TABLA DE CONTENIDO

0 CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCION DEL CAMBIO
1	30/06/2021	Adaptación de los documentos dejados por el ente tercerizado Álzate y Asociados Asesores jurídicos, en el formato institucional.
2	10/03/2022	Se solicita la actualización del Manual Privacidad y Protección de Datos Personales

Tabla 1 Control de cambios

1 OBJETIVO

Garantizar el apropiado tratamiento de los datos personales desde la política, procedimientos establecidos, y velar por el derecho que tienen todas las personas, de conocer, actualizar, rectificar o suprimir la información que se haya recogido en el Centro Dermatológico Federico Lleras Acosta

2 ALCANCE

El Centro Dermatológico Federico Lleras Acosta, como responsable del tratamiento de los datos personales, está comprometida con el adecuado tratamiento de los datos de sus empleados, los estudiantes, los egresados, los clientes, los proveedores y los terceros. Por lo tanto, en el presente documento se articulan los procedimientos y actividades que involucran el tratamiento de los datos personales, los cuales están alineados con la política normas y directrices que lo regulan.

3 RESPONSABLE DEL MANUAL

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOS, 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 donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en el artículo 4 literal g) de la Ley de protección de datos.

4 A QUIÉN VA DIRIGIDO

Este manual como la política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable de la DR-PLE-PO-002 POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

5 NORMATIVIDAD

Artículos 15 y 20 de la Constitución Política

- Ley 21 de 1982.
- Ley 100 de 1993.
- Ley 789 de 2002.
- Artículo 15, 20, 44 y 45 CPC.
- Ley 527 de 1999.
- Ley 1266 de 2008.

- Ley 1581 de 2012.
- Ley 1273 de 2009.
- Decreto 886 de 2014.
- Decreto 1377 de 2013.
- Decretos Reglamentarios 1727 de 2009 y 2952 de 2010.
- Sentencia C - 748 del 2011, de la Corte Constitucional.

6 DEFINICIONES Y SIGLAS

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

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar los datos personales.

Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

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

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.

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 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 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 pertenecía a sindicatos, organizaciones sociales, de derechos humamos 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.

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.

LEPD: Ley de protección de datos.

Perfil se 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.

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.

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.

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.

Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

7 DESARROLLO DEL MANUAL

7.1. PRINCIPIOS RECTORES

El tratamiento de los datos personales se rige por los principios rectores conformes a la normatividad, los cuales se utilizan para determinar los lineamientos de seguridad y privacidad en las operaciones de recolección, almacenamiento, intercambio, uso y procesamiento de los datos personales.

Acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones del presente manual de protección de datos personales, la ley, decretos y la Constitución Política de Colombia. En este sentido, el tratamiento es realizado por personas autorizadas por la institución o por las personas previstas en la Ley 1581 de 2012. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la LEPDP. En atención a este mandato, la información personal que ha sido autorizada a Centro Dermatológico Federico Lleras para su tratamiento no se encuentra disponible en medios masivos o divulgados a través de Internet sin que medien mecanismos de control de acceso y seguridad

Confidencialidad: Todas las personas que en intervienen en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPDP y en los términos de esta. El cumplimiento de este requisito se lleva a cabo a través de cláusulas de confidencialidad que protegen la información personal ante situaciones de posible divulgación de datos por parte de colaboradores y terceras partes autorizadas para el tratamiento.

Finalidad: El tratamiento de datos realizado por Compensar obedece a las actividades que le otorgan las Leyes 21 de 1982, 789 de 2002, 100 de 1993 y decretos reglamentarios bajo la tutela de la Constitución Política de Colombia, que corresponden a servicios y productos relacionados con el Régimen de Subsidio Familiar, Sistema Integral de Seguridad Social, apoyo al empleo, a la protección social, al bienestar y recreación de las personas. Dentro de las operaciones legítimas corresponde la transferencia al Sistema Integral de Seguridad Social de la información personal, ello en cumplimiento del deber como empleador. Legalidad en materia de tratamiento de datos: El tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen, que para Compensar estas actividades se desarrollan en el marco de las Leyes 21 de 1982, 789 de 2002 y 100 de 1993.

Libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que se refiere la presente ley, 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. Para lo cual Compensar en calidad de responsable del tratamiento de la información personal de sus afiliados, colaboradores y contratistas ha adoptado las medidas administrativas, humanas y técnicas necesarias para

asegurar los datos y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

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. Compensar tiene a disposición de los titulares de la información personales los canales y procedimientos para que puedan ejercer su libre derecho de acceso a los datos que de ellos reposan en los sistemas de información.

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.

7.2. CATEGORÍAS ESPECIALES DE DATOS La LEPDP

Considera dentro de la categoría de datos especiales los datos sensibles y los relativos a las niñas, niños y adolescentes, Artículos 5° y 7° respectivamente.

Datos sensibles para los propósitos de la Ley 1581 de 2012, 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 o de derechos humanos. De la misma forma datos que promuevan intereses de cualquier partido político o que avalen 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.

En la categoría de datos sensibles, la institución realiza tratamiento de información relativa a la salud. La LEPDP prohíbe el tratamiento de datos sensibles, excepto cuando:

a. 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.
b. El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
c. El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
d. El tratamiento tenga una finalidad histórica, estadística o científica. En este evento se adoptan las medidas conducentes a la supresión de identidad de los titulares.

Por disposición del Decreto 1377 de 2013 se informa al titular que:

a. Por tratarse de datos sensibles no está obligado a autorizar su tratamiento.

b. Además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, que los datos relativos a la salud y biométrico objeto de tratamiento son sensibles y la finalidad del tratamiento corresponde a las necesidades para la prestación de los servicios en la institución, por lo cual se debe obtener su consentimiento expreso.

c. Ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles.

Derechos de los niños, niñas y adolescentes

En el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública. 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 al 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.

7.3. Finalidad del Tratamiento.

Teniendo en cuenta la misionalidad de la institución y las distintas categorías de titulares, a continuación, se especificará, sin ser taxativa, la finalidad con la cual se efectúa al Tratamiento de datos personales para cada caso. Se precisa que el tratamiento y sus finalidades pueden ejecutarse directamente o por un tercero encargado ubicado en Colombia o en el extranjero, pero siempre bajo la responsabilidad de la institución de conformidad con la Ley.

Adicionalmente, la información personal podrá almacenarse y/o tratarse en países diferentes a Colombia, donde la institución, empresas vinculadas o proveedores de servicios, tengan sus instalaciones, por lo que al usar nuestros servicios o entablar una relación laboral, comercial u otra afín, el titular autoriza transferir y/o transmitir la información a otros países, los cuales podrán tener medidas diferentes para garantizar la protección de datos personales.

7.3.1. Finalidades generales para el tratamiento de datos personales:

- Garantizar la seguridad en el marco de la política de la institución de seguridad de personas, bienes de la institución, instalaciones, salud ocupacional, seguridad industrial, informática y de la información.
- Controlar el acceso a La institución y establecer medidas de seguridad, incluyendo el establecimiento de zonas videovigiladas.
- Prevenir, monitorear, detectar, investigar, analizar y/o controlar amenazas o incidentes de seguridad informática o de la información y ejecutar las medidas pertinentes para solucionarlos.
- Efectuar el proceso de conocimiento y debida diligencia.
- Prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- Enviar al correo físico, electrónico, dispositivo móvil vía mensajes de texto (SMS y/o MMS) o a través de cualquier otro medio de comunicación existente o que llegare a existir, información institucional, publicitaria o comercial sobre los servicios de La institución, sus socios comerciales, proyectos o eventos en los cuales participa y son invitados.
- Dar respuesta a consultas, peticiones, quejas y reclamos que sean realizadas por los Titulares y organismos de control y trasmitir los Datos Personales a las demás autoridades que en virtud de la ley aplicable deban recibir los Datos Personales.
- Administrar sistemas de información, contabilidad, facturación y auditorias, procesamiento y verificación de medios de pago, registro contable y control de pagos, liquidación y reportes de impuestos, beneficios.

- Suministrar, compartir, enviar o entregar sus datos personales a Compañías de seguros, asesores jurídicos, autoridades fiscales, autoridades administrativas, autoridades judiciales, y proveedores o terceros en operaciones conjuntas que procesen, administren o utilicen la información, para la ejecución de contratos o acuerdos suscritos con La institución.
- Transferir y/o transmitir la información recolectada a distintas áreas de La institución, y/o a la compañía matriz, sus filiales, subsidiarias, así como a compañías vinculadas en Colombia y en el exterior, cuando ello sea necesario para el desarrollo de sus operaciones (recaudo de cartera y cobros administrativos, tesorería, contabilidad, analítica y estadísticas, inteligencia de negocios, análisis de riesgos, seguridad, entre otros).
- Así mismo podrán ser destinatarios de la información personal recolectada por la institución, todos los accionistas, sus filiales, subsidiarias y sus empresas vinculadas en Colombia y en el exterior, aun aquellas ubicadas en países que no cuenten con los mismos niveles de protección de datos, así como también aquellos proveedores nacionales o internacionales autorizados por éstos, para garantizar la seguridad de la información, la revisión de incidentes de seguridad y, en todo caso, velar por los intereses de La institución y de los titulares.
- Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sean necesarias para desarrollar el objeto social de La institución.

7.3.2. Datos personales de pacientes, familiares y/o acompañantes:

- Procesar, confirmar, programar y prestar los servicios de salud solicitados.
- Solicitar autorización a quien corresponda, ubicado en el país o en el extranjero, dependiendo del asegurador, para la prestación de los servicios de salud requeridos.
- Solicitar a terceros los insumos, productos o servicios requeridos para la prestación de los servicios de salud.
- Efectuar estudios, investigaciones, publicaciones, mensajes publicitarios.
- Realizar y presentar informes estadísticos, analíticos, epidemiológicos, de riesgo, construcción de GRD (Grupos Relacionados por el Diagnóstico), entre otros, que permitan la optimización de los servicios brindados en la institución.
- Contactar al titular con el fin de evaluar la calidad y/o satisfacción de los servicios de salud recibidos.
- Asesorar y/o apoyar la necesidad de servicios distintos del objeto social de la institución, o que no sean prestados por ésta, pero sean requeridos por los pacientes, familiares y/o acompañantes.

7.3.3. Datos personales de empleados o de personas que participan en procesos de selección:

- Desarrollar el proceso de selección, evaluación y vinculación laboral, incluyendo la evaluación y calificación de los participantes y la verificación de referencias laborales y personales, y la realización de estudios de seguridad.
- Cumplir a cabalidad con todas las obligaciones laborales de orden legal, contractual, judicial y administrativo incluyendo pero sin limitarse a: pago de nómina, aportes y reportes al sistema de seguridad social (salud, pensiones, administración de riesgos laborales, cesantías, cajas de compensación familiar, entre otros); declaraciones de impuestos; atención de programas de compensación; bienestar laboral; medición de productividad y promoción; programas de fidelización; salud ocupacional y seguridad industrial;

prevención de acoso laboral; acreditación de órdenes judiciales y administrativas, entre otros.
- Administrar usuarios, correo electrónico, aplicativos internos.
- Publicar información en el directorio institucional.
- Contratar beneficios laborales con terceros, tales como seguros de vida, gastos médicos, entre otros.
- Reproducir fotografías o publicar información en comunicaciones, boletines o publicaciones institucionales.

7.3.4. Datos personales de contratistas:

- Desarrollar el proceso de contratación.
- Prestar en debida forma los servicios por parte de La institución.
- Realizar informes de gestión de acuerdo con lo establecido en el proceso contratación.
- Administrar usuarios y aplicativos internos.
- Publicar información en el directorio institucional.
- Publicar información de interés para los pacientes y la comunidad en la página web u otros medios de comunicación de la institución.
- Medir productividad y ejecutar programas de fidelización.
- Reproducir fotografías o publicar información en comunicaciones, boletines o publicaciones de la institución.
- Compartir los Datos Personales a terceros para la celebración y/o ejecución de actos o negocios jurídicos relacionados con el desarrollo de planes de beneficios de cualquier naturaleza, en favor del Titular.

7.3.5. Datos personales de proveedores:

- Cumplir con las disposiciones contractuales para las adquisiciones de bienes y servicios demandados por La institución para su normal funcionamiento: obligaciones contractuales, judiciales y administrativas, incluyendo registro contable y control de pagos, liquidación y reportes de impuestos, salud ocupacional, seguridad industrial y prevención de riesgos, acreditación de órdenes judiciales y administrativas, entre otros.
- Efectuar estudios, investigaciones e informes de mercado, financieros, estadísticos y de riesgos, entre otros.
- Consultas, auditorias y revisiones derivadas de la relación con el proveedor.
- Evaluar la ejecución y calidad de los servicios y bienes contratados.
- Administrar usuarios, correos electrónicos y aplicativos internos.

7.3.6. Datos personales de empleados en misión y de empleados de nuestros proveedores.

Asegurar, en general, el cumplimiento de las normas que resulten aplicables conforme a la vinculación contractual y al tipo de servicio que se relacione.

7.3.7. Finalidades del tratamiento de datos personales de exfuncionarios

- La institución realiza el Tratamiento de información personal de los exfuncionarios con las siguientes finalidades:
- Servir como base para la expedición de los certificados laborales de que establece la normatividad vigente a solicitud del Exempleado o sus causahabientes.

- Servir como histórico para las solicitudes de pensión, historia clínica ocupacional.

7.4. LEGITIMACIÓN PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR

Los derechos de los Titulares establecidos en la Ley podrán ejercerse por las siguientes personas:

- Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro o para otro.
- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos

7.5. PROCEDIMIENTO QUE DEBE SEGUIR EL TITULAR PARA EJERCER SUS DERECHOS

El titular que quiera consultar sus datos personales contenidos o almacenados en las bases de datos de la clínica o que quiera presentar un reclamo para que dicha información sea objeto de corrección, actualización o supresión, o que advierta el presunto incumplimiento de cualquiera de los deberes y principios contenidos en la normatividad sobre protección de datos personales por parte de la clínica, podrá presentar reclamación mediante un escrito enviado al correo electrónico: atencion1@dermatologia.gov.co o a la Avenida 1 N 13A 61., dirigido a atención al usuario, con copia al área de área jurídica, adjuntando fotocopia de su documento de identidad o cualquier otro documento equivalente que acredite su identidad y titularidad de los datos personales.

7.5.1. Procedimiento para la realización de consultas:

- El titular podrá consultar sus datos personales en cualquier momento. para tal fin, podrá elevar una solicitud indicando la información que desea conocer, a través de cualquiera de los mecanismos arriba señalados.
- El titular deberá acreditar su identidad, la de su representante, la representación o estipulación a favor de otro o para otro. Cuando la solicitud sea formulada por persona distinta del titular y no se acredite que la misma actúa en representación de aquél, se tendrá por no presentada.
- a consulta debe contener como mínimo el nombre y dirección de contacto del titular o cualquier otro medio para recibir la respuesta, así como una descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer su derecho de consulta.
- Si la consulta realizada por el titular del dato resulta incompleta, la institución requerirá al interesado dentro de los cinco (5) días siguientes a la recepción de la consulta 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 de su consulta.
- Las consultas serán atendidas por La Institución en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender la consulta dentro de dicho término, este hecho se informará al solicitante, 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.

7.5.2. Procedimiento para la realización de quejas y reclamos:

De conformidad con lo establecido en el Artículo 14 de la Ley 1581 de 2012, cuando el Titular considere que la información tratada por La Clínica deba ser objeto de corrección, actualización o supresión, o cuando deba ser revocada por advertirse el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley, podrán presentar una solicitud ante La Clínica, la cual será tramitada bajo las siguientes reglas:

- El titular o su representante deberán acreditar su identidad, la de su representante, la representación o estipulación a favor de otro o para otro. cuando la solicitud sea formulada por persona distinta del titular y no se acredite que la misma actúa en representación de aquél, se tendrá por no presentada.
- La solicitud de rectificación, actualización, supresión o revocatoria debe ser presentada a través de los medios habilitados por la clínica indicados en el presente documento y contener, como mínimo, la siguiente información:
- El nombre y dirección de domicilio del titular o cualquier otro medio para recibir la respuesta.
- Los documentos que acrediten la identidad del solicitante y en caso dado, la de su representante con la respectiva autorización.
- La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos y la solicitud concreta.
- Si la solicitud se presenta incompleta, la institución deberá requerir al interesado dentro de los cinco (5) días siguientes a su recepción 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 de su solicitud.
- El término máximo para atender esta solicitud será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderla dentro de dicho término, se informará al interesado sobre 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.

7.5.3. Procedimiento para la solicitud de supresión, modificación y/o actualización de datos de la historia clínica.

- Si se trata de una solicitud para la supresión, modificación y/o actualización de datos de la historia clínica; la misma, deberá ser dirigida al Comité del Historia Clínicas de la Clínica; el cual previo el estudio de esta y las pruebas aportadas, tomará la decisión a que haya lugar y dará respuesta en los términos de ley.
- No obstante, y teniendo en cuenta la obligatoriedad del registro de la historia clínica, establecida en la Ley 23 de 1981 y demás normas complementarias, no será sujeto de modificación y/o supresión los diagnósticos y conceptos médicos impartidos por los profesionales de la salud, los resultados de los paraclínicos, los antecedentes médicos y, en general todas las condiciones clínicas del paciente

7.6. 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.

Las bases de datos responsabilidad de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades de tratamiento y sin perjuicio de normas legales que dispongan lo contrario. EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

7.7. Cumplimiento y actualización

El Manual en el numeral de Seguridad es un documento de la empresa de obligatorio cumplimiento para todo el personal de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

- Gestión de documentos y soportes

La Entidad ha implementado el formato DR-PLE-FO-035 AUTORIZACIÓN DE TRATAMIENTO DE DATOS, Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de los datos personales; una vez diligenciado deberá remitir al área funcional correspondiente para incorporarse como tipología (anexo), como ejemplo: cajas diligencia el formato y deberá remitirlo al archivo de gestión de historias clínicas para que haga parte integral del del mismo.

Para reposar en la serie documental – HISTORIAS CLÍNICAS de acuerdo con la Tabla de Retención Documental, en la cual reposará en el expediente y será el custodio de esta. Una vez cumpla con el tiempo de retención, gestión, trámite y cierre del expediente.

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

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.

La identificación de los documentos y soportes que contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de las 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 servidor público será responsable de la adecuada conservación, organización, uso y manejo de los documentos y archivos que se deriven del ejercicio de sus funciones, deberá llevar el control de los archivos debidamente inventariados para garantizar la continuidad de la gestión pública, en el formato establecido por la Entidad DR-GIC-FO-007 FORMATO UNICO DE INVENTARIO DOCUMENTAL y soportes de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA.

La conservación, custodia, trazabilidad, disposición final, identificación, inventario y demás controles, procesos y seguimientos realizados; sí como la protección de los archivos físicos y/o electrónicos se harán de acuerdo con lo establecido en la Ley 594 de 2000- Ley General de Archivo y lo establecido en la entidad en los procesos de sistema de gestión de calidad. Para esto se deberá obedecer a los lineamientos de las tablas de retención documentales aprobadas en la Entidad.

7.8. Control de acceso

El personal de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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 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 o 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA, 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.

7.9. Ejecución del tratamiento en sedes

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de sedes requiere una autorización previa por parte de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

7.10. 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 s 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. Asimismo, el responsable de área funcional de Informática deberá garantizar que en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

7.11. 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.

a. Los funcionarios y servidores públicos serán responsables de la protección de datos personales, de manera solidaria, de acuerdo con los preceptos establecidos en la Constitución y la ley.

b. Las dependencias del Centro Dermatológico “Federico Lleras Acosta “serán las encargadas de velar por la protección de la confidencialidad de los datos personales de las personas denunciantes, ejerciendo controles sobre aquellos que tenga a su cargo.

7.12. Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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 estas.

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 presente Manual de Seguridad y quedarán a disposición de la Autoridad de Control.

7.13. Medidas de seguridad para bases de datos no automatizadas

- Archivo de documentos

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA fija los criterios s 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.

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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

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 estos 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 el 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA, podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente manual.

- Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el manual, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con el 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 l 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA.

7.14. Medidas de seguridad para bases de datos automatizadas

- Identificación y autenticación

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOS, 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.

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 con 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 recomienda que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas números y letras. La política de contraseñas de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA.

Por otra parte, EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA, 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.

- 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.

- 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.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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 o sus características físicas y las medidas de seguridad física existentes.

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.

- Copias de respaldo y recuperación de datos

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de estos 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.

- Registro de acceso

De los intentos de acceso a los sistemas de información de EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

- 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.

7.15. 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.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOS, 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA es sancionable de acuerdo con 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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 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. 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 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 estos.

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 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. Así mismo, 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 7.11 del presente manual.

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 realizará un acata o se llevará 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 EMPRESA SOCIAL DEL ESTADO CENTRO DERMATOLOGICO FEDERICO LLERAS ACOSTA 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.

8 BIBLIOGRAFÍA

https://prodata.com.co/proteccion/documentos-imprimir.aspx?tipo=35&strsecgk=1075&clteid=1103

Álzate y asociados Asesores jurídicos Pro-data

9 APROBACIÓN DEL DOCUMENTO:

	ELABORÓ	REVISÓ	APROBÓ
FIRMA:			
NOMBRE:	William Narváez Mendoza	Juan Carlos Vásquez Ramírez	William Narváez Mendoza
CARGO:	Asesor de la Dirección	Responsable de informática	Asesor de la Dirección