POLÍTICAS INTERNAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

La presente política tiene como propósito dar a conocer cuáles son los requisitos básicos de seguridad de la información para establecer controles efectivos sobre todas las actividades que se desarrollan en CREDIANTIOQUIA, con el fin de que todos los involucrados en la operación o que prestan servicios garanticen el buen uso de los sistemas, herramientas, recursos e información a la que tienen acceso.

Así como, presentar los lineamientos de control para todos los empleados, terceros y entes que tengan acceso a la información de CREDIANTIOQUIA, para garantizar su seguridad a través de los principios de confidencialidad, integridad y disponibilidad, estableciendo las políticas de seguridad que se aplican a todos los sistemas de información, la red, así como, a todas las instalaciones en las que procesan, almacenan, o transmiten información.

Enmarcado en las buenas prácticas y disposiciones legales como son los estándares internacionales de seguridad (ISO 27001:2013), la Ley 1581 de 2012 y los aspectos establecidos por la Superintendencia de Industria y Comercio mediante la Guía de para la Implementación del Principio de Responsabilidad Demostrada (Accountability).

Lo anterior, teniendo en cuenta que la organización se enfrenta a amenazas relativas a la seguridad, en especial relacionados con el fraude asistido por computadores, como también a las acciones de personas, los cuales cada vez se han vuelto más comunes, ambiciosos y sofisticados. A continuación, se describen los principales objetivos específicos:

- Establecer y capacitar al personal de CREDIANTIOQUIA en seguridad de la información, buscando el aumento en la cultura, así como en el compromiso con la adopción de buenas prácticas, el reporte de incidentes de seguridad y la identificación de riesgos.
- Minimizar los incidentes de seguridad de la información presentados en CREDIANTIOQUIA.
- Mantener los sistemas y los recursos tecnológicos adecuados, que fortalezcan la seguridad de la información.
- Establecer los fundamentos para el desarrollo y la implantación de un Modelo de Seguridad de la información.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.

2. BASE LEGAL Y ÁMBITO DE APLICACIÓN

CREDIANTIOQUIA, con objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y del Decreto 1377 de 2013, adopta estas Políticas Internas de Seguridad donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en el artículo 4 literal g) de la LEPD.

Las disposiciones de este documento se aplican a las bases de datos objeto de responsabilidad de CREDIANTIOQUIA, así como a los sistemas de información, soportes y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, sin importar el medio, formato o presentación. De igual forma aplican para todas las personas que

participan en el tratamiento, tales como: usuarios (empleados y accionistas), socios, proveedores y entes de control que accedan independiente de su ubicación (interna o externamente), a cualquier activo de información.

El cumplimiento de las políticas de la seguridad de la información es obligatorio y todos los usuarios de la información deben entender su rol, y asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de la misma.

Por consiguiente, cualquier situación en la que se comprometa la integridad, confidencialidad y disponibilidad de la información resultará en una acción disciplinaria, que pueden llegar hasta la terminación del contrato laboral por justa causa y/o un posible establecimiento de un proceso judicial bajo las leyes nacionales que apliquen, sin perjuicio de acciones civiles y/o penales a que haya lugar.

3. DEFINICIONES

Establecidas en el artículo 3 de la Ley 1581 de 2012 y en el artículo 2.2.2.25.1.3 Decreto 1074 de 2015 (artículo 3 del Decreto 1377 de 2013).

Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

Autenticación: Procedimiento de verificación de la identidad de un usuario.

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

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Contraseña: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

Control de acceso: Mecanismo que permite acceder a sitios, dispositivos, información o bases de datos mediante la autentificación.

Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.

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

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

Identificación: Proceso de reconocimiento de la identidad de los usuarios.

Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

Información: Representación de conocimiento mediante datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere (nombre empresa).

Perfil de usuario: Grupo de usuarios a los que se da acceso.

Recurso protegido: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos

personales.

Responsable de administrar base de datos: Una o varias personas designadas por (Nombre empresa), como Responsable del Tratamiento, para el control y la coordinación de las medidas de seguridad.

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

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos, que para los efectos de las políticas planteadas corresponde (Nombre empresa).

Sistema de información: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

Soporte: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, las memorias USB, etc.

Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

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

4. CLASIFICACIÓN DE LA INFORMACIÓN

Publica: Información que puede ser conocida por todos los miembros enmarcados en el alcance y el público en general. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Interna: Información que requiere la organización para la ejecución de su objeto social y puede ser accedida por el personal de CREDIANTIOQUIA para el cumplimiento de las actividades diarias, alineadas a las funciones y responsabilidades del cargo o de la prestación de servicios de terceros y su conocimiento es de carácter general. Su disponibilidad a terceros es únicamente mediante un acuerdo contractual que exprese la necesidad de su uso para efectos del cumplimiento del mismo y para lo cual se debe comprometer a no divulgarla.

Confidencial: Información propia que solo está disponible para los colaboradores de CREDIANTIOQUIA en función de sus labores y que no puede ser conocida por otros empleados o terceros sin autorización del Responsable de administrar la base de datos. También se refiere a un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como Números telefónicos y correos electrónicos personales; datos laborales,

sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

Reservada: Información que solo debe tener acceso personal específico y la revelación al público puede causar daño a la reputación, marca o estrategias de organización. También, hace referencia a aquellos datos privados que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

5. CUMPLIMIENTO Y ACTUALIZACIÓN

La Políticas Internas de Seguridad es un documento interno de obligatorio cumplimiento de todo el personal asociado con los servicios de CREDIANTIOQUIA, con acceso a los sistemas de información que contengan las bases de datos, en especial la que contienen información de personas.

Este documento debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

6. MEDIDAS DE SEGURIDAD

6.1. Medidas de seguridad comunes

6.1.2. Gestión de documentos y soportes

Los directores serán los encargados de vigilar y controlar qué personas son las autorizadas a acceder a los documentos y soportes con datos personales.

Los documentos y soportes deben catalogar los datos según la clasificación de la información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada.

La identificación de los documentos y soportes de contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de las instalaciones o equipos de la organización deben estar bajo control y se autoriza por el Responsable de administrar la base de datos. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

El inventario de documentos y soportes de CREDIANTIOQUIA, debe incluirse como anexo del presente manual.

6.1.3. Control de acceso

El personal de CREDIANTIOQUIA, solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el Responsable de administras la base de datos.

CREDIANTIOQUIA se ocupa del almacenamiento actualizado de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, consiste en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a CREDIANTIOQUIA, que de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

6.1.4. Ejecución del tratamiento fuera de las instalaciones

El almacenamiento de datos personales en dispositivos portátiles y su tratamiento fuera de la organización requiere una autorización previa por parte de CREDIANTIOQUIA, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

6.1.5. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias deben ser borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

6.1.6. Responsable de administrar las Bases de Datos

CREDIANTIOQUIA, ha designado a los Directores como los responsables de seguridad encargados de coordinar y controlar las medidas de seguridad contenidas en el presente manual.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

6.1.7. Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por CREDIANTIOQUIA, clasificadas con nivel de seguridad sensible o privado, se han de someter, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

CREDIANTIOQUIA, realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

Las auditorías concluirán con un informe de auditoría que contendrá:

- El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- La identificación de las deficiencias halladas y la sugerencia de medidas correctoras o complementarias necesarias.
- La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

6.2. Medidas de seguridad para bases de datos no automatizadas

6.2.1. Archivo de documentos

CREDIANTIOQUIA, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares.

Los documentos deben ser archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los sitios de almacenamiento de documentos deben disponer de llaves u otros mecanismos que controlen su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso CREDIANTIOQUIA, adoptará medidas alternas para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos. La destrucción de documentos se debe hacer mediante mecanismos que realicen un corte adecuado del papel, que garantice que el documento no se pueda restaurar.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados en Sensible deben encontrarse en áreas o lugares en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no sea necesario el uso de dichos documentos. Si no fuera posible cumplir con lo anterior, CREDIANTIOQUIA, podrá adoptar medidas alternativas debidamente motivadas.

6.2.2. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada como Sensible, tanto por usuarios autorizados como por personas no autorizadas de manera permanente, tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como Sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el Responsable de administrar la base de datos.

6.3. Medidas de seguridad para bases de datos automatizadas

6.3.1. Identificación y autenticación

CREDIANTIOQUIA debe instalar sistemas que permitan identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, estas deben tener un mínimo de nueve caracteres y contener mayúsculas, minúsculas, números y letras.

Por otra parte, CREDIANTIOQUIA, debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 60 días.

CREDIANTIOQUIA, también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados y bloquear el acceso tras tres intentos.

6.3.2. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según la clasificación de la información, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número

de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío.

6.3.3. Control de acceso físico

Los lugares que son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; asimismo, han de cumplir con las medidas de seguridad, correspondientes al documento o soporte acorde con la clasificación de la información que contiene.

CREDIANTIOQUIA tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en el presente manual.

6.3.4. Copias de respaldo y recuperación de datos

CREDIANTIOQUIA debe llevar a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez al mes, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, se deben establecer los procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán o complementaran manualmente los datos.

CREDIANTIOQUIA, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

CREDIANTIOQUIA, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

6.3.5. Redes de Comunicaciones

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

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo (Por ejemplo: archivo con clave) que garantice que la información no sea inteligible ni manipulada por terceras personas.

6.3.6. Consolidado medidas de seguridad

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

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

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

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

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

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

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

Bases de datos no automatizadas				Bases de datos automatizadas		
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**	**Gestión de documentos y soportes**	**Control de acceso**	**Telecomunicaciones**
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos.	1. Definición de perfiles de usuarios acordes con su función. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando se encuentren fuera.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control mensual del registro de accesos por el responsable de administrar las bases de datos.	1. Transmisión de datos mediante redes electrónicas cifradas.

7. FUNCIONES Y OBLIGACIONES DEL PERSONAL

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

CREDIANTIOQUIA, debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, cartelera de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente documento para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.

CREDIANTIOQUIA cumple con el deber de informar con la inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos mediante comunicación informativa dirigida a los mismos.

Las funciones y obligaciones del personal de CREDIANTIOQUIA, se definen, con carácter general, según el tipo de actividad que desarrollan y, específicamente, por el contenido de este documento. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este documento por parte del personal al servicio de CREDIANTIOQUIA, es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el usuario y CREDIANTIOQUIA.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de CREDIANTIOQUIA, son las siguientes:

Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de CREDIANTIOQUIA no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

Funciones de control y autorizaciones delegadas: CREDIANTIOQUIA puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.

Obligaciones relacionadas con las medidas de seguridad implantadas:

- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
- No revelar información a terceras personas ni a usuarios no autorizados. Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.
- No sacar información de las instalaciones de la organización sin la debida autorización.

Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas.

No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los Responsables de administrar las bases de datos que podrán autorizarla y, en su caso, registrarla.

Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los Responsables de administrar las bases de datos u Oficial de protección de datos, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída de los sistemas de información o módulos que permitan el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, entre otros.

Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados.

Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en CREDIANTIOQUIA.

Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar o recuperar la contraseña, el usuario debe comunicarlo al administrador del sistema.

Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.

Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el numeral 6 del presente manual.

8. BASES DE DATOS Y SISTEMAS DE INFORMACIÓN

Las bases de datos almacenadas y tratadas por CREDIANTIOQUIA, con las siguientes características de cada una de ellas:

- Nombre de la Base de Datos
- Información contenida

- Finalidades
- Tipo de Dato
- Sistema de tratamiento
- Cantidad de Titulares
- Origen y procedencia de los datos
- Encargados del Tratamiento
- Responsable de administrar la base de datos
- Control de Acceso
- Sistema de identificación y autenticación.

Nota: El nombramiento de los Responsables de Administrar las Bases de Datos no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

CREDIANTIOQUIA identifica cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente documento.

9. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

CREDIANTIOQUIA establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

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

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

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

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

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte, se define el tipo de disposición que se le debe dar a cada uno de los documentos que se incluyen en el sistema de gestión de protección de datos.

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

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

11. DISPOSICIÓN FINAL

El presente manual ha sido aprobado por CREDIANTIOQUIA, como responsable del tratamiento de datos, aceptando su contenido, ordenando su ejecución y cumplimiento, con carácter general por todo el personal de la empresa, y en particular, por aquellos a los referidos en este documento.

12. APENDICE

No Aplica.