TABLA DE CONTENIDO

2. GLOSARIO

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El propósito de este documento es dar a conocer a los funcionarios de FIDUCIARIA CORFICOLOMBIANA S.A., la Política de Seguridad de la Información y Ciberseguridad establecida para la protección de la información.

En el presente documento se incluyen los aspectos que deben tenerse en cuenta por parte de todos los funcionarios para que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (Confidencialidad); que esté protegida contra modificaciones no autorizadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad), que sea utilizada para los propósitos que fue obtenida (Privacidad) y que se deje el rastro de los eventos que ocurren al tener acceso a la información (Auditabilidad).

Por lo tanto, los funcionarios de FIDUCIARIA CORFICOLOMBIANA S.A., deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos, ya que éstos soportan la Política de Seguridad de la Información y Ciberseguridad.

Para facilitar el cumplimiento de lo establecido en este documento, la Alta Gerencia se encargará de proveer los recursos humanos, legales, técnicos y tecnológicos, que permitan el cumplimiento de las metas y/o principios de Seguridad de la Información y Ciberseguridad, así como la definición de las responsabilidades de la organización entorno de la Seguridad de la Información y Ciberseguridad.

1.1 OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La presente Política de Seguridad de la Información y Ciberseguridad es una declaración de las políticas, responsabilidades y de la conducta aceptada para proteger la Información del Negocio en FIDUCIARIA CORFICOLOMBIANA S.A.

Esta Política establece las directrices y los lineamientos relacionados con el manejo seguro de la información, enmarcado en estándares internacionales de seguridad (v gr. ISO 27001, NIST 800-53) y en normas de entes reguladores (Superintendencia Financiera - Circular 042/2012 "Requerimientos Mínimos de Seguridad y Calidad para la Realización de Operaciones", Circular038/2009, Circular Externa 007 de 2018, Superintendencia de Industria y Comercio (SIC) – Ley 1581 de 2012 y sus decretos reglamentarios o posteriores que las deroguen o modifiquen).

1.1.1Principios

FIDUCIARIA CORFICOLOMBIANA S.A. ha establecido como fundamentales los siguientes principios que soportan la Política de Seguridad de la Información y Ciberseguridad:

- La Información es uno de los activos más importantes de FIDUCIARIA CORFICOLOMBIANA S.A. y por lo tanto debe ser utilizada acorde con los requerimientos del negocio y conservando criterios de calidad (Efectividad, Eficiencia y Confiabilidad).
- La confidencialidad de la Información del Negocio, así como aquella perteneciente a terceros debe ser mantenida, independientemente del medio o formato donde se encuentre.
- La Información del Negocio debe ser preservada en su integridad, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.

- La Información del Negocio debe estar disponible cuando sea requerida y por quienes tengan autorización de utilizarla; asimismo, presentarse de forma oportuna cuando por requisitos legales y reglamentarios así se requiera.
- La privacidad de la información de FIDUCIARIA CORFICOLOMBIANA S.A. debe ser preservada.
- Los eventos que ocurren al tener acceso a la información de FIDUCIARIA CORFICOLOMBIANA S.A. deben dejar rastro y permitir la reconstrucción, revisión y análisis de la secuencia de los mismos.

1.1.2 Objetivo General

El principal objetivo de la Política de Seguridad de la Información y Ciberseguridad, es que FIDUCIARIA CORFICOLOMBIANA S.A., se proteja frente a situaciones que representen riesgo para la Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros

1.1.3 Objetivos específicos

Los objetivos específicos que persigue La Política de Seguridad de la Información y Ciberseguridad son:

- Establecer los fundamentos para el desarrollo y la implantación del Modelo de Seguridad de la Información y Ciberseguridad;
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información que se encuentran en los aplicativos locales como en los implementados en el ciberespacio;
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio que se ejecuten en la infraestructura tecnológica local y la establecida en el ciberespacio;
- Administrar los riesgos en Seguridad de la Información y Ciberseguridad;
- Establecer los canales de comunicación que le permitan a la Gerencia General y Junta Directiva mantenerse informada de los riesgos y uso inadecuado de los activos de información que se puedan presentar en la infraestructura tecnológica local y la establecida en el ciberespacio y las acciones tomadas para su mitigación y corrección;
- Proteger la imagen, los intereses y el buen nombre de FIDUCIARIA CORFICOLOMBIANA S.A.
- Establecer las condiciones en el manejo de la información que permita a FIDUCIARIA CORFICOLOMBIANA S.A., el cumplimiento del marco normativo exigido por los entes de control que la vigilan.

1.1.4 Organización del Documento

El documento está organizado fundamentalmente en dos partes: En la primera, se describe el objetivo general de la Política de Seguridad de la Información y Ciberseguridad, sus características, los responsables y la forma en que debe ser desarrollada, implantada y mantenida. En la segunda, se desarrollan Políticas individuales, que especifican la conducta aceptada por FIDUCIARIA CORFICOLOMBIANA S.A. en el manejo de su información y las acciones que deben ser tomadas para lograr los objetivos de la presente Política.

1.2 ALCANCE

La Política de Seguridad de la Información y Ciberseguridad da las directrices requeridas para implantar un Modelo de Seguridad de la Información y Ciberseguridad confiable y flexible, define el marco básico que guiará la implantación de cualquier norma, proceso, procedimiento, estándar y/o

acción, relacionados con La Seguridad de la Información y Ciberseguridad.

Esta Política de Seguridad de la Información y Ciberseguridad aplica para todos los niveles de la organización: Usuarios (que incluye empleados y accionistas), Clientes, Terceros (que incluye proveedores y contratistas), Entes de Control, Entidades Relacionadas de FIDUCIARIA CORFICOLOMBIANA S.A.; que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación. Adicionalmente, la presente Política aplica a toda la información creada, procesada o utilizada en el soporte al negocio, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Declaración de Compromiso

Fiduciaria Corficolombiana S.A. está comprometida con la política de seguridad de la información y ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el sistema de gestión de seguridad de la información y ciberseguridad. Por lo anterior deben:

- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la política de seguridad de la información y ciberseguridad.
- Promover continuamente una cultura de seguridad de la información y ciberseguridad.
- Gestionar de manera estructurada y estratégica los riesgos de seguridad de la información y ciberseguridad asociados al negocio y su relacionamiento con terceros.

Cada colaborador, funcionario temporal y proveedor, es responsable por aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos y lineamientos establecidos en seguridad de la información y ciberseguridad, de igual forma es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

1.3 ORGANIZACIÓN Y RESPONSABILIDADES

La administración de esta Política será responsabilidad de quienes al interior de FIDUCIARIA CORFICOLOMBIANA S.A. desempeñen los roles que componen la Organización de Seguridad de la Información y Ciberseguridad así (para ampliar la información por favor referirse al reglamento "Normas de organización de Seguridad de la Información y Ciberseguridad" FID-RG-GSI-0003):

1.3.1 Comité de Seguridad de la Información y Ciberseguridad

Responsable por asegurar la planeación, implantación y mantenimiento de La Política de Seguridad de la información y Ciberseguridad; al igual que la ejecución de las acciones requeridas para mantener los niveles de seguridad establecidos en la infraestructura tecnológica local y en el ciberespacio. La conformación, atribuciones, responsabilidades y funcionamiento del comité se describen en el reglamento **"Organización de Seguridad de la Información y Ciberseguridad FIDUCIARIA CORFICOLOMBIANA S.A" FID-RG-GSI-0002.**

1.3.2 Líder de Seguridad de la Información y Ciberseguridad

El Líder de Seguridad de la Información y Ciberseguridad, será el responsable por asegurar la implantación, mejoras, mantenimiento, verificación y cumplimiento de la Política de Seguridad de la Información y Ciberseguridad y los medios requeridos para lograrlo. Uno de estos medios es la realización de un Modelo de Seguridad de la Información y Ciberseguridad, del cual debe velar por su correcto desarrollo, mantenimiento e implantación. Adicionalmente el citado

funcionario representará a FIDUCIARIA CORFICOLOMBIANA S.A. interna y externamente en todo lo referente al tema de Seguridad de la Información y Ciberseguridad.

1.3.3 Seguridad Informática y Ciberseguridad

Atendiendo los lineamientos emitidos por el área de Seguridad de la Información y Ciberseguridad, debe realizar una gestión efectiva de la Seguridad de la Información y Ciberseguridad en la infraestructura tecnológica local y la establecida en el ciberespacio para la entidad con el fin de mantener la confidencialidad, integridad y disponibilidad de la información, mediante el aseguramiento, actualización, identificación de ciberamenazas, remediación de vulnerabilidades, mantenimiento y monitoreo de los elementos físicos y lógicos necesarios para la prestación de los servicios de la entidad y los prestados a través de terceros.

Los resultados de tal gestión serán presentados semestralmente a la junta directiva a través del área de Seguridad de la Información y Ciberseguridad. Sus atribuciones, responsabilidades y funcionamiento se encuentran descritas en el documento denominado "Organización de Seguridad de la Información de Leasing Corficolombiana S.A".

1.3.4 Responsable de la Información

Todos los funcionarios de FIDUCIARIA CORFICOLOMBIANA S.A. deben ser responsables por la confidencialidad y preservación de la información. Se considera Responsable de la información, quien requiere de la información con el objetivo de llevar a cabo su negocio y quien tiene la responsabilidad de administrarla y clasificarla, acorde con la importancia que la misma tiene para su área. También debe velar por el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios para su uso.

1.3.5 Comunidad (Usuarios de la Información)

Son los demás sujetos que utilizan la información y son responsables de proteger los activos de información de FIDUCIARIA CORFICOLOMBIANA S.A. por medio del cumplimiento de La Política de Seguridad de la información y Ciberseguridad. Así mismo, deben estar alerta para identificar y reportar cualquier incumplimiento o falta de las normas o procedimientos establecidos.
FIDUCIARIA CORFICOLOMBIANA S.A. definirán los roles y responsabilidades requeridos para completar la definición de la Organización de Seguridad de la Información y Ciberseguridad, propendiendo siempre por la segregación de tareas como método para reducir los riesgos en el mal uso de la información.

1.3.6 Líneas de defensa.

Con el fin de adoptar y mantener una sólida cultura de Seguridad de la Información y Ciberseguridad, las tres líneas de defensa deben tomar la iniciativa de acuerdo con las siguientes definiciones:

1.3.6.1 Primera línea de defensa

La primera línea de defensa la constituyen las áreas de seguridad informática y todos los colaboradores de Fiduciaria Corficolombiana S.A., las políticas de seguridad de la información y ciberseguridad reconoce a las áreas de seguridad informática y demás colaboradores como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los

riesgos e incidentes de seguridad de la información y ciberseguridad inherentes a los productos, actividades, procesos y sistemas de seguridad críticos de la organización.

Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas. Así mismo deben cumplir con políticas y procedimientos definidos por la Organización, contribuyendo a una sólida cultura en Seguridad de la Información y Ciberseguridad.

1.3.6.2 Segunda línea de defensa

Esta línea de defensa está conformada por las áreas de seguridad de la información o áreas equivalentes de cada entidad, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de Riesgo en Seguridad de la Información y Ciberseguridad.

El Director SI y ITRM también puede desempeñar la función de Director de Riesgos, Director de Cumplimiento o equivalente. Este responsable debe presentar los resultados de gestión directamente a la alta Gerencia o al Comité de Auditoría. En caso de separación de tareas, la relación entre los oficiales previamente citados y sus respectivas funciones debe definirse y conocerse con claridad.

Así mismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de Seguridad de la Información derivados del negocio, incluyendo temas específicos de Ciberseguridad.

1.3.6.3 Tercera Línea de Defensa

La tercera línea de defensa juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la seguridad de la información y ciberseguridad, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control.

Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados

1.4 CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

El cumplimiento de La Política de Seguridad de la Información y Ciberseguridad con sus respectivas normas es obligatorio para la Comunidad. Cada miembro de la Comunidad debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en seguridad de la información y Ciberseguridad y la protección de los activos de información de FIDUCIARIA CORFICOLOMBIANA S.A..

Cualquier incumplimiento de esta Política que comprometa la Confidencialidad, Integridad, Disponibilidad, Privacidad y/o Auditabilidad de la información, puede resultar en una acción

disciplinaria que puede llegar hasta la terminación del contrato de trabajo y a un posible establecimiento de un proceso judicial bajo las leyes nacionales o internacionales que apliquen.

La Política de Seguridad de la Información y Ciberseguridad está basada en las mejores prácticas en seguridad de la información y está acorde con la legislación nacional e internacional y por ende tomará los pasos necesarios, incluyendo las medidas disciplinarias y/o legales aplicables, para proteger sus activos y el uso de ellos. Por lo anterior, en caso de presentarse algún incumplimiento podrán ser objeto de acciones disciplinarias por parte de Fiduciaria Corficolombiana de acuerdo con las políticas internas de la entidad relacionadas con el manejo de Incidentes de Seguridad de la Información y Ciberseguridad; sin perjuicio de la eventual responsabilidad que pudiera derivarse por el incumplimiento de la normatividad aplicable a Seguridad de la Información y Ciberseguridad.

1.5 ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO

La Política de Seguridad de la Información y Ciberseguridad se debe preservar en el tiempo. Por lo anterior, es necesario efectuar una revisión ante cambios estructurales y normativos que afecten a FIDUCIARIA CORFICOLOMBIANA S.A., para asegurar que ésta cumple con el cambio de las necesidades del negocio. El Director SI y ITRM es responsable por esta tarea y debe llevarla a cabo con la participación del Comité de Seguridad de la Información y Ciberseguridad.

Es decir, ante la necesidad de una adición o cambio en la Política, el Director SI y ITRM proyectará dichos cambios y solicitará aprobación al Comité de Seguridad de la Información y Ciberseguridad de FIDUCIARIA CORFICOLOMBIANA S. A, para su posteriormente ser aprobada por presentación ante la Junta Directiva. La publicación y divulgación de la actualización de la Política de Seguridad de la Información será realizada por el proceso encargado

Cualquier miembro de la Comunidad puede identificar la necesidad de modificar La Política de Seguridad de la Información y Ciberseguridad. Dichas inquietudes y sugerencias deben ser comunicadas al Director SI y ITRM.

1.6 EXCEPCIONES A LA POLÍTICA

No hay excepciones a la presente Política.

1.7 IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA

La Política de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un vasto programa de Seguridad de la Información y Ciberseguridad, integrado en el día a día de la operación de FIDUCIARIA CORFICOLOMBIANA S.A..

Un programa efectivo de Seguridad de la Información y Ciberseguridad es un proceso continuo, no un evento. Para lograr los objetivos establecidos en este documento, la presente Política anticipa y autoriza el desarrollo de normas, estándares, procedimientos operativos detallados y otras medidas administrativas, los cuales serán publicados para conocimiento de los funcionarios; así como el desarrollo o la adquisición de herramientas de software que ayuden a detectar o prevenir ataques contra los sistemas donde reside la información de FIDUCIARIA CORFICOLOMBIANA S.A. ya sea que se encuentre en los aplicativos locales o en el ciberespacio.

1.8 POLÍTICAS INDIVIDUALES

1.8.1 Seguridad de la Información y Ciberseguridad

Política: La información del negocio es un activo vital de FIDUCIARIA CORFICOLOMBIANA S.A. y por lo tanto debe ser protegido.

La información de FIDUCIARIA CORFICOLOMBIANA S.A., sin importar su presentación, medio o formato, en el que sea creada o utilizada para el soporte a las actividades del negocio, se califica como información del negocio o activo de información.

La Seguridad de la información y Ciberseguridad del negocio es el conjunto de medidas de protección que toma FIDUCIARIA CORFICOLOMBIANA S.A. contra la divulgación, modificación, hurto o destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los responsables de la información son los encargados de asegurar que la información del negocio, cuenta con la protección apropiada para así preservar la Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información.

FIDUCIARIA CORFICOLOMBIANA S.A. debe disponer de los medios necesarios para asegurarse de que cada miembro de la Comunidad preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de una acción disciplinaria inmediata.

FIDUCIARIA CORFICOLOMBIANA S.A. debe contar con una estructura organizacional de seguridad la información y Ciberseguridad que permita gestionar y controlar lo dispuesto en el Modelo de Seguridad de la Información y Ciberseguridad.

1.8.2 Propiedad Intelectual

Política La propiedad de la información se debe mantener

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención ó información que es propiedad de FIDUCIARIA CORFICOLOMBIANA S.A.. Todo el material que es desarrollado mientras se trabaja para FIDUCIARIA CORFICOLOMBIANA S.A. se considera que es de su propiedad intelectual y de uso exclusivo de la misma, por lo tanto, debe ser protegido contra un develado, descubrimiento o uso que menoscabe la competitividad de FIDUCIARIA CORFICOLOMBIANA S.A.

1.8.3 Responsables de la Información

Política: Cada activo de información de FIDUCIARIA CORFICOLOMBIANA S.A. debe tener un responsable que debe velar por su seguridad con base en los riesgos a los que está expuesta.

FIDUCIARIA CORFICOLOMBIANA S.A. utiliza información para realizar sus actividades. Esta se crea y se entrega a cada miembro de la Comunidad para que pueda desarrollar y cumplir sus respectivas metas dentro del marco del negocio.

La información que FIDUCIARIA CORFICOLOMBIANA S.A. utilice para el desarrollo de sus objetivos de negocio debe tener asignado un responsable, quién la utiliza en su área y es el responsable por su correcto uso. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso. En FIDUCIARIA

CORFICOLOMBIANA S.A actuarán como Responsables de la información, los Responsables de los procesos o a quienes éstos deleguen.

1.8.4 Cumplimiento de Regulaciones

Política: FIDUCIARIA CORFICOLOMBIANA S.A. debe cumplir con las regulaciones locales e internacionales de Privacidad y Seguridad de la Información y Ciberseguridad.

La Política de Seguridad de la Información y Ciberseguridad está acorde y apoya el cumplimiento de las leyes y regulaciones locales e internacionales relativas a la privacidad, seguridad de la Información y la Ciberseguridad. Por lo tanto, tales requerimientos deben ser incluidos en el desarrollo del Modelo de Seguridad de la Información y Ciberseguridad y se deben establecer acciones específicas para mantener alineada permanentemente a FIDUCIARIA CORFICOLOMBIANA S.A. con tales disposiciones.

Ejemplos de dichas disposiciones son la reserva bancaria, el licenciamiento de software, las circulares de la Superintendencia Financiera y las provenientes de grupos Internacionales como el Grupo de Supervisión a las Entidades Financieras de Basilea. Así mismo y con el fin de mantener un buen nivel de seguridad, esta Política se debe apoyar en las mejores prácticas de Seguridad de la Información y de la Ciberseguridad.

1.8.5 Administración del Riesgo en Seguridad de la Información y Ciberseguridad.

Política: Los Riesgos de Seguridad de la Información y Ciberseguridad a que está expuesta la información de FIDUCIARIA CORFICOLOMBIANA S.A. deben ser identificados, evaluados y mitigados acorde con su valor, probabilidad de ocurrencia e impacto en el negocio.

La información del negocio se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, a través del Comité de Seguridad de la Información y Ciberseguridad, se debe realizar periódicamente un análisis del estado del negocio frente a la Seguridad de la Información y la Ciberseguridad, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo Responsable.

Establecidos el nivel de riesgo y el valor de la información, cada Responsable debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por FIDUCIARIA CORFICOLOMBIANA S.A.

Cada usuario de la información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la Seguridad de la Información y la Ciberseguridad de FIDUCIARIA CORFICOLOMBIANA S.A., y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la Seguridad de la Información y Ciberseguridad.

1.8.6 Capacitación y creación de cultura en Seguridad de la Información y Ciberseguridad.

Política: FIDUCIARIA CORFICOLOMBIANA S.A. debe establecer un programa permanente de creación de cultura en Seguridad de la Información y Ciberseguridad para los usuarios y terceros.

FIDUCIARIA CORFICOLOMBIANA S.A. debe contar con un programa permanente que permita asegurar que los usuarios y terceros están informados acerca de sus responsabilidades en Seguridad de la Información y Ciberseguridad, y de las continuas amenazas que ponen en riesgo la información que maneja.

Los funcionarios y terceros deben estar enterados de los procedimientos de Seguridad de la Información y Ciberseguridad que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo. Como parte de su programa de capacitación, el nuevo personal debe asistir durante el periodo de inducción, a una charla sobre los requerimientos de Seguridad de la Información y Ciberseguridad de FIDUCIARIA CORFICOLOMBIANA S.A..

1.8.7 Seguridad en el personal

Política: FIDUCIARIA CORFICOLOMBIANA S.A. debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades en Seguridad de la Información y Ciberseguridad desde su ingreso hasta su retiro.

Los empleados que ingresen a FIDUCIARIA CORFICOLOMBIANA S.A. deben seguir un proceso de selección, y una vez vinculados, recibirán copia del documento "Política de la Seguridad de la Información y Ciberseguridad" para su conocimiento y certificación.

Los contratos de los empleados deben incluir cláusulas que indiquen las responsabilidades correspondientes para con la Seguridad de la Información y Ciberseguridad y el cumplimiento del código de conducta, haciéndole conocer las consecuencias en caso de no ser seguidas y cumplidas.

Se debe mantener un registro por empleado de su conocimiento y entendimiento de la Política de Seguridad de la Información y Ciberseguridad, mediante la certificación de este documento y las demás normas y procedimientos que se expidan al respecto.

FIDUCIARIA CORFICOLOMBIANA S.A. desarrollará un programa de manejo de sugerencias en Seguridad de la Información y Ciberseguridad, por medio del cual los empleados reportarán vulnerabilidades y riesgos que detecten.

1.8.8 Terceros que acceden a la información de FIDUCIARIA CORFICOLOMBIANA S.A. de forma local o remota en los aplicativos locales o en el ciberespacio

Política: Los Terceros que utilizan local o remotamente información de FIDUCIARIA CORFICOLOMBIANA S.A. deben cumplir con la Política de Seguridad de la Información y Ciberseguridad.

El uso de la información de FIDUCIARIA CORFICOLOMBIANA S.A. por Terceros, ya sea que se encuentre en los aplicativos locales o en el ciberespacio y acceda de forma local o remota, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política. En los contratos de servicios se debe incluir un acuerdo formal de Niveles de Servicios en Seguridad de la Información y Ciberseguridad, que detalle su obligación en la protección de la información de FIDUCIARIA CORFICOLOMBIANA S.A., los requisitos de seguridad para mitigar los riesgos de Seguridad de la Información y Ciberseguridad sobre la información y las consecuencias a que estarían sujetos en caso de incumplirlos. El cumplimiento de los Niveles de Servicios en Seguridad de la Información y Ciberseguridad con terceros debe ser verificado periódicamente.

Cada relación con un tercero, debe tener un representante de alto nivel (Gerente Administrativo y/o Gerente Jurídico) dentro de FIDUCIARIA CORFICOLOMBIANA S.A., que vele por el correcto uso y la protección de la información del negocio. Por lo anterior, y dadas las características de los negocios que se manejan en FIDUCIARIA CORFICOLOMBIANA S.A., donde terceros suministran información financiera para procesos de análisis y valoración, deberán suscribirse los acuerdos de confidencialidad respectivos con el fin de garantizar que la información suministrada se conserve en reserva.

1.8.9 Identificación y Autenticación Individual

Política: Todos los usuarios que acceden la información de FIDUCIARIA CORFICOLOMBIANA S.A. deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal.

Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de FIDUCIARIA CORFICOLOMBIANA S.A. ya sea local o en el ciberespacio. Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser establecida y autenticada de una manera única y no podrá ser compartida.

Los usuarios de FIDUCIARIA CORFICOLOMBIANA S.A. una vez creados y asignadas sus autorizaciones en el Sistema de Información, podrán acceder a la información mediante su usuario y clave de autenticación. Dependiendo del valor de la información y del nivel de riesgo, FIDUCIARIA CORFICOLOMBIANA S.A. definirán medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

1.8.10 Control y Administración del Acceso a la Información local o en el ciberespacio

Política: El uso de la información de FIDUCIARIA CORFICOLOMBIANA S.A. debe ser controlado para prevenir accesos no autorizados. Los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a lo que es requerido.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos localmente o en el ciberespacio de una manera consistente con su valor para el negocio y con los riesgos de pérdida de Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información.

Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso a la información de FIDUCIARIA CORFICOLOMBIANA S.A. deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de FIDUCIARIA CORFICOLOMBIANA S.A. debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.

1.8.11 Clasificación de la información

Política: Los Responsables de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida o compromiso, y/o requerimientos legales de retención.

Al igual que otros activos, no toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Toda la información de FIDUCIARIA CORFICOLOMBIANA S.A. será clasificada por el Responsable del Proceso de la Información con base en un análisis de alto nivel del impacto al negocio en Seguridad de la Información y Ciberseguridad, que determine su valor relativo y nivel de riesgo a que está expuesta.

Según los riesgos que se detecten, el Responsable de la información y el Líder de Seguridad de la Información y Ciberseguridad, determinarán los controles que sean necesarios para proveer un nivel de protección de la información apropiado y consistente en toda la FIDUCIARIA CORFICOLOMBIANA S.A, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Por lo tanto, no se debe asumir que otros protegen la información, ya que es deber de los funcionarios de FIDUCIARIA CORFICOLOMBIANA S.A., tomar las medidas necesarias para proteger la información.

De acuerdo a la clasificación de la información y a los riesgos a los que está expuesta, se deben implementar controles de cifrado durante los procesos de transmisión y almacenamiento de la misma.

1.8.12 Continuidad del Negocio

Política: Todos los recursos de información y los procesos asociados ya sean locales o en el ciberespacio, deben contar con un Plan de Continuidad del Negocio y estar preparados para ataques a la Seguridad de la Información y Ciberseguridad. La continuidad de la gestión de la Seguridad de la Información y Ciberseguridad se mantiene durante situaciones de contingencia.

La información debe estar disponible para su uso autorizado cuando FIDUCIARIA CORFICOLOMBIANA S.A. la requiera en la ejecución de sus tareas regulares. Por lo que se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de FIDUCIARIA CORFICOLOMBIANA S.A., tanto localmente como en el ciberespacio, sin disminuir los niveles de seguridad establecidos.

Esto debe ser independiente tanto del medio tecnológico que utilice FIDUCIARIA CORFICOLOMBIANA S.A. como de la posibilidad de que la información se dañe, se destruya o no esté disponible por un lapso de tiempo.

FIDUCIARIA CORFICOLOMBIANA S.A. establecerán medidas de reacción inmediata que permitan detectar y mitigar los efectos de ataques en Seguridad de la Información y Ciberseguridad como son los de negación de servicios y el ingreso de código no autorizado. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informada a FIDUCIARIA CORFICOLOMBIANA S.A. de la existencia de estas amenazas, detectar los ataques de manera inmediata y ejecutar las acciones consiguientes.

1.8.13 Seguridad Física

Política: Todas las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas. La información confidencial o sensitiva al negocio debe mantenerse en lugares con acceso restringido

cuando no es utilizada. Todos los funcionarios deben cumplir con las directrices para la protección física de la información Restringida o Sensitiva que usen.

Las áreas físicas construidas para soportar toda la operación del negocio, deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, entre otros) según el valor de la información que contienen.

Los recursos informáticos de FIDUCIARIA CORFICOLOMBIANA S.A. deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de negocio.

La información clasificada como confidencial o restringida no se dejará desatendida o sin control, por lo que FIDUCIARIA CORFICOLOMBIANA S.A. desarrollarán un programa que permita prevenir que la información crítica del negocio sea accedida sin autorización, dentro de lo cual está comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.

1.8.14 No repudio

Política: La autenticidad de un negocio o transacción electrónica que realice FIDUCIARIA CORFICOLOMBIANA S.A. debe ser asegurada ya sea localmente o en el ciberespacio.

FIDUCIARIA CORFICOLOMBIANA S.A. se está apoyando día a día más en los medios electrónicos para realizar su negocio. Por lo tanto para cualquier negocio o transacción que se haga por estos medios, FIDUCIARIA CORFICOLOMBIANA S.A. debe asegurar la autenticidad de cada parte que interviene y evitar que alguna de ellas niegue su participación (no repudio).

Al realizar negocios electrónicos ya sea localmente o en el ciberespacio, se deben generar rastros que le permitan a FIDUCIARIA CORFICOLOMBIANA S.A. resolver conflictos cuando alguna de las partes niegue su participación. Estos se deben generar, guardar y ser accedidos acorde con las Políticas y las Normas que regulen estos aspectos en FIDUCIARIA CORFICOLOMBIANA S.A.

1.8.15 Administración de Alertas

Política: FIDUCIARIA CORFICOLOMBIANA S.A. debe ser alertada en el mismo instante en que existan violaciones a la Política de Seguridad de la Información y Ciberseguridad.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas e informadas a la Gerencia General de FIDUCIARIA CORFICOLOMBIANA S.A. de manera inmediata (alertas). Se debe desarrollar un programa de manejo de eventos e incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información para FIDUCIARIA CORFICOLOMBIANA S.A. Dicho programa debe incluir la definición de una organización de reacción inmediata, con el objetivo de atender éstas y otras situaciones que FIDUCIARIA CORFICOLOMBIANA S.A. consideren como críticas.

1.8.16 Auditabilidad de los eventos de Seguridad de la Información y Ciberseguridad

Política: Los registros de Seguridad de la Información y Ciberseguridad de FIDUCIARIA CORFICOLOMBIANA S.A. deben ser revisados permanentemente para asegurar el cumplimiento del Modelo de Seguridad de la Información y Ciberseguridad.

Los responsables de la Información deben definir los eventos considerados como críticos (por ejemplo: intentos de acceso fallidos al sistema de información, borrado o alteración de información, entre otros) y los respectivos registros de Seguridad de la Información y Ciberseguridad que deben ser generados. Los registros de seguridad deben ser activados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera oportuna a los responsables, así como a los niveles requeridos. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas.

1.8.17 Conectividad

Política: Todas las conexiones a redes públicas deben ser autenticadas para prevenir que la información sea develada o alterada.

Las conexiones a la red privada de FIDUCIARIA CORFICOLOMBIANA S.A. deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida al ciberespacio y a otras empresas deben realizarse sobre redes aprobadas por FIDUCIARIA CORFICOLOMBIANA S.A.

Los miembros de la Comunidad que se conecten a la red privada deben cumplir con la presente Política antes de que se realice la conexión. Esto aplica igualmente a cualquier conexión actual o futura en la red de FIDUCIARIA CORFICOLOMBIANA S.A., que utilice redes públicas.

Se requiere la aprobación del responsable de la información para poder acceder remotamente la información de FIDUCIARIA CORFICOLOMBIANA S.A., y dichos accesos deben cumplir con la Política de Identificación y Autenticación.

1.8.18 Uso de los recursos informáticos del negocio local y en el ciberespacio, de dispositivos móviles y de trabajo móvil

Política: Los recursos informáticos locales y en el ciberespacio son provistos a la Comunidad para uso exclusivo del negocio.

Los recursos informáticos de FIDUCIARIA CORFICOLOMBIANA S.A. tanto locales como en el ciberespacio, son exclusivamente para propósitos del negocio y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Miembros de la Comunidad que intenten acceder información para la que no tienen un requerimiento autorizado de negocio, están violando la presente Política.

En el uso de la información de FIDUCIARIA CORFICOLOMBIANA S.A. no se debe presumir privacidad, por lo que cuando ésta sea utilizada se podrán crear registros de la actividad realizada, que pueden ser revisados por FIDUCIARIA CORFICOLOMBIANA S.A. de acuerdo con los dispuesto en el documento que contiene las Normas de Seguridad de la Información y Ciberseguridad, que deben ser conocidas y aceptadas por todos los funcionarios. En caso de ser así, se ejecutarán los procedimientos correspondientes acorde con las regulaciones de FIDUCIARIA CORFICOLOMBIANA S.A.

FIDUCIARIA CORFICOLOMBIANA S.A. se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado por FIDUCIARIA CORFICOLOMBIANA S.A. podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa

autorización formal del Lider de Seguridad de la Información y Ciberseguridad o el Gerente Corporativo de Servicios de TI y Administrativos de Corficolombiana.

Para acceder a la información tanto local como en el ciberespacio de FIDUCIARIA CORFICOLOMBIANA S.A. a través de medios tales como los dispositivos móviles o trabajo móvil, se deben implementar los controles necesarios para reducir los riesgos introducidos por estas prácticas.

1.8.19 Seguridad de Información y Ciberseguridad en los procesos de Administración de Sistemas.

Política: Cada proceso de Administración de sistemas de FIDUCIARIA CORFICOLOMBIANA S.A. debe cumplir con la Presente Política de seguridad de la información y Ciberseguridad.

Actividades, normas y responsabilidades en Seguridad de la Información y Ciberseguridad deben ser incluidas dentro de cada uno los procesos de administración de sistemas de FIDUCIARIA CORFICOLOMBIANA S.A., para lograr el cumplimiento de la Política y las Normas de Seguridad de la Información y Ciberseguridad.

El área de desarrollo e innovación de TI debe crear y mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas e infraestructura. Los requerimientos de Seguridad de la Información y Ciberseguridad deben ser identificados previo al diseño y desarrollo de los sistemas de tecnología de la información y ciberseguridad. Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de desarrollo seguro y seguridad de la información y ciberseguridad que han sido previamente establecidos.

El nivel de Seguridad de la Información y Ciberseguridad de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

La implantación de un sistema nuevo o cambio significativo a los existentes, debe ser revisada por medio de una evaluación de riesgo, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen o eliminen y la operación segura.

La realización de un cambio tecnológico que no considere los requerimientos de Seguridad de la Información y Ciberseguridad hace que FIDUCIARIA CORFICOLOMBIANA S.A. esté expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad y sus respectivas normas, y en caso de exponer a FIDUCIARIA CORFICOLOMBIANA S.A. a un riesgo en Seguridad de la Información y/o Ciberseguridad, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo responsable de la Información.

El proceso de Administración de problemas registra, asigna, hace seguimiento y resuelve situaciones (problemas) que comprometen la disponibilidad de los servicios que provee tecnología al negocio. Las fuentes de este proceso son los problemas derivados de situaciones que rompen o comprometen la Política de Seguridad de la Información y Ciberseguridad.

Por lo tanto, todos los problemas de Seguridad de la Información y Ciberseguridad de FIDUCIARIA CORFICOLOMBIANA S.A. deben ser administrados por este proceso, el que con base en un análisis posterior determinará si corresponden a violaciones, problemas o vulnerabilidades

en Seguridad de la Información y/o Ciberseguridad, dando paso a los procedimientos establecidos para cada caso.

Las actividades realizadas por el personal técnico vinculado a la Corporación Financiera Corficolombiana se desarrollarán enmarcados en los acuerdos de colaboración empresarial existentes entre la Corporación y FIDUCIARIA CORFICOLOMBIANA S.A.

2. GLOSARIO.

Las siguientes definiciones son algunos de los conceptos usados dentro del Documento de Política de Seguridad de la Información y Ciberseguridad, los cuales se distinguen en el texto por iniciar con mayúscula y con los que los miembros de la Comunidad deben estar familiarizados:

ACTIVO DE INFORMACIÓN: conjunto de datos con un contexto dato que vale la pena identificar, clasificar y proteger de acuerdo con su valor, criticidad y nivel de exposición.

CIBERAMENAZA O AMENAZA CIBERNÉTICA: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar un ciberataque contra la población, el territorio y la organización política del Estado.

CIBERATAQUE O ATAQUE CIBERNÉTICO: Acción organizada o premeditada de uno o más agentes para causar daño o problemas a un sistema a través del ciberespacio.

CIBERESPACIO: Corresponde a un ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado en dispositivos tecnológicos y redes conectadas a la red mundial, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios.

CIBERIESGO O RIESGO CIBERNÉTICO: Posibles resultados negativos asociados a los ataques cibernéticos.

CIBERNÉTICA: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnicas de funcionamiento de las conexiones de los seres vivos y de las máquinas.

CIBERSEGURIDAD: Es el conjunto de políticas, conceptos de seguridad, recursos, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos, con el fin de proteger a los consumidores financieros y los activos de la entidad en el ciberespacio.

CIRCULAR 052/2007: Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios de comunicación de canales de distribución de productos y servicios.

CIRCULARES 014 - 038/2009: Instrucciones relativas a la revisión y adecuación del sistema de control interno (SCI)

CIRCULAR 022/2010: Requerimientos mínimos de Seguridad y Calidad para la realización de Operaciones.

CONTROLES:

- Son las políticas, procedimientos y actividades implementados o no, que proporcionan reducción de la probabilidad y el impacto de los riesgos.(AUDITORIA)

- Salvaguardas basadas en dispositivos o mecanismos que se requieren para cumplir con los requisitos de una política.(ADMINISTRATIVO)

CONFIABILIDAD: La información debe ser la apropiada para la administración de la Entidad y el cumplimiento de obligaciones.

CONFIDENCIALIDAD: Es la reserva o secreto que se deben guardar los funcionarios sobre la información de los clientes y sobre los reportes de información de clientes a las autoridades, articulo 105 Decreto 663 de 1993.

DISPONIBILIDAD: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

EFECTIVIDAD: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

EFICIENCIA: Relación entre el resultado alcanzado y los recursos utilizados. Definición tomada de la Norma Técnica Colombiana NTC-ISO9000:2000, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) 2000/12/15

ESCRITORIO LIMPIO: Mantener en el escritorio únicamente los materiales, información y documentos que requiere el funcionario para el trabajo que está realizando, investigando, consultando o elaborando.

EVENTO DE CIBERSEGURIDAD: Ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad.

INFORMACIÓN DEL NEGOCIO: Es toda aquella que sin importar su presentación, medio o formato, en el que sea creada o utilizada, sirve de soporte a las actividades de negocio y la toma de decisiones. Esta definición aplica para las partes del documento donde se cite la frase Información del Negocio.

INFORMACIÓN EN REPOSO: Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, bases de datos, almacenes de datos, hojas de cálculo, archivos, cintas, copias de seguridad externa, dispositivos móviles, discos duros, entre otros).

INFORMACIÓN EN TRÁNSITO: Información que fluye a través de la red pública o que no es de confianza, como Internet y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.

INTEGRIDAD: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

INTERNET: Es la conexión lógica de múltiples redes de comunicaciones, las cuales utilizan como estándar el protocolo TCP/IP para comunicarse y compartir datos entre dichas redes.

MIEMBRO DE LA COMUNIDAD: Un individuo que tiene autoridad limitada y específica del dueño (Responsable) de información para ver, modificar, adicionar, divulgar o eliminar información.

MODELO DE SEGURIDAD DE LA INFORMACIÓN: Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad, elementos de seguridad y topologías que garantizan la protección de la información del negocio.

NORMA: conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnología, metodología, procedimientos de aplicación y otros factores involucrados y son de obligación cumplimiento.

NTC-ISO/IEC 27001: Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos

ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN: Estructura organizacional que soporta la Seguridad de la Información, donde se definen roles y responsabilidades de cada uno de sus integrantes.

PANTALLA LIMPIA: Mantener en el escritorio del equipo de cómputo asignado la información que requiera para sus labores. Si la información es restringida y debe mantener copias de respaldo, debe ser almacenada preferiblemente en las carpetas de red que dispone la organización para este fin.

PERIMETROS Ó AREAS SEGURAS: Un área o agrupación dentro de la cual un conjunto definido de políticas de seguridad y medidas se aplica, para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para agrupar entidades con requisitos de seguridad y niveles de riesgo similares, para asegurar que cada zona se separa adecuadamente de las otras.

POLITICA: Documento que contiene la filosofía, los parámetros y las condiciones generales para el ejercicio de las actividades de la organización.
Es un conjunto de ordenamientos y lineamientos enmarcados, en los diferentes instrumentos jurídicos y administrativos que rigen una función, en este caso la Seguridad de la Información y ciberseguridad.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN: Documento donde establece las directrices y los lineamientos relacionados con el manejo seguro de la información en FIDUCIARIA CORFICOLOMBIANA S.A.

PROCEDIMIENTO: Forma específica para llevar a cabo una actividad o un proceso. Definición tomada de la Norma Técnica Colombiana NTC-ISO9000:2000, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) 2000/12/15.

Pasos operacionales específicos que los individuos deben tomar para lograr las metas definidas en las políticas.

RECURSOS DE INFORMACIÓN: Dispositivos o elementos que almacenan datos, tales como: registros, archivos, Bases de Datos, equipos y el software propietario o licenciado por FIDUCIARIA CORFICOLOMBIANA S. A.

RESPONSABLE DE LA INFORMACIÓN: Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información. También es el primer responsable de implantar la Política de Seguridad de la Información y ciberseguridad dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios que requieren para su uso.

RIESGO: La probabilidad de que ocurra un evento en seguridad de la información, que cause pérdida a FIDUCIARIA CORFICOLOMBIANA S. A. Es la probabilidad de ocurrencia de un evento. Ejemplo Riesgo de una caída o el riesgo de ahogamiento (R. Humano.)

SEGURIDAD DE LA INFORMACIÓN: Protección de la información contra el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación.

SEGURIDAD FISICA: Protección de los equipos de procesamiento de la información de daños físicos, destrucción o robo; asimismo, se protege al personal de situaciones potencialmente dañinas.

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT): Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de logs.

SOC (SECURITY OPERATION CENTER): Entidad o dependencia, donde los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos) son monitoreados, evaluados y defendidos.

TERCEROS CRÍTICOS: Terceros con quien se vincula la entidad y que pueden tener incidencia directa en la seguridad de su información.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

3. REGULACIÓN.

En Fiduciaria Corficolombiana se deben cumplir con las regulaciones de Seguridad de la Información y Ciberseguridad vigentes en el país y con regulaciones internacionales que se le obliguen a adoptar, como ejemplo se encuentran:

• **Circular 007 de 2018 de SFC PARTE I - TITULO IV - CAPITULO V:** Requerimientos mínimos para la gestión de la Seguridad de la Información y la Ciberseguridad.

• **Circular 029 de 2019 de la SFC:** Modifica la Circular Básica Jurídica en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones y acceso e información al consumidor financiero y uso de factores biométricos.

• **Circular 005 de 2019 de la SFC:** Imparte instrucciones relacionadas con el uso de servicios de computación en la nube.

• **Circular Básica Jurídica Parte I, Título II, Capítulo I:** Canales, Medios, Seguridad y Calidad en el manejo de la información en la prestación de servicios financieros.

• **Circular 014-038/2009:** Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI).

• **Ley 1581 de 2012 (Habeas Data):** Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.

• **Ley 1273 de 2009:** Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

• **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

• **Ley SOX:** Ley federal de los Estados Unidos de América emitida en 2002 que tiene como objetivo

mejorar el ambiente de control interno de las empresas que cotizan en las bolsas de valores de los estados unidos; definir y formalizar responsabilidades sobre su cumplimiento para la prevención de errores contables y de reporte.

• **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en

ANEXOS

Acta 281 del 29 Julio de 2011
Acta 300 del 14 Diciembre de 2012
Acta 330 del 18 de marzo de 2015
Acta 374 del 15 de noviembre de 2018

LISTA DE VERSIONES

VERSION	FECHA DE ELABORACIÓN	RAZON DE LA ACTUALIZACION
1	30/Jun/2010	Creación del documento Aprobado en la Junta Directiva de Julio 29/2011 - # acta 281 * Revisión de la política por parte del Oficial de Seguridad de la información fecha: 29 Julio 2011, donde se concluye que no es necesario ninguna modificación.
2	06/Jul/2012	Revisión de la política por parte del Oficial de Seguridad de la información fecha: 27 Junio 2012 se incluye en el numeral 1.1 "Objetivo de la Política de Seguridad de la Información" la Circular Externa 022/2010 antes 052/2007
3	09/Ene/2013	Ratificación aprobación Política en acta 281 de 29 de julio de 2011
4	20/Feb/2013	Actualización Política en Acta 300 de 14 Diciembre 2012, Modificación punto 1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN y 1.1 OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
5	14/Abr/2015	Se actualiza el documento para alinearlo con la nueva versión de la norma ISO 27001:2013 y con nuevas directrices de Seguridad de la Información (Ej: Ley de Protección de Datos Personales). Actualización de acuerdo al acta 330 de 18 del marzo de 2015.
6	30/Nov/2018	Viene del documento FID-PO-GSI-002 " POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA FIDUCIARIA CORFICOLOMBIANA S.A_V5 Se actualiza la política incluyendo lo relacionado con los temas de ciberseguridad para dar cumplimiento con lo requerido en la CE 007 de 2018 emitida por la

		Superfinanciera. Se incluyen las circulares 029/2014 parte I, Título II, capítulo I (Circulares predecesoras: 052/2008, Circular 022/2010 y 042/2012 y se retira la circular 022/2010. Se incluyen como nuevas definiciones NIST 800-53, Ciberseguridad, Ciberespacio, Ciberamenaza o amenaza cibernética, Cibernetica, Ciberiesgo o riesgo cibernético, evento de ciberseguridad, SIEM, SOC, Vulnerabilidad, Información en reposo, Información en tránsito, Terceros críticos. Actualización de acuerdo al acta 374 del 15 de noviembre de 2018
7	31/May/2021	Revisión, actualización y alineamiento con la Política Corporativa de Seguridad de la Información y Ciberseguridad del Grupo AVAL, así: Inclusión de la Declaración de Compromiso, donde se menciona que Fiduciaria Corficolombiana y sus Entidades Subordinadas están comprometidas con la política de seguridad de la información y ciberseguridad. Incluir en el numeral 1.3.6 los conceptos de las tres líneas de defensa. Se realizan ajustes en el contenido del numeral 1.5 Administración de la Política y Procedimiento de Cambio. Aprobado mediante acta 404 de la junta directiva realizada el 27 de Mayo de 2021
8	21/Abr/2022	Se actualiza la política de seguridad de la información incluyendo los siguientes cambios: Se complementa el numeral 1.3.6.1 Primera línea de defensa, teniendo en cuenta los productos, actividades, procesos y sistemas de seguridad críticos de la organización, adicionalmente se incluye que se deben cumplir con políticas y procedimientos definidos por la Organización, contribuyendo a una sólida cultura en Seguridad de la Información y Ciberseguridad. Se complementa el numeral 1.4 “Cumplimiento y Manejo de Violaciones a la Política”, aclarando las acciones a tomar cuando se presente algún incumplimiento de La Política de Seguridad de la Información y Ciberseguridad. Se elimina la palabra "anual" del numeral 1.5 con respecto a la revisión de cambios estructurales y normativos. En el capítulo dos (2) Glosario, se incluyen las definiciones “Activo de Información” "Escritorio Limpio" y se complementa la definición de “Responsable de la información”.

		Se incluye el capítulo tres (3) Regulación, con las normas de Seguridad de la Información y Ciberseguridad vigentes en el país y regulaciones internacionales que se le obliguen a adoptar. Lo anterior aprobado mediante el acta N° 415 de la junta directiva realizada el 21 de Abril de 2022

ELABORO		REVISO		APROBO	
Nombre:	Alieth Gomez Gonzalez	**Nombre:**	Martha Isabel Gonzalez Cristancho	**Nombre:**	Roberto Carlos Loaiza Zuluaga
Cargo:	ANALISTA DE PRODUCTIVIDAD-USC	**Cargo:**	ANALISTA SI Y TRM I	**Cargo:**	DIRECTOR SI, ITRM
Fecha:	20/May/2022	**Fecha:**	25/May/2022	**Fecha:**	31/May/2022