CAJA DE COMPENSACIÓN FAMILIAR DE BOYACÁ

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

GRUPO DE SISTEMAS COMFABOY

1. DERECHOS DE AUTOR

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

2. INTRODUCCION

La información de la Caja de Compensación Familiar de Boyacá, es considerada por el Grupo Administrativo de la entidad como un activo de alta prioridad, pues es a través de esta que se alcanza el desarrollo de la misión y el cumplimiento del objetivo de la misma. Es por esta razón que surge la necesidad de implementar las políticas que brinden la debida protección de la confidencialidad, integridad y disponibilidad de dicha información durante todo su ciclo de vida, aunado al correcto tratamiento de datos personales, derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos de propiedad de COMFABOY, o cuyo tratamiento haya sido encargado a COMFABOY, y los demás derechos, libertades y garantías constitucionales, de conformidad con la Ley 1581de 2012 y su Decreto reglamentario 1377 de 2013.

En el presente documento se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los trabajadores, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación la Entidad. Estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013

3. OBJETIVO

Establecer las políticas que regulan la seguridad de la información y tratamiento de datos personales, en forma clara y coherente, las cuales deben ser conocidas y acatadas por todos los trabajadores, contratistas, visitantes y terceros que presten sus servicios a la Caja de Compensación

4. ALCANCE

Las Políticas de Seguridad de la Información y tratamiento de datos personales son aplicables para todos los aspectos administrativ
os y de control que deben ser cumplidos por los directivos, trabajadores, contratistas y terceros, para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas.

5. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas se aplican y son de obligatorio cumplimiento para los Consejeros, Dirección, Jefes de División, Jefes de Área,

trabajadores, contratistas, y en general a todos los usuarios de la información. Que permitan el cumplimiento de los propósitos generales de la empresa.

6. TÉRMINOS Y DEFINICIONES

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las es
trategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

APT: (Advance Persistent Threat) Amenaza Avanzada Persistente Especie de ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.

Administración de incidentes de seguridad: herramientas de control y procedimientos enfocados a una correcta valoración de las amenazas existentes. Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización –tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Impacto: Resultado de un incidente de seguridad de la información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Plan de continuidad del negocio (BussinesContinuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risktreatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social
caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante en cripta los datos de la víctima y exige un pago por la clave de descifrado.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/IEC 27002:2013]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computa
dor personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

7. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

La Dirección de COMFABOY, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con sus afiliados, organismos de vigilancia y control y demás partes interesadas, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para COMFABOY, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus trabajadores, terceros, aprendice
s, practicantes, proveedores empleadores y afiliados en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los trabajadores, terceros, aprendices, practicantes y clientes de COMFABOY
- Garantizar la continuidad del negocio frente a incidentes.
- COMFABOY ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

COMFABOY en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información, crea un esquema de seguridad
de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la creación del Comité y el Administrador de Seguridad de la Información.

El Grupo de Sistemas debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información a los trabajadores disponibles, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

8.2 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

COMFABOY establece mediante el reglamento interno que es el dueño del desarrollo de los avances tecnológicos e intelectuales desarrollados por los trabajadores y contratistas, derivadas del objeto y del cumplimiento de sus funciones.

COMFABOY mantiene un inventario actualizado mediante el software de gestión de activos quedando bajo la responsabilidad de cada propietario y centralizado por el Grupo de Sistemas.

8.3 POLÍTICA DE USO DE LOS ACTIVOS

La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de los equipos o discos virtuales de red, archivos de vídeo, músic
a, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "smartphones", tabletas), ya sean suministrados por la empresa o dispositivos personales que hagan uso de los servicios de información de la Entidad.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles.

8.5 POLÍTICA DE SEGURIDAD PARA LOS RECURSOS HUMANOS

COMFABOY implementa acciones para asegurar que los trabajadores, contratistas y demás colaboradores de la Entidad, entiendan sus responsabilidades, como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

8.6 POLÍTICA DE USO DE INTERNET.

COMFABOY permite el acceso a internet, estableciendo parámetros que garanticen la navegación segura y el uso adecuado de

la red
por parte de los usuarios, evitando pérdidas, modificaciones no autorizadas o el uso inadecuado de la información en las aplicaciones.

El jefe del Grupo Sistemas establecerá las políticas de navegación basada en niveles de usuario, por jerarquía, categorías y funciones; con previa autorización del jefe de cada una de las dependencias.

El área de Sistemas implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en internet para prevenir la fuga de información.

Los usuarios tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a Jefe del Grupos Sistemas, para que sea autorizado y será objeto de auditorías de seguridad mediante el módulo de seguridad web de la entidad.

8.7 POLÍTICA DE MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

La entidad establece planes para evitar la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena y procesa la información, deben mantenerse con las medidas de protección físicas y lógic
as, que permitan su monitoreo y correcto estado, para ello se realizan los mantenimientos preventivos y correctivos que se requieran según lo establecido en el manual de mantenimiento de equipos P-21-028

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

Se debe realizar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el trabajador haya sido retirado de la entidad, de acuerdo a lo definido en las Políticas generales gestión tecnológica_v3 D-21-014

8.8 POLÍTICA DE CONTROL DE ACCESO.

La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información, considerándolas como importantes para el SGSI.

La conexión remota a la red de área local debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el Grupo Sistemas.

Todo aplicativo informático o software debe ser comprado o aprobado por el Grupo Sistemas en concordancia con la política de Adquisición de bienes de informática y sistemas.

Las políticas se encuentran definidas en las Políticas generales gestión tecnológica_v3 D-21-014, Adquisición de equipos de cómputo
y comunicaciones y contratación de servicios especializados P-21-032, Adquisición de software P-21-035.

8.9 POLÍTICA DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO.

El Grupo Sistemas suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

Ningún usuario deberá acceder a los aplicativos, utilizando una cuenta de usuario o clave de otro usuario.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose al área de sistemas donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato

Las claves o contraseñas deben tener mínimo ocho (8) caracteres alfanuméricos.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfanuméricos (Ejemplo: i$, %,&)

8.10 POLÍTICA DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL – LAN).

Asegurar la operación correcta y segura de los puntos de red.

Las políticas de Administración de la red, se encuentran definidas en el documento de Políticas generales gestión tecnológica_v3 D-21-014

8.11 POLÍTICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN.

Asegurar el manejo correcto y seguro de las impresoras y del servicio de impresión.

Las Directrices de uso de impresoras y servicio de impresión, se encuentran definidas en el documento de Utilización de la

impresora kyocera_v1 I-21-040

8.12 POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO.

Asegurar la protección de las redes y la infraestructura.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

• Fumar dentro del Data Center.

• Introducir alimentos o bebidas al Data Center

• Mover, desconectar y/o conectar equipo de cómputo sin autorización.

• Modificar la configuración del equipo o intentarlo sin autorización.

• Alterar software instalado en los equipos sin autorización.

• Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.

• Extraer información de los equipos en dispositivos externos.

• Abuso y/o mal uso de los sistemas de información.

• Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

8.13 POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS.

Asegurar la protección física y de la información en los equipos.

Las Directrices de seguridad de equipos se encuentran definidas en el documento de Políticas generales gestión tecnológica_v3 D-21-014

8.14 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN.

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por entidad.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Las Directrices de respaldo y restauración de Información, se encuentran definidas en el documento de plan de contingencia de tecnología de información D-21-081, Restauración Información. P-21-119

8.15 POLÍTICA DE GESTIÓN DE VULNERABILIDADES

Evitar las vulnerabilidades de los sistemas de información y de las comunicaciones.

Las directrices de gestión de vulnerabilidades se encuentran definidas en el documento plan de contingencia de tecnología de información D-21-081

8.16 POLÍTICA DE GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN.

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

Las Directrices de gestión de incidentes de seguridad de la Información, se encuentran definidas en el documento de registro de incidencias /protección de datos personales_v0 F-18-872.

8.17 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Aplicar las políticas de tratamiento de datos personales a los afiliados, trabajadores, contratistas, visitantes y terceros que presten sus servicios a la Caja de Compensación para proteger el derecho a conocer, actualizar y rectificar las informaciones que se haya recogido sobre ellos en bases de datos o archivos.

Se encuentra definido en el documento Manual de Políticas WEB –M-18-023

9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la entidad, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una eventualidad.

Se encuentran definidas en el documento plan de contingencia de tecnología de información D-21-081

10. CUMPLIMIENTO

Las políticas contenidas en este documento son de cumplimiento obligatorio para todos los trabajadores, contratistas y otros colaboradores. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia se tomarán las acciones disciplinarias y legales correspondientes.

11. CONTROLES

Este documento esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a

este manual. Los usuarios de los servicios y recursos de tecnológicos pueden consultar los procedimientos a través de la intranet en
ISOLUCION.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN

ELABORÓ	REVISÓ	APROBÓ
Nombre: Nidia Esperanza Pulido Aguilar **Cargo:** Técnico I- Planeación y Calidad **Fecha:** 02/Ene/2020	**Nombre:** Orlando Rodriguez Castillo **Cargo:** Jefe Grupo Sistemas **Fecha:** 02/Ene/2020	**Nombre:** Jaime Fernando Diaz Molina **Cargo:** Jefe Departamento de Planeación e Informática **Fecha:** 02/Ene/2020