Ladrillera Los Cerros | Ladrillera San Miguel

# Política de Protección de Datos Personales


Km 34 Via Montería
Planeta Rica – Córdoba – Colombia

www.ladrilleraloscerros.com
www.ladrillerasanmiguel.com
314 550 3333 -321 665 7848

# CONTENIDO

# POLITICA DE PROTECCIÓN DE DATOS PERSONALES

## 1. GENERALIDADES

### 1.1. INTRODUCCIÓN

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S en concordancia con las políticas establecidas de dar cumplimiento a los requisitos legales aplicables adopta el presente manual teniendo en cuenta que la ley 1581 de 2012, señala los principios y obligaciones aplicables a todos aquellos que realicen tratamiento de datos personales para garantizar la protección del derecho fundamental de habeas data.*

*Por tanto, la finalidad del presente manual es dar cumplimiento a dicha ley la cual establece en el artículo 7, numeral 4 lo siguiente: "Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares".*

### 1.2. OBJETIVO

*El presente documento tiene por objetivo establecer los principios, términos y condiciones para el tratamiento de datos personales, actividad que incluye la recolección, almacenamiento, procesamiento, actualización, uso, circulación, transmisión, transferencia y supresión de la información que se suministra a LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, en el desarrollo de su objeto social.*

*Adicionalmente, la Política de Tratamiento de Datos Personales establece los derechos de los Titulares de la Información y los procedimientos para hacerlos efectivos.*



## IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

*LADRILLERA LOS CERROS DEL 34 SA NIT 900022189-2*
*LADRILLERA SAN MIGUEL DE LOS CERROS SAS NIT 900590610-8*
*DIRECCIÓN: KM 34 VIA MONTERÍA – PLANETA RICA*

*CORREO: protecciondatos@grupocsm.co*
*TELÉFONO: 3145503333 - 3216657848*

### *1.3. ALCANCE*

*El presente manual es aplicable a todos los datos personales de personas naturales o jurídicas registradas en las bases de datos de LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, relativas a empleados, empleados pote|nciales, clientes, clientes potenciales, proveedores y proveedores potenciales, las cuales sean susceptibles de tratamiento.*

*Todos los empleados de LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S deben cumplir integralmente con la normatividad que regula la protección de datos y la presente política.*

*Igualmente, clientes, contratistas y proveedores de LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S estarán obligados a cumplir con la normativa que regula la protección de datos personales y la presente política en la medida que tengan alguna responsabilidad respecto de su tratamiento.*

*Comprende desde la recolección, almacenamiento, procesamiento, actualización, uso, circulación, transmisión, transferencia y supresión de los datos e información que se suministra a las empresas.*

### *1.4. AMBITO DE APLICACIÓN*

*La presente política, será aplicable a los datos personales que se generen en virtud del vínculo laboral existente entre la compañía y sus partes interesadas y que se encuentren registrados en las bases de datos de hojas de vida del personal, nómina del personal, contratos clientes y contratos proveedores y contratistas.*

*Igualmente será objeto de la presente política, los datos sensibles contenidos en las historias clínicas aportadas por el trabajador para realizar el trámite de transcripción y/o recobro de las incapacidades; y de la información sensible denominada preexistencia contenida en los formularios de solicitud de inclusión en la póliza colectiva.*

*1.5. MARCO LEGAL*

*De conformidad con el artículo 15 de la Constitución Política las personas tienen el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos tanto de entidades públicas como privadas.*

*Este derecho fundamental fue desarrollado por la jurisprudencia de la Corte Constitucional y por la ley. En el 2012 se expidió la ley 1581, ley especial y sectorial que regula las disposiciones generales para la protección de datos personales aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.*

*1.6. MARCO TEÓRICO*

*1.6.1. TÉRMINOS Y DEFINICIONES:*

*Los siguientes términos y definiciones corresponden a las definidas en el marco de la ley 1581 de 2012*

- *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.*
- *DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.*
- *DATOS SENSIBLES: Se entiende por datos sensibles aquellos que afectan la intimidad de Titular o cuyo uso indebido puede generar su discriminación , tales como aquellos 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 promuevan 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.*

- *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.*

*1.6.2. PRINCIPIOS*

*Los principios presentados a continuación, componen los fundamentos generales mediante los cuales se dará aplicación a lo establecido en el presente manual referente a los datos personales de los titulares de la información:*

- *PRINCIPIO DE FINALIDAD: El tratamiento de datos personales por parte de LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S debe obedecer a una finalidad legítima, la cual debe ser informada al Titular.*

- *PRINCIPIO DE LIBERTAD: El tratamiento de datos personales sólo podrá ejercerse mediando con el consentimiento, previo, expreso e informado del Titular de la información. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.*

- *PRINCIPIO DE VERACIDAD O CALIDAD: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.*

- *PRINCIPIO DE TRANSPARENCIA: En el tratamiento debe garantizarse el derecho del Titular a obtener de LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.*

- *PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA: Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.*

- *PRINCIPIO DE SEGURIDAD: La información sujeta a tratamiento por LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, 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.*

- *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.*

## *2. AUTORIZACIÓN Y CONSENTIMIENTO DEL TITULAR*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, recolecta los datos personales de los Titulares de la Información, requeridos para el desarrollo de su objeto social y les da el tratamiento necesario para cumplir los compromisos contractuales con trabajadores, sus clientes y proveedores, con las finalidades que se señalan en la presente Política de Tratamiento de Datos Personales.*

*Para la recolección de los datos personales, LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, solicitarán la autorización de los Titulares de la Información de conformidad con el modelo de autorización, que constituye un anexo del presente documento. Las empresas, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:*

- *El tratamiento al cual serán sometidos sus datos personales y la finalidad de mismo.*
- *El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas correspondan a 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.*

*2.1. MANIFESTACIÓN DE LA AUTORIZACIÓN*

*La autorización para el tratamiento debe ser otorgada por:*

- *El titular de la información.*
- *El apoderado del titular.*

*2.2. MEDIOS PARA OTORGAR LA AUTORIZACIÓN*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S obtendrá la autorización al acceso a la información mediante los siguientes medios:*

- *Documento físico.*
- *Correo electrónico.*

- *Sitio web.*
- *Mensaje de texto.*
- *Formularios de registro*
- *Cualquier otro formato que permita la autorización de un consentimiento.*

*2.3. PRUEBA DE LA AUTORIZACIÓN*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S conservarán la prueba de autorización otorgada por el titular de los datos personales.*

*2.4. REVOCATORIA DE LA AUTORIZACIÓN*

*El titular de los datos personales puede en cualquier momento, revocar la autorización otorgada a LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S para el tratamiento de sus datos personales. Cuando se reciba dicha solicitud las empresas deberán cesar cualquier actividad de tratamiento de datos.*

*2.5. FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES*

*Los datos personales de los Titulares de la Información serán recolectados, almacenados, procesados, usados, circulados, transferidos, transmitidos, compartidos y/o suprimidos, de conformidad con el vínculo contractual que se haya establecido, en las bases de datos según sean de clientes, proveedores y empleados. Lo anterior de plasmado en el Registro Nacional de Bases de Datos.*

*En general las empresas utilizan la información suministrada para el desarrollo de su objeto social. En caso de que se vaya a realizar un uso diferente al señalado anteriormente, LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, solicitarán de forma previa a los Titulares de la Información la autorización correspondiente.*

*2.6. TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES*

*El tratamiento de la información incluye la recolección, almacenamiento, procesamiento, actualización, uso, circulación, transferencia y supresión de los datos personales que se suministren a LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, de conformidad con lo previsto en la Ley 1581 de 2012 y las demás normas que la modifiquen, sustituyan, desarrollen y/o complementen.*

*Para el tratamiento de la información LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, podrán:*

- *Administrar la información recolectada en una o varias bases de datos según forma y organización que estime conveniente,*
- *Verificar, corroborar, comprobar, validar, investigar o comparar la información suministrada por los Titulares de Información, con cualquier información de que disponga legítimamente*

*Información recolectada que serán usadas para:*

- *Desarrollo de las actividades de Gestión Humana*
- *Aplicación del proceso de Proveedores*
- *Aplicación del proceso de Gestión Comercial*
- *Aplicación del proceso de Facturación*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, tiene un compromiso con el adecuado manejo de la información que le suministran sus Clientes, Proveedores, Empleados y demás personas que tienen relación ella. Para el efecto, deberá velar por la conservación de la confidencialidad de aquella información que tiene carácter reservado.*

*De forma previa al tratamiento de los datos personales, solicitará a los Titulares de la Información la autorización correspondiente de conformidad con lo previsto en la presente Política de Tratamiento de Datos Personales, utilizando para el efecto el modelo anexo a ella.*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, está obligada a suministrar datos personales de los Titulares de la Información a entidades judiciales o administrativas y a entidades de control, previo requerimiento por parte de ellas. Así mismo, los datos personales de los titulares podrán ser conocidos debido a procesos de auditoría externa por parte de los revisores fiscales, quienes tienen la obligación legal de mantener su confidencialidad.*

*La información recolectada por LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, se conserva por el tiempo requerido por la normatividad aplicable.*



*2.6.1. DATOS SENSIBLES:*

*Los datos sensibles serán protegidos de la siguiente manera:*

- *Ninguna persona puede estar obligada a proporcionar datos sensibles, tales como: origen racial o étnico, opinión política, convicción religiosa, información referente a la vida sexual o cualquier otro dato que pueda producir algún dato discriminatorio al titular de los datos.*
- *Los datos sensibles solo pueden ser tratados cuando sean de interés general, autorizados por la ley.*
- *Queda prohibida la creación de bases de datos que almacenen información, directa o indirecta que revelen datos sensibles, salvo que la ley lo disponga.*
- *Los datos relativos a antecedentes penales, sólo pueden ser objeto de tratamiento por parte de las autoridades.*

- *Las historias clínicas que posea la entidad serán devueltas al titular de la información contenida en ellas, una vez finalice el trámite de transcripción y recobro frente a la E.P.S.*
- *Sin perjuicio de las excepciones previstas en la ley, en el tratamiento de datos sensibles se requiere la autorización expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.*

*2.6.2. DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, recolecta y da tratamiento a datos personales de niños, niñas y adolescentes en concordancia con el artículo 12 del decreto 1377 de 2013, respetando el interés superior, sus derechos prevalentes y fundamentales.*

*2.7. SEGURIDAD DE LA INFORMACIÓN*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, cuentan con procedimientos y herramientas tecnológicas que permiten una administración segura de la información recolectada y el funcionamiento de los controles para verificar el cumplimiento de la presente Política de Tratamiento de Datos Personales. Igualmente, LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, cuentan con planes de contingencia orientados a mantener la continuidad de la operación y que le permiten administrar situaciones que puedan poner en riesgo la información recolectada.*

*Las bases de datos que administran LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, están almacenadas y protegidas en un servidor dentro las instalaciones de la compañía, aislado de accesos no autorizados. La información puede ser consultada únicamente por las personas que tienen claves de seguridad asignadas, las cuales se entregan exclusivamente a los empleados de las áreas responsables de cada una de las bases de datos.*

*No obstante, LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, no será responsable por ataques informáticos y, en general, por cualquier acción que tenga como objetivo infringir las medidas de seguridad establecidas para la protección de los datos personales, ya sea por la*

*empresa o por los terceros con los que ella tenga la relación contractual respectiva.*

*2.8. AVISO DE PRIVACIDAD*

*El aviso de privacidad es el documento físico o electrónico que se pone a disposición del titular para informarle acerca del tratamiento de sus datos personales, el aviso de privacidad de LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, contendrá la siguiente información.*

- *Identidad y domicilio del responsable del tratamiento*
- *Finalidad y tipo de tratamiento*
- *Derechos del titular*

*3. PROCEDIMIENTO PARA LA ATENCIÓN DE CONSULTA, RECLAMOS, RECTIFICACIÓN, ACTUALIZACIÓN Y SUSPENSIÓN DE DATOS*

*3.1. DERECHO DE ACCESO O CONSULTA.*

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

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

*Las consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de radicación. Cuando no fuere posible atender una 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.*

*Para consultas cuya periodicidad sea mayor a una por cada mes calendario, LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán*

*ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar 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 dirigido a nuestra empresa, enviado mediante correo electrónico, indicando en el asunto "ejercicio del derecho de acceso o consulta" 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:*

- *Visualización en pantalla.*
- *Por escrito, con copia o fotocopia remitida por correo certificado o no.*
- *Correo u otros medios electrónicos.*
- *Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por las empresas.*

*3.2. DERECHOS DE QUEJAS Y RECLAMOS.*

*El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a las empresas enviando mediante correo electrónico indicando en el asunto "ejercicio del derecho queja o reclamo", 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.*

*Las quejas y reclamos serán atendidas en término máximo de 15 días hábiles contados a partir de la fecha de radicaciónn. Cuando no fuere posible atender el reclamo dentro de dicho término se le informará al interesado los motivos de la demora y la fecha en la que será atendido el reclamo 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.*

*3.3. ACTUALIZACIÓN Y SUSPENSIÒN DE DATOS PERSONALES.*

- *Los titulares que consideren que la información obtenida en las bases de datos, se deba corregir, actualizar, o eliminar deberán enviar un correo electrónico a LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S identificando los datos acompañados de los documentos, soportes necesarios.*

- *El titular podrá solicitar que sean removidos sus datos cuando considere que los mismos no están siendo tratados mediante los principios, deberes y obligaciones previstos en la normatividad vigente o cuando hayan dejado de ser necesarios.*

*3.4. MECANISMOS PARA LA ATENCIÓN DE CONSULTA, RECLAMOS, RECTIFICACIÓN, ACTUALIZACIÓN Y SUSPENSIÓN DE DATOS*

*Se podrán enviar las Peticiones Quejas, y Reclamos al correo electrónico protecciondatos@grupocsm.co o radicarla de forma física en la siguiente dirección KM 34 vía Montería – Planeta Rica.*

*4. REGISTRO NACIONAL DE BASES DE DATOS*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, procederá a realizar el registro nacional de bases de datos, de acuerdo con la normatividad vigente en el sitio:*

https://www.sic.gov.co/registro-nacional-de-bases-de-datos#:~:text=El%20Registro%20Nacional%20de%20Bases,libre%20consulta%20para%20los%20ciudadanos.

*4.1. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, en el desarrollo de sus actividades, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.*

*De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información la empresa realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión, entrega de los datos a terceras entidades a título de encargados o de responsables; esto de acuerdo con el acuerdo al que entre las partes se llegue. Este tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información de nuestra empresa, en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Así mismo y en ejecución del objeto social de nuestras empresas, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:*

| *Nombre* | *Finalidad* |
|---|---|
| *Base de Datos Clientes* | *Comprende información relacionada con los datos personales y sensibles de los clientes: Nombres completos, N° de Cedula, número de teléfono, dirección, fecha y lugar de nacimiento, datos biométricos, etc. También incluye la entrega de información sensible tales como: RUT, cámara de Comercio, información financiera del cliente, entre otros.* |

| | |
|---|---|
| *Base de Datos: Proveedores* | *Comprende información relacionada con los datos personales de los proveedores de productos y servicios tales como: Nombre de la empresa, Representante Legal, Nit o número de Cédula, Dirección, Teléfono. También incluye la entrega de información sensible tales como: RUT, cámara de Comercio, Fichas técnicas de producto.* |
| *Base de Datos: Nómina* | *Comprende información relacionada con los datos personales y sensibles de los trabajadores, personal en misión, contratistas tales como: Nombres completos, N° de Cedula, teléfono, dirección, fecha y lugar de nacimiento, composición familiar, datos biométricos, etc. También incluye la entrega de información sensible tales como: Hoja de vida del trabajador, pruebas de selección, certificados médicos ocupacionales, etc.* |

*4.2. RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE LOS DATOS PERSONALES*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, será la responsable del tratamiento de los datos personales.*

*La Dirección Comercial y Administrativa será la responsable del tratamiento de los datos personales, por cuenta de LADRILLERA LOS CERROS y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S*

*5. MEDIDAS DE SEGURIDAD*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley Estatutaria de Protección de Datos, 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, la empresa mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.*

*A continuación, se exponen las medidas de seguridad implantadas por la empresa, que están recogida y desarrolladas en este documento en las tablas relacionadas a continuación:*

## *5.1. MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICOS, SEMIPRIVADOS, PRIVADOS, SENSIBLES) Y BASES DE DATOS (AUTOMATIZADAS, NO AUTOMATIZADAS)*

| | |
|---|---|
| *Auditoria* | ❖ *Auditoría ordinaria (interna o externa) cada año.*<br>❖ *Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.*<br>❖ *Informe de detección de deficiencias y propuesta de correcciones.*<br>❖ *Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.*<br>❖ *Conservación del Informe a disposición de la autoridad.* |
| *Gestión de documentos y soportes* | ❖ *Medidas tales como: destructora de papel que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.*<br>❖ *Acceso restringido al lugar donde se almacenan los datos.*<br>❖ *Sistema de etiquetado o identificación del tipo de información.*<br>❖ *Inventario de los soportes en los que se almacenan bases de datos.*<br>❖ *Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.* |
| *Control de acceso* | ❖ *Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña.*<br>❖ *Lista actualizada de usuarios y accesos autorizados.*<br>❖ *Autorización escrita del titular de la información para la entrega de sus datos a terceras personas, para evitar el acceso a datos con derechos distintos de los autorizados.*<br>❖ *Concesión, alteración o anulación de permisos por el personal autorizado.* |
| *Incidencias* | ❖ *Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.*<br>❖ *Procedimiento de notificación y gestión de incidencias.* |
| *Personal* | ❖ *Definición de las funciones y obligaciones de los usuarios con acceso a los datos.*<br>❖ *Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.* |

| | |
|---|---|
| | ❖ *Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas.* |
| *Políticas y Procedimientos* | ❖ *Elaboración e implementación del Manual de obligatorio cumplimiento para el personal.*<br>❖ *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.* |

## *5.2. 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* | | |
|---|---|---|
| *Archivo* | *Almacenamiento de documentos* | *Custodia de documentos* |
| *Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.* | *Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.* | *Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.* |

| *BASES DE DATOS AUTOMATIZADAS* | |
|---|---|
| *Identificación y autenticación* | *Telecomunicaciones* |
| • *Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.*<br>• *Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.* | *Acceso a datos mediante redes seguras.* |

## *5.3. MEDIDAS DE SEGURIDAD PARA DATOS PRIVADOS SEGÚN EL TIPO DE BASES DE DATOS.*

| *BASES DE DATOS AUTOMATIZADAS Y NO AUTOMATIZADAS* |
|---|

| Auditoría | Responsable de seguridad | Políticas y Procedimientos Habeas Data |
|---|---|---|
| • Auditoría ordinaria (interna o externa) cada año.<br>• Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.<br>• Informe de detección de deficiencias y propuesta de correcciones.<br>• Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.<br>• Conservación del Informe a disposición de la autoridad. | • Designación de uno o varios responsables de seguridad.<br>• Designación de uno o varios encargados del control y la coordinación de las medidas del Manual políticas y procedimientos.<br>• Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad. | • Controles al menos una vez al año de cumplimiento, consistente en la auditoria anual, así como la capacitación al personal mínimo una vez al año. |

| BASES DE DATOS AUTOMATIZADAS | | | |
|---|---|---|---|
| Gestión de documentos y soportes | Control de acceso | Identificación y autenticación | Incidencias |
| • 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. | • Control de acceso al lugar o lugares donde se ubican los sistemas de información. | • Mecanismo que limite el número de intentos reiterados de acceso no autorizados. | • Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.<br>• Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación. |



## 5.4. MEDIDAS DE SEGURIDAD PARA DATOS SENSIBLES SEGÚN EL TIPO DE BASES DE DATOS

| BASES DE DATOS NO AUTOMATIZADAS | | | |
|---|---|---|---|
| Control de acceso | Almacenamiento de documentos | Copia o reproducción | Traslado de documentación |

| | | | |
|---|---|---|---|
| • *Acceso solo para personal autorizado.*<br>• *Mecanismo de identificación de acceso.*<br>• *Registro de accesos de usuarios no autorizados.* | • *Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.* | • *Solo por usuarios autorizados.*<br>• *Destrucción que impida el acceso o recuperación de los datos.* | • *Medidas que impidan el acceso o manipulación de documentos.* |

| *BASES DE DATOS AUTOMATIZADAS* | | |
|---|---|---|
| *Gestión de documentos y soportes* | *Control de acceso* | *Telecomunicaciones* |
| • *Sistema de etiquetado confidencial.*<br>• *Cifrado de datos.*<br>• *Cifrado de dispositivos portátiles cuando sean retirados.* | • *Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.*<br>• *Control del registro de accesos por el responsable de seguridad. Informe mensual.*<br>• *Conservación de los datos: por el periodo que las leyes impongan.* | • *Transmisión de datos mediante redes electrónicas cifradas.* |



## *5.5. ENCARGADOS DE SEGURIDAD*

*Los encargados de seguridad tienen las siguientes funciones:*

- *Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del Manual de Políticas y Procedimientos Habeas Data.*
- *Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.*
- *Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en este manual.*
- *Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.*

- *Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización en este manual y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.*
- *Definir los tiempos dentro de los cuales se realizarán las auditorias, los cuales NO podrán ser superiores a un año.*
- *Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.*
- *Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.*

*5.6. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS NO AUTOMATIZADAS.*

*5.6.1. ARCHIVO DE DOCUMENTOS.*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares.*

*Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la*

*actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la institución.*

*Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso las empresas, adoptarán las medidas necesarias para impedir el acceso de personas no autorizadas.*

*Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se*

*encuentre a cargo de estos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.*

*Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, las empresas, podrán adoptar medidas alternativas debidamente motivadas que se incluirán en el presente documento.*

*La descripción de las medidas de seguridad de almacenamiento se encuentra recogidas en este documento.*

*5.6.2. ACCESO A LOS DOCUMENTOS.*

*El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en este manual.*

*El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad en cuestión designado por las empresas.*

*5.7. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS AUTOMATIZADAS.*

*5.7.1. IDENTIFICACIÓN Y AUTENTICACIÓN*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de*

*información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.*

*También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc. La nomenclatura utilizada para la asignación de nombres de usuario para acceder al sistema de información y el sistema de autenticación de los usuarios que se recogen en este documento.*

*Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y letras.*

*Por otra parte, de las empresas deben vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días.*

### *5.8. ENTRADA Y SALIDA DE DOCUMENTOS O SOPORTES*

*La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío. El sistema de registro de entrada y salida se encuentra anexado en el presente documento.*

*Las instalaciones de las empresas son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; así mismo, han de*

*cumplir con las medidas de seguridad físicas correspondientes al documento o soporte donde incluyen los datos.*

*Las empresas, tienen el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en el presente manual. Las instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes se señalan en el presente documento.*

*Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.*

### *5.9. COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS.*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez a la semana, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.*

*De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello en este manual.*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses. Las empresas deben conservar una copia de respaldo de los datos y de los procedimientos de recuperación de estos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.*

*5.10. REGISTRO DE ACCESO.*

*De los intentos de acceso a los sistemas de información de la ladrillera, deberá guarda, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.*

*Los responsables de seguridad de las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.*

*Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.*

*No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente en el presente documento.*

*El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.*

*La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.*

*5.11. FUNCIONES Y OBLIGACIONES DEL PERSONAL*

*Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.*

*Las empresas deben informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de*

*su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, tablón de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente manual de Políticas y Procedimientos Habeas Data para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.*

*Las funciones y obligaciones del personal de la ladrillera se definen, con carácter general, según el tipo de actividad que desarrollan al interior de la institución, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos sobre bases de datos y sistemas de información. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.*

*El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente manual por parte del personal al servicio de la ladrillera es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre las partes.*
*Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de las empresas son las siguientes:*

- *Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de estos.*
- *Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos, estos se anexarán en el presente manual.*

*Las obligaciones relacionadas con las medidas de seguridad implantadas:*

- *Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.*
- *No revelar información a terceras personas ni a usuarios no autorizados.*

- *Observar las normas de seguridad y trabajar para mejorarlas.*
- *No realizar acciones que supongan un peligro para la seguridad de la información.*
- *No sacar información de las instalaciones de la organización sin la debida autorización.*
- *Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.*
- *Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de estos.*
- *Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérfida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.*
- *Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.*
- *Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el*

*deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.*

- *Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades al interior de las empresas.*

- *Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.*
- *Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales propiedad de las empresas.*
- *Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad.*

## *6. INCIDENCIAS*

### *6.1. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS.*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, establece un procedimiento de notificación, gestión y respuesta de incidencias 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, deben conocer 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 que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la institución deberá comunicarlo, de manera inmediata, a los responsables de seguridad, 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 ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.*

*LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de esta, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos y debe incluirse como anexo en el presente manual.*

*Asimismo, debe implementar los procedimientos para la recuperación de los datos, 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.*

*6.1.1. REPORTE*

*Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por las empresas. Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el responsable de la información debe ser notificado de forma inmediata. Los funcionarios deben reportar a su jefe directo y/o al Oficial de Protección de Datos Personales cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de la Entidad. A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega*

*de información o datos en virtud de orden de autoridad, Oficina Asesora Jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.*

*El responsable de la información debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado, apoyado con Oficina de Tecnologías e Informática.*

*7. CONTROL DE ACCESO Y VIDEO VIGILANCIA*

- *Control acceso: Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados y que permita guardar la trazabilidad de los ingresos y salidas.*

- *Video Vigilancia: Las empresas cuentan con cámaras de video vigilancia que tienen como finalidad dar cumplimiento a las políticas de seguridad física, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control. Las imágenes deberán ser conservadas por un tiempo máximo de 90 días. En caso que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.*

*8. MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN Y REUTILIZACIÓN DE DOCUMENTOS Y SOPORTES.*

*Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.*

*Antes de iniciar la destrucción se realizará un acta o se llevará el registro en un libro o agenda, en dicha a notación se describirá el documento objeto de*

*destrucción, la fecha, hora y firma de las dos personas que evidencian la destrucción.*

*Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.*

*Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de las empresas. Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en el presente manual.*

## *9. INFRACCIONES Y SANCIONES*

*De acuerdo con el Capítulo II de la Ley Estatutaria 1581 de 2012 de Protección de Datos, la Superintendencia de Industria y Comercio puede imponer sanciones por el incumplimiento de la normativa sobre protección de datos al responsable del tratamiento o al encargado del tratamiento. Las posibles sanciones son:*

- *Multas de carácter personal e institucional hasta por el equivalente a dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.*
- *Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.*
- *Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.*
- *Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.*

## *10. VIGENCIA*

*La presente versión de la Política de Tratamiento de Datos Personales es aplicable por el responsable de datos personales a partir de la fecha de aprobación de la presente.*

- *LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, difundió la presente política a sus empleados, asesores, proveedores, clientes y demás personas que tienen alguna responsabilidad en el tratamiento de datos personales.*

- *LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S, se reserva el derecho de modificar esta política de tratamiento de datos personales en cualquier momento*

- *LADRILLERA LOS CERROS DEL 34 S.A y LADRILLERA SAN MIGUEL DE LOS CERROS S.A.S está comprometida con la realización de difusión y capacitación para el debido entendimiento y aplicación de la presente política de tratamiento de Datos Personales.*

- *Clausula WhatsApp*
- *Recogida Datos Formularios*
- *Reporte de incidente*
- *Video Vigilancia.*

*HENRY ARDILA MORENO*
*GERENTE GENERAL*