

1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Bases de datos no automatizadas: Control de acceso

1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.

Bases de datos no automatizadas: Identificación y autenticación

1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.

Bases de datos no automatizadas: Incidencias

1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.
2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Tabla 5. Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas: Control de acceso

1. Acceso solo para personal autorizado.
2. Mecanismo de identificación de acceso.
3. Registro de accesos de usuarios no autorizados.

Bases de datos no automatizadas: Almacenamiento de documentos

1. Archiveros, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.

Bases de datos no automatizadas: Copia o reproducción

1. Sólo por usuarios autorizados.
2. Destrucción que impida el acceso o recuperación de los datos.

Bases de datos no automatizadas: Traslado de documentación

1. Medidas que impidan el acceso o manipulación de documentos.

Bases de datos automatizadas: Gestión de documentos y soportes

1. Sistema de etiquetado confidencial.
2. Cifrado de datos.
3. Cifrado de dispositivos portátiles cuando salgan fuera.

Bases de datos automatizadas: Control de acceso

1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.
2. Control del registro de accesos por el responsable de seguridad. Informe mensual.
3. Conservación de los datos: 2 años.

Bases de datos automatizadas: Telecomunicaciones

1. Transmisión de datos mediante redes electrónicas cifradas.

10. Transferencia de datos a terceros países

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia en la de acuerdo con la circular 005 de 10 de agosto de 2017, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.

- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

11. Vigencia

Las bases de datos responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, dicha base de datos ha sido creada sin un periodo de vigencia definido.

La presente política de tratamiento permanece vigente desde .

Firma:

Representante legal:
AURA VICTORIA CARRASCAL MARQUEZ

Documento de identidad:
51624869

Protocolo de atención al titular de los datos

1. Objetivo del documento

El objetivo del presente Protocolo es poner en conocimiento de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, el procedimiento a seguir para dar respuesta a las solicitudes de acceso y reclamos ejercitadas en virtud de los derechos de acceso, corrección, supresión, revocación o reclamo por infracción del Titular de los datos personales objeto de tratamiento por la empresa.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, adoptará las medidas oportunas para difundir el presente documento a todas las personas que forman parte de su organización y tienen acceso a los datos personales, para que puedan informar a los titulares del procedimiento a seguir en estos casos.

2. Base legal y derechos de los Titulares

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD); y en el Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior.

De acuerdo con el artículo 8 de la LEPD y a los artículos 21 y 22 del Decreto 1377 de 2013, los Titulares de los datos pueden ejercer una serie de derechos en relación al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

1. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
2. Por sus causahabientes, quienes deberán acreditar tal calidad.
3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que se le han dado a sus datos personales.
- **Derechos de quejas y reclamos:** La Ley distingue cuatro tipos de reclamos:
 - **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
 - **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
 - **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
 - **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.
- **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.
- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento

3. Definiciones establecidas en el artículo 3 de la LEPD y el artículo 3 del Decreto 1377 de 2013

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **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.
- **Datos sensibles:** Se entiende por datos sensibles aquellos 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.

- **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.
- **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.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

4. Atención a los Titulares de datos

Instituto Colombiano del sistema Nervioso-Clínica Montserrat, identificado(a) con CC No. **860007400-5**, de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, será el encargado(a) de la atención de peticiones, consultas y reclamos ante el(la) cual el Titular de los datos puede ejercer sus derechos. Teléfono: 2596000 Correo electrónico: atencionalusuario@icsn.co y comunicaciones@icsn.co.

5. Procedimientos para ejercer los derechos del Titular

5.1. Derecho de acceso o consulta

Según el artículo 21 del Decreto 1377 de 2013, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, **NOMBRE DE LA INSTITUCIÓN O EMPRESA**, solo podrá sobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, enviado, mediante correo electrónico a **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a **CL 134 17 71 Bogotá, Distrito Capital - Colombia**. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Telecopia.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

Una vez recibida la solicitud, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

5.3. Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, enviado, mediante correo electrónico a **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal

remitido a **CL 134 17 71 Bogotá, Distrito Capital - Colombia**, la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane 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.

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. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

6. Infracciones y sanciones

De acuerdo con el Capítulo 2 de la Ley Estatutaria 1581 de 2012 de Protección de Datos, la Superintendencia de Industria y Comercio puede imponer sanciones por el incumplimiento de la normativa sobre protección de datos al responsable del tratamiento o al encargado del tratamiento. Las posibles sanciones son:

- Multas de carácter personal e institucional hasta por el equivalente a dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

- Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
- Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.
- Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

7. Vigencia

Los presentes protocolos de atención al titular de los Datos permanece vigente desde **lunes, 1 de abril de 2019**

Firma:

Representante legal:
AURA VICTORIA CARRASCAL MARQUEZ

Documento de identidad:
51624869



INSTITUTO COLOMBIANO
DEL SISTEMA NERVIOSO

ATENCIÓN Y SERVICIO CON CALIDAD HUMANA

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT

NIT: 8600074005

2596000

CL 134 17 71

Bogotá, Distrito Capital - Colombia

atencionalusuario@icsn.co y comunicaciones@icsn.co

Políticas de seguridad para usuarios de protección de datos

1. Base legal y ámbito de aplicación

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos Personales (LEPD); y en el Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior.

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una organización u empresa, pública o privada, ésta se hace responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en la organización u empresa responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la organización u empresa responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la empresa y el Manual Interno de Seguridad; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar con el cumplimiento de sus obligaciones de seguridad, **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, nombra a cuatro responsables de seguridad encargados de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en el Manual Interno de Seguridad.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**.

Todos los usuarios identificados en el Manual Interno de Seguridad están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los

datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización o empresa responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

2. Definiciones establecidas en el artículo 3 de la ley de Protección de Datos Personales (LEPD) y el artículo 3 del Decreto 1377 de 2013

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **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.
- **Datos sensibles:** Se entiende por datos sensibles aquellos 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.
- **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.
- **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.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **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.

- **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.

3. Principios de la protección de datos

El artículo 4 de la LEPD establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

- **Principio de legalidad:** El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, el Decreto 1377 de 2013 y en las demás disposiciones que la desarrollen.
- **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.
- **Principio de libertad:** El tratamiento solo 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 revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la LEPD:
 - Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
 - Datos de naturaleza pública.
 - Casos de urgencia médica o sanitaria.
 - Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
 - Datos relacionados con el Registro Civil de las personas.
- **Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **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. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de

manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
 - El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
 - Los derechos que le asisten como Titular.
 - La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.
- **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 LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.
 - **Principio de seguridad:** La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas 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. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el Manual Interno de Seguridad, de obligado cumplimiento para todo usuario y personal de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.
 - **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 solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de la misma.

4. Categorías especiales de datos

4.1. Datos sensibles

Los datos sensibles son aquellos 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.

Según el artículo 6 de la LEPD, se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El 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.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2. Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales.

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

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los

que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

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, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1377 de 2013. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

5. Funciones y obligaciones

5.1. Responsable del tratamiento

Las obligaciones en materia de seguridad de los datos de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el Manual Interno de Seguridad.
- Difundir el referido documento entre el personal afectado.
- Mantener el Manual Interno de Seguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la empresa, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos en el Manual Interno de Seguridad.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en el Manual Interno de Seguridad, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel; y el uso de módems y las descargas de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.

- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada tres meses.
- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada dos años.

5. Funciones y obligaciones

5.1. Responsable del tratamiento

Las obligaciones en materia de seguridad de los datos de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el Manual Interno de Seguridad.
- Difundir el referido documento entre el personal afectado.
- Mantener el Manual Interno de Seguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la empresa, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos en el Manual Interno de Seguridad.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en el Manual Interno de Seguridad, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módems y las descargas de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada dos meses.
- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada año.

5.2. Encargados de seguridad

Los encargados de seguridad tienen las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del Manual Interno de Seguridad.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en el Manual Interno de Seguridad.
- Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.
- Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización del Manual Interno de Seguridad y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.
- Definir los tiempos dentro de los cuales se realizarán las auditorías, los cuales no podrán ser superiores a un año.
- Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.
- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales

5.3. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la empresa y, específicamente, por el contenido de este Manual. La lista de usuarios y perfiles con acceso a los

recursos protegidos están recogidos en el Manual Interno de Seguridad. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este Manual por parte del personal al servicio de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la empresa.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la empresa u organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.
- **Funciones de control y autorizaciones delegadas:** El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.
- **Obligaciones relacionadas con las medidas de seguridad implantadas:**
 - Acceder a las bases de datos con la solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
 - No revelar información a terceras personas ni a usuarios no autorizados.
 - Observar las normas de seguridad y trabajar para mejorarlas.
 - No realizar acciones que supongan un peligro para la seguridad de la información.
 - No sacar información de las instalaciones de la organización sin la debida autorización.
- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.
- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

- **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.
- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción
- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la empresa.
- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.
- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en el Manual de Políticas y Procedimiento y en el Manual Interno de Seguridad.

6. Vigencia

La presente política de tratamiento permanece vigente desde **lunes, 1 de abril de 2019**

Firma:

Representante legal:
AURA VICTORIA CARRASCAL MARQUEZ

Documento de identidad:
51624869

Autorización expresa con transferencia de datos

En caso de eventos que soliciten datos de la Institución

De conformidad con la Ley Estatutaria 1581 de 2012 de Protección de Datos y con el Decreto 1377 de 2013, autorizo como titular de mis datos personales, que éstos sean incorporados en una base de datos responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, los cuáles serán tratados con las finalidades estipuladas en el manual de políticas y procedimientos al cual podré tener acceso a través del correo electrónico: **atencionalusuario@icsn.co y comunicaciones@icsn.co**

De igual modo, autorizo la transferencia de mis datos a terceras entidades, cuyo objeto social sea **Cesión de contrato y transferencia de datos a la sociedad que adquiere los derechos de uso de la plataforma.** con la finalidad específica de:

Se define la finalidad del uso de datos para el evento solicitado.

Asimismo, declaro haber sido informado de que puedo ejercitar los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre mis datos, mediante escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, a la dirección de correo electrónico **atencionalusuario@icsn.co y comunicaciones@icsn.co**, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido a la dirección: **CL 134 17 71 Bogotá, Distrito Capital - Colombia**

Firma:

Nombre:

Instituto Colombiano del Sistema Nervioso- Clinica Montserrat

Documento de identidad:

8600074005

Autorización expresa para la utilización de imágenes

Autorización para incluir cuando se hagan eventos o eventos en los cuales se tomen fotos y se requieran publicar

Autorización expresa para la utilización de imágenes

De acuerdo con la Ley Estatutaria 1581 de 2012 de Protección de Datos Personales, al Decreto 1377 de 2013, y a las demás normas concordantes, autorizo como titular de mis datos biométricos y en particular de mi imagen, para que las imágenes hechas dentro de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, bien en fiestas internas, cumpleaños, actividades puntuales o bien fuera de la institución, como excursiones, cursos, capacitaciones o cualquier otra actividad externa, sean incorporados en una base de datos responsabilidad de **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT** y puedan ser utilizados en sus publicaciones con la finalidad de:

Algunas de las finalidades pueden ser: Difusión de actividades. Promoción de la marca en redes sociales, mediante piezas gráficas

De igual modo, declaro haber sido informado de que puedo ejercitar los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre mis datos, mediante escrito dirigido a **INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLINICA MONTSERRAT**, a la dirección de correo electrónico **atencionalusuario@icsn.co** y **comunicaciones@icsn.co**, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido a la dirección: **CL 134 17 71 Bogotá, Distrito Capital - Colombia**.

Firma:

Nombre:

Instituto Colombiano del Sistema Nervioso-Clinica Montserrat

Documento de identidad:

8600074005