

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

1 BASE LEGAL Y ÁMBITO DE APLICACIÓN

La presente política de tratamiento de la información se desarrolla en cumplimiento de los artículos 15 y 20 de la Constitución Política; de los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD), del artículo 2.2.2.25.1.1 sección 1 capítulo 25 del Decreto 1074 de 2015, el cual, reglamenta parcialmente la Ley 1581 de 2012 (Artículo 13 del Decreto 1377 de 2013).

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

1.1 ALCANCE

El presente documento aplicará para todos aquellos datos personales que sean utilizados o que reposen en las bases de datos y archivos de CERREJÓN, respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las responsabilidades de CERREJÓN y de sus empleados y contratistas en el manejo y tratamiento de los datos personales que reposen en sus bases de datos y archivos.

1.2 NORMATIVIDAD APLICABLE

- Constitución Política de Colombia
- Ley 1581 de 2012
- Decreto 1074 de 2015 Capítulo 25 y Capítulo 26 compilatorios de los decretos:
 - o Decreto 1377 de 2013
 - o Decreto 886 de 2014
- Decreto 090 de 2018
- Y demás normas concordantes

2 DEFINICIONES

Las siguientes definiciones están basadas en el régimen legal Colombiano en materia de Protección de Datos Personales

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 del Tratamiento, 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.

Dato personal

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

Dato público

Es el dato que no es semiprivado, privado o sensible. Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos, ejemplo: número de la cédula, dirección, teléfono, datos contenidos en sentencias judiciales ejecutoriadas, datos sobre el estado civil de las personas, entre otros.

Dato semiprivado

Es aquel 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, como son: bases de datos que contengan información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Dato privado

Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

Dato sensible

Se entiende por datos sensibles aquellos que afectan la intimidad del [Titular](#) o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías

de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado del tratamiento

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del [Responsable del tratamiento](#).

Responsable del tratamiento

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Responsable de Administrar las Bases de Datos

Colaborador encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos específica; así como de poner en práctica las directrices que dicte el [Responsable del tratamiento](#) y el [Oficial de Protección de datos](#).

Oficial de protección de datos

Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.

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 de datos

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 de datos

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 determinado por el encargado por cuenta del responsable.

3 PRINCIPIOS DE LA PROTECCIÓN DE DATOS

CERREJÓN aplicará los siguientes principios en el tratamiento de datos personales de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

- **Principio de legalidad**

El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, y en las demás disposiciones que la desarrollen.

- **Principio de finalidad**

El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular de manera clara y expresa.

- **Principio de libertad**

El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad.

- **Principio de veracidad o calidad**

La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Principio de transparencia**

El Responsable del tratamiento o el Encargado del tratamiento deben garantizarle al Titular de los datos el derecho a obtener en cualquier momento y sin restricciones, información acerca de la existencia de los datos que le conciernen.

En el momento de solicitar la autorización al Titular, se informa de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

- **Principio de acceso y circulación restringida**

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

- **Principio de seguridad de la información**

La información sujeta a tratamiento por el Responsable del tratamiento o Encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El Responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento de todo el personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del Responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en las Prácticas Generales de Seguridad de la Información, de obligado cumplimiento para todo usuario y personal de la empresa. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del Responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

- **Principio de confidencialidad**

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

4 AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

Para el tratamiento de datos personales CERREJÓN requiere de la autorización previa e informada del Titular y para ello se utilizarán los mecanismos idóneos que permitan su consulta posterior. Asimismo, mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales estará consintiendo el tratamiento de sus datos por parte de CERREJÓN en los términos y condiciones recogidos en el consentimiento.

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

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.

- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizada por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

5 RESPONSABLE DEL TRATAMIENTO

El Responsable del tratamiento de las bases de datos objeto de esta política es CERREJÓN, cuyos datos de contacto son los siguientes:

- Dirección: Calle 100 No. 19 - 54 P 12, Edificio Prime Tower - Bogotá D.C.
- Correo electrónico: PPInf@cerrejon.com
- Teléfono: 57 (1) 5955555

6 TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

CERREJÓN, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

El Anexo 1 Organización de las Bases de Datos con Información Personal, contiene la información relativa a las distintas bases de datos de responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

7 DERECHOS DE LOS TITULARES

CERREJÓN cuenta con un protocolo de atención a los Titulares de los datos, quienes pueden ejercer una serie de derechos en relación al tratamiento de sus datos personales. Estos derechos podrán ser ejercidos por las siguientes personas:

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

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

Los derechos del Titular son los siguientes:

7.1 DERECHO DE ACCESO O CONSULTA

CERREJÓN garantizará el derecho del Titular a ser informado, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus datos personales al interior de la compañía.

7.2 DERECHOS DE QUEJAS Y RECLAMOS

CERREJÓN garantizará los derechos de los Titulares de los datos enmarcados en los siguientes tipos de reclamos:

- Reclamo de corrección: el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Reclamo de supresión: el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- Reclamo de revocación: el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- Reclamo de infracción: el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

7.3 DERECHO A SOLICITAR PRUEBA DE LA AUTORIZACIÓN OTORGADA AL RESPONSABLE DEL TRATAMIENTO

CERREJÓN, guardará soporte de las autorizaciones otorgadas por los Titulares de los datos y garantizará el derecho a solicitar prueba de ello, salvo los siguientes casos expresamente exceptuados como requisito para el tratamiento de conformidad con lo previsto en la Ley.

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

Quien pretenda acceder o consultar los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

7.4 DERECHO A PRESENTAR ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO QUEJAS POR INFRACCIONES

El Titular o su representante podrá elevar queja o denuncia a la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del tratamiento o Encargado del tratamiento.

8 SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL

Con antelación y/o al momento de efectuar la recolección del dato personal, CERREJÓN solicitará al Titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca.

9 TRATAMIENTO DE DATOS DE MENORES

CERREJÓN solicitará al representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. El Responsable y Encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, aplicando los principios y obligaciones establecidas por la ley, observando los siguientes criterios:

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

10 ATENCIÓN A LOS TITULARES DE DATOS

El Oficial de Protección de Datos de CERREJÓN será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos. Correo electrónico: PPInf@cerrejon.com

11 PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

11.1 DERECHO DE ACCESO O CONSULTA

CERREJÓN garantizará el derecho de acceso o consulta de los Titulares de los datos de acuerdo con los siguientes parámetros:

El Titular podrá consultar de forma gratuita sus datos personales en los siguientes casos:

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

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, CERREJÓN solamente cobrará al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción serán mayores a los costos de recuperación del material correspondiente. Para tal efecto, CERREJÓN demostrará a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos podrá ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a CERREJÓN enviado, mediante correo electrónico a: PPInf@cerrejon.com, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a: Calle 100 No. 19 - 54 P 12, Edificio Prime Tower - Bogotá D.C. La solicitud deberá contener los siguientes datos:

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

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

- Por escrito, con copia o fotocopia remitida por correo certificado.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por CERREJÓN.

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

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

11.2 DERECHOS DE QUEJAS Y RECLAMOS

CERREJÓN garantizará el derecho de presentar quejas o reclamos de los Titulares de los datos de acuerdo con los siguientes parámetros:

El Titular de los datos podrá ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a CERREJÓN enviado, mediante correo electrónico a PPInf@cerrejon.com, indicando en el Asunto: "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a Calle 100 No. 19 - 54 P 12, Edificio Prime Tower - Bogotá D.C. La solicitud deberá contener los siguientes datos:

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

Cuando el reclamo no contenga la información suficiente para dar respuesta de fondo, es decir, resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

CERREJÓN resolverá la petición de reclamo en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez agotado el trámite de reclamo y que este no haya sido resuelto, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

12 MEDIDAS DE SEGURIDAD

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

Por otra parte, CERREJÓN, mediante la suscripción de los correspondientes contratos de transmisión, exigirá a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por CERREJÓN que están recogidas y desarrolladas en su Prácticas Generales de Seguridad de la Información, (Tablas II, III, IV y V).

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

Gestión de documentos y soportes	Control de acceso	Incidentes	Personal	Prácticas Generales de Seguridad de la Información
<p>1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.</p> <p>2. Acceso restringido al lugar donde se almacenan los datos.</p> <p>3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.</p> <p>4. Sistema de etiquetado o identificación del tipo de información.</p> <p>5. Inventario de soportes</p>	<p>1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones.</p> <p>2. Lista actualizada de usuarios y accesos autorizados.</p> <p>3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados.</p> <p>4. Concesión, alteración o anulación de permisos por el personal autorizado</p>	<p>1. Registro de incidencias: tipo de incidente, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.</p> <p>2. Procedimiento de notificación y gestión de incidentes.</p>	<p>1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos</p> <p>2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.</p> <p>3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas</p>	<p>1. Elaboración e implementación de las Prácticas Generales de Seguridad de la Información de obligado cumplimiento para el personal.</p> <p>2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.</p>

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

Bases de datos no automatizadas			Bases de datos automatizadas	
Archivo	Almacenamiento de documentos	Custodia de documentos	Identificación y autenticación	Telecomunicaciones
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.

Bases de datos automatizadas y no automatizadas			Bases de datos automatizadas			
Auditoría	Responsable de seguridad	Manual Interno de Seguridad	Gestión de documentos y soportes	Control de acceso	Identificación y autenticación	Incidentes
<p>1. Auditoría ordinaria (interna o externa) cada dos meses.</p> <p>2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información.</p> <p>3. Informe de detección de deficiencias y propuesta de correcciones.</p> <p>4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.</p> <p>5. Conservación del Informe a disposición de la autoridad.</p>	<p>1. Designación de uno o varios responsables de seguridad.</p> <p>2. Designación de uno o varios encargados del control y la coordinación de las medidas de las Prácticas Generales de Seguridad de la Información</p> <p>3. Prohibición de delegación de la responsabilidad del Responsable del tratamiento en el Responsable de seguridad.</p>	<p>1. Controles periódicos de cumplimiento</p>	<p>1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega</p>	<p>1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.</p>	<p>1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.</p>	<p>1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.</p> <p>2. Autorización del Responsable del tratamiento para la ejecución de los procedimientos de recuperación.</p>

Bases de datos no automatizadas				Bases de datos automatizadas		
Control de acceso	Almacenamiento de documentos	Control de acceso	Almacenamiento de documentos	Control de acceso	Almacenamiento de documentos	Control de acceso
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.	1. Sistema de etiquetado confidencial. 2. Cifrado de datos.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control del registro de accesos por el responsable de seguridad. Informe mensual. 3. Conservación de los datos: 2 años.	1. Transmisión de datos mediante redes electrónicas seguras.

13 PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

CERREJÓN establece el siguiente procedimiento de notificación, gestión y respuesta de incidencias (pérdida, hurto y/o acceso no autorizado) con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

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

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

- Cuando una persona tenga conocimiento de una incidencia (pérdida, hurto y/o acceso no autorizado) que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa o alguno de los Encargados deberá comunicarlo, de manera inmediata, al Oficial de Protección de Datos, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.
- Una vez comunicada la incidencia solicitará al Oficial de Protección de Datos un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
- El Oficial de Protección de Datos gestionará el registro de incidencias diligenciando los siguientes datos: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, ejecución y administración de procesos), fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro será gestionado por el Oficial de Protección de Datos, a través del documento Registro de incidencias y plan de acción.
- Asimismo, CERREJÓN implementará los procedimientos para la recuperación de los datos cuando se presenten estas incidencias, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.
- Adicionalmente, el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el Registro Nacional de Bases de Datos - RNBD dentro de los 15 días hábiles siguientes de haber sido detectado.
- Finalmente, CERREJÓN notificará del incidente a los Titulares, cuando se identifique que puedan verse afectados de manera significativa.

14 ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

CERREJÓN ha establecido un sistema de gestión de riesgos documentado en el Manual de Gestión de Riesgos, el cual será utilizado para la gestión de riesgos relacionados con el tratamiento de datos personales y que contempla su identificación, evaluación, tratamiento, monitoreo y revisión.

El sistema de gestión de riesgos considerará las causas tales como: tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo. Por lo que, para garantizar la protección de datos personales se tendrá en cuenta el tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), tales como:

- Criminalidad: entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por ésta.
- Sucesos de origen físico: entendidos como los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.
- Negligencia y decisiones institucionales: entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionadas con el comportamiento humano.

CERREJÓN, de acuerdo con su en el sistema de gestión de riesgos implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

15 ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES

Cuando por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial se soliciten a CERREJÓN 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 suscribirá acta de la entrega de la información personal solicitada, precisando la obligación de garantizar los derechos del Titular, tanto al funcionario que hace la solicitud, a quien la recibe, así como a la entidad requirente.

16 TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

CERREJÓN, no hará transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos, salvo en los casos que expresamente indica la LEPD. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la ley 1581 de 2012 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, se comunicará a la Superintendencia de Industria y Comercio para que profiera la declaración de conformidad relativa a la transferencia internacional de datos personales a países que no cumplan con los requisitos establecidos en las normas que rigen a materia.

17 TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos almacenados en las bases de datos serán recolectados y tratados por motivos estrictamente de seguridad, para verificar la identidad personal y realizar control de acceso a los empleados, clientes y visitantes. Los mecanismos biométricos de identificación capturan, procesan y almacenan información relacionada con, entre otros, los rasgos físicos de las personas (las huellas dactilares, reconocimiento de voz y los aspectos faciales), para poder establecer o “autenticar” la identidad de cada sujeto.

La administración de las bases de datos biométrica se ejecutará con medidas de seguridad técnicas que garantizan el debido cumplimiento de los principios y las obligaciones derivadas de Ley Estatutaria en Protección de Datos asegurando además la confidencialidad y reserva de la información de los titulares.

18 REGISTRO NACIONAL DE BASES DE DATOS – RNBD

CERREJÓN inscribirá sus bases de datos en el Registro Nacional de Bases de Datos en la Superintendencia de Industria y Comercio de acuerdo con las instrucciones que para el efecto impartan los entes competentes. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

19 PROTECCIÓN, SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

El cumplimiento del marco normativo en Protección de Datos Personales, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para CERREJÓN. Por ello, hemos establecido políticas, lineamientos y procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades de CERREJÓN cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.

Asimismo, garantizamos 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.

En caso de ser necesario suministrar información a un tercero por la existencia de un vínculo contractual, suscribimos contrato de transmisión para garantizar la reserva y confidencialidad de la información, así como, el cumplimiento de la presente Política del tratamiento de los datos, de las políticas y manuales de seguridad de la información y los protocolos de atención a los titulares establecidos en CERREJÓN. En todo caso, adoptamos compromisos para la protección, cuidado, seguridad y preservación de la confidencialidad, integridad y privacidad de los datos almacenados.

20 GESTIÓN DE DOCUMENTOS

Los documentos que contengan datos personales deben ser fácilmente recuperables, es por ello que será documentado el lugar donde reposa cada uno de los documentos tanto físicos como digitales, se harán inspecciones a estas rutas de almacenamiento de forma frecuente, se garantizará su conservación dejando definido en qué soporte y bajo qué condiciones se llevará a cabo esta conservación, teniendo en cuenta condiciones ambientales, lugares de almacenamiento, riesgos a los cuales están expuestos entre otros, el tiempo de retención de los documentos se determina en función de los requisitos legales si aplica, de lo contrario cada organización lo define de acuerdo a sus necesidades, así mismo tendrá clara la disposición final de los mismos, identificando si se recicla, reutiliza, se conserva, se digitaliza entre otros.

A fin de que sean fácilmente trazables, los documentos estarán codificados, serán actualizados y modificados por el personal responsable, esta modificación se efectuará siempre y cuando sea necesario, para la eliminación de un documento se debe tener la justificación para ello descrita en el histórico el cual se encuentra en la parte inferior de todos los documentos.

Los documentos tanto físicos como digitales que contengan datos personales, serán protegidos por agentes externos o internos que puedan alterar su contenido, siguiendo los lineamientos descritos en el PL-02 Manual Interno de Políticas de Seguridad.

La distribución de los documentos que contengan datos personales la efectuará el Responsable del tratamiento, este dejará documentada la evidencia de dicha distribución, donde entre otros se especifique; el tipo de documento y la identificación de la persona a la cual se le entregó la información

Se designará un responsable de garantizar la confidencialidad de los datos personales de los titulares, este será quien custodie documentos, garantice su protección tanto física como digital, evite alteraciones de la información, así mismo garantizará que los documentos que salgan de su custodia sean identificados y fácilmente trazables.

21 VIGENCIA

La presente actualización de la Política estará vigente desde el 1 de noviembre de 2018, las bases de datos responsabilidad de CERREJÓN serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos y de acuerdo con la autorización otorgada por los Titulares de los datos personales.

22 ANEXOS

Documentos asociados: OD-TISE-101 Organización de las Bases de Datos