MANUAL INTERNO DE PROCESOS DE PROTECCIÓN DE DATOS PERSONALES

CREDIALIANZA

CREDIALIANZA

Contenido

CREDIALIANZA

MANUAL DE PROCESOS PARA LA PROTECCION DE DATOS PERSONALES

1. Ámbito de aplicación

Mediante el presente manual interno de procesos de **CREDIALIANZA SAS** en cumplimiento de los requerimientos de la normatividad que regula el habeas data y la protección de la información personal busca proteger la información personal frente a accesos y manipulaciones indebidas, así como frente a revelaciones y accesos ilícitos.

Este documento ha sido elaborado bajo estándares presentados por las Directivas de la entidad y se considera de obligatorio cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información, que permiten al acceso a los mismos. El documento se aplica a todas las bases de datos (manuales y automatizadas) de las que es responsable la entidad, así como a aquellas que se puedan tratar en calidad de Encargada del Tratamiento.

2. Objetivo

Definir procesos generales, roles y responsabilidades para la administración y tratamiento de la información de carácter personal, así como las herramientas que todos los funcionarios deben utilizar para este fin.

3. Glosario

Autorización
Consentimiento previo, expreso e informado del titular del dato para llevar a cabo el tratamiento de datos personales.

Aviso de Privacidad
Documento que es puesto a disposición del Titular para el tratamiento de sus datos personales en caso de no poder poner a su disposición la política de privacidad. En caso de ser necesaria la implementación de este aviso para un determinado proyecto o canal de comunicación, debe contener, al menos la información relativa a la existencia de las políticas de Tratamiento de información que serán aplicables y las características del Tratamiento que se pretende dar a los datos.

Base de datos con información personal
Conjunto organizado de datos personales que es objeto de tratamiento, sin importar si estos son estructurados o no.

Dato personal
Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Los datos personales pueden ser públicos, semiprivados o privados.

Dato privado
Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular, como es el caso de los datos biométricos, historia clínica, entre otros. Este tipo de datos no son generalmente objeto de tratamiento por parte de la entidad, a menos de que se trate de la información requerida necesariamente para poder adelantar una determinada actividad o se trate del manejo interno de sus funcionarios, previa autorización por su parte para ello, en caso de ser necesario.

Dato público
Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado
Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar, no sólo a su titular, sino a cierto sector o grupo de personas, o a la sociedad en general, como lo es el relativo al cumplimiento de las obligaciones consignado en las centrales de riesgo crediticio.

Dato Sensible
Aquel que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que 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 y la vida sexual.

Este tipo de datos podrán ser objeto de tratamiento por parte de la entidad, en relación con sus funcionarios, previa autorización por su parte para ello, o se trate datos imprescindibles de sus empleados o clientes y sus familias, sin los cuales sea imposible adelantar las labores propias de su objeto social.

Encargado del tratamiento
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Fraude Externo
Actos, realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos o información de la misma para beneficio propio o de un tercero, o incumplir normas o leyes.

Fraude Interno
Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad, información confidencial o incumplir normas o leyes, en los que está implicado, al menos, un funcionario de la entidad con beneficio propio o de un tercero.

Oficial de Privacidad
Área o persona perteneciente a la entidad encargada de la función de protección de datos personales.

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

Superintendencia de Industria y Comercio
Autoridad nacional en materia de protección de datos personales, a través de la Delegatura de Protección de Datos Personales.

Titular de la información
Persona natural cuyos datos personales son objeto de Tratamiento.

Transmisión
Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por parte del Encargado por cuenta del Responsable.

Tratamiento
Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

4. Caracterización de bases de datos personales y flujos de información personal

4.1. Criterios para la definición de bases de datos personales:

Las bases de datos personales se definen como todos aquellos repositorios de información físicos o digitales que contienen información estructurada de naturaleza personal.

Como parte de los lineamientos para el adecuado tratamiento de la información personal, a continuación, se describen los criterios definidos por la Compañía para la identificación de las bases de datos que integran tratamiento de información personal:

a) *Identidad:* Hace referencia a la base de datos cuyo contenido permite identificar o asociar a un grupo de personas claramente determinado. La base de datos que responde al criterio de identidad se caracteriza por contender datos que de manera directa o sin mayores esfuerzos técnicos, revela la identidad de un grupo de personas.

b) *Formalidad:* Hace referencia a la base de datos que se constituye como repositorio habitual o preestablecido para la documentación o registro de información personal como parte de un proceso de la entidad

c) Unidad: Hace referencia a la base de datos cuyo contenido se encuentra asociado por una misma finalidad, medio y contenido. La base de datos que responde al criterio de unidad puede estar documentada en varios repositorios independientes, por ejemplo, en distintas AZ o carpetas, pero por la unidad de su contenido, medio y propósito, se considera como una sola base de datos. De igual manera la información digital puede estar contenida en diversos archivos digitales, pero en su conjunto conforman una sola base de datos al estar asociados a un mismo contenido y propósito.

Los anteriores criterios han sido definidos por la Compañía como un lineamiento de gobierno de la información para la identificación de las bases de datos personales, específicamente para el propósito de elaboración y actualización del inventario de bases de datos personales y su respectivo registro ante la Superintendencia de Industria y Comercio.

4.2. Flujos de información personal:

Corresponde al conjunto de datos personales que no cumple con los criterios establecidos en el presente manual para ser considerados como bases de datos personales. Para efectos del entendimiento y documentación del ciclo de la información personal, los flujos de información tienen las siguientes características:

a) Modalidad: Pueden corresponder a:
- Información en tránsito dentro de las actividades de un proceso o servicio de la entidad, o
- Repositorios no formales de información personal.

b) Origen: Los flujos de información pueden tener origen en:
- Fuentes primarias de recolección de información personal.
- Bases de datos formales.

c) Destino: Los flujos de información personal pueden tener su destino en:
- Bases de datos formales.
- Repositorios no formales de información personal.

- Herramientas de disposición o eliminación de información.

Los mencionados flujos de información personal son tenidos en cuenta para el entendimiento y documentación del ciclo del tratamiento de información de la entidad, pero no para el inventario de bases de datos personales. Sin embargo, se propende por la adecuada gestión de la seguridad de los mismos

5. Criterios para la determinación del número de titulares de bases de datos personales

La determinación del número de titulares de las bases de datos con información personal de la entidad es una de las obligaciones asociadas a la efectiva realización del Registro de Bases de Datos Personales ante la Superintendencia de Industria y Comercio.

No obstante, lo anterior, la adecuada y completa identificación del número de titulares de información personal de todas las bases de datos de la Compañía es una labor de avance progresivo debido a la entrada y salida constante de titulares en sus bases de datos personales:

6. Metodología para la Administración de Riesgo de Cumplimiento de Protección de Datos

El riesgo de cumplimiento es la posibilidad de que el tratamiento de la información en la entidad no sea íntegro. Esto significa que la entidad falle (o sea así percibido) en el cumplimiento de las leyes, regulaciones y estándares que son relevantes por ser responsable de la protección de datos personales, lo cual puede traer como consecuencia la pérdida de reputación, pérdidas de información sensible, multas, sanciones, entre otros.

Con el fin de mitigar este riesgo, la entidad, como “Responsable del Tratamiento de Datos Personales”, hace claridad sobre las responsabilidades al interior de la misma así:

DIRECCIÓN GENERAL

- Propender por el cumplimiento de la protección de datos personales a todo nivel en la entidad, a través de la asignación de los recursos necesarios para tal fin y de la aprobación de políticas generales que faciliten la implementación y capacitación de los funcionarios en cuanto a los mecanismos de control necesarios para el cumplimiento de la protección de datos personales.

- Decidir y establecer el enfoque metodológico que gobierna la entidad para el manejo de la información personal, de acuerdo con las propuestas que el Oficial de Privacidad hace para el efecto.

- Establecer dentro del organigrama el funcionario o área responsable de las labores correspondientes a Oficial de Privacidad.

- Designar al funcionario área o asesor externo responsable de las labores correspondientes a oficial de privacidad.

OFICIAL DE PRIVACIDAD

De acuerdo con lo requerido en la normatividad vigente en el sentido de asignar a una persona o área la función de cumplimiento de la normatividad de datos personales dentro de la entidad, se ha decidido radicar tal actividad en la Gerencia Legal.

Sin embargo, cada una de las directivas de la entidad, de acuerdo con sus funciones particulares, apoya su labor.

La Oficial de Privacidad cumple con las siguientes funciones, además de todas aquellas que generalmente establecen las leyes de protección de datos personales vigentes:

- Establecer los lineamientos mínimos requeridos para garantizar una adecuada administración y protección de la información contenida en las bases de datos de la entidad.

- Monitorear y hacer seguimiento a la normatividad expedida en materia de protección de la información y hacer recomendaciones de ajustes al interior de la entidad.

- Efectuar el registro de las bases de datos ante la Superintendencia de Industria y Comercio, en cuanto sea requerido por ser responsable de una determinada base de datos.

- Detectar y, en su caso, notificar a la Superintendencia la creación o modificación de bases de datos de la entidad.

- Emitir y actualizar periódicamente las políticas que deben ser implementadas en la entidad para la protección de los datos personales, las cuales deben ser aprobadas por la Gerencia General.

- Promover capacitaciones a los funcionarios de la entidad y a terceros en torno a la importancia del cumplimiento de la protección de datos personales y realizar evaluaciones que permitan medir el grado de conocimiento de la legislación al interior de la entidad.

- Atender las consultas e inquietudes relacionadas con el tratamiento de información personal que titulares, funcionarios y personas o entidades con los que se comparte la información puedan manifestar.

- Atender los requerimientos de las autoridades, así como los procesos administrativos o judiciales en materia de protección de datos personales, en conjunto con las áreas y asesores que considere adecuados para el efecto.

- Valorar los incidentes de seguridad de la información relacionados con información personal con el fin de establecer las medidas correctivas que ameriten y su posterior comunicación a la Superintendencia de Industria y Comercio, en caso de considerarlo necesario.

- Monitorear los procedimientos establecidos para que los Titulares puedan ejercer sus derechos al habeas data, verificando que estén disponibles y acordes con lo establecido por la regulación vigente.

En materia de auditoría y control la Oficial de Privacidad mantiene las siguientes funciones

- Verificar de manera directa o a través de terceros, que las políticas y procedimientos se implementen adecuadamente en la entidad, así como que los mismos se mantengan en el tiempo.

- Realizar las investigaciones en materia de inadecuada administración de la información por parte de los funcionarios de la entidad o sus colaboradores.

- Realizar procesos de revisión o auditorías internas en materia de protección de datos personales.

DEMÁS FUNCIONARIOS DE LA ENTIDAD

- Dar un adecuado uso de la información en el normal desarrollo de sus funciones y de acuerdo con la finalidad establecida para cada uno de los datos personales objeto de tratamiento.

- Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.

- Conocer y acatar las políticas y reglamentaciones internas establecidas en materia de protección de la información personal.

- Informar al Oficial de Privacidad acerca de la ocurrencia de posibles incumplimientos o riesgos de incumplimiento a la normatividad y reglamentaciones internas, en materia de administración de la información personal.

- Conocer, respetar y dar cumplimiento a la normatividad de tipo penal y administrativo existente en Colombia en materia de protección de datos personales y sus implicaciones en el evento de un incumplimiento.

- Garantizar que los accesos a la información solo se realizan siguiendo los procedimientos establecidos y para uso exclusivamente de tipo laboral y no para uso personal o de terceros sin autorización.

7. Principios de la administración de datos personales en la entidad

La entidad en el desarrollo, interpretación e implementación de la Ley, ha definido como sus pilares para el tratamiento armónico e integral de datos personales los siguientes principios:

- **Finalidad**: el tratamiento obedece a una finalidad legítima de acuerdo con la Constitución y la ley.

  La finalidad de las bases de datos es la establecida en la autorización del Titular, en las políticas de privacidad de la entidad o en la normatividad vigente.

- **Veracidad o Calidad**: La entidad cuida que la información sujeta a tratamiento, ya sea capturada por los funcionarios de la misma o sus proveedores, sea veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Legalidad**: El tratamiento de datos se sujeta a lo establecido en la Ley y en las demás disposiciones que la desarrollen.

  Esto quiere decir que la recolección, uso, acceso, transferencia, almacenamiento y destrucción de datos personales no se realiza de manera ilícita, fraudulenta, por medios desleales o en forma contraria a la legislación vigente.

- **Libertad**: Los datos personales no pueden ser obtenidos o divulgados sin previa autorización del Titular, o en ausencia de mandato o permiso legal o judicial.

  Se deberá informar al titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y, por tanto, no podrán recopilarse datos sin la clara especificación acerca de la finalidad de los mismos.

- **Acceso y circulación restringida**: el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las leyes vigentes y la Constitución. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, a menos que se tenga una autorización para su utilización incluyendo esta posibilidad por parte de los titulares de la

información o se haga necesario para el cumplimiento de los fines institucionales de la entidad.

- **Principio de limitación de la recolección:** Sólo deben recolectarse los datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo del tratamiento.

  En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos.

- **Transparencia**: En el tratamiento se garantiza el derecho del titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernen.

- **Confidencialidad**: todos los funcionarios y proveedores que intervienen en el tratamiento de datos personales que no tienen la naturaleza de públicos, están obligados a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

8. Procesos y Procedimientos para la protección de datos personales.

A continuación, se establecen los lineamientos aplicados por la entidad con el fin de cumplir con sus obligaciones en cumplimiento de los principios para la administración de datos personales.

Estos lineamientos son complementarios a las normas actualmente existentes y las políticas generales implementadas por la entidad y en ningún momento pretenden remplazarlas o desconocerlas.

8.1. Tratamiento de la Información.

Políticas de privacidad

Las políticas de privacidad de la entidad cumplen con las normas vigentes en materia de protección de datos personales.

Las políticas y/o sus modificaciones son diseñadas por la Oficial de Privacidad y son aprobadas por la Gerencia General.

Las políticas de tratamiento de información son puestas en conocimiento de los titulares cuando sean solicitadas en las oficinas principales de la entidad, según se indica en el aviso de privacidad que hace parte de los documentos de vinculación de asociados y/o clientes.

El contenido principal de las políticas establece:

- Nombre o razón social de la entidad
- Domicilio, dirección, correo electrónico y teléfono de la entidad
- Tratamiento al cual son sometidos los datos
- Finalidad del tratamiento de los datos en caso de ser la información recolectada por la entidad
- Derechos que asisten a los titulares de la información
- Persona o área responsable de la atención de peticiones, consultas y reclamos
- Procedimiento para el ejercicio del habeas data de los titulares
- Tratamiento de datos personales de menores de edad
- Tratamiento de datos sensibles

Cualquier modificación o cambio sustancial a las políticas de privacidad es comunicado a los titulares de los datos antes de su implementación con una antelación de, al menos, 10 días hábiles

Captura de Información

En general la captura se hace en medio físico a través de formularios de vinculación obteniendo autorización del Titular de la información y se guarda prueba de la misma, a menos que dicha autorización se haya otorgado por parte del titular por medio de acciones inequívocas, tales como aceptar comunicaciones por parte de la entidad y responderlas.

En caso de obtener los datos de terceros o proveedores, a través de los acuerdos o convenios que se realizan con ellos se establecen los términos del tratamiento que se da a la información en desarrollo de su actividad, indicando claramente que, en materia de autorizaciones, cuando se comparten datos con la entidad, el responsable exclusivo de contar con los permisos para el tratamiento de los mismos es quien provee los datos.

Autorización para tratamiento de datos sensibles

Cuando se trate de la recolección de datos sensibles se deben cumplir los siguientes requisitos:

- La autorización debe ser explícita.

- Se debe informar al Titular que no está obligado a autorizar el tratamiento de dicha información.

- Se debe informar de forma explícita y previa al Titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del mismo.

Autorización de tratamiento de datos de niños, niñas o adolescentes (NNA)

Cuando se trate de la recolección y tratamiento de datos de niños, niñas o adolescentes se deben cumplir los siguientes requisitos:

- La autorización debe ser otorgada por personas que estén facultadas para representar los NNA. El representante de los NNA deberá garantizarles el derecho a ser escuchados y valorar su opinión del tratamiento teniendo en cuenta la madurez, autonomía y capacidad de los NNA para entender el asunto.

- Se debe informar que es facultativo responder preguntas sobre datos de los NNA.

- El tratamiento debe respetar el interés superior de los NNA y asegurar el respeto de sus derechos fundamentales.

Uso de la Información

Los funcionarios sólo pueden hacer uso de la información contenida en las bases de datos de la entidad para el fin establecido en la Ley, las autorizaciones del titular y los propósitos sociales de la entidad.

Cualquier uso de la información diferente al establecido es previamente consultado con el Oficial de Privacidad.

Únicamente los funcionarios autorizados de acuerdo con sus funciones pueden introducir, modificar o anular los datos contenidos en las bases de datos o documentos objeto de protección.

8.2. Procedimientos de Seguridad de la información

La información personal una vez es recogida por la entidad cuenta con los niveles de seguridad adecuados a lo largo del tratamiento, garantizando la confidencialidad, integridad y disponibilidad de la información de tal forma que se impide su manipulación, acceso, eliminación o adulteración sin los debidos niveles de autorización, según corresponda.

Los siguientes procedimientos pretenden complementar a los definidos en las Políticas de la entidad.

8.2.1. Procedimiento de Notificación y Gestión de Incidentes.

Los incidentes de seguridad de la información que estén relacionados con requerimientos legales y que puedan afectar a bases de datos que contengan información personal deben ser reportados a la Oficial de Privacidad por el dueño de proceso afectado quien determinará si se procede al reporte de este en el Registro Nacional de Bases de Datos.

Igualmente se tiene establecido un registro en el que se hace constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

1. El usuario que tenga conocimiento de la incidencia se responsabiliza directa y personalmente de comunicarla por los medios habilitados por la compañía, sin demora al Oficial de Privacidad.
2. El Oficial de Privacidad tomará de inmediato las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.
3. En el caso de que se hayan visto afectadas bases de datos automatizadas con información personal y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible que el Oficial de Privacidad autorice la ejecución del citado procedimiento.
4. No registrar una incidencia de la que se haya tenido conocimiento será considerado una falta contra la que se impondrán las sanciones correspondientes a una falta grave.

8.2.2. Gestión de Usuarios

Un adecuado programa integral de protección de los datos recomienda la definición de procedimientos de altas, modificaciones y bajas de usuarios para conceder al acceso por parte de estos a las bases de datos que contengan datos personales o aplicaciones que gestionen las mismas.

La entidad cuenta con un procedimiento específico implementado para la gestión de usuarios con acceso a la información personal. La gestión se realiza con el apoyo de la Gerencia General.

8.2.3. Uso del correo electrónico

Como complemento a los procedimientos de gestión de usuarios, el uso de Internet y la política de filtrado de contenido de correo electrónico y acceso a Internet, como norma general los usuarios de la plataforma de correo electrónico de la entidad deben cumplir lo siguiente:

- El usuario dueño del buzón es responsable de todos los mensajes que se envíen a su nombre.
- Los usuarios no deben abrir programas desconocidos que lleguen adjuntos en los mensajes; deben ser eliminados o reportados al Oficial de Privacidad antes de ser ejecutados.
- La entidad puede limitar el ingreso de menajes de correo electrónico que contengan archivos ejecutables, batch, virus, troyanos, videos, sonido, contenido sexual y spam.

- No se debe utilizar la cuenta de correo electrónico corporativo en las siguientes situaciones:
    - Distribución o divulgación de información corporativa sin previa autorización de la entidad.
    - Envío de mensajes que busquen ocultar o modificar la identidad del remitente.
    - Envío de mensajes personales que aparenten ser comunicaciones oficiales de la Empresa.
    - Promoción de actividades no relacionadas con el negocio.

8.2.4. Política de Tratamiento de Bases de Datos Temporales

Los datos personales están ubicados físicamente en bases de datos que están sujetas a todos los procedimientos y medidas de seguridad que garantizan su protección.

Por otra parte, en la operación diaria de tratamiento de los datos pueden producirse copias de los datos protegidos para tratamientos especiales. En estos casos se presta la adecuada protección a esas bases de datos mientras existan.

8.2.5. Capacitación de empleados

La entidad capacita a sus funcionarios en la administración de los datos personales con una periodicidad al menos anual, con el fin de medir sus conocimientos sobre el particular.

Dentro de las capacitaciones se tienen planes especiales para los nuevos funcionarios, de tal manera que los cambios en el personal no afecten el conocimiento de la planta en torno a sus obligaciones en materia de protección de la información.

8.2.6. Proveedores y tercerización

Todos los proveedores o terceros (Encargados del tratamiento), que realizan tratamiento de datos por cuenta de la entidad, deben cumplir la totalidad de las obligaciones establecidas en la Ley y la política de privacidad de la entidad.

La entidad suscribe contratos con todos los proveedores o terceros que cumplan las características de Encargados en los términos previstos por la legislación vigente.

Una vez cumplida la prestación contractual, los datos de carácter personal son destruidos o devueltos a la entidad responsable del tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

La entidad tiene establecidos lineamientos para la relación con agentes externos que tengan acceso o puedan tener acceso potencial a la información o recursos informáticos y por tanto a las bases de datos.

- El tercero que accede a la información y a los recursos informáticos de la entidad debe acatar los lineamientos establecidos en sus políticas de privacidad.
- En el acceso a la información y a los recursos informáticos se establecen acuerdos de confidencialidad para que no se otorgue acceso a la información sin la existencia de una autorización y compromiso explícito.
- En el contrato establecido entre la entidad y los agentes externos, se especifica la necesidad de acceso a la información.

9. Procedimiento De Peticiones, Quejas, Consultas y Reclamos

El titular de los datos personales respecto de cuyo tratamiento la entidad es responsable, tiene los siguientes derechos:

a) Acceder a sus datos personales que hayan sido objeto de un tratamiento.

b) Rectificar los datos personales que hayan sido objeto de un tratamiento.

c) Revocar su autorización para el tratamiento de sus datos personales, cuando en el tratamiento de estos no se hayan respetado los principios establecidos en la Ley 1581 de 2012.

d) Solicitar prueba de la autorización otorgada para el tratamiento de sus datos personales.

Estos derechos podrán ser ejercidos directamente por el titular de la información, su apoderado o su causahabiente, según el caso, y se les aplicará las siguientes reglas:

- Derecho de Acceso. Los titulares tienen el derecho de conocer si sus datos personales han sido sometidos a un tratamiento por parte de la entidad en los términos expresados en la norma, además de ejercer el derecho de conocer el origen de sus datos y si los mismos han sido cedidos o no a terceros y, por ende, la identificación de los cesionarios.

- Derechos de Rectificación y Cancelación. Los titulares tienen derecho solicitar la rectificación de sus datos personales recolectados cuando los mismos resulten inexactos, estén incompletos o conlleven a error. Los titulares de la información deberán indicar los datos que solicitan corregir y además acompañar la documentación que justifique lo solicitado.
  Igualmente, el titular podrá solicitar la supresión o cancelación de sus datos personales cuando el tratamiento de los mismos por parte del responsable o encargado resulte excesivo o inadecuado.

La cancelación de la información dará lugar al bloqueo de los datos del titular, conservándolos por parte de la entidad, con el único fin de que éstos sean accesibles a autoridades administrativas o judiciales.
En todo caso la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular tenga el deber legal o contractual de permanecer en la base de datos.

Atención de peticiones, consultas y reclamos.

Área responsable. La entidad a través del área de Atención al Cliente atenderá todas las peticiones, consultas, quejas y/o reclamos del titular de la información, relacionadas con los derechos establecidos en la ley para conocer, actualizar, rectificar y suprimir sus datos personales. De conformidad con el artículo 14 de la ley 1581 de 2012

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

El Titular o sus causahabientes 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 esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

a. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

b. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha 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.

La consulta, rectificación, actualización o supresión debe contener como mínimo, la siguiente información:

- El nombre y dirección de contacto del titular o cualquier otro medio para recibir la respuesta.

- Los documentos que acrediten la identidad y capacidad de su representante. Tal como se indica para los siguientes casos:

✓ Titular: Documento de identificación.
✓ Causahabiente: Registro civil y documento de identificación.
✓ Representante legal en caso de menores:
- Padres de familia: Registro civil de nacimiento y documento de identidad.
- Tutores: Sentencia judicial que confiere representación legal.
✓ Representante legal autorizado por el titular: Poder autenticado.
✓ Por estipulación a favor de otro: Manifestación en este sentido.

- La descripción clara y precisa del tipo de reclamo que realiza el titular de información (corrección, actualización o supresión).

- La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer el derecho de reclamo, así como los hechos que dan lugar al mismo.

- Aportar la documentación que avale su petición en caso de que por la naturaleza del dato sea procedente.

- En caso dado, otros elementos o documentos que faciliten la localización de los datos personales.

MEDIOS DE CONTACTO

Para el ejercicio del derecho a realizar consultas, reclamos, correcciones, actualizaciones o supresión de datos personales, el titular podrá contactar a la entidad a través de los siguientes medios de contacto:

- Correo electrónico: atencionalcliente@credialianza.com
- Dirección física: Calle 113 No. 7 – 45 Oficina 503 Torre B Edificio Teleport Business Park

- Número telefónico: (57 601) 7940100.
- Whatsapp (57) 318 7303606
- Horario de atención: lunes a viernes 8:00 am a 5:30 pm.

10. Actividades de verificación y control.

Con el propósito de garantizar la mejora continua de las políticas y procedimientos para el tratamiento de la información personal, la entidad a través del Oficial de Privacidad coordinará y ejecutará acciones periódicas de auditoría o verificación del cumplimiento de las disposiciones del presente manual tomando en consideración de los siguientes lineamientos centrales:

a) Aspectos centrales de la revisión o control:

- Debida identificación y actualización del ciclo del tratamiento de la información:
  - Escenarios de tratamiento
  - Canales y fuentes de recolección de información
  - Finalidades del tratamiento
  - Flujos de información
  - Terceros encargados y responsables del tratamiento de la información personal

- Inventario y actualización de bases de datos personales:
  - Identificación y reporte oportuno de nuevas bases de datos personales
  - Actualización de las bases de datos existentes
  - Adaptación de controles para conteo y seguimiento de número de titulares de bases de datos personales.

- Verificación de los procedimientos internos para el tratamiento de información personal:
  - Procedimiento de atención de consultas y reclamos de titulares de información personal.
  - Procedimiento de reportes de incidentes de seguridad.

- Implementación y aplicación de modelos y cláusulas de naturaleza legal:
  - Avisos de privacidad y solicitudes de autorización.
  - Cláusulas contractuales con terceros encargados.
  - Cláusulas contractuales con trabajadores de la entidad.
  - Cláusulas contractuales escenarios de transmisión y transferencia de datos.

- Seguridad de la información y gestión del riesgo:

- Valoración de los riesgos, impactos y niveles de criticidad.
- Valoración de la clasificación de las bases de datos en función de su nivel de riesgo.
- Valoración del diseño y asignación de controles de seguridad.
- Eficacia de los controles de seguridad.

b) Resultados de la verificación: Los resultados de la verificación deberán reflejar los siguientes elementos centrales:

- Resultados de la última verificación y estado de implementación de los planes de mejora definidos.
- Estado actual de cumplimiento de la ley de protección de datos.
- Efectividad de las medidas y controles implementados.
- Relación de incidentes significativos que afectaron el cumplimiento de la ley y disposiciones internas durante el periodo objeto de revisión.
- Planes de acción (preventivos, correctivos y de mejora) respecto de cada uno de los eventuales hallazgos de la verificación.

c) Periodicidad y reporte: Las revisiones al cumplimiento de la política y procedimiento de tratamiento de la información personal deberá realizarse al menos una vez cada año o de manera inmediata ante la ocurrencia de un incidente que comprometa o amenace comprometer la seguridad de la información personal o el adecuado nivel de cumplimiento de la normatividad aplicable.

Los resultados de la revisión junto con los eventuales planes de mejora definidos, serán presentados por el Oficial de Privacidad ante la Gerencia General de la Compañía, para su valoración y aprobación.

11. Comunicación Externa Alcance del Manual de Políticas y Procesos

Las políticas y procesos aquí establecidos y aquellos procesos que sean diseñados con el fin de garantizar el cumplimiento de las leyes vigentes en materia de información personal, son de obligatorio cumplimiento por parte de los funcionarios de la entidad, así como sus aliados, proveedores, operadores y en general terceros que traten datos por parte de la entidad.