Clínica BELÉN®
DE FUSAGASUGÁ

POLÍTICAS DE PROTECCIÓN DE DATOS

POLÍTICAS DE PROTECCIÓN DE DATOS

Elaborado por:

ALZATE & ASOCIADOS
ASESORES JURÍDICOS

SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ S.A.S.
2024

TABLA DE CONTENIDO

INTRODUCCIÓN

La Ley de Protección de Datos Personales reconoce y protege el derecho de las personas de conocer, actualizar y rectificar sus datos personales en bases de datos o archivos que sean susceptibles de tratamiento por entidades públicas y privadas . En este caso la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGA S.A.S**, en cumplimiento de la Ley 1581 de 2012 y sus decretos, ha definido las políticas y procedimientos para la recolección, almacenamiento y transferencia de datos, comprometida con el cumplimiento normativo colombiano.

1. OBJETIVOS

- Cumplimiento normativo de la ley 1581 de 2012 y demás decretos reglamentarios para poder realizar operaciones de recolección, almacenamiento, uso, circulación o supresión de datos personales.
- Salvaguardar todas las bases de datos automatizadas y físicas en las cuales se almacenan los datos de los titulares que forman parte de las bases de datos de la clínica.
- Cumplir con las medidas de seguridad establecidas para la protección de cada una de las bases de datos.
- Contar con la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.
- Capacitar al mayor número de personas colaboradores/empleados para que se cumpla la Política de Protección de Datos.

2. ALCANCE

Cumplir con el derecho constitucional al Habeas Data en las cuales la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ S.A.S** en desarrollo de sus actividades empresariales, haya recopilado, administrado o tratado de sus datos de carácter personal bien sea pacientes, empleados, proveedores, accionistas y demás colaboradores.

3. RESPONSABLE

La **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS**, es la responsable del tratamiento como persona jurídica, que por sí misma o en asocio con otros, reciba, custodie o comparta la información de las bases de datos y/o el tratamiento de los datos.

4. DEFINICIONES

Autorización: Consentimiento previo, expreso e informado del Titular del dato para llevar a cabo el tratamiento de su información personal.

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: Son aquellos que no son semi privados, privados o sensibles pueden encontrase en

registros públicos, boletines y sentencias judiciales no reservadas.

Datos sensibles: Información que afecta la intimidad de una persona o cuyo uso indebido pueda generar discriminación.

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 del titular de datos, que informa sobre las políticas de tratamiento de datos, como el acceso y las finalidades del uso de sus datos.

Transferencia: Implica el envío de datos personales de (transmisión nacional) o fuera de Colombia (Transmisión Internacional).que realiza el responsable.

Transmisión: Implica la comunicación de estos dentro (transmisión nacional)o fuera de Colombia y que tiene como objeto la realización de un tratamiento por el encargado por cuenta del responsable.

5. CONTENIDO

Capítulo I
Políticas y Seguridad de Procedimientos

I. 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.el cual se evidencia 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); en el decreto 1377 de 2013, y capítulo 25 sección 3 Articulo 2.2.2.25.3.2. del decreto 1074 de 2015, por el cual se reglamenta parcialmente la Ley anterior.

El tratamiento de datos personales debe estar fundamentado en una finalidad legítima conforme a lo establecido en la Constitución y la ley. Esta finalidad debe ser claramente informada al titular de los datos, quien debe contar con las medidas técnicas, humanas y administrativas necesarias para garantizar la confidencialidad de la información. El tratamiento de los datos personales solo podrá llevarse a cabo con el consentimiento previo, expreso e informado del titular. Además, los datos personales no podrán ser obtenidos ni divulgados sin la autorización previa, a menos que exista un mandato legal o judicial que exija el tratamiento sin necesidad de consentimiento.

Para velar con el cumplimiento de sus obligaciones de seguridad, la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGA SAS** nombra al coordinador del área Tics como responsable de seguridad encargado de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en el Manual Interno de Seguridad.

Todos los usuarios están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deberde confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento.

Tipo de Norma	Número y fecha de expedición	Titulo	Expedida por	Aplicación especifica
Ley Estatutaria	1581de 2012	*"Por la cual se dictan disposiciones generales para la protección de datos personales".*	Congreso de la Republica.	Todas las personas tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.
Decreto	1377 de 2013	*"Por medio del cual se reglamenta parcialmente la ley 1581 de 2012"*	Presidente de la República de Colombia.	Mediante la cual se reglamenta la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	1074 de 2015	*"Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo."*	Presidente de la República de Colombia.	El Ministerio de Comercio, Industria y Turismo tiene como objetivo dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria.

II. Definiciones establecidas en el artículo 3 de la LEPD y el capítulo 25 sección 1 artículo 2.2.2.25.1.3 del decreto 1074 de 2015.

Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos.

Autenticación: Procedimiento de verificación de la identidad de un usuario.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita dirigida al Titularpara el tratamiento de sus datos personales, en donde se informa de las políticas de tratamiento de información que le serán aplicables, y las finalidades del tratamiento que se pretende dar a los datos personales.

Contraseña: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

Control de acceso: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.

Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

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.

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.

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.

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.

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

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 estos 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.

III. Principios de la protección de datos.

El artículo 4 de la Ley de Protección de Datos (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 Ley de Protección de Datos (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 de datos personales debe contar con el consentimiento previo, expreso e informado por el Titular. Los cuales no pueden ser obtenidos ni divulgados sin autorización excepto en los siguientes casos por el artículo 10 de la ley de protección de datos (LEPD):

- Información solicitada por entidades públicas o judiciales.
- Datos de naturaleza pública.
- Urgencia médica o sanitarias.
- Tratamiento para fines históricos, estadísticos o científico.
- Datos del 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 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 yexpresa lo siguiente:

- 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 la Ley de Protección de

Datos (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.

Principio de seguridad: La información sujeta a 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. 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: Quienes manejen los datos personales no públicos deben mantener reserva incluso después de su relación laboral y solo podrá compartir la información de acuerdo con lo autorizado por la LEPD**.**

IV. Categorías especiales de datos.
V. 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.

Según el artículo 6 de la Ley Estatuaria de Protección de datos Personales (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 de datos por fundaciones, ONG asociaciones u organismos sin animo de lucro con fines políticos, filosóficos, religiosos o sindicales debe realizarse de manera legitima y segura y solo puede referirse a sus miembros o personas en contacto regular. Los datos no se pueden compartir con 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.

VI. 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.

El Estado y las entidades educativas deben informar y capacitar a representantes legales y tutores sobre los riesgos del tratamiento indebido de datos personales de niños y adolescentes, así como enseñarles sobre el uso responsable, la privacidad y la protección de la información personal.
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 se ejercerán por las personas que estén facultadas para representarlos.

VII. Derechos de los Titulares.

De acuerdo con el artículo 8 de la LEPD y el capítulo 25, sección 4 del decreto 1074 de 2015, los derechos sobre los datos personales pueden ser ejercidos por:

- **El Titular**: Debe acreditar su identidad con los medios disponibles del responsable.
- **Causahabientes**: Deben demostrar su calidad de causahabientes.
- **Representante o Apoderado**: Deben probar la representación o apoderamiento.
- **Estipulación a Favor de Otro**: Se aplica para quienes hayan sido designados.
- **Niños, Niñas o Adolescentes**: Los derechos deben ser ejercidos por sus representantes legales.

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 les 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 rectifique 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: Es el derecho del titular a que se eliminen los datos inadecuados, excesivos o que no cumplan con los principios y garantías legales**.**

Reclamo de revocación: Es derecho del Titular dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

Reclamo de infracción: Es 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.

VIII. Autorización de la política de tratamiento.

De acuerdo con el 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 política, todo Titular está consintiendo el tratamiento de sus datos por parte de Clínica, 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.

IX. Responsable del tratamiento.

Los canales establecidos por la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS**, son los siguientes

Dirección:	TV 12 # 17-01 Fusagasugá
Correo electrónico	gerenciageneral@clinicabelen.com.co
Teléfono	8868888
Celular	315 7823277

X. Las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos de la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS** 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.
- El Manual Interno de Seguridad debe mantenerse actualizado y revisado en caso de posibles

cambios relevantes en el sistema de información, la organización , el contenido de las bases de datos.

- 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 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.

XI. Tratamiento y finalidades de las bases de datos

La Clínica en el desarrollo de sus actividades, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas afinalidades legítimas, cumpliendo con la Constitución y la Ley.

La siguiente tabla (Tabla I) presenta las distintas bases de datos que maneja la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS** y las finalidades asignadas a cada una de ellas.

Tabla I. Bases de datos y finalidades

Nombre	Finalidad
Proveedores Responsable: Coordinador de compras	Los datos se utilizarán para solicitar ofertas y propuestas económicas, analizar productos y servicios, enviar comunicaciones via correo electrónico, presentar informes a entes de control, verificar referencias comerciales y gestionar aspectos precontractuales y contractuales.
Empleados Responsable: Coordinador de talento humano	Los datos se utilizarán para: Identificación personal, contacto, y datos académicos, laborales y financieros, Registro y vinculación laboral, envío de información sobre el cargo, bienestar laboral, Difusión de ofertas laborales, comunicación institucional, y actividades estadísticas, Inscripción en congresos, actualización de datos, y verificación de identidad, Entrevistas, referencias laborales, y colaboración con empresas para artículos de dotación, Envío de información por SMS y correo, asignación de equipos, informes de gestión humana, Afiliación a seguridad social y cajas de compensación, entrega de referencias laborales, Uso de imágenes y videos con fines corporativos, actividades recreativas, y bienestar, Evaluaciones de ascenso, procesos de auditoría, control interno y externo, informes institucionales, Desactivación d sistemas, afiliación y retiro de fondos, informes de terminación de contrato, Procesos administrativos ante el Ministerio de Salud.

Pacientes Responsable: TIC	Los datos se tratarán para: Crear y mantener una base de datos con la historia clínica de los pacientes, Integrar procesos y registrar actividades en la historia clínica electrónica, Gestionar la atención y administración de pacientes, órdenes médicas, formulaciones, inventarios, facturación y recaudos, Utilizar imágenes con previa autorización de los pacientes.
Visitantes Biométricos Responsable: TIC	Los datos se usarán para: Autorizar el acceso a diferentes áreas de la organización, Verificar videos de cámaras de seguridad en casos específicos, Enviar información promocional e informativa por mensajes de texto y correos electrónicos, Estas finalidades son enunciativas y no taxativas.

Capitulo II

PROTOCOLO DE ATENCIÓN AL TITULAR DE DATOS.

XII. Atención a los Titulares de datos

El gerente general será el encargado de la atención de peticiones, consultasy reclamos, las cuales deberán ser enviado al siguiente correo electrónico: **gerenciageneral@clinicabelen.com.co**

XIII. Derecho de acceso o consulta.

Según el capítulo 25 sección 4 del decreto 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

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

Para las consultas que se realicen más de una vez al mes, la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGA S.A.S** solo podrá cobrar al titular por gastos de envío los cuales no pueden exceder los costos reales del material el responsable deberá demostrar estos gastos a la Superintendencia de Industria y comercio. El Titular de datos puede solicitar acceso a sus datos enviando un correo a gerenciageneral@clinicabelen.com.co con el asunto "ejercicio del derecho de acceso o consulta". La solicitud debe incluir:

- Nombre completo y fotocopia de la cédula del Titular y su representante, si aplica.
- Descripción de la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma.
- El Titular puede elegir recibir la información solicitada por:
  - Visualización en pantalla.
  - Copia física por correo.
  - Correo electrónico.
  - Otro sistema adecuado ofrecido por la Clínica.

Una vez recibida la solicitud, la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS**, 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 días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo14

de la LEPD.

XIV. Derechos de quejas y reclamos.

El Titular de datos puede presentar un reclamo enviando un correo a **gerenciageneral@clinicabelen.com.co** con el asunto "ejercicio del derecho queja o reclamo". La solicitud debe incluir:

- Nombre completo y fotocopia de la cédula del Titular y su representante, si aplica.
- Descripción de la solicitud (corrección, supresión, revocación).
- Dirección para notificaciones y firma.

Si el reclamo es incompleto, se solicitará subsanación en cinco días. Si no se recibe la información adicional en dos meses, el reclamo se considerará desistido. Una vez recibido el reclamo completo, se marcará como "reclamo en trámite" en la base de datos dentro de dos días hábiles.

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de esta. 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.

XV. Medidas de seguridad

La **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE Belén DE FUSAGASUGÁ SAS**, 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 como se evidencia en las 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	Gestión de documentos y soportes	Control de acceso	Incidencias	Personal	Manual Interno de Seguridad
1. Auditoría ordinaria (interna o externa) anualmente 2. Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de	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	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña. 2. Lista actualizada de usuarios y accesos autorizados.	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.	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos 2. Definición de las funciones de control y autorizaciones	1. Elaboración e implementación del Manual de obligatorio cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad,

deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad ydel responsable del tratamiento. 5. Conservación del Informe adisposición dela autoridad.	donde sealmacenan 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. Inventario delos soportes enlos que se almacenan bases de datos.	3. Autorización escrita del titular de la información para la entregade sus datos aterceras personas, para evitar el acceso a datoscon derechos distintos de losautorizados. Concesión,alteración o anulación depermisos por elpersonal autorizado.	Procedimiento de notificación y gestión de incidencias.	delegadas por el responsabledel tratamiento. 3. Divulgación entre el personal de las normas yde las consecuenci as del incumplimiento de las mismas.	funciones y obligaciones del personal, descripción delas bases dedatos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad parael transporte, destrucción y reutilización de documentos, identificación de los encargados

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			Bases de datos automatizadas	
Archivo	**Almacenamiento o de documentos**	**Custodia de documentos**	**Identificación y autenticación**	**Telecomunicaciones**
1. Archivo de documentación siguiendo procedimientos que garanticenuna correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.	1. Dispositivosde almacenamientocon mecanismos que impidan elacceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información yverificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación,caducidad y almacenamiento cifrado.	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	Bases de datos automatizadas

Auditoría	Responsable de seguridad	Manual Interno de Seguridad	Gestión de documentos y soportes	Control de acceso	Identificación y autenticación	Incidencias
1 Auditoría ordinaria (interna o externa) cada año. **2** eventuales Auditorías extraordinaria por modificaciones los sistemas de información. **3** Informe de detección de deficiencias y propuesta de correcciones. **4** Análisis y conclusiones del de seguridad ydel tratamiento. 5. Conservación del Informe adisposición dela autoridad	**1** designación a responsables de seguridad **2** designación a encargados del control y la coordinación de las medidas del Manual Interno deSeguridad. **3** prohibición de delegación de la Responsabilidad del responsable del tratamiento en el responsable de seguridad	1. Controles al menos unavez al año de cumplimiento consistente así como la capacitación al personal mínimo unavez al año.	1. Registro de entrada y salida de documentos fecha, emisor y receptor, número, tipo de información , forma de envío,entrega.	. Control de accesoal lugar olugares donde se ubican los sistemas de información ón.	1. Mecanismoo que limite el número de intentos reiterados de acceso no autorizados.	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. autorización del responsable del tratamiento para la ejecución de los procedimientos.

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

Bases de datos no automatizadas		Bases de datos automatizadas	
Control de acceso	**1.**Acceso solo parapersonal autorizado. **2.**Mecanismo deidentificación de acceso. **3.**Registrode accesosde usuariosno autorizados.	**Gestión de documentos y soportes**	**1**. Sistema detiquetado confidencial. **2** cifrado de datos. **3.** Cifradode dispositivosportátiles cuando salgan.
Almacenamiento de documentos	**1** .Archivadores, armarios uotros ubicados en áreas de acceso protegidas con llaves u otras medidas.	**Control de acceso**	**1** registro deaccesos: usuario hora,base de datos ala que accede,tipo de acceso,registro al que accede. **2** Control del registro de accesos por el responsable de seguridad Informe mensual. **3** Conservaciónde los datos: por el periodo que las leyes impongan.
Copia o reproducción	**1** solo por usuarios autorizados. **2** destrucción que impida el acceso a recuperación de los datos.	**Telecomunicaciones**	Transmisión de datos mediante redes electrónica s cifradas.
Trasladoo de documentación	**1 .**Medidasque impidan el acceso o manipulación de documentos.		

Capitulo III

POLÍTICAS DE SEGURIDAD PARA USUARIOS.

XVI. Encargado de seguridad

El encargado de seguridad tiene las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad, y colaborar en la difusión delManual 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 autorizadosidentificados en el Manual Interno de Seguridad. Habilitar a todos los usuarios para registrar incidencias de seguridad de datos y coordinar con el responsable del tratamiento de las medidas correctivas, registrándolas.

- Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, ka validez de las copias de seguridad, 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 auditorias, 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.

XVII. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta de los datos personales y sistemas de información de la Clínica, deben actuarde conformidad a las funciones y obligaciones recogidas en el presente apartado.

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE Belén DE FUSAGASUGÁ SAS cumple con el deber de información de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datosy sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de la Clínica se definen, según sus actividades y el manual interno de seguridad el cual contiene la lista de usuarios y perfiles de acceso a recursos protegidos, los usuarios deben custodiar y controlar los latos personales para evitar al personal no autorizado.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este Manual por parte del personal al servicio de la Clínica es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el usuario y la misma.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGA SAS**. son las siguientes:

Deber de secreto: En cumplimiento de este deber, los usuarios de la Clínica no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargode 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:

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 ser exclusivamente para las funciones asignadas no se permite para fines personales si es necesario retirar dispositivos periféricos se debe comunicar al responsable de seguridad para su autorización.

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.

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

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

Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente , debe bloquear dicho terminal para impedir la visualización o el acceso a la información quecontiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados 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.

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.

Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la organización.

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.

XVIII. Transferencia de datos a terceros países.

De acuerdo con el Título VIII de la LEPD, se prohíbe transferir datos personales a países sin niveles adecuados de protección, según lo definido por la Superintendencia de Industria y Comercio y la circular 005 de 2017. Las excepciones a esta prohibición incluyen:

- Transferencias con autorización expresa del Titular.
- Intercambio de datos médicos por razones de salud pública.
- Transferencias bancarias o bursátiles conforme a la legislación aplicable.
- Transferencias bajo tratados internacionales con principios de reciprocidad.
- Transferencias necesarias para ejecutar un contrato o medidas precontractuales, con autorización del Titular.
- Transferencias para interés público o defensa de derechos en procesos judiciales.

Capitulo IV

MANUAL INTERNO DE POLÍTICAS DE SEGURIDAD

XIX. Cumplimiento y actualización.

El Manual Interno de Seguridad es un documento interno de obligatorio cumplimiento para todo el personal de la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS** con acceso a datos personales.

Este manual debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, 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.

XX. Medidas de seguridad

Las bases de datos son accesibles únicamente por las personas designadas por la Clínica Los cuales , 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 la **SOCIEDADMEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS**.

XXI. Medidas de seguridad comunes.

XXII. Gestión de documentos y soportes.

Los documentos y soportes con base de datos están listados en el inventario correspondiente, en el cual solo los usuarios autorizados podrán acceder a ellos y deben ser clasificadas y ser accesibles solo a personal autorizados. deben estar etiquetados claramente, la salida de estos documentos fuera de las instalaciones o por correo electrónico requieren autorización del responsable del tratamiento.

XXIII. Control de acceso.

El personal de la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS** 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.

La clínica, se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y 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 corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a la clínica, 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.

XXIV. Ejecución del tratamiento fuera de la institución.

El almacenamiento de datos personales del responsable del tratamiento en dispositivos portátiles y su tratamiento fuera del lugar natural de trabajo, requiere una autorizaciónprevia por parte de la clínica, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

XXV. 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.

XXVI. Responsable de seguridad

De acuerdo con la normativa sobre protección de datos, el responsable de la seguridad es el coordinador de área Tics, el cual no exonera de responsabilidad al responsable del tratamiento de datos.

XXVII. Auditoría.

Las bases de datos que contengan datos personales se deberán someter, a una auditoria cada año,ya sea auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad

contenidas en este manual.

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS, 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,

- Las auditorías concluirán con un informe que contendrá: (El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protecciónde datos, La identificación de las deficiencias halladas y la sugerencia y la descripción de los datos, hechos y observaciones)

El coordinador del área Tics estudiará el informe y trasladará las conclusiones para que implemente las medidas correctoras.

XXVIII. Medidas de seguridad para bases de datos no automatizadas.
XXX. 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.

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.

XXXI. Medidas de seguridad para bases de datos automatizadas.

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS, 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.

Además, cuando el sistema de autenticación use contraseña se deberá implementar la política de contraseñas no superior a 365 días garantizando el almacenamiento cifrado de contraseñas y limitara intentos reiterados de acceso no autorizados.

XXXIII. Entrada y salida de documentos o soportes

La entrada y salida de documentos o soportes debe registrarse detallando tipo, fecha, hora, emisor o receptor, número de documentos, nivel de seguridad, forma de envío y responsable. Este registro debe anexarse al documento. Las instalaciones de la Clínica que alojan datos personales deben estar protegidas para asegurar la integridad y confidencialidad de los datos, cumpliendo con las medidas de seguridad físicas adecuadas.

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS, debe informar a su personal sobre sus obligaciones para proteger físicamente los documentos y soportes con bases de datos. Solo el personal autorizado podrá acceder a las instalaciones que

alojan estos datos, cumpliendo con las medidas de seguridad especificadas en el manual.

XXXIV. Copias de respaldo y recuperación de datos.

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ S.A.S realiza copias de respaldo semanales a todas las Bases de Datos y ha establecido procedimientos para la recuperación de datos. En caso de pérdida o destrucción, los datos deberán grabarse manualmente y se registrarán el respectivo manual. También las copias de respaldo y los procedimientos de recuperación se deben almacenar en un lugar distinto, pero con las mismas medidas de seguridad que los datos originales.

XXXV. Registro de acceso.

***La* SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS** debe registrar los intentos de acceso a los sistemas de información incluyendo usuario, fecha, hora, base datos, tipo de acceso y autorización Los responsables de seguridad deben controlar estos registros, revisarlos mensualmente, elaborar informes y evitar la manipulación de los mecanismos de registro. Los datos de acceso deben conservarse al menos dos años. No es necesario registrar accesos si el responsable del tratamiento es una persona natural con acceso exclusivo a los datos. El acceso a través de redes debe cumplir con medidas de seguridad equivalentes al acceso local, y la transmisión de datos por redes públicas o inalámbricas debe estar cifrada o protegida para evitar accesos no autorizados.

XXXVI. 11. Funciones y obligaciones del personal

La **SOCIEDAD MÉDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS** debe informar a su personal sobre medidas de seguridad y consecuencias de incumplimiento mediante diversos medios (correo, tablones, etc.) y proporcionar acceso al manual de seguridad. Además, incluye acuerdos de confidencialidad para los usuarios de sistemas de identificación y envía circulares informativas.

Las funciones y obligaciones del personal están definidas en el manual y se basan en sus actividades y el acceso a recursos protegidos. Los usuarios deben custodiar documentos con datos personales y prevenir accesos no autorizados. El incumplimiento de estas medidas es sancionable según la normativa aplicable. Las funciones específicas de los usuarios de bases de datos se detallan a continuación:

- **Deber de secreto**: Aplica a todas las personas que, accedan a bases de datos ,por lo tanto, los usuarios de la organización nopueden comunicar o relevar 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 estos.

- **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.

    - 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.

- Al imprimir y escanear algún documento este deberá ser recogida inmediatamente.

- **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.

- **Deber de custodia de los soportes utilizados:** El usuario autorizado deberá vigilar y controlar que las personas no autorizadas accedan a la información contenida en los soportes.

- **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.

- **Uso limitado de Internet y correo electrónico:** El envío de información por vía está limitado al desempeño de sus actividades al interior de la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS**.

- **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.

- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales propiedad de la Clínica.

- **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 presente capitulo.

XXXVII. Bases de datos y sistemas de información.

Las bases de datos almacenadas por la **SOCIEDAD MEDICO QUIRÚRGICA NUESTRASEÑORA DE BELEN DE FUSAGASUGÁ SAS** se recogen en la siguiente tabla (Tabla I), donde seindica 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	Sistema de tratamiento	Clasificación de datos
Proveedores	Mixto	Privada
Empleados	Mixto	Sensible
Pacientes	Mixto	Sensible
Visitantes-Biométrica	Mixto	Sensible

La siguiente tabla (Tabla II) recoge la estructura de las bases de datos de la **SOCIEDAD MEDICOQUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGÁ SAS**

Tabla II. Estructura de las Bases de datos

Nombre de la base de datos	Proveedores
Responsable del tratamiento	**SOCIEDAD MEDICO QUIRÚRGICA NUESTRASEÑORA DE BELEN DE FUSAGASUGÁ SAS** **NIT**: Número de identificación **Dirección**: Dirección **Teléfono**: Teléfono **Correo electrónico**: Correo electrónico
Encargado de consultas y reclamos	**Encargado de consultas y reclamo** **Tipo de documento del encargado:** Numero dedocumento del encargado.
Tipo de datos	**Privados**
Control de acceso físico:	Usuarios Autorizados
Control de acceso lógico	Usuarios y Contraseñas
Copias de respaldo	**Tiempo de copias de respaldo**
Nombre de la base de datos	Empleados
Responsable del tratamiento	**SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGA SAS**
Encargado de consultas y reclamos	**Encargado de consultas y reclamos** **Tipo de documento del encargado:** Numero dedocumento del encargado.
Tipo de datos	**Sensibles**
Control de acceso físico:	Usuarios Autorizados
Control de acceso lógico	Usuarios y Contraseñas
Copias de respaldo	**Tiempo de copias de respaldo**
Nombre de la base de datos	Pacientes
Responsable del tratamiento	**SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELEN DE FUSAGASUGA SAS**
Encargado de consultas y reclamos	Encargado de consultas y reclamos Tipo de documento del encargado: Numero dedocumento del encargado.
Tipo de datos	Tipo de datos
Control de acceso físico:	Usuarios Autorizados
Control de acceso lógico	Usuarios y Contraseñas
Copias de respaldo	Tiempo de copias de respaldo

El nombramiento de responsables de seguridad no exime al responsable del tratamiento de sus obligaciones. La **SOCIEDAD MÉDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS** especifica en el manual a los encargados del tratamiento y sus responsabilidades en materia de seguridad Los contratos de transmisión de datos se detallan en un anexo.

XXXVIII. 2.8. Procedimiento de notificación, gestión y respuesta ante incidencias.

La SOCIEDAD MÉDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGÁ SAS ha establecido un procedimiento para notificar, gestionar y responder a incidencias que afecten la confidencialidad, disponibilidad e integridad de la información.

- **Notificación:** Los usuarios deben informar de inmediato cualquier incidencia a los responsables de seguridad, detallando el tipo de incidencia, personas involucradas, fecha y hora, efectos y la persona que notifica.
- **Registro:** Se debe crear un registro de incidencias que incluya el tipo, fecha, hora, personas involucradas y medidas correctoras. Este registro será gestionado por el responsable de seguridad y anexado al manual.
- **Recuperación de Datos:** Implementar procedimientos para la recuperación de datos, especificando quién ejecuta el proceso, los datos restaurados y cualquier dato grabado manualmente.

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

La SOCIEDAD MEDICO QUIRÚRGICA NUESTRA SEÑORA DE BELÉN DE FUSAGASUGA S.A.S establece las siguientes directrices para la gestión de documentos y soportes de datos personales :

- Destrucción: Antes de destruir documentos o soportes, se debe registrar el proceso, incluyendo una descripción del documento, fecha, hora y firmas de dos testigos.
- Traslado: Los documentos o soportes deben ser cifrados o protegidos durante el traslado para evitar acceso indebido.
- Dispositivos portátiles: Los datos en dispositivos portátiles deben estar cifrados cuando esta fuera de las instalaciones y si no es posible estas deberán tomar medidas de seguridad para proteger los datos.

XL. Infracciones y sanciones

La superintendencia de industria y comercio puede interponer las siguientes sanciones por incumplimiento de la ley 1581 de 2012 sobre protección de datos:

Multas: Hasta 2.000 salarios mínimos mensuales.

Suspensión: Hasta de 6 meses de las actividades relacionadas con el tratamiento de los correctivos necesarios.

Cierre temporal: Cierre temporal si no se adopta los correctivos tras suspensión.

Cierre Definitivo: Cierre inmediato y definido de operaciones que involucre el tratamiento de datos sensibles.

-

XLI. **Vigencia**

Los presentes protocolos de atención al titular de los Datos permanecen vigentes desde 13 de enero2022.

1. BIBLIOGRAFÍA

Tipo de Norma	Número y fecha de expedición	Titulo	Expedida por	Aplicación especifica
Ley Estatutaria	Ley 1581 de 2012	*"Por la cual se dictan disposiciones generales para la protección de datos personales".*	Congreso de la Republica.	Por medio de la cual desarrollarel derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma
Decreto	1377 de 2013	*"Por medio del cual se reglamenta parcialmente la ley 1581 de 2012"*	Presidente de la República de Colombia.	Mediante la cual se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	1074 de 2015	*"Por mediodel cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo."*	Presidente de la República de Colombia.	El Ministerio de Comercio, Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con lacompetitividad, integración y desarrollo de los sectores productivos de la industria

2. ANEXOS

- Formato de incidencias

3. REVISIÓN Y APROBACIÓN

APROBACIÓN				
	Nombre	**Cargo**	**Fecha**	**Firma**
Elaboró	Alzate & Asociados	Asesores Jurídicos	13/01/2022	
Revisó	Nilson Avella	Coordinador de las Tics	25/03/2022	
Aprobó	Norangela Quicasaque	Coordinadora de calidad	22/03/2022	

4. CONTROL DE CAMBIOS DEL DOCUMENTO

Nombre de quien modificó	Descripción del cambio o revisión	Versión	Vigencia
Alzate & Asociados	Versión inicial	V1	22/03/2022