

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Política no. 433

Versión no.1 Fecha: 27 de Junio de 2013

ÁREAS DE APLICACIÓN

Perimeter: Colombia

Staff Function: -

Service Function: Security

Business Line: -

CONTENIDO

OBJETIVOS Y ALCANCE DEL DOCUMENTO	5
1.UNIDADES RESPONSABLES DEL DOCUMENTO	6
2.REFERENCIAS.....	6
3.POSICIÓN DEL PROCESO CON RESPECTO A LA TAXONOMÍA DE PROCESOS	7
4.DEFINICIONES Y ACRÓNIMOS	7
5.CONDICIONES GENERALES	11
5.1.PRINCIPIOS ORIENTADORES	11
6.TRATAMIENTO DE LOS DATOS PERSONALES	14
6.1.CREACIÓN DE BASES DE DATOS QUE CONTENGAN DATOS PERSONALES.....	14
6.2.MEDIOS PARA LA OBTENCIÓN DE DATOS PERSONALES.....	14
6.3.AUTORIZACIÓN	14
6.4.DATOS PERSONALES PROCEDENTES DE FUENTES EXTERNAS.....	16
6.5.RESERVA Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES	16
6.6.VERACIDAD Y CALIDAD DE LOS DATOS PERSONALES	16
6.7.FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES.....	17
7.DERECHOS QUE ASISTEN AL TITULAR DE LOS DATOS PERSONALES	18

8.CONSULTAS Y RECLAMOS SOBRE EL TRATAMIENTO DE DATOS PERSONALES	19
8.1.CONSULTAS.....	19
8.2.RECLAMOS	20
8.3.CANALES PARA REALIZAR CONSULTAS PETICIONES Y RECLAMOS.....	21
9.DEBERES DE LA EMPRESA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES ..	22
9.1.DEBERES PARA LOS RESPONSABLES DEL TRATAMIENTO	22
9.2.DEBERES PARA ENCARGADO DEL TRATAMIENTO	23
10.TRANSFERENCIA DE DATOS PERSONALES A OTROS PAÍSES	25
11.TRATAMIENTO DE DATOS PERSONALES EN LA CADENA DE ABASTECIMIENTO.....	25
12.ENTREGA DE DATOS PERSONALES A AUTORIDADES	26
13.DATOS DE IDENTIFICACIÓN DE LA EMPRESA.....	26
14.VIGENCIA DE LA POLÍTICA	26

OBJETIVOS Y ALCANCE DEL DOCUMENTO

Establecer y definir los lineamientos y responsabilidades para EMGESA SA ESP, en adelante: La Empresa en Colombia en relación con el tratamiento de los datos de carácter personal de los clientes, contratistas, proveedores, aliados y demás personas naturales cuyos datos sean tratados por la Empresa, para asegurar el cumplimiento de la legislación colombiana en materia de protección de datos; garantizando el ejercicio de los derechos de los titulares en relación con sus datos personales.

Mediante el presente lineamiento se adoptan y establecen reglas aplicables al tratamiento de datos de carácter personal tratados por la Empresa en desarrollo de su objeto social y demás actividades empresariales, bien sea en calidad de responsable y/o encargado del tratamiento.

Lo establecido en esta (en adelante Política) será de obligatorio cumplimiento para todos los directivos, empleados y contratistas; Gestores de Seguridad de la Información, Administradores de Seguridad de la Información respecto a la protección de Datos Personales de la Empresa.

Comprende los lineamientos de las actividades que regulan el actuar en la Empresa para cumplir la normativa en materia de protección de Datos Personales.

Esta política es de aplicación, de la forma más extensiva posible, en Colombia, y de conformidad con cualquier ley, regulación y normas de gobierno corporativo aplicables, incluyendo cualquier disposición relacionada con el mercado de valores o de separación de actividades que, en cualquier caso, prevalecen sobre las disposiciones contenidas en el presente documento.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LOS CAMBIOS
1	01/12/2017	Elaboración inicial de la Política [Este documento deroga la Norma NO068, PL008].
1	01/02/2018	Actualizada conforme a los desarrollos normativos sobre protección de datos personales
1	29/05/2019	Cambio de formato y ajustes no sustanciales.

1. UNIDADES RESPONSABLES DEL DOCUMENTO

Responsable de la elaboración del documento:

- Unidad Security Colombia;
- Unidad de Asuntos Corporativos

Responsable de la autorización del documento

- Unidad de Servicios y Seguridad Colombia;
- Unidad de Asuntos Legales y Corporativos Colombia

2. REFERENCIAS

- Código Ético del Grupo Enel;
- Modelo de Prevención de Riesgos Penales
- Plan de Tolerancia Cero contra la Corrupción (PTZC)
- Ley Estatutaria 1581 de 2012 (Protección de Datos Personales)

- Decreto No. 886 de 2014
- Decreto 1377 de 2013
- Documentos reglamentarios emitidos por la Autoridad Competente que regulen la protección de los datos personales
- Demás legislación Colombiana aplicable
- PL 26 Organizational Guidelines

3. POSICIÓN DEL PROCESO CON RESPECTO A LA TAXONOMÍA DE PROCESOS

Cadena de Valor / Área de proceso: Security

Macro Proceso: Clasificación de la información y Protección de datos

Proceso: Protección de datos

4. DEFINICIONES Y ACRÓNIMOS

ACRÓNIMO Y PALABRAS CLAVE	DESCRIPCIÓN
Autorización o Consentimiento	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. El consentimiento puede ser declarado por escrito, medios electrónicos, o incluso de forma oral.
Accesos autorizados	Autorizaciones concedidas a un usuario para la utilización y consulta de un activo de información.

ACRÓNIMO Y PALABRAS CLAVE	DESCRIPCIÓN
Autenticidad	Manifiesta la garantía existente sobre la identificación del origen y destino de la información y sobre la autorización para que se transmita entre ellos.
Aviso de privacidad	Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales
Base de datos	Conjunto organizado de datos personales que sea objeto de tratamiento. Se considera tanto el tratamiento automatizado (aplicaciones informáticas) como también el tratamiento en papel.
Control de accesos	Mecanismo que en función de la identificación ya autenticada permite acceder a los datos.
Copia de respaldo	Copia de los datos en un soporte que posibilite su recuperación.
Dato Personal o Dato de Carácter Personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Dato Público	Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y aquel que no sea semiprivado, privado o sensible. Son públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
Dato Semiprivado	Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.
Datos Sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

ACRÓNIMO Y PALABRAS CLAVE	DESCRIPCIÓN
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.
Fuentes accesibles al público	Bases de datos cuya consulta, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación, puede ser realizada por cualquier persona. Tienen consideración de fuentes de acceso público, exclusivamente, el censo promocional, las guías de servicios de telecomunicaciones en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.
Gestor de la Base de Datos	Será la persona responsable de una Base de Datos que contenga Datos de Carácter Personal
Habeas data	Derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países
Identificación	Procedimiento de reconocimiento de la identidad de un usuario
Incidencia	Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
Procedimiento de disociación	Todo tratamiento de datos personales cuyo resultado es información que no puede asociarse a persona identificada o identificable.

ACRÓNIMO Y PALABRAS CLAVE	DESCRIPCIÓN
Responsable del Tratamiento	<p>La Empresa es la organización responsable de los Activos de Información en su dominio o ámbito de responsabilidad. Materializa las funciones exigidas por la legislación al Responsable de la base de datos.</p> <p>Para una empresa, el Propietario de la base de datos será el responsable funcional que en dicha empresa tiene capacidad de decisión sobre los datos incluidos en dicha base de datos.</p> <p>Para las bases de datos que conforman los sistemas informáticos corporativos y multiempresa, el Propietario del activo soportado en estas bases de datos será el responsable funcional de La Empresa que, a través del oportuno Contrato de Encargo de tratamiento, tiene capacidad de decisión sobre los datos incluidos en dicho sistema.</p>
Unidad de Seguridad	Tiene como propósito proteger la información de una Organización, independientemente del lugar en que se localice. Tiene tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad de la información.
Seguridad Patrimonial	Función especializada en la detección y análisis de las actuaciones que supongan amenazas físicas para los activos de información. Asimismo, esta función es especialista en la implantación de las protecciones que garanticen la integridad física de los activos de información, de forma que no sean manipulados y/o sustraídos por personas no autorizadas.
GDS Cyber Security	Función especializada en el estudio e implantación de las protecciones tecnológicas que garanticen la integridad, confidencialidad, disponibilidad, autenticidad y no repudio lógicos de los Activos de Información que se hallen en soporte informático.
SIC	Superintendencia de Industria y Comercio
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.

ACRÓNIMO Y PALABRAS CLAVE	DESCRIPCIÓN
Transferencia	La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
Transmisión	Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

5. CONDICIONES GENERALES

La Empresa reconoce la importancia constitucional que tiene la protección del derecho de las personas a su intimidad personal y familiar y a su buen nombre, asimismo se compromete a cumplir con los procedimientos establecidos por el Estado Colombiano para el tratamiento de datos respetando la libertad y demás garantías consagradas en la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013 y la demás normatividad aplicable.

En este sentido, la Empresa expresa su respeto y compromiso hacia la protección de los datos de carácter personal y hacia el cumplimiento de la legislación vigente en la materia garantizando el ejercicio del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales.

5.1. PRINCIPIOS ORIENTADORES

Los siguientes son los principios orientadores bajo los cuales se rige el tratamiento de los datos personales en la Empresa, los mismos se encuentran contenidos en la normatividad vigente y en la jurisprudencia constitucional colombiana que se deben tener en cuenta al momento de interpretar el presente documento:

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

- **Principio de Legalidad en materia de Tratamiento de Datos:** El tratamiento de los datos personales es una actividad reglada, que debe sujetarse a lo establecido en la Constitución Política de Colombia y en las normas que la desarrollen.
- **Principio de Finalidad:** El tratamiento debe obedecer a una finalidad determinada, específica y legítima, de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular por parte de la Empresa.
- **Principio de Libertad:** Es política de La Empresa establecer medidas para que el tratamiento de la información personal solo pueda ejercerse con el consentimiento previo, expreso e informado del titular. Para La Empresa, los datos personales no podrán ser obtenidos o divulgados sin previa autorización o en ausencia de mandato legal o judicial que releve el consentimiento. Se entenderá que existe consentimiento previo, expreso e informado cuando el titular haya adelantado acciones que indiquen que este se dio de forma inequívoca.
- **Principio de Necesidad y Proporcionalidad:** Los datos personales registrados en una base de datos de La Empresa deben ser los estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, informadas al titular en atención al principio de finalidad. En tal sentido, deben ser adecuados, pertinentes y acordes con las finalidades para los cuales fueron recolectados.
- **Principio de Veracidad o Calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. La Empresa prohíbe para sus procesos internos el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales la Empresa adoptará las medidas razonables para asegurar que los datos personales que reposan en las bases de datos registradas, sean precisos y suficientes, cuando exista una obligación contractual o legal, cuando así lo solicite el titular o, cuando el Responsable haya podido advertirlo, actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento.

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

- **Principio de Transparencia:** En el tratamiento la Empresa implementará medidas para garantizar el derecho del Titular a obtener del Responsable o del Encargado, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Salvo en los casos en los cuales la autorización no sea necesaria de acuerdo con las normas aplicables, el Responsable del tratamiento debe adoptar procedimientos que permitan a los titulares conocer, a más tardar en el momento de la recolección inicial de sus datos, cual información será recolectada sobre ellos y todas las finalidades del tratamiento.

- **Principio de Temporalidad o Caducidad:** El período de conservación de los datos personales autorizados para tratamiento de la Empresa será el necesario para alcanzar la finalidad para la cual se han recolectado.
- **Principio de acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, es política para la Empresa que el tratamiento de los datos personales sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley; exceptuando la información categorizada como de carácter público, es política de la Empresa, no publicar datos personales en medios de divulgación o comunicación masivos a menos que se cuente con la autorización respectiva para ello y/o responda a un mandato legal. La Empresa implementará medidas técnicas para controlar el acceso, evitar el acceso no autorizado y permitir el uso hacia los titulares o terceros autorizados conforme a la ley.
- **Principio de seguridad:** Para que la información sujeta a tratamiento por el Responsable o Encargado del a que se refiere la presente política y la ley esté protegida, La empresa implementará 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.
- **Principio de confidencialidad:** La Empresa implementará medidas hacia las personas que intervengan en el tratamiento de datos personales que no ten-

gan la naturaleza de públicos para guardar la reserva de la información personal, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la ley y en los términos de la misma.

6. TRATAMIENTO DE LOS DATOS PERSONALES

6.1. CREACIÓN DE BASES DE DATOS QUE CONTENGAN DATOS PERSONALES.

La Empresa creará bases de datos que contengan información de carácter personal cuando resulte necesario para el logro de la actividad de la Empresa de acuerdo con lo establecido en la ley.

6.2. MEDIOS PARA LA OBTENCIÓN DE DATOS PERSONALES

Para la recolección de datos personales pueden emplearse medios impresos, cuestionarios electrónicos, entrevistas personales o telefónicas, o cualquier otro medio que pueda ser objeto de consulta posterior.

6.3. AUTORIZACIÓN

Al momento de obtener los datos personales se debe solicitar al titular la autorización correspondiente, la cual debe ser informada, previa, expresa e inequívoca para el tratamiento de los datos personales. En todo caso, el modo de obtener la autorización debe ser adecuado para el propósito para el que se pide y debe atender a la naturaleza de la información recolectada. Esta autorización implica que su titular autoriza el tratamiento de sus datos personales, incluyendo su transmisión y/o transferencia a nivel nacional o internacional para las finalidades descritas en este documento, conforme a la ley.

Al momento de solicitar la autorización al titular se le debe informar como mínimo lo siguiente:

- a) El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre Datos Sensibles o sobre los datos de las niñas, niños y adolescentes.
- c) Los derechos que le asisten como titular.
- d) La identificación, dirección física o electrónica y teléfono del responsable del tratamiento.

Sin excepción, se debe conservar prueba del cumplimiento de lo arriba previsto y, cuando el titular o la autoridad competente lo solicite, entregar copia de la autorización. Asimismo, se deben mantener registros de cuándo y cómo se obtuvo la autorización por parte de los titulares de datos personales para el tratamiento de los mismos.

De conformidad con el régimen legal vigente, esta autorización no será requerida en los siguientes casos:

- a) Cuando sea requerida por una entidad pública o administrativa en cumplimiento de sus funciones legales, o por orden judicial.
- b) Cuando se trate de datos de naturaleza pública.
- c) En casos de emergencia médica o sanitaria.
- d) Cuando sea tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

- e) Cuando se trate de datos personales relacionados con el registro civil de las personas,
- f) Y en los demás casos que establezca la normatividad vigente.

En estos casos, si bien no se requiere de la autorización del titular, si tendrán aplicación los demás principios y disposiciones legales sobre protección de los datos personales.

6.4. DATOS PERSONALES PROCEDENTES DE FUENTES EXTERNAS

Cuando se decida la inclusión de datos personales en una base de datos que no hayan sido recabados directamente por la Empresa, se debe comprobar la procedencia lícita, leal y no fraudulenta de dichos datos, estableciendo por escrito y mediante contrato que quien suministra los datos dispone de la prueba de autorización de cada uno de los titulares para su transmisión o transferencia.

6.5. RESERVA Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES

La Empresa, los contratistas, proveedores y aliados están obligados a guardar el secreto profesional respecto de los datos personales durante su tratamiento. Es decir, este deber aplica a todos aquellos que utilicen los datos personales y/o tengan acceso a los mismos para el desarrollo de su trabajo y respecto de los directivos, empleados y contratistas de los encargados del tratamiento en cualquiera de los servicios que se contraten y que impliquen manejo y/o acceso a datos de carácter personal. Estas obligaciones subsistirán aún después de finalizar sus relaciones laborales.

6.6. VERACIDAD Y CALIDAD DE LOS DATOS PERSONALES

Es política de la Empresa utilizar información personal veraz, completa, exacta, actualizada, comprobable y comprensible, para lo cual la Empresa implementará

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

medidas de control para aumentar la calidad de la información, y pondrá a disposición de sus titulares, los medios para asegurar que los titulares de la Información personal puedan actualizarla cuando sea necesario.

El titular de la información deberá revelar información personal veraz y exacta, así como realizar la actualización de la misma cuando se produzcan cambios que puedan facilitar la prestación de los servicios contratados. De acuerdo con lo anterior, la Empresa no se hace responsable por errores causados por información errónea proporcionada por el titular.

6.7. FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES

La información suministrada por el Titular de los datos personales, se tratará por EMGESA S.A ESP y las empresas del Grupo ENEL para:

- 1) Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información.
- 2) Realizar invitaciones a eventos y ofrecer productos y servicios de las Empresas y de terceros que tienen vínculo comercial con la Empresas
- 3) Realizar invitaciones a eventos y ofrecer productos y servicios financieros de nuestros aliados estratégicos/comerciales.
- 4) Efectuar encuestas de satisfacción respecto de los bienes y servicios ofrecidos por las Empresas
- 5) Realizar investigaciones de mercado directamente o a través de terceros con los cuales las Empresas tengan un vínculo contractual para el desarrollo de actividades contempladas dentro de su objeto social.
- 6) Contactar al Titular de la información a través de medios electrónicos y virtuales para el envío de información y ofertas relacionadas con los productos y

servicios que prestan las Empresas.

7. DERECHOS QUE ASISTEN AL TITULAR DE LOS DATOS PERSONALES

Los titulares de los datos de carácter personal contenidos en bases de datos que reposen en los sistemas de información de la Empresa, tienen los derechos descritos en este documento en cumplimiento de las garantías fundamentales consagradas en la Constitución política y en la ley.

- a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado;
- b) 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 la presente ley;
- c) Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;
- d) Presentar ante los entes de control las quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
- e) Revocar la autorización y/o solicitar la supresión del dato personal en cualquier momento para las finalidades no contempladas en el contrato de condiciones uniformes de prestación del servicio de energía eléctrica u otros contratos de servicio vigentes entre la Empresa y el titular de la información. Para revocar la autorización y/o solicitar la supresión del dato personal, de debe realizar el

trámite previsto en la presente política para presentar reclamos sobre el tratamiento de los datos personales, y conforme lo establecido en la ley.

- f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, para lo cual se debe seguir lo estipulado en la presente política para realizar consultas sobre los datos personales suministrados por el titular.

8. CONSULTAS Y RECLAMOS SOBRE EL TRATAMIENTO DE DATOS PERSONALES

8.1. CONSULTAS

Los titulares o sus causahabientes que acrediten debidamente su facultad, podrán consultar la información personal del titular que repose en cualquier base de datos de la Empresa. La Empresa deberá suministrar a éstos toda la información contenida en el registro individual o que esté vinculada con la identificación del titular. La consulta será realizada previa confirmación de la identidad del titular o de sus causahabientes.

La consulta se podrá formular por los medios habilitados por la Empresa y descritos en el numeral 8.3.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

8.2. RECLAMOS

El titular o sus causahabientes que acrediten debidamente su facultad, que consideren que la información contenida en una base de datos propiedad de la Empresa, debe ser corregida, actualizada, suprimida, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley, podrán presentar un reclamo a la Empresa. El reclamo será atendido previa confirmación de la Identidad del titular o de sus causahabientes.

Cuando se presente un reclamo por cualquiera de los medios habilitados para tal fin por la Empresa, descritos en el numeral 8.3, éste será tramitado de la siguiente manera:

- 1) El interesado debe formular el reclamo mediante solicitud dirigida a la Empresa que por lo menos deberá contener: (i) la identificación del titular, (ii) la descripción del reclamo, (iii) la dirección para efectos de notificación, (v) la documentación que pretenda hacer valer y (vi) si se actúa por intermedio de apoderado o como causahabiente, el documento que lo acredite como tal
- 2) Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- 3) Si la Empresa no es competente para resolver el reclamo, le debe dar traslado a quien corresponda en un término máximo de dos (2) días hábiles e informar de la situación al interesado.
- 4) Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo en un término no mayor a dos (2) días hábiles. Dicha etiqueta se mantendrá hasta que el reclamo sea decidido.

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

- 5) El término máximo para atender el reclamo es de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo completo. Cuando no fuere posible atender el reclamo dentro de dicho término, se debe informar 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.

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

8.3. CANALES PARA REALIZAR CONSULTAS PETICIONES Y RECLAMOS.

La Empresa ha dispuesto de los siguientes canales de atención para realizar consultas y reclamos:

- **Línea para Bogotá 636 4379** y fuera de Bogotá **01 8000 110 128**
- Página Web **www.enel.com.co**
- Comunicación escrita a la cuenta de correo: **emlinea@enel.com**, o con el Coordinador Comercial de Zona asignado
- Ventanilla de radicación ubicada en la Carrera 11 No. 82 – 76 Piso 4
- Comunicación escrita en la dirección Carrera 13A # 93 – 66

9. DEBERES DE LA EMPRESA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

9.1. DEBERES PARA LOS RESPONSABLES DEL TRATAMIENTO

Cuando se actúe en calidad de responsables del tratamiento de datos personales bajo su custodia, deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la Ley:

- a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Solicitar y conservar, en las condiciones previstas en el presente documento, copia de la respectiva autorización otorgada por el titular.
- c) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

- h) Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley.
- i) Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
- j) Tramitar las consultas y reclamos formulados en los términos señalados en la ley y en el presente documento.
- k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley y en especial, para la atención de consultas y reclamos.
- l) Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- m) Informar a solicitud del titular sobre el uso dado a sus datos.
- n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

9.2. DEBERES PARA ENCARGADO DEL TRATAMIENTO

Cuando se actúe en calidad de encargados del tratamiento de datos personales bajo su custodia, deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la Ley:

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

- a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley y este documento.
- d) Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- e) Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la Ley y en este documento.
- f) Adoptar políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
- g) Registrar en la base de datos la leyenda “reclamo en trámite” o similares en la forma en que se regula en la Ley y en el presente documento.
- h) Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- i) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

- k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- m) En el evento en que concurren las calidades de responsable del tratamiento y encargado del tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

10. TRANSFERENCIA DE DATOS PERSONALES A OTROS PAÍSES

La empresa podrá transferir los datos personales a terceros países que proporcionen niveles adecuados de protección de datos de acuerdo con la normatividad vigente. 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. La lista de países que no requieren una autorización del Titular para la transferencia de los datos personales será provista por el ente regulador SIC.

11. TRATAMIENTO DE DATOS PERSONALES EN LA CADENA DE ABASTECIMIENTO

Es política de la Empresa incluir los mismos niveles para la protección de los datos personales cuando contrate con aliados estratégicos y/o contratistas de servicios en los cuales tenga que asignar el rol del encargado de su tratamiento. Adicionalmente la Empresa validará y homologará las medidas de protección de la información que los terceros aliados de negocio y/o contratistas en calidad de responsables del tratamiento, cuando le asignen a la Empresa el rol de encargado del tratamiento.

ÁREAS DE APLICACIÓN

Perimeter: Colombia
Staff Function: -
Service Function: Security
Business Line: -

Para toda contratación entre la Empresa y un tercero donde se incluya el tratamiento de datos personales es obligatorio el establecimiento de acuerdos de confidencialidad y no divulgación.

12. ENTREGA DE DATOS PERSONALES A AUTORIDADES

Cuando las autoridades del Estado soliciten a la Empresa el acceso y/o entrega de datos de carácter personal contenidos en cualquiera de sus bases de datos, se verificará la legalidad de la petición, la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad, y se documentará la entrega de la información personal solicitada previendo que la misma cumpla con todos sus atributos (autenticidad, confiabilidad e integridad), y advirtiendo el deber de protección sobre estos datos.

13. DATOS DE IDENTIFICACIÓN DE LA EMPRESA

En cumplimiento del deber legal, y toda vez que la Empresa podrá actuar como Responsable y/o encargado del tratamiento de datos personales, se indican para los fines pertinentes, lo siguientes datos de identificación:

Razón social: EMGESA S.A E.S.P

Domicilio: Bogotá D.C

Dirección principal: Carrera 13A # 93 – 66

Correo electrónico: emlinea@enel.com

Teléfono del Responsable: 636 4379

14. VIGENCIA DE LA POLÍTICA

La política resulta aplicable desde el 1 de febrero de 2018 de su publicación en la página web de Emgesa S.A. ESP. y estará vigente hasta tanto sea modificada o derogada.

enel
emgesa