

# POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

## 1. Propósito

La presente norma o política de tratamiento de la información se desarrolla en cumplimiento de: (i) los artículos 15 y 20 de la Constitución Política de Colombia de 1991; (ii) 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; y (iii) el 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 apoya el cumplimiento de la Política de Gobernanza de la Información, para garantizar que el tratamiento de los datos personales relacionados con las personas cumpla con la legislación de protección de datos aplicable, y cubre 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.

## 2. Alcance

Esta norma aplica 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 fija 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.

## 3. Términos clave

Las siguientes definiciones se encuentran establecidas en el artículo 3 de la Ley 1581 de 2012 y artículo 2.2.2.25.1.3 sección 1 Capítulo 25 del decreto 1074 de 2015 (Artículo 3 del decreto 1377 de 2013).

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

**Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento, pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

**Dato personal:** Cualquier información relacionada directa o indirectamente con una persona identificada o identificable, en particular mediante referencia a un identificador como el nombre, el número de identificación, el número de teléfono, la dirección de correo electrónico o los datos de la

ubicación, es decir, cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable. Estos datos se clasifican en públicos, semiprivados, privados y sensibles:

- **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 del servidor público. 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 aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo 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: (i) números telefónicos y correos electrónicos personales; (ii) datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social; (iii) solvencia patrimonial o de crédito; (iv) información suficiente para evaluar la personalidad del titular; (v) 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:**

Líder de área o de proceso encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base de datos a su cargo; 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 (OPD):**

También llamado Contacto de Protección de Datos (CPD), es la Persona designada por CERREJÓN como primer punto de contacto en materia de protección de datos y encargada de las tareas de protección de datos, incluida la implementación y el cumplimiento de las normas en protección de datos.

**Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.

**Tratamiento:**

Cualquier operación con datos personales por cualquier medio, como la recopilación, registro, almacenamiento, conservación, uso, adaptación o alteración, divulgación, transferencia, borrado o destrucción.

**Aviso de privacidad:**

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

**Transferencia:**

La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país.

**Transmisión:**

Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento determinado por el encargado por cuenta del Responsable.

## 4. Transferencia

### 4.1 Contacto interno para la protección de datos

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

- Dirección: Carrera 15 # 91-46 Piso 7
- Correo electrónico: [protecciondatos@cerrejon.com](mailto:protecciondatos@cerrejon.com)

Para facilitar la aplicación de las normas en materia de protección de datos, CERREJÓN ha designado un Oficial de Protección de Datos, quien participa en todos los asuntos relacionados con su cumplimiento. En particular, el OPD debe:

- (i) Mantener una visión general de los datos personales tratados.
- (ii) Auditar el tratamiento de los datos personales y recomendar medidas correctivas en caso de incidencias.
- (iii) Asesorar sobre los aspectos de protección de datos de los nuevos proyectos o procesos que impliquen el Tratamiento de Datos Personales.
- (iv) Garantizar que se mantenga un registro de actividad de tratamiento de datos o un inventario similar.
- (v) Informar sobre violaciones de datos a Glencore, a las autoridades de protección de datos o al/a los interesado/s.
- (vi) Promover la concientización y la comprensión de los problemas de privacidad.
- (vii) Actuar como punto de contacto entre Cerrejón y las Autoridades Locales de Protección de Datos.
- (viii) Establecer e implementar los controles del Programa Integral de Gestión de Datos Personales.

(ix) Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.

(x) Promover una cultura de protección de datos dentro de la organización.

(xi) Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.

(xii) Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.

(xiii) Obtener las declaraciones de conformidad de la SIC cuando sea requerido.

(xiv) Redactar y validar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.

(xv) Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos específico para cada uno de ellos.

(xvi) Realizar un entrenamiento general en protección de datos para todos los empleados de la compañía.

(xvii) Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

(xviii) Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores).

(xix) Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.

(xx) Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.



Puede contactar a nuestro OPD (Especialista de Aseguramiento de Tecnologías de la Información TI) a través de los siguientes medios:

- Correo Electrónico: protecciondatos@cerrejon.com
- Dirección: Carrera 15 # 91-46 Piso 7, Bogotá D.C.

#### 4.2 Procedimiento local

##### 4.2.1 Normatividad Aplicable

- Constitución Política de Colombia
- Ley 1581 de 2012
- Decreto 1074 de 2015 Capítulo 25 y Capítulo 26 compilatorios de los decretos:
  1. Decreto 1377 de 2013
  2. Decreto 886 de 2014
- Actos administrativos (Resoluciones, Circulares, otros) expedidos por la Superintendencia de Industria y Comercio.

La descripción del procedimiento local lo encontrará en los siguientes anexos que hacen parte íntegra del presente documento:

- Anexo 1: Procedimiento de Atención a Titulares (Consultas y Reclamos).
- Anexo 2: Procedimiento de Reporte de Incidentes.
- Anexo 3: Procedimiento Declaración de Conformidad sobre las Transferencias Internacionales de Datos Personales.

#### 4.3 Requisitos mínimos

##### 4.3.1 Principios del tratamiento de datos

El artículo 4 de la Ley 1581 de 2012 establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

##### **Principio de Legalidad y Equidad:**

El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios, compilados en el Capítulo 25 y 26 del Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen. Este principio incluye dar cumplimiento a la normativa vigente con relación a cumplir con el tiempo y forma de conservación de los datos.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, es la obligación de garantizar la exista una autorización previa para el uso de los datos personales y que la recolección de los mismos sea justificada.*

##### **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.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, es la obligación de informar qué uso se dará a los datos personales recolectados.*

### **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.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, es establecer un mecanismo que permita al Titular de los datos indicar de manera inequívoca que aprueba su uso con las finalidades o usos informados.*

### **Principio de Veracidad, Calidad o Precisión:**

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. Los datos personales serán adecuados, pertinentes y limitados a lo necesario con relación a los fines para los que se tratan.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, cuando el Titular de los datos solicita la eliminación o modificación de los mismos, es obligatorio actualizar la información en las bases de datos conforme a la petición del Titular.*

### **Principio de Transparencia:**

En el tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del tratamiento o del Encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

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

La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, utilizar métodos o mecanismos de recolección de información deben permitir al Titular conocer el uso que se dará a los datos personales.*

### **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 1581 de 2012 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.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, en caso de compartir o suministrar datos del Titular a Terceros, es obligatorio informar al Titular los fines de esta circulación y contar con su autorización.*

### **Principio de Seguridad:**

La información sujeta a tratamiento por el Responsable del tratamiento o Encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El Responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento 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 el PL-02 Políticas Internas de Seguridad, 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 Ley 1581 de 2012 y en los términos de la misma.

*Un ejemplo para cumplir con el este principio, sin perjuicio de que existan otros casos, establecer acuerdos de confidencialidad con los colaboradores para garantizar la reserva de la información que conocen en cumplimiento de sus funciones.*

#### **4.3.2 Reportar las solicitudes de acceso y las quejas de los interesados**

Para la atención a las consultas y reclamos de los titulares de la información, se establece:

##### **4.3.2.1 Derechos de los Titulares:**

Para la atención a las consultas y reclamos de los titulares de la información, se establece:

- 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;



- Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;
- 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;
- Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución;
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Estos derechos podrán ser ejercidos por las siguientes personas:

- Por el Titular, quién 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 y para otro.

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

#### **4.3.2.2 Derechos de petición que deben ser atendidos por el Responsable:**

##### **Derecho de acceso o consulta**

Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

##### **Derechos de quejas y reclamos**

##### **La Ley distingue cuatro tipos de reclamos:**

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

### **Derecho a solicitar prueba de la autorización otorgada al Responsable del tratamiento**

Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

#### **4.3.2.3 Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones**

El Titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el Responsable del tratamiento o Encargado del tratamiento.

#### **4.3.2.3 Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones**

El Titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el Responsable del tratamiento o Encargado del tratamiento.

#### **4.3.2.4 Atención a las peticiones presentadas por los titulares de datos**

Para la atención a las consultas y reclamos en materia de protección de datos personales, se ha designado un Oficial de Protección de Datos. Los Titulares de los datos podrán remitir sus peticiones o consultas a través de los siguientes canales:

Correo: [protecciondatos@cerrejon.com](mailto:protecciondatos@cerrejon.com)  
Dirección: Carrera 15 # 91-46 Piso 7, Bogotá D.C.

Electrónico:

#### **4.3.2.4.1 Procedimientos para el ejercicio de los derechos del titular**

### **Derecho de acceso o consulta**

Se garantizará al Titular la consulta de forma gratuita de sus datos personales en los siguientes casos (Artículo 2.2.2.25.4.2. sección 4 capítulo 25 del Decreto 1074 de 2015):

- Al menos una vez cada mes calendario.
- 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, podrá realizarse un cobro al Titular por concepto de gastos de envío, reproducción y/o certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, se demostrará a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito enviado a la dirección de domicilio, mediante correo electrónico: [protecciondatos@cerrejon.com](mailto:protecciondatos@cerrejon.com), indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de los canales habilitados para atención disponibles en <https://www.cerrejon.com/>. 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 para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro mecanismo que permita la respuesta de fondo y oportuna de la petición presentada.

Una vez recibida la solicitud, se 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 Ley 1581 de 2012.

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

### ***Derechos de quejas y reclamos***

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito enviado a la dirección de domicilio, mediante correo electrónico a [protecciondatos@cerrejon.com](mailto:protecciondatos@cerrejon.com), indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a la Carrera 15 # 91-46 Piso 7, 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 inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

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

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

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

#### **4.3.2.5 Facultados para recibir información mediante petición**

Las siguientes personas se encuentran habilitadas o facultadas para solicitar y recibir información sobre los datos personales, de acuerdo con el artículo 13 de la Ley 1581 de 2012:

- A los Titulares, sus causahabientes o sus representantes legales;
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
- A los terceros autorizados por el Titular o por la ley.

#### **4.3.2.6 Verificación de la facultad para solicitar o recibir información**

Para la gestión de la solicitud de consulta o reclamo, el solicitante deberá aportar los siguientes documentos para acreditar su titularidad o la facultad para recibir la información requerida, de acuerdo con los siguientes casos:

- Titular: Copia del documento de identidad.
- Causahabiente: Documento de identidad, registro civil de defunción del Titular, documento que acredite la calidad en que actúa y copia del documento de identidad del Titular.
- Representante legal y/o apoderado: Documento de identidad válido, documento que acredite la calidad en la que actúa (Poder) y copia del documento de identidad del Titular.

#### **4.3.1 Notificación de infracciones**

Para la gestión de los incidentes de seguridad se aplicará el procedimiento de reporte de incidentes señalado en el Anexo 2 de este documento, asimismo, el Oficial de Protección de Datos reportará cualquier violación de los datos personales al CDPO(cpdo@glencore.com). Es necesaria la comunicación y/o notificación, entre los colaboradores, oficial de protección de datos personales, encargados de tratamiento, Titulares de los datos, ente de vigilancia y control, así como, los entes judiciales; para la gestión y respuesta ante incidentes de seguridad desde el momento en que son detectados con el fin de ser evaluados y gestionar las vulnerabilidades identificadas, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros.

Todos los usuarios y responsables de administrar bases de datos, así como, cualquier persona que tenga relación con la recolección, el almacenamiento, uso, circulación o cualquier tratamiento o consulta de las bases de datos, deberá conocer el procedimiento para actuar en caso de incidentes de seguridad para garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que se encuentran bajo su responsabilidad.



Algunos ejemplos de incidencias de seguridad son: caída de sistemas de seguridad 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, entre otros.

En caso de presentarse un incidente de seguridad, el equipo o Comité de respuesta tendrá en cuenta los siguientes criterios:

#### *Estrategia para identificar, contener y mitigar los incidentes de seguridad*

- Aplicar las medidas para contener y revertir el impacto que puede tener el incidente de seguridad.
- Evaluar adecuadamente el incidente de seguridad y su impacto en los Titulares de la información.
- Verificar los requisitos legales o contractuales con proveedores de servicios asociados al incidente de seguridad.
- Determinar el nivel de riesgo para los Titulares de la Información y notificar la ocurrencia.
- Verificar los roles y responsabilidades del personal responsable de la operación de la información o datos afectados.
- Identificar la naturaleza de la vulneración y, en la medida de lo posible, también las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de Datos Personales afectados.
- Describir las consecuencias potenciales de la vulneración.

- Identificar las medidas adoptadas o propuestas para hacer frente a la violación y sus posibles efectos adversos.

#### *Línea de tiempo para la gestión del incidente de seguridad*

Aplicar el procedimiento para atender los incidentes de seguridad, de acuerdo con parámetros que permitan una adecuada gestión y mitigación de impacto. Verificar de acuerdo con la evaluación del incidente de seguridad, la necesidad de notificar a entidades, tales como: la Fiscalía General de la Nación, la Procuraduría General de la Nación, Guala, Policía Nacional, Superintendencia Financiera de Colombia, Centro Cibernético Policial, colCERT; CSIRT Policial, CSIRT Asobancaria, CSIRT Sectorial, entre otras.

#### *Progreso del reporte del incidente de seguridad*

Realizar monitoreo en la gestión estableciendo plazos, evaluar su progreso e identificar los posibles puntos conflictivos que se puedan generar en el manejo del incidente de seguridad.

#### *Evaluación de respuesta ante el incidente de seguridad*

Una vez se haya gestionado y controlado el incidente de seguridad, el equipo de respuesta deberá revisar las acciones ejecutadas para contenerlo y realizar los ajustes pertinentes para implementar plan de mejora.

### *Acciones implementadas y planes de mejora*

Establecer las acciones necesarias para mitigar el impacto del incidente de seguridad y evitar que vuelva a ocurrir, mediante acciones correctivas y preventivas, así como, planes de mejora que debe adoptar el equipo de respuesta.

### *Documentación y reporte ante el ente de vigilancia y control*

Documentar en un registro interno la información relacionada con el incidente de seguridad, así como, elaborar informe con soportes de las acciones adelantadas que deberá ser radicado ante Superintendencia de Industria y Comercio, a través del RNBD dentro de los 15 días hábiles siguientes de haber sido detectado del incidente.

Sin perjuicio de lo anterior, el OPD deberá informar al Corporate IT Security sobre el incidente de seguridad en un plazo de 72 horas contadas a partir del momento en que se tiene conocimiento del hecho que le dio origen. También informara al Oficial de Cumplimiento Regional en el mismo plazo.

### *Revisión*

Evaluación de las causas que ocasionaron el incidente de seguridad y el éxito de su gestión para valorar la efectividad de los controles y acciones implementadas. Documentar las lecciones aprendidas para tenerlas presentes en futuras ocasiones.

### *Ejemplos de Violaciones de Datos*

A continuación se presentan dos ejemplos de violaciones de datos:

- Unos piratas informáticos accedieron al sistema de Recursos Humanos de Cerrejón y descargaron datos relativos a los empleados.

- Un procesador de datos tuvo una pérdida de datos y se hicieron públicos Datos Personales.

#### **4.3.1 Divulgación a terceros**

##### **4.3.4.1 Transferencia y Transmisión internacional de datos personales**

Se realizará transferencia de datos personales a países que proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la 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 en los cuales sea necesaria la transferencia de los datos y el país de destino no se encuentre en el listado de países considerados como puertos seguros señalados por la Superintendencia de Industria y Comercio, se deberá gestionar ante el mismo ente una declaración de conformidad relativa a la aprobación para la transferencia internacional de datos personales.

Las transmisiones internacionales de datos personales que se efectúen 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. Este contrato de transmisión de datos personales deberá suscribirse entre el Responsable y el Encargado para definir el alcance del tratamiento de datos personales bajo su control y responsabilidad, así como, las actividades que el encargado realizará por cuenta del Responsable y las obligaciones en calidad de Encargado para con el titular. Adicionalmente, el Encargado deberá cumplir con las siguientes obligaciones y aplicar las normas vigentes en Colombia en materia de protección de datos.

1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
3. Guardar confidencialidad respecto del tratamiento de los datos personales.

Las anteriores condiciones fijadas para las transmisiones de datos internacionales, también le serán aplicables a las transmisiones de datos nacionales.

#### **4.3 Otras consideraciones**

##### **4.3.1 Autorización uso de datos personales.**

De acuerdo con el artículo 9 de la Ley 1581 de 2012, para el tratamiento de datos personales se requiere la autorización del Titular, salvo en los casos expresamente señalados en las normas que reglamentan la protección de los datos personales. Con antelación y/o al momento de efectuar la recolección del dato personal, se 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 descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015.

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

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

#### **4.4 Otras consideraciones**

##### **4.4.1 Autorización uso de datos personales**

#### 4.4 Otras consideraciones

##### 4.4.1 Autorización uso de datos personales.

De acuerdo con el artículo 9 de la Ley 1581 de 2012, para el tratamiento de datos personales se requiere la autorización del Titular, salvo en los casos expresamente señalados en las normas que reglamentan la protección de los datos personales. Con antelación y/o al momento de efectuar la recolección del dato personal, se 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 descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015.

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

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

##### 4.4.1.1 Solicitud de autorización al titular del dato personal

La autorización se gestionará con antelación y/o al momento de efectuar la recolección del dato personal, informando de manera clara y expresa al Titular, lo siguiente:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
- El carácter facultativo de la respuesta a las preguntas que le sean realizadas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- Los derechos que le asisten como Titular;
- La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.
- Los canales de atención dispuestos para atender las peticiones del titular.

La autorización para el uso y/o tratamiento de los datos será gestionada a través de mecanismos que garanticen su consulta posterior y la manifestación de la voluntad del Titular a través de los siguientes medios:

- Por escrito.
- De forma oral.
- Mediante canales automatizados.
- Mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

El mecanismo elegido debe permitir guardar un soporte de la autorización dada por el titular en el cual se pueda evidenciar inequívocamente que aprobó el tratamiento de sus datos.



#### **4.4.2 Tratamiento y finalidades de las bases de datos**

El tratamiento de datos personales relativos a personas naturales se realiza con finalidades legítimas, cumpliendo con la Constitución y la Ley. El tratamiento al cual serán sometidos los datos personales incluye recolección, almacenamiento, uso, circulación o supresión. El tratamiento de los datos estará sujeto a las finalidades autorizadas por el Titular, a las obligaciones contractuales entre las partes, así como, a los casos en los cuales existan obligaciones legales que deba cumplir.

La información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento, podrán ser consultadas en el Anexo OD-TISE-101 Organización de las Bases de Datos.

##### **4.4.2.1 Tratamiento de datos de menores**

De acuerdo con el artículo 7° de la Ley 1581 de 2012, el Tratamiento de datos personales de niños, niñas y adolescentes se realizará en el marco de los criterios señalados en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013), con observancia de los siguientes parámetros y requisitos:

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

Cumplidos los anteriores requisitos, se 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. En calidad de Responsable y/o Encargado velará por el uso adecuado de los datos de niños, niñas y adolescentes aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias. Asimismo, identificará los datos sensibles recolectados o almacenados con el fin de incrementar la seguridad y tratamiento de la información.

##### **4.4.2.2 Tratamiento de datos en los sistemas de videovigilancia**

Para el tratamiento de datos informará a las personas sobre la existencia de mecanismos de videovigilancia, mediante la fijación de anuncios visibles al alcance de todos los titulares e instalados en las zonas de videovigilancia, principalmente en las zonas de ingreso a los lugares que están siendo vigilados y monitoreados. En estos avisos informará quién es el Responsable del Tratamiento, las finalidades del tratamiento, los derechos del Titular, los canales habilitados para ejercer los derechos del Titular, así como, dónde se encuentra publicada la Política de Tratamiento de la Información.

De otra parte, conservará las imágenes solo por el tiempo estrictamente necesario para cumplir con la finalidad del e inscribirá la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos, salvo que el Tratamiento consista solo en la reproducción o emisión de imágenes en tiempo real.

El acceso y divulgación de las imágenes será restringido a personas autorizadas por el Titular y/o por solicitud de una autoridad en ejercicio de sus funciones. En consecuencia, la divulgación de la información que se recolecta será controlada y consistente con la finalidad establecida por el Responsable del Tratamiento.

#### **4.4.2.3 Tratamiento de datos biométricos**

Los datos biométricos almacenados en las bases de datos son 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 ejecuta 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.

#### **4.4.3 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 solicita acceso y/o entrega de datos de carácter personal contenidos en cualquiera de las 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. Para la entrega se suscribirá un acta indicando los datos de la entidad solicitante y las características 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.

#### **4.5 Registro Nacional de Bases de Datos – RNBD**

Las bases de datos identificadas en CERREJÓN y el registro de actividades de tratamiento serán inscritos y actualizados periódicamente en el Registro Nacional de Bases de Datos – RNBD, en el término establecido legalmente. Para inscribir una base de datos nueva en el Registro Nacional de Bases de Datos se acogen los plazos y fechas indicadas por la Superintendencia de Industria y Comercio y las instrucciones que para el efecto imparta esa entidad. Una vez creada una base de datos será inscrita dentro de los dos (2) meses siguientes, contados a partir de su creación. Las actividades del tratamiento y/o finalidades podrán ser consultadas en el Anexo OD-TISE-101 Organización de las Bases de Datos.



#### 4.6 Vigencia de la base de datos

Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.

#### 4.7 Medidas de seguridad

CERREJÓN con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley 1581 de 2012, 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. Las políticas de seguridad de la información serán aplicadas de acuerdo con el documento interno.

A continuación, se exponen algunas medidas de seguridad implantadas y desarrolladas en las Políticas Internas de Seguridad (Tablas I, II, III y IV).

**TABLA I: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) y bases de datos (automatizadas, no automatizadas)**

#### Gestión de documentos y soportes

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

#### Control de acceso

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

<b>Incidencias</b>	<ol style="list-style-type: none"> <li>1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.</li> <li>2. Procedimiento de notificación y gestión de incidencias.</li> </ol>
<b>Personal</b>	<ol style="list-style-type: none"> <li>1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos.</li> <li>2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.</li> <li>3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.</li> </ol>
<b>Manual Interno de Seguridad</b>	<ol style="list-style-type: none"> <li>1. Elaboración e implementación del Manual de obligado cumplimiento para el personal.</li> <li>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, identificación de los encargados del tratamiento.</li> </ol>

<b>TABLA II: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) según el tipo de bases de datos</b>	
<b>Bases de datos no automatizadas</b>	
<b>Archivo</b>	<ol style="list-style-type: none"> <li>1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta, que permitan el ejercicio de los derechos de los Titulares.</li> </ol>
<b>Almacenamiento de documentos</b>	<ol style="list-style-type: none"> <li>1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.</li> </ol>
<b>Custodia de documentos</b>	<ol style="list-style-type: none"> <li>1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.</li> </ol>



<b>Bases de datos automatizadas</b>	
<b>Identificación y autenticación</b>	<ol style="list-style-type: none"> <li>1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.</li> <li>2. Mecanismos de identificación y autenticación; Contraseñas: asignación y caducidad.</li> </ol>
<b>Telecomunicaciones</b>	<ol style="list-style-type: none"> <li>1. Acceso a datos mediante redes seguras.</li> </ol>

<b>Responsable de seguridad</b>	<ol style="list-style-type: none"> <li>1. Designación de uno o varios Administradores de las bases de datos.</li> <li>2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad.</li> <li>3. Prohibición de delegación de la responsabilidad del Responsable del tratamiento en los Administradores de las bases de datos.</li> </ol>
<b>Manual interno de seguridad</b>	Controles periódicos de cumplimiento.

**TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos**

<b>Bases de datos no automatizadas</b>	
<b>Auditoría</b>	<ol style="list-style-type: none"> <li>1. Auditoría ordinaria (interna o externa) cada dos meses.</li> <li>2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información.</li> <li>3. Informe de detección de deficiencias y propuesta de correcciones.</li> <li>4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.</li> </ol>

<b>Bases de datos automatizadas</b>	
<b>Gestión de documentos y soportes</b>	<ol style="list-style-type: none"> <li>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.</li> </ol>
<b>Control de acceso</b>	<ol style="list-style-type: none"> <li>1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.</li> </ol>

<b>Identificación y autenticación</b>	<ol style="list-style-type: none"> <li>1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.</li> <li>2. Mecanismos de cifrado de datos para la transmisión.</li> </ol>
<b>Incidencias</b>	<ol style="list-style-type: none"> <li>1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.</li> <li>2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.</li> </ol>

**TABLA IV: Medidas de seguridad para datos sensibles según el tipo de bases de datos**

<b>Bases de datos no automatizadas</b>	
<b>Control de acceso</b>	<ol style="list-style-type: none"> <li>1. Acceso solo para personal autorizado.</li> <li>2. Mecanismo de identificación de acceso.</li> <li>3. Registro de accesos de usuarios no autorizados.</li> <li>4. Destrucción que impida el acceso o recuperación de los datos.</li> </ol>

<b>Almacenamiento de documentos</b>	<ol style="list-style-type: none"> <li>1. Archiveros, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.</li> <li>2. Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.</li> </ol>
-------------------------------------	--

**Bases de datos automatizadas**

<b>Control de acceso</b>	<ol style="list-style-type: none"> <li>1. Sistema de etiquetado confidencial.</li> </ol>
<b>Identificación y autenticación</b>	<ol style="list-style-type: none"> <li>1. Mecanismos de cifrado de datos para la transmisión y almacenamiento.</li> </ol>
<b>Almacenamiento de documentos</b>	<ol style="list-style-type: none"> <li>1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede</li> <li>2. Control del registro de accesos por el responsable de seguridad. Informe mensual.</li> </ol>
<b>Telecomunicaciones</b>	<ol style="list-style-type: none"> <li>1. Acceso y transmisión de datos mediante redes electrónicas seguras.</li> <li>2. Transmisión de datos mediante redes cifradas (VPN).</li> </ol>



#### 4.8 Cookies o web bugs

CERREJÓN puede recolectar información personal de sus Usuarios mientras utilizan la Página Web, la aplicación o las páginas vinculadas (Landing Page). Los Usuarios pueden optar por almacenar esta información personal en la página web, la aplicación o en el portal vinculado (Landing Page), con el fin de facilitar las transacciones y los servicios a prestar por parte de CERREJÓN y/o de sus portales vinculados (Landing Page). Por lo que, CERREJÓN utiliza diferentes tecnologías de seguimiento y recopilación de datos como, Cookies propias y de terceros, esta es la herramienta de análisis que ayuda a los propietarios de sitios web y de aplicaciones a entender cómo interactúan los visitantes con sus propiedades. Esta herramienta puede utilizar un conjunto de cookies para recopilar información y ofrecer estadísticas de uso de los sitios web sin identificar personalmente a los visitantes de Google. Al acceder a nuestro al sitio web, el usuario podrá configurar, aceptar y/o rechazar las cookies que se encuentran activas.

Las cookies se asocian únicamente a un usuario anónimo y su ordenador y no proporcionan referencias que permitan deducir datos personales del usuario, esta información nos permite conocer sus patrones de navegación y ofrecerle servicios personalizados. CERREJÓN podrá utilizar estas tecnologías para recordar sus preferencias para el uso de la página web, la aplicación y las páginas vinculadas (Landing Page), ofrecer funciones de redes y analizar tráfico, enlace a redes sociales, facilitar transacciones, para analizar el uso de la página web, la aplicación o de las páginas vinculadas y sus servicios.

Nuestro sitio incluye otras funcionalidades proporcionadas por terceros. Si al acceder a nuestro sitio web, el Usuario no desea que su información personal sea recogida a través de Cookies, puede cambiar las preferencias en su propio navegador web. No obstante, es importante señalar que, si el Usuario web no acepta Cookies, algunas de las funcionalidades de la página web, la aplicación y/o las página vinculadas (Landing Page) podrían no estar disponibles o no funcionar correctamente. Como Usuario puede permitir, bloquear o eliminar las cookies instaladas en su dispositivo mediante la configuración de las opciones del navegador instalado en su dispositivo, así:

Chrome: Configuración -> Mostrar opciones avanzadas -> Privacidad -> Configuración de contenido.

Microsoft Edge (en el Menú Herramientas): Opciones de Internet > Privacidad > Avanzada

Firefox: Herramientas -> Opciones-> Privacidad -> Historial -> Configuración Personalizada.

Safari: iPad y iPhone: Preferencias >Privacidad-> Historial -> Configuración Personalizada.

Opera: Configuración > Opciones > Avanzado > Cookies

Internet Explorer: Herramientas -> Opciones de Internet -> Privacidad -> Configuración.

#### 4.9 Administración de riesgos asociados al tratamiento de los datos

CERREJÓN ha identificado los riesgos relacionados con el tratamiento de los datos personales y ha establecido controles con el fin de mitigar sus causas, mediante la implementación de políticas internas de seguridad, una metodología y matriz de riesgos. Para la gestión de riesgos ha establecido herramientas, indicadores y recursos necesarios para su administración, acordes con la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización cuando se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

En la gestión de riesgos se han identificado distintas fuentes asociadas al uso de tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas. 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 probabilidad de ocurrencia y el impacto 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 relacionado con el comportamiento humano.

En la gestión de riesgo se han implementado los controles y medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

#### 4.10 Director de protección de datos

CERREJÓN, una empresa Glencore, se permite informar los datos de contacto del Director de protección de datos del Grupo Glencore:

- Director de protección de datos (CDPO) Grupo Glencore
- Baarermattstrasse 3
- 6340 Baar Suiza
- Tel: +41 41 709 20 00
- Email: [cdpo@glencore.com](mailto:cdpo@glencore.com)
- Intranet: <https://group.glencore.net/cdpo>

#### 5. Recursos adicionales

Política de gobernanza de la información  
Procedimiento de protección de datos – Anexos

Anexo 1. PROCEDIMIENTO DE ATENCIÓN A TITULARES

Anexo 2. PROCEDIMIENTO DE REPORTE DE INCIDENTES

Anexo 3. DECLARACIÓN DE CONFORMIDAD