PROGRAMA INTEGRAL DE GESTIÓN INFORMACIÓN
CONCESIÓN LA PINTADA S.A.S

Contenido

I. INTRODUCCIÓN

La OCDE[1] publicó en el 2013 una versión actualizada sobre las guías para la Protección de la Privacidad y los Flujos Transfronterizos de Información. Dicha guía incluyó el principio denominado **Responsabilidad Demostrada** ("accountability" en inglés), según el cual, *una entidad que recoge y hace tratamientos de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos*[2].

Este principio ha sido acogido por la normatividad colombiana[3] y exige que los sujetos obligados a proteger la privacidad de la información no solo cuenten con unas políticas de datos personales, sino que también deban adoptar una política con medidas apropiadas y efectivas que permitan garantizar el cumplimiento efectivo de las obligaciones que conlleva la Ley 1581 de 2012 y sus decretos reglamentarios. Esta política debe ser concreta, clara y fácil de hacer cumplir, de tal forma que se encuentre al alcance de todas las personas sin excepción.

El presente programa introduce una política de seguridad de la información cumpliendo lo determinado en el Decreto 1078 de 2015[4], que consiste en la declaración general que representa la posición de la CONCESIÓN LA PINTADA S.A.S con respecto a la protección de los activos de información que soportan los procesos de la compañía y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Así las cosas, luego de la reunión del Comité Jurídico de la CONCESIÓN LA PINTADA S.A.S; llevada a cabo el día 8 de septiembre 2021 y según aprobaciones de Junta Directiva los años 2020 y 2022, en estricto cumplimiento de la mencionada normativa y comprometida para lograr una cultura organizacional de respeto a la protección de datos personales, ha dispuesto el presente PROGRAMA INTEGRAL DE GESTIÓN DE INFORMACIÓN que permitirá documentar, implementar y monitorear una política de seguridad de la información que contenga medidas técnicas, humanas y

[1] Organización para la Cooperación y el Desarrollo Económico.
[2] Guía para la implementación del principio de Responsabilidad Demostrada, Superintendencia de Industria y Comercio – SIC- de Colombia.
[3] Ley 1581 de 2012: Artículo 17°, Decreto 1377 de 2013: Artículos 11°, 26° y 27° y la Constitución Política de Colombia: Artículo 15°, entre otros.

[4] Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

administrativas necesarias para otorgar seguridad a la información evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Todo lo anterior, con base en la Guía para la Implementación del Principio de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio – SIC- de Colombia y en los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

II. DEFINICIONES.

Las definiciones que se relacionan a continuación se encuentran conforme con la normatividad vigente en materia de protección de la información, citada anteriormente:

a) **Autorización:** Es el consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de sus Datos Personales.

b) **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.

c) **Base de Datos**: Es el conjunto organizado de Datos Personales que sean objeto de Tratamiento

d) **Compañía:** Concesión la Pintada S.A.S.

e) **Dato Personal:** Es cualquier información de cualquier tipo, vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

f) **Dato Público:** Es el Dato Personal calificado como tal según los mandatos de la Ley o de la Constitución Política y aquel que no sea semiprivado, privado o sensible. Son públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, etc.

g) **Dato Sensible**: Es el Dato Personal que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen afiliaciones sindicales, el origen racial o étnico, la orientación política, entre otros.

h) **Encargado del Tratamiento**: Es la 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. Para efectos de este Manual, la Compañía es uno de los Encargados del Tratamiento

i) Incidente: Se refiere a cualquier evento en los sistemas de información o bases de datos manuales o sistematizados, que atente contra la seguridad de los datos personales en ellos almacenados.

j) Manual de Políticas de datos: Documento que incorpora las Políticas y Procedimientos para la protección de Datos Personales que fue adoptado por la CONCESIÓN LA PINTADA S.A.S.

k) Oficial de Protección de Datos: Según el artículo 23° del Decreto 1377 de 2013, es la persona o área de la Compañía que asume la función de protección de datos personales y que dará trámite a las solicitudes de los Titulares, entre otras funciones que serán indicadas más adelante en el presente documento.

l) Permiso: Es la legitimación que expresamente y por escrito mediante contrato o documento que haga sus veces, otorgue la Compañía a terceros, en cumplimiento de la Ley aplicable, para el Tratamiento de Datos Personales, convirtiendo a tales terceros en Encargados del Tratamiento de los Datos Personales entregados o puestos a su disposición.

m) Programa Integral de Gestión de información: Es una herramienta fundamental que da cuenta del compromiso del responsable del tratamiento, al tiempo que es una medida eficaz para evitar cualquier infracción a la política de datos personales.

n) Responsable de Tratamiento: Es la 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 Personales, para efectos de este Manual es la Compañía, es decir, CONCESIÓN LA PINTADA S.A.S.

o) 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.

p) Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

III. ESTRUCTURA DEL PROGRAMA DE GESTIÓN DE DATOS

El presente programa se estructura a partir de los siguientes dos componentes, 1) La implementación del Principio de Responsabilidad Demostrada y, 2) la elaboración de la Política general de seguridad y privacidad de la información.

1. IMPLEMENTACIÓN DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA:

1.1. OBJETIVO.

Definir y establecer los lineamientos y procedimientos por medio de los cuales LA CONCESIÓN LA PINTADA S.A.S se compromete con la protección de la información que recolecta de sus titulares, así como realizar la implementación del principio de Responsabilidad Demostrada frente al tratamiento de datos mediante la implementación, desarrollo y seguimiento del Programa Integral de Gestión de Datos. Lo anterior, de conformidad con la Ley 1581 de 2012 y el Decreto 1377 de 2013.

1.2. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES.

La CONCESIÓN LA PINTADA S.A.S emitió en el año 2016 su política de tratamiento de datos personales. Incluye definiciones, principios, responsables del tratamiento, derechos de los titulares, entre otros aspectos. No obstante, a partir de la emisión del presente Programa, dicha política de tratamiento de datos personales fue modificada actualizándola en varios de sus aspectos según la normativa vigente y la pertinencia de este Programa.

A partir de la emisión de este Programa, tanto la política como el aviso de privacidad serán revisados anualmente y en caso de que sea necesario algún ajuste, este será el procedimiento:

a. El oficial de protección de datos junto con un abogado de la compañía, generan un borrador de los cambios o de los documentos que se asocian a la política.
b. El oficial de protección presenta a la Gerencia y/o Comité Jurídico los borradores de los documentos.
c. Aprobado el cambio, se dará su publicación en página WEB de la compañía y por envío de correo electrónico a todo su personal.

1.3. COMPROMISO INSTITUCIONAL.

La Gerencia de la CONCESIÓN LA PINTADA S.A.S se encuentra comprometida en crear una cultura organizacional que avance hacia el respeto de los datos personales que sean recolectados, almacenados, usados, puestos en circulación o eliminados en estricto cumplimiento de sus fines misionales y la Ley.

Por tal motivo, ha realizado un análisis de su estructura organizacional y ha considerado necesario realizar modificaciones que permitan crear el siguiente cargo y procedimientos internos.

1.3.1. OFICIAL DE PROTECCIÓN DE DATOS.

De acuerdo con lo establecido en el artículo 23 del Decreto 1377 de 2013, "*Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto.*"

Esta persona o área se denominará OFICIAL DE PROTECCIÓN DE DATOS y tendrá, entre otras, las siguientes funciones:

- Velar por la implementación efectiva del Programa integral de Gestión de Datos Personales, realizando una debida administración de este.
- Diseñar controles del Programa que permitan su evaluación y revisión permanente, con el objetivo de mitigar cualquier riesgo en su implementación.
- Servir de enlace y coordinar con las demás áreas de la Compañía para garantizar el cumplimiento del Programa Integral de Gestión de Datos Personales.
- Garantizar entrenamiento a todos los miembros de la Compañía y a los nuevos miembros, sobre el cumplimiento del Programa Integral de Gestión de Datos Personales. Este entrenamiento se realizará como mínimo a los miembros antiguos; como mínimo una (1) vez cada semestre, y a los miembros nuevos; a más tardar dentro del mes siguiente a su vinculación. Ambos, siempre y cuando el personal tenga responsabilidad con el tratamiento de datos.
- Registrar las bases de datos de la compañía en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo las instrucciones que emita la SIC o la autoridad competente.
- Responder los requerimientos de la SIC o autoridad competente en asuntos de datos personales.
- Implementar auditorias constantes para garantizar que los miembros de la compañía y las respectivas áreas estén dando cumplimiento a la política de tratamiento de datos personales. Estas auditorias serán realizada como mínimo una (1) vez por semestre.
- Validar que los países a los cuales se realizará la transmisión cuenten con el nivel adecuado de protección de datos personales, y en su defecto realizar el trámite para la obtención de la declaración de conformidad ante la SIC, en el evento de no contar con la autorización del titular.
- Realizar seguimiento al programa integral de gestión de datos personales.

- Establecer responsabilidades específicas para otras áreas de la Compañía respecto a la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales.
- Recibir, analizar y canalizar ante la dependencia responsable al interior de la Compañía (éste último si es del caso) cualquier requerimiento, solicitud, petición o queja que realice alguna autoridad o titular, garantizando una respuesta clara, oportuna y de fondo.
- Generar informes semestrales que serán presentados a la Gerencia y/o Comité Jurídico con el objetivo de mantenerlas informadas sobre la implementación del Programa de Gestión de Datos Personales. La Gerencia a su vez lo presentará semestralmente a los socios en la Junta Directiva. Estos informes, como mínimo, deberán contener:
    - ✓ Nivel de cumplimiento por parte de la Compañía en la implementación del Programa Integral de Gestión de Datos Personales.
    - ✓ Número de quejas, solicitudes o requerimientos que ha realizado alguna autoridad o titular de la información, así como el estado de la respuesta.
    - ✓ Incumplimientos encontrados por parte de las áreas responsables del tratamiento de datos personales en la implementación del Programa y la hoja de ruta para su mitigación.
    - ✓ Acciones de mejora implementadas durante el periodo del informe.

La persona que cumplirá este rol será quien ostente el cargo de COORDINACIÓN JURÍDICA de la CONCESIÓN LA PINTADA S.A.S, sus datos de contacto son:

- Dirección física: Cra 29c No. 10c -125 de Medellín
- Dirección electrónica: info@concesionlapintada.com
- Teléfono: (4) 5208340
- Cargo de la persona de contacto: COORDINACIÓN JURÍDICA de la CONCESIÓN LA PINTADA S.A.S.

1.3.2 RESPONSABILIDAD DE LAS ÁREAS DE LA COMPAÑÍA.

Si bien es cierto que principalmente la función de vigilar la protección de datos personales recae en el Oficial de Protección de Datos antes mencionado (entre otras funciones), el líder de cada área deberá reportar de manera oportuna a dicho Oficial cualquier solicitud o queja que provenga de cualquier autoridad o titular, así como cualquier violación a la seguridad de la información, de tal forma que como se mencionó anteriormente, toda respuesta sea dada de manera unificada a través del Oficial de Protección de Datos.

El procedimiento para este reporte será el siguiente:

- El área correspondiente recibe la solicitud, consulta, queja o requerimiento (o su equivalente) por parte de la autoridad respectiva o el titular.
- Dentro de los tres (3) días siguientes a la recepción, el líder del área la envía al Oficial de protección de Datos Personales para su análisis correspondiente.
- El Oficial dentro de los cinco (5) días siguientes a la recepción, emitirá su concepto sobre la hoja de ruta para dar respuesta, remitiendo si es del caso a la dependencia responsable para que le provea información para dar respuesta final, otorgando un plazo para ello el cual podrá variar dependiendo de la complejidad de la información.
- Finalmente, el Oficial de Protección de Datos dentro del plazo legal otorgado, emitirá respuesta por escrito al solicitante.

1.4 CONTROLES DEL PROGRAMA

A continuación, se describirán los controles que deberá implementar el Oficial de Protección de Datos para asegurar que las políticas adoptadas por la Compañía en el presente Programa sean implementadas en debida forma. No obstante, el Oficial también puede implementar otros controles que considere necesarios:

1.4.1 AUDITORÍAS INTERNAS.

Con el objetivo de garantizar la efectividad de estos compromisos de las áreas de la Compañía, el Oficial de Protección de Datos realizará como mínimo una (1) vez por semestre auditorías a cada área de la Compañía para revisar el cumplimiento de todo lo anterior. De todas las auditorías, levantará un acta que presentará a la Gerencia para que ésta a su vez analice lo sucedido y prepare la presentación en la Junta Directiva. Dicha acta, como mínimo tendrá la siguiente información:

- Áreas de la Compañía auditadas.
- Nivel de cumplimiento del Programa Integral de gestión de Datos por cada una de las áreas.
- Incidentes o violaciones a la protección de datos personales y el posible responsable de dicha transgresión. En este caso, también se indicarán las consecuencias que traen a la Compañía estos sucesos y la forma de cómo evitarlos a futuro.
- Recomendaciones para acciones de mejora en el Programa. (si existen)

En caso de que se presente un incidente o violación a la protección de datos por algún funcionario o área de la compañía, el Oficial de Protección reportará de manera inmediata a la Gerencia y/o comité Jurídico para que éstos analicen la situación y tomen las acciones correctivas y sancionatorias correspondientes.

Sumado a lo expuesto, cada 2 meses los lideres de cada área deberán presentar un informe al Oficial de Protección de datos con información relacionada con este Programa.

1.4.2 RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS

La compañía es la responsable por el tratamiento de la Base de Datos y al interior de ésta el Oficial de Protección de Datos será el responsable de la recepción y atención de peticiones, quejas, reclamos y consultas de todo tipo relacionadas con los datos. La persona encargada de esta área tramitará las consultas y reclamaciones en materia de Datos Personales de conformidad con la Ley y este Manual.

- Dirección física: Cra 29c No. 10c -125 de Medellín
- Dirección electrónica: info@concesionlapintada.com
- Teléfono: (4) 5208340
- Cargo de la persona de contacto: COORDINACIÓN JURÍDICA de la CONCESIÓN LA PINTADA S.A.S.

- **RESPONSABLES**. La compañía, en calidad de responsable del tratamiento, deberá cumplir con los siguientes deberes, sin perjuicio del cumplimiento de las demás normas que le impongan otros deberes:

  a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

  b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el titular.

  c) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

  d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

  e) Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible

  f) Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

  g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

  h) Suministrar al encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley.

  i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
k) 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.
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
m) Informar a solicitud del Titular sobre el uso dado a sus datos.
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio

- **ENCARGADOS.** La Compañía, en calidad de Encargado del Tratamiento, así como otras personas que debido a su actividad o relación con la Compañía ejerzan funciones de Encargado del Tratamiento, deberán cumplir con los siguientes deberes, sin perjuicio del cumplimiento de las demás normas que le impongan otras obligaciones:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.
f) 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.
g) Registrar en la Base de Datos las leyendas “reclamo en trámite” en la forma en que se regula en la presente ley.
h) Insertar en la Base de Datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad.
del Dato Personal.
i)Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

1.4.2.1 TRATAMIENTO Y FINALIDAD

Los datos tratados por la compañía deberán someterse a las finalidades que se señalan a continuación. Así mismo, los encargados o terceros que tengan acceso a los Datos mantendrán el tratamiento dentro de las siguientes finalidades:

a) Registrar toda la información necesaria para el cumplimiento de las obligaciones tributarias, laborales legales y extralegales derivadas del contrato de trabajo, y de registro contable de las obligaciones comerciales contraídas por la compañía.
b) Registrar toda la información necesaria de los accionistas y posibles inversionistas de la Compañía con el fin de garantizarles sus derechos como accionistas y mantener informados a quienes lo deseen acerca de los eventos que puedan interesarles
c) Cumplir con los procesos internos de la compañía en materia de selección y administración de empleados, proveedores y contratistas.
d) Cumplir los contratos celebrados con los clientes.
e) Cumplir con el control y la prevención del fraude y de lavado de activos y obtener la información requerida para el SARLAFT.
f) Cumplir aspectos fiscales y legales con las entidades del gobierno.
g) Realizar el pago de nómina, de aportes legales al sistema de seguridad social y de beneficios extralegales de los empleados.
h) Registrar el control y los pagos por los bienes y servicios recibidos
i) Realizar capacitaciones y acceder a convenios interempresariales
j) Cualquier otra actividad necesaria para el efectivo cumplimiento de la relación comercial que tiene la Compañía con proveedores y clientes.
k) Cualquier otra actividad necesaria para el efectivo cumplimiento de la relación laboral que tiene la Compañía con sus empleados.
l) La Transmisión de datos a terceros con los cuales se hayan celebrado contratos con este objeto, para fines comerciales, administrativos u operativos, incluyendo, pero sin limitarse a la expedición de carnés, y certificaciones a terceros, de acuerdo con las disposiciones legales vigentes.
m) Mantener y procesar por computadora u otros medios, cualquier tipo de información relacionada con el negocio del proveedor o del cliente con el fin de brindar los servicios y productos pertinentes.

n) Las demás finalidades que determinen los responsables en procesos de obtención de Datos Personales para su Tratamiento, con el fin de dar cumplimiento a las obligaciones legales y regulatorias, así como de las políticas de la Compañía.

1.4.3 PRINCIPIOS

La Compañía, en el desarrollo de sus actividades comerciales recolectará, utilizará, almacenará, transmitirá y realizará diversas operaciones sobre los Datos de los titulares.

En todo tratamiento de Datos realizado por la compañía, los responsables, encargados y/o terceros a quienes se les transfiera Datos deberán dar cumplimiento a los principios y reglas establecidas en la Ley 1581 de 2012 (artículo 4°), con el fin de garantizar el derecho al habeas data de los Titulares y dar cumplimiento a las obligaciones de Ley de la compañía.

En el marco de la implementación de este Programa, estos principios se aplicarán de manera armónica e integral de la siguiente manera:

PRINCIPIO	**FINALIDAD DE LA COMPAÑÍA**	**ACTIVIDADES PARA EL CUMPLIMIENTO**
Principio de legalidad en materia de Tratamiento de Datos	Busca el cumplimiento de las disposiciones legales vigentes	La Compañía respetará la siguiente normativa: - Constitución Política de Colombia - Ley 1581 de 2012 - Decreto No 1377 de 2013. - Cualquier otra emitida relacionada con el tratamiento de datos personales.
Principio de finalidad	La información entregada por el titular solo puede ser utilizada para los fines previstos en la Ley, por tanto, la Compañía avisa al titular las condiciones para su uso.	- Documento “Aviso de privacidad”, publicado en la página web y relacionada en los medios (físico o digitales) por los cuales se recolecta la información. Ver Anexo. Aviso de Privacidad. - Los derechos que le asisten a los titulares están relacionados en la Política de tratamiento de datos personales que puede ser consultada por los mismos a través de la página web.
Principio de Libertad	El Tratamiento sólo puede ejercerse con el consentimiento previo, expreso e informado del	- Solicita y conserva la autorización para el tratamiento de los datos dada por el titular, la cual se obtiene mediante los diferentes medios (físico o digital) por los cuales se recolectan los datos. Ver Anexo.

	Titular. Los Datos Personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia del mandato legal o judicial que releve el consentimiento.	Consentimiento expreso tratamiento de datos. Ver Anexo. Contrato de Transmisión de datos personales.
Principio de veracidad o calidad	La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Cuando existan Datos Personales parciales, incompletos, fraccionados o que induzcan a error, la Compañía deberá solicitar a su Titular la actualización o corrección de la información o abstenerse de Tratarlos	La Compañía realiza campañas de actualización de datos o por iniciativa propia del titular mediante el uso de los canales de comunicación.
Principio de Transparencia	Garantiza al titular que puede ejercer su derecho de obtener en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o dato personal que sea de	La Compañía ha proporcionado para la atención de consultas y reclamos de los titulares los siguientes canales: - Teléfono: 4 - 5208340 - Correo Electrónico: notificaciones@concesionlapintada.com, info@concesionlapintada.com

	su interés o titularidad.	
Principio de acceso y circulación restringida	Conserva la información bajo las condiciones de seguridad necesarias para impedir su adulteración, consulta, uso o acceso no autorizado o fraudulento y no deja disponible en internet u otros medios masivos de información datos personales privados, salvo que el acceso sea controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la ley.	- Se suscriben acuerdos de confidencialidad o cláusulas de confidencialidad en los acuerdos de voluntades suscritos por la Compañía. Ver Anexo. Contrato con cláusula de confidencialidad. - Se respetan las autorizaciones otorgadas por los titulares cuando aceptan las políticas de datos personales de la compañía.
Principio de Seguridad y Principio de Confidencialidad.	La información sujeta a Tratamiento por parte de la Compañía, se deberá proteger mediante el uso de las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta,	**Medidas Técnicas:** - La información recolectada se carga a un espacio de almacenamiento virtual (nube) y su acceso está limitado a las personas que tengan autorización al interior de la Compañía para consultarla. - Reporte y seguimientos a los accidentes o incidentes de seguridad en los que pueda suceder la violación a los códigos de seguridad y existencia de riesgos en la administración de la información. - Generación de backup periódicos. **Medidas Humanas**

	uso o acceso no autorizado o fraudulento	- Cláusulas en los contratos de cada uno de los colaboradores durante el tiempo que dure su labor, en la que se compromete a conservar y mantener de manera confidencial y no revelarla a terceros cuando administren, manejen, actualicen o tengan acceso a información que se encuentren en las bases de datos. - Archivos con información sensible o confidencial deben contar con contraseña para proteger su confidencialidad. **Medidas Administrativas** - Lineamientos de seguridad establecidos en el "Manual de seguridad de la Información". - Cumplimiento del Ciclo de vida de la información establecido en el Manual "Gestión Documental".

1.4.4 BASES DE DATOS

1.4.4.1 INVENTARIO DE LAS BASES DE DATOS

En la siguiente tabla se relacionan los tipos de bases de datos que ha reportado la compañía ante la SIC:

NOMBRE DE LA BASE DE DATOS	ENCARGADO DE LA BASE DE DATOS	RECOLECCIÓN DE LOS DATOS	FINALIDAD
Hojas de vida físicas del personal*	Gestión humana	Proceso de contratación de personal y demás asuntos laborales	Mantener actualizada la información de los empleados para la debida gestión laboral
Personal *	Gestión humana	Proceso de contratación de personal y demás asuntos laborales	Mantener actualizada la información de los empleados para la debida gestión laboral
Base de datos física de control de tiempos	Gestión humana	Proceso de seguimiento en el	Control de horario

		cumplimiento de horario de trabajo	
Base de datos digital de control de tiempos	Gestión humana	Proceso de seguimiento en el cumplimiento de horario de trabajo	Control de horario
Réplica base de datos digital de terceros	Área de Contratación	Los medios por los cuales se recolecta la información de los clientes son: - Inscripción en página Web -Información de FlyPass -PQRS - talleres y capacitaciones a la comunidad	Finalidades varias - Atención al ciudadano/cliente (Gestión PQR)/Recepción y gestión de requerimientos internos o externos sobre productos o servicios
Base de datos física de proveedores	Área de contratación	Los medios por los cuales se recolecta la información de los proveedores, acreedores y otros son: -Formulario de inscripción del proveedor físico o virtual. -Documentación del proveedor en el sistema de gestión documental	Recolección de datos personales con el fin de realizar gestión administrativa de la contratación de proveedores.
Base de datos digital de proveedores	Área de contratación	Los medios por los cuales se recolecta la información de los proveedores, acreedores y otros son: -Formulario de inscripción del	Recolección de datos personales con el fin de realizar gestión administrativa de la contratación de proveedores.

		proveedor físico o virtual. -Documentación del proveedor en el sistema de gestión documental	

*La información recaudada en las bases de datos de hojas de vida de los empleados al contener información sensible, será utilizada únicamente para asuntos laborales y no podrá ser usada ni divulgada a terceros. De igual forma, al titular al momento de su recolección se le advierte de dicha seguridad. Al momento que un empleado se retira, éste podrá solicitar que su información sensible se elimine.

La compañía normalmente no recolecta datos personales de menores de edad. No obstante, en algunas actividades que se realicen en estricto cumplimiento del objeto social de la Concesión, las personas mayores de edad asisten con sus hijos; siendo éstos algunos menores de edad. Por tal motivo, la Concesión garantiza la autorización de sus padres o acudientes haciendo firmar el documento CONSENTIMIENTO INFORMADO TRATAMIENTO DE DATOS DE MENORES DE EDAD, el cual se puede observar en el Anexo. Consentimiento expreso tratamiento de datos. Estos datos solo se recopilan para registros de asistencia y no se usarán para ningún otro fin.

CLASIFICACIÓN DE LOS DATOS PERSONALES

La CONCESIÓN LA PINTADA S.A.S usa la clasificación de datos personales relacionada en el Registro Nacional de Bases de Datos como son: datos generales, de identificación, de ubicación, sensibles, socioeconómico y otros datos; así:

- Datos generales de identificación como: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, etc.
- Datos específicos de identificación como: firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, etc.
- Datos biométricos como: huella, fotografías, vídeos, fórmula dactiloscópica, voz, etc. (Datos sensibles)
- Datos de ubicación relacionados con actividad privada de las personas como: domicilio, teléfono, correo electrónico, etc.
- Datos relacionados con la salud de la persona en cuanto a órdenes y relación de pruebas complementarias como laboratorio, imagen, endoscópicas, patológicas, estudios, etc. (Datos sensibles)
- Datos sobre personas en situación de discapacidad. (Datos sensibles)
- Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, etc.

- Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, etc.
- Datos generales relacionados con afiliación y aportes al Sistema Integral de Seguridad Social como son: EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, etc.
- Datos personales de acceso a sistemas de información como: usuarios, IP, claves, perfiles, etc.
- Datos de antecedentes judiciales y/o disciplinarios de las personas.

1.4.4.2 TRATAMIENTO DE LAS BASES DE DATOS:

- <u>RECOLECCIÓN:</u>

Los medios que utiliza la compañía para la recolección de los datos personales de los titulares son:

a. Formularios físicos: Cuando hay capacitaciones o socializaciones, durante el proceso de contratación o compra.
b. Formularios digitales o en aplicativos: En la página WEB a través de formulario PQRS.

En los medios mencionados anteriormente la compañía garantiza que en la recolección de los datos personales se solicite la autorización del titular para el tratamiento de los datos personales, de manera voluntaria, explícita, informada e inequívoca. Y en los casos que no se requiere la autorización de los titulares estas excepciones cumplirán según lo enunciado en la ley 1581 de 2012 en el Artículo 10.

- <u>ALMACENAMIENTO</u>

Los medios que utiliza la compañía para el almacenamiento de los datos personales de los titulares son:

- Servidores propios o a cargo de terceros. Cuando son terceros, se tienen suscritos cláusulas de confidencialidad.
- Servicios en la Nube.
- Archivo físico administrado por un tercero, con quien se tiene suscrito cláusulas de confidencialidad.

- <u>USO</u>

Los datos personales de los titulares son utilizados según la finalidad establecida en el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio (SIC) y en cumplimiento a lo establecido en el “Aviso de Privacidad” de la compañía.

- CIRCULACIÓN

La circulación de los datos personales de los titulares se hace al interior de la compañía según las necesidades de acceso o consulta de los trabajadores activos en la compañía, con quienes se tienen suscritos los respectivos acuerdos de confidencialidad.

La información se comparte con otras áreas de la compañía de manera digital en las carpetas compartidas a través de OneDrive y se da acceso únicamente para visualizar los archivos sin permiso de edición o eliminación, el control depende del responsable interno asignado, es responsabilidad del dueño de la información garantizar que solo pueda ser vista por las personas que lo requieren para el desarrollo de sus actividades, partiendo del principio del mínimo privilegio.

Adicionalmente, la compañía comparte información a entidades públicas o por requerimientos judiciales, para lo cual no se requiere autorización según lo descrito en el artículo 10° de la Ley 1581 de 2012.

- SUPRESIÓN

La compañía realiza la supresión de los datos personales cuando se haya cumplido la finalidad para la cual fueron recolectados o en los casos que el titular de los datos solicite la eliminación de estos mediante el ejercicio del derecho de habeas data que se enuncia en la política de tratamiento de datos.
Igualmente, el tiempo de retención de los documentos que contienen información personal está determinado en las tablas de retención documental según lineamientos establecidos en el Manual de Gestión Documental.

1.4.5 DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES Y PROCEDIMIENTO PARA EJERCERLOS

De acuerdo con la Ley, los Titulares de Datos Personales tienen los siguientes derechos:

a) Conocer, actualizar y rectificar sus Datos Personales frente a los Responsables o los Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
b) Solicitar prueba de la Autorización otorgada al Responsable del Tratamiento salvo que la Ley indique que dicha Autorización no es necesaria.
c) Ser informado por el Responsable o el Encargado del Tratamiento, previa solicitud, respecto del uso que se le ha dado a sus Datos Personales.
d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la Ley.

e) Revocar la Autorización y/o solicitar la supresión de sus Datos Personales de las Bases de Datos de la Compañía, cuando la Superintendencia de Industria y Comercio haya determinado que el Tratamiento no respeta los principios, derechos, garantías constitucionales y legales.
f) Solicitar acceso y acceder en forma gratuita a sus Datos Personales que hayan sido objeto de Tratamiento.

Los menores de edad podrán ejercer sus derechos personalmente, o a través de sus padres o los adultos que detenten la patria potestad, quienes deberán demostrarlo mediante la documentación pertinente. Así mismo podrán ejercer los derechos del Titular los causahabientes que acrediten dicha calidad, el representante y/o apoderado del Titular con la acreditación correspondiente y aquellos que han hecho una estipulación a favor de otro o para otro.

CONSULTAS.

El Titular, sus causahabientes, sus representantes y/o apoderados, podrán formular consultas respecto al contenido de los Datos Personales del Titular que reposan en las Bases de Datos de la Compañía y ésta suministrará la información que posea del Titular. Para realizar la consulta se requiere:

a) Presentar la solicitud por escrito en las oficinas de la Compañía ubicadas en la Cra 29c No. 10c-125 -45 piso 3 de Medellín.
b) Dirigidas al correo electrónico dirigido a notificaciones@concesionlapintada.com, info@concesionlapintada.com
c) A la solicitud deberá anexarse la copia del documento de identidad del Titular. Cuando la solicitud sea realizada por un causahabiente, apoderado y/o representante del Titular, deberá acreditar dicha calidad, de conformidad con la Ley vigente aplicable sobre la materia.
d) La solicitud deberá indicar la dirección y datos de contacto e identificación del solicitante.
e) El Responsable de atender la consulta dará respuesta al solicitante siempre y cuando tuviere derecho a ello por ser el Titular del Dato Personal, su causahabiente, apoderado o representante cuando sea casos de menores de edad. Esta respuesta se enviará dentro de los diez (10) días hábiles contados a partir de la fecha en la que la solicitud fue recibida por la Compañía.
f) En caso de que la solicitud no pueda ser atendida dentro de los diez (10) hábiles contados a partir de la fecha en la que la solicitud fue recibida por la Compañía, se contactará al solicitante para comunicarle los motivos de la demora y para señalarle otra fecha en la cual será respondida su consulta, que no superará los cinco (5) días hábiles siguientes al vencimiento del primer término. Para ello se utilizará el mismo medio o uno similar al que fue utilizado por el Titular para su comunicar su solicitud.
g) Cualquiera que sea el medio empleado para realizar la consulta, la Compañía guardará prueba de ésta y su respuesta.

RECLAMO.

El Titular, sus causahabientes, representante y/o apoderados que consideren que la información contenida en una Base de Datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012 o en este Manual, podrán presentar un reclamo escrito ante la Compañía, el cual será tramitado bajo las siguientes reglas:

a) El reclamo se formulará por correo electrónico dirigido a notificaciones@concesionlapintada.com o info@concesionlapintada.com
b) Al reclamo deberá anexarse la copia del documento de identidad del Titular. Cuando el reclamo sea realizado por un causahabiente, apoderado y/o representante del Titular, deberá acreditar dicha calidad, de conformidad con la Ley vigente aplicable sobre la materia.
c) El reclamo deberá contener una descripción de los hechos que dan lugar al reclamo y lo que se pretende con éste, es decir, la actualización, corrección, supresión de la información o cumplimiento de los deberes de la Ley o de este Manual.
d) Se deberá indicar la dirección y datos de contacto e identificación del reclamante.
e) Se deberá acompañar por toda la documentación que el reclamante quiera hacer valer.
f) La Compañía antes de atender el reclamo verificará la identidad del Titular del Dato Personal sobre el cual se hace el reclamo, su representante y/o apoderado y con ese fin podrá exigir el documento de identificación original del Titular, y los poderes especiales, generales o documentos que se exijan según sea el caso.
g) Si la documentación o el reclamo resultan incompletos, se requerirá al reclamante 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 se presente la información requerida, se entenderá que se ha desistido del reclamo.

a) En caso de que la Compañía no sea competente para resolver el reclamo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al reclamante.
b) Una vez recibido el reclamo con la documentación completa, se incluirá en la Base de Datos de la Compañía donde reposen los Datos del Titular sujetos a reclamo una leyenda que diga “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles. Esta leyenda deberá mantenerse hasta que el reclamo sea decidido.
c) El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el 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.

QUEJA.

El Titular, sus causahabientes, representante y/o apoderados sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante la Compañía.

1.4.6 ADMINISTRACIÓN DE RIESGOS

- **Identificación y medición:** a través de la matriz de riesgos se identifican y miden los riesgos asociados al tratamiento de datos. El riesgo relacionado con el tratamiento de datos personales se identificó como medio. Consultar Matriz de Riesgo anexo. Matriz de Riesgo
- **Control:** los riesgos relacionados con el tratamiento de datos se controlan a través de la ejecución del plan de protección de datos y de las diferentes políticas, actividades, capacitaciones, planes, etc. que se aprueban, implementan y ejecutan al interior de la Compañía.
- **Monitoreo:** el monitoreo al cumplimiento del programa y sus medidas de control se realiza a través de la auditoría semestral a cargo de la auditoría interna realizada por el Oficial de Protección de Datos.

En la auditoría que se realiza al cumplimiento de la normatividad de protección de datos y a las medidas de control implementadas se valida, entre otras cosas:

1. Los indicadores, los cuales evidencian la efectividad del sistema de administración de riesgos.
2. Funcionamiento de forma oportuna, efectiva y eficiente de los controles.
3. Que los riesgos residuales se encuentren en niveles aceptables.
4. Ocurrencia y atención de incidentes de seguridad.

Para la CONCESIÓN LA PINTADA S.A.S se priorizan los siguientes factores de riesgo de la información:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad.
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura.
- Identificación y protección de los datos de carácter personal.
- Adecuada clasificación de la información bajo custodia de la compañía de acuerdo con el marco legal vigente.
- Entorno global digital inseguro.
- Aislamiento forzoso del personal en sus residencias debido a situaciones de salud.
- Segregación apropiada de roles y privilegios en todos los sistemas de información.

VALORACIÓN DEL RIESGO

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la compañía. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad).

Esta valoración se realizará como mínimo, una vez al año por parte del Oficial de Protección de Datos.

ESTRATEGIA DE TRATAMIENTO DE RIESGO

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

- Transferir: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia a otros actores.
- Mitigar: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.
- Evitar: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.
- Aceptar: consiste en hacer frente a un riesgo (positivo o negativo) porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:

- **Estrategias Orientadas al Conocimiento**

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los trabajadores de la CONCESIÓN LA PINTADA S.A.S apropien conocimientos en materia de:

- Ley de protección de datos personales
- Ley de transparencia y acceso a la información
- Políticas institucionales de seguridad digital
- Modalidades y control de ataques informáticos
- Uso seguro de los recursos informáticos

- **Estrategias Orientadas a la continuidad**

Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, la compañía adelantará en las siguientes acciones específicas en materia de:

- Fortalecimiento de su infraestructura de servicios básicos de energía.
- Actualización de planes alternos de operación por dependencias en caso de: pérdida de continuidad de servicios informáticos, imposibilidad de accesos a sedes y aislamiento obligatorio por emergencia sanitaria o similares.
- Mejoramiento de sus capacidades de detección oportuna de eventos adversos de seguridad de la información

- **Estrategias orientadas al Control de Acceso**

Con el fin de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados la CONCESIÓN LA PINTADA S.A.S emprenderá acciones específicas para:

- Actualizar los instrumentos de acceso a la información
- Reforzar los controles de acceso a activos de información con roles y privilegios más precisos
- Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información

- **Estrategias de fortalecimiento de controles técnicos**

Ante el aumento del tipo y complejidad de amenazas informáticas la entidad implementará estrategias específicas en:

- Identificación de eventos potencialmente nocivos
- Reforzamiento de controles de acceso a servicios en la nube.
- Verificación y control de copias de respaldo.
- Control de cambios en plataformas tecnológicas.
- Aplicación de parches de seguridad y actualización de equipos de procesamiento de datos.

2. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

2.1 Introducción:

La compañía tiene información en distintas modalidades: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones. Para la CONCESIÓN LA PINTADA S.A.S la seguridad de la información es la protección contra una gama de amenazas buscando garantizar la continuidad de la actividad comercial, con el propósito de disminuir los riesgos empresariales frente a la pérdida de información propia o de terceros.

2.2 Objetivos de seguridad de la información:

- Entender y gestionar los riesgos operacionales y estratégicos en seguridad de la información con la finalidad que puedan mantenerse en niveles aceptables para la compañía.
- Proteger la confidencialidad de la información relacionada con los clientes, los empleados, los proveedores y demás personas que interactúan con la compañía.
- Garantizar que los servicios web de acceso público y las redes internas cumplen con las especificaciones de disponibilidad requeridas.

2.3 Principios de seguridad de la información:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios o terceros.
- la CONCESIÓN LA PINTADA S.A.S protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- la CONCESIÓN LA PINTADA S.A.S protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- la CONCESIÓN LA PINTADA S.A.S protegerá su información de las amenazas originadas por parte del personal.
- la CONCESIÓN LA PINTADA S.A.S protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- la CONCESIÓN LA PINTADA S.A.S controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- la CONCESIÓN LA PINTADA S.A.S implementará control de acceso a la información, sistemas y recursos de red.

- la CONCESIÓN LA PINTADA S.A.S garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- la CONCESIÓN LA PINTADA S.A.S garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- la CONCESIÓN LA PINTADA S.A.S garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- la CONCESIÓN LA PINTADA S.A.S garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Responsabilidades:

1. Cada líder de área es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la compañía.
2. Cada líder de área es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la compañía.
3. Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

Cuando algunas de las normas o políticas de seguridad de la información se distribuyen fuera de la compañía, se deberá tener cuidado de no revelar información confidencial.

Todas estas políticas deben servir de apoyo para la identificación de riesgos mediante la disposición de controles con relación a un punto de referencia que pueda ser utilizado para identificar las deficiencias en el diseño e implementación de los sistemas, y el tratamiento de los riesgos mediante la posible identificación de tratamientos adecuados para las vulnerabilidades y amenazas localizadas.

2.4 Política De Mesas Limpias

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos.
- Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

2.5 Gestión de las Copias de Seguridad

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, mensual, salvo que en dicho período no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de impacto alto para la compañía y/o de elevado nivel de transaccionalidad.

Como normal general, la frecuencia con la que se realizarán las copias de seguridad se determinará en función de la sensibilidad de las aplicaciones o datos, de acuerdo con los criterios de clasificación de información.

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados.

Como norma general y siempre que sea posible, se deberá requerir que la información en las copias de seguridad esté cifrada. Este requerimiento será obligatorio para determinados tipos de información confidencial. Se deberán realizar pruebas de restauración de las copias de seguridad disponibles y de los procesos de restauración definidos, a fin de garantizar el funcionamiento correcto de los procesos. Estas se realizarán de forma periódica y quedarán documentadas.

Se deberá establecer un período de retención de las copias de seguridad hasta su destrucción una vez terminado el periodo de existencia. Las copias de seguridad, tanto de archivos maestros como de aplicaciones y archivos de información se deberán ubicar en lugares seguros con acceso restringido. Asimismo, las copias de respaldo se ubicarán preferentemente en un centro distinto al que las generó.

2.6 Teletrabajo o Trabajo en Casa.

Se deberá controlar el acceso remoto a la red de la compañía en las modalidades de trabajo a distancia, esto es, desde fuera de las instalaciones propias. Los servicios de conexión al trabajo en remoto estarán destinados exclusivamente a personal de la compañía. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del responsable de seguridad.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto podrá ser propiedad del empleado o proporcionado por la compañía. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

- Capacidad de realizar una conexión a través de una VPN.
- Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.
- Software antivirus instalado.
- Software de firewall/cortafuegos personal instalado.

El teletrabajo desde un equipo propio del trabajador requerirá de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo en remoto no suponga una amenaza para la seguridad de la información. Además, se podrán establecer medidas de seguridad adicionales a las existentes para asegurar de una manera más fiable la conexión segura en remoto. El servicio de trabajo a distancia o en casa se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad.

2.7 Política de SGSI

En vista de la importancia para el correcto desarrollo de los procesos de la CONCESIÓN LA PINTADA S.A.S, los sistemas de información deben estar protegidos adecuadamente.

Una protección fiable permite a la compañía percibir mejor sus intereses y llevar a cabo eficientemente sus obligaciones en seguridad de la información**.** La inadecuada protección afecta al rendimiento general y puede afectar negativamente la imagen, reputación y confianza de los clientes, proveedores y terceros.

El objetivo de la seguridad de la información es asegurar la continuidad de la operación y reducir al mínimo el riesgo de daño mediante la prevención de incidentes de seguridad, así como reducir su impacto potencial cuando sea inevitable.

Para lograr este objetivo, la compañía ha desarrollado una metodología de gestión del riesgo que permite analizar regularmente el grado de exposición de nuestros activos importantes frente a aquellas amenazas que puedan aprovechar ciertas vulnerabilidades e introduzcan impactos adversos a las actividades de nuestro personal o a los procesos importantes de nuestra compañía.

El éxito en el uso de esta metodología parte de la propia experiencia y aporte de todos los empleados en materia de seguridad**,** y mediante la comunicación de cualquier consideración relevante a sus responsables directos en las reuniones semestrales establecidas por parte de la dirección, con el objeto de localizar posibles cambios en los niveles de protección y evaluar las opciones más eficaces en coste/beneficio de gestión del riesgo en cada momento, y según el caso.

Los principios presentados en la política de seguridad que acompaña a esta política fueron aprobados el Comité Jurídico y/o de Gerencia con el fin de garantizar que las futuras decisiones se basen en preservar la confidencialidad, integridad y disponibilidad de la información relevante de la compañía**.** La compañía cuenta con la colaboración de todos los empleados en la aplicación de las políticas y directivas de seguridad propuestas.

El uso diario de los ordenadores o equipos de cómputo por el personal determina el cumplimiento de las exigencias de estos principios y un proceso de inspección para confirmar que se respetan y cumplen por parte de toda la compañía. Adicionalmente a esta política, y a la política de seguridad

de la compañía, se disponen de políticas específicas para las diferentes actividades. Se pretende que los colaboradores no usen equipos personales para asuntos de la compañía, así poder garantizar la custodia de la información.

Todas las políticas de seguridad vigentes permanecerán disponibles en los documentos de la compañía y serán de acceso libre para los colaboradores, además se actualizarán regularmente. El acceso es directo mediante la página Web. El objetivo de la política es proteger los activos de información de la compañía en contra de todas las amenazas y vulnerabilidades internas y externas, tanto si se producen de manera deliberada como accidental.

2.8 La dirección de la empresa y el oficial de protección de datos harán seguimiento a los siguientes puntos:

- La información estará protegida contra cualquier acceso no autorizado.
- La confidencialidad de la información, especialmente aquella relacionada con los datos de carácter personal de los empleados y clientes.
- La integridad de la información se mantendrá con relación a la clasificación de la información (especialmente la de "uso interno").
- La disponibilidad de la información cumple con los tiempos relevantes para el desarrollo de los procesos críticos de negocio.
- Se cumplen con los requisitos de la reglamentación vigente, especialmente con la Ley de Protección de Datos y de Firma Electrónica.
- Los planes de continuidad de negocio serán mantenidos, probados y actualizados al menos con carácter anual.
- La capacitación en materia de seguridad se cumple y se actualiza suficientemente para todos los empleados.
- Todos los eventos que tengan relación con la seguridad de la información, reales como supuestos, se comunicarán al responsable de seguridad y serán investigados.

El cumplimiento de esta política, así como de la política de seguridad de la información y de cualquier procedimiento o documentación incluida dentro del repositorio de documentación del SGSI, es obligatorio y atañe a todo el personal de la compañía**.**

Las visitas y personal externo que accedan a nuestras instalaciones no están exentas del cumplimiento de las obligaciones indiciadas en la documentación del SGSI, y el personal interno observará su cumplimiento.

2.9 Revisión de la Política

La aprobación de esta política implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus

requisitos. En caso existir situaciones que tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de la CONCESIÓN LA PINTADA S.A.S

En cualquier caso, de duda, aclaración o para más información sobre el uso de esta política y la aplicación de su contenido, por favor, consulte por teléfono o e-mail al responsable del SGSI designado formalmente en el organigrama corporativo.

III. NORMATIVA Y DOCUMENTOS RELACIONADOS

- Ley 1581 de 2012.
- Decreto 1377 de 2013.
- Constitución política de Colombia.
- Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) emitida por la SIC.
- Documento “A privacy office guide to demonstrating accountability”, Toronto, Canadá, 2014.

IV. ANEXOS

- Aviso de Privacidad
- Consentimiento Expreso Tratamiento de Datos
- Contrato con Cláusula de Confidencialidad
- Contrato Transmisión de datos personales
- Matriz de Riesgos
- Procedimiento para la atención de PQRS
- Contrato de Cesión y Derechos de Imagen videos corporativos
- Registro de Atención al usuario – octubre diciembre 2021-
- Anexos de Contrato – Confidencialidad y autorización.
- Política de Tratamiento de Datos Personales.

Emitido por:

CONCESIÓN LA PINTADA S.A.S