Contenido

## 1. DERECHOS DE AUTOR

Este documento es creación de la caja de compensación Familiar de Boyacá COMFABOY, por lo tanto, la utilización parcial o total de este documento debe ser enunciada en los derechos de autor de cualquier documento.

Este documento se basa y hace referencia a los documentos, recomendaciones y los lineamientos de Ministerio del trabajo, superintendencia de subsidio familiar, Ministerio de Tecnologías de la Información y las Comunicaciones en seguridad de los activos de información de la entidad

## 2. INTRODUCCIÓN

COMFABOY con el fin de garantizar la adecuada protección, de todos sus activos de Información, además, de prevenir la materialización de riesgos o vulnerabilidades que puedan afectar la integridad, disponibilidad, confiabilidad y confidencialidad de los activos de información, y buscando generar un mecanismo para darle carácter de obligatoriedad al cumplimiento del plan de seguridad de la información y las políticas de seguridad de la Información, se crea este manual de políticas de seguridad y privacidad de la información y los datos para la entidad.

Los activos de información de COMFABOY (datos, información, documentos, aplicaciones, hardware, red, tecnología digital, personal, instalaciones, equipamiento auxiliar, en general) para la alta Dirección, son objeto de alta prioridad y atención inmediata ante riesgos o vulnerabilidades detectadas, debido a que son el insumo para alcanzar los objetivos, la misión y la visión de la entidad; es así que se implementan las políticas de seguridad de la información que garanticen privacidad, continuidad, autenticidad y no repudio de los activos de información; aunado al correcto tratamiento del ciclo del dato (datos sensibles, datos personales, en general), al derecho constitucional y los demás derechos, libertades y garantías constitucionales, de conformidad con las leyes, decreto y demás relacionadas, como la ley 1273 del 2009, Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013, Decreto 1081 del 2015, Decreto 255 del 2022, y/o ley 1712 del 1214, en general

## 3. OBJETIVO

Integrar las políticas que regulan la seguridad y privacidad de los activos de información de la Caja de Compensación Familiar de Boyacá - COMFABOY, que permitan salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

Ser el documento de consulta para que la entidad y el personal, en general, adopten y adapten, dentro de los procesos y procedimientos las buenas prácticas, normas y leyes nacionales e internacionales, que aporten al Sistema de Gestión de Seguridad de la Información calidad del servicio y de los datos, información y documentos, en cada una de las actividades tendientes al desarrollo de la misión, visión y objetivos de la Entidad.

## 4. ALCANCE

Las Políticas de Seguridad de la Información y tratamiento de datos personales aplican a todos los trabajadores, contratistas, terceros, usuarios y visitantes de la Caja de Compensación Familiar de Boyacá - COMFABOY, que por alguna razón tengan cualquier tipo de interacción con los activos de información.

Este Manual de Políticas de Seguridad de los Activos de Información cubren el framework (marco de ciberseguridad ) del Sistema de Gestión de Seguridad de la Información - SGSI Comfaboy, por lo tanto, se recomienda a la totalidad de los procesos y personal (trabajadores, contratistas, visitantes y terceros que interactúen con los activos de Información y/o presten sus servicios a la Entidad) sean conocida, aplicadas y adoptadas, con el fin de cumplir la normatividad legal colombiana vigente (en especial NTC-ESO-IECC 27000) y las buenas prácticas.

## 5. TÉRMINOS Y DEFINICIONES

**Activo:** representan las propiedades de la entidad, vinculada al desarrollo de proveer servicios sociales y bienestar a sus afiliados y a la comunidad; los activos son bienes y derechos intangibles de propiedad del ente económico, de cuya utilización se espera beneficios presentes y futuros .
**Activo de Información:** los activos de Información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la política General de seguridad y privacidad de la información, la cual determina que activos posee la entidad, como deben ser utilizados, así como roles y responsabilidades que tienen los funcionarios o personal sobre los mismos.
**Archivo:** Conjunto ordenado de documentos que una persona, una empresa, una institución, en general, producen en el ejercicio de sus funciones o actividades .
**Archivo de gestión:** lugar físico o lógico donde se conserva y organiza la documentación Activa (según TRD) desde su creación o recepción hasta su eliminación o transferencia, esta documentación activa es la de uso habitual en la oficina productora.
**Archivo central:** es la unidad administrativa que coordina y controla el funcionamiento de los archivos de gestión y reúne los documentos transferidos por los mismos una vez finalizado su tramite y cuando su consulta es constante . Los cuales siguen siendo objeto de consulta por las propias oficinas y particulares en general.
**Archivo histórico:** es el archivo que recibe la transferencia secundaria del archivo central, previamente revisada y cotejadas, con su respectivo inventario en las unidades de conservación adoptadas por la entidad y conforme con las directrices establecidas.
**Dato:** información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho .
**Información:** Conjunto de datos que se dan a conocer o son objeto de información.
**Documento original:** es la fuente primaria de información con todos los rasgos y características que permiten garantizar su autenticidad e integridad.
**Integridad.** La integridad de los datos es un concepto y proceso que garantiza la precisión, integridad, consistencia y validez de los datos, sino que también garantizan que tengan datos precisos y correctos en sus bases de datos.
**Disponibilidad:** de la información o de los activos de información es el principio que asegura la fiabilidad y el acceso oportuno a los datos o recursos por parte de los individuos o personas autorizadas.
**Confiabilidad:** la característica de confiabilidad implica que la información carece de errores o irregularidades significativas debido a la existencia de un sistema de control interno eficaz y permanente.
**Confidencialidad:** implica mantener los datos, en especial los sensibles, a salvo de acceso no autorizado y posibles filtraciones, disponiendo los medios técnicos, humanos y administrativos necesarios para garantizarlo, relacionado con el principio de temporalidad que consiste en que solo puede ser sometido a tratamiento los datos dentro del tiempo necesario para su finalidad.
**Autenticidad:** de la información se refiere a la veracidad y confiabilidad que se genera, siendo completa, exacta y presenta integridad, sin alteraciones o manipulaciones.
**No repudio:** hace referencia a la capacidad de afirmar la autoría de un mensaje, información, documentos o datos, evitando que el autor niegue la existencia de su recepción o creación.
**Certificado digital de información:** sirve para autenticar datos e información, certificar documentos electrónicos y proteger contraseñas, no puede existir dos certificados similares, ya que se genera un código único que está asociado de forma exclusiva a un documento o archivo. Así mismo debe permitir identificar cualquier modificación de un documento, por mas pequeño que sea, pues la secuencia cambiaria con la modificación.
**Política de seguridad de la Información:** documento de alto nivel que denota el compromiso de la dirección con la seguridad de la Información, los datos, los documentos, sistemas de información y todos los procesos, contiene el conjunto de lineamientos y procedimientos que deben ser implementados y acatados para gestionar la seguridad de la Información.
**Internet:** Red Informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicaciones.
**La nube:** es una red de servidores distribuidos por todo el mundo que este operativo 24 horas del día, los 365 días del año y que funcionan simulando un único ecosistema digital para que podamos almacenar todo tipo de datos, programas o plataformas informáticas.
**Servidor:** es una computadora o sistema Informático que proporciona servicios o recursos a otros dispositivos o programas, conocidos como clientes, a través de una red de computadores o de internet.
**Redes sociales:** plataforma de comunicaciones a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean

accesibles de forma inmediata por todos los usuarios del grupo.
**Correo electrónico:** aplicación y sistema de trasmisión de mensajes computarizados, con conexión entre computadoras a través de redes de comunicación informáticas.
**Delitos informáticos:** se refiere a aquellas acciones que infringen la ley y que se llevan a cabo mediante el uso de computadoras, redes o dispositivos relacionados. Son una variedad de conductas ilícitas en el ámbito digital y electrónico.
**Gestión de seguridad de la Información:** es el conjunto de políticas, lineamientos, procesos, herramientas tecnológicas y recursos humanos integrados para proteger la información y los recursos informáticos de la entidad.
**Dispositivos móviles:** aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a internet, con memoria limitada, se consideran aparatos desde reproductores de audio, portátiles, GPS, teléfonos móviles, tablets, en general.
**Centro de datos:** ubicación física que almacena máquinas de computación y sus equipos hardware relacionados. Contiene la infraestructura computacional que requiere el sistema de Tecnologías de la Información y las Comunicaciones, como servidores, unidades de almacenamiento de datos y equipos de red; en esta instalación física se almacenan los datos digitales mas importantes de la entidad.
**Riesgos de seguridad de la Información:** posibles amenazas, vulnerabilidades o debilidades en los sistemas de información, aplicaciones, información, datos o documentos de la entidad que podrían ser explotados por atacantes.
**Vulnerabilidad:** es una debilidad en un sistema que puede ser utilizada por una persona con mala intención o por descuido para comprometer que compromete la seguridad. Las vulnerabilidades pueden ser de tipo hardware, software, procedimental, humana y pueden estar o no relacionadas con intrusos, atacantes o hacker negros, normalmente afectan el tiempo de atención del usuario o servicio o comprometen datos, información o documentos.
**Incidencia:** es la ocurrencia de uno o varios eventos que atenta contra la integridad, disponibilidad, confiabilidad, confidencialidad de los activos de información de la entidad y que violan la o las políticas de seguridad de la Información de la entidad.
**Backup o copia de seguridad:** es una copia de reserva que se hace de información, datos o documentos para evitar la perdida de los datos originales que se puedan causar por errores, accidentes o contingencias y que permita recuperarlos con facilidad.
**Escritorio limpio:** este término se refiere a que el usuario sea atendido en el momento indicado y se le dé solución a sus inquietudes o necesidades (disponibilidad), dado que en el escritorio no existen documentos o procesos que no permitan agilidad en el proceso o se de espacio para que sea consultados documentos o información o datos a quien no corresponda, protegiendo la confidencialidad.
**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 ISO 27001
**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 (Bussines Continuity 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 (Risk treatment 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.
**Repografia:**Reproducción de los documentos por diversos medios, como la fotografía, el microfilme, etc.
**Folio:** hoja de un expediente, libro o cuaderno
**Las definiciones expuestas en la ley 594 del 2000**, articulo 3, deben ser conocidas, estudiadas y aplicadas en el diario trasegar de sus funciones en la entidad.



## 6. MARCO LEGAL Y/O NORMATIVO

La Caja de Compensación Familiar de Boyacá - COMFABOY, hace referencia a las siguientes normas para la gestión de la seguridad y privacidad de la información.

Constitución Política De Colombia 1991. Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

Constitución Política De Colombia 1991. Artículo 20. "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999. Por 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 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1928 DE 2018. Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest.

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Capítulos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

CONPES 3995 de 2020. Política Nacional De Confianza y Seguridad Digital.

Familia de Norma Técnica NTC-ISO/IEC 27000, que cubre tecnologías de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información con los respectivos requisitos y controles.

La familia NTC-ISO/IEC 27000 trae consigo la Norma técnica Colombiana 27001 objetivos de control y los análisis que desarrolla, SGSI, 27002 buenas prácticas SI, 27003 Ciclo PHVA, 27004 técnicas de medida y las métricas determina la eficacia, 27005, gestión del riesgo, 27007 auditoria SGSI, 27011 telecomunicaciones, 27031 plan de continuidad, 27032 organización SI, 27034 seguridad en aplicaciones, 27036 proveedores.



## 7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El propósito del Manual de políticas generales de seguridad de la información (MPGSI) es delinear un marco de ciberseguridad para que la organización pueda aplicar, utilizando su gestión de riesgos, proteger sus sistemas de tecnología de la información y tecnología operativa, aplicaciones y datos de las ciberamenazas.

Las políticas trazadas por la Caja de Compensación Familiar de Boyacá - COMFABOY, tiene la finalidad y compromiso de administrar adecuadamente los riesgos de seguridad de la información, con la implementación y monitoreo de controles que garanticen la confidencialidad, integridad y disponibilidad de sus activos de información, estableciendo un marco de confianza en el ejercicio de sus deberes con el estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Las políticas que comprende son:

8. Política de Seguridad de la Información.
8.1 Política para el manejo y seguridad de la Información (A5)
8.2 ¨Política de Organización de la Gestión (A6)
8.2.1 Política de Escritorio y pantalla Limpia
8.2.2. Política Clasificación de la Información

**Directrices Generales**

Todos los directivos, trabajadores, contratistas, terceros y/o usuarios de las Tecnologías de la Información y Comunicaciones de la Caja de Compensación Familiar de Boyacá, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente documento.

Es deber de los trabajadores, contratistas y terceros sin excepción, que administren equipos servidores, bases de datos y sistemas de información que manejen información clasificada como sensible, privada y semiprivada, garantizar la absoluta confidencialidad, integridad y confidencialidad de la información, como del uso de credenciales de administración usuario y contraseña.

La entidad debe Verificar periódicamente que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

La entidad debe Manejar un programa continuo de socialización y capacitación que permita incorporar una cultura progresiva que dé importancia a la seguridad y privacidad de información en los trabajadores, contratistas y usuarios de los sistemas de información de la Caja de Compensación Familiar de Boyacá.

Los jefes de cada área deben aportar asegurando que todos los procedimientos dentro de su área de responsabilidad se realicen acorde con las políticas de seguridad de la información establecidas.

La Caja de Compensación Familiar de Boyacá protegerá su información de las amenazas originadas por parte del personal.

La Caja de Compensación Familiar de Boyacá protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, así como el control de acceso a la información, sistemas y recursos de red.

## 8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

### 8.1 Política Para el Manejo y Seguridad de la Información

La Caja de Compensación Familiar de Boyacá - COMFABOY, mediante estas políticas establecerá las directrices para salvaguardar la información y los activos de información del uso no autorizado, daño, pérdida, modificación o divulgación de esta y velará por el estricto cumplimiento de la normatividad vigente aplicable, por lo tanto, es responsabilidad de todos los funcionarios y contratistas de la entidad velar por el continuo cumplimiento de esta política.

Acuerdos de Confidencialidad:
Todos los trabajadores y contratistas de la entidad deberán firmar como parte de sus términos y condiciones iniciales de trabajo, un acuerdo de confidencialidad y reserva al momento de realizar la legalización de su contrato, donde se comprometen a no divulgar, ni usar la información suministrada para el desarrollo de su contrato o a la cual tengan acceso para labores externas a la entidad. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013 y decreto 255 del 2022.
Los proveedores deberán firmar un acuerdo de confidencialidad para tener acceso a la información de la entidad, En el caso que el proveedor se niegue a firma este acuerdo de confidencialidad, no obtendrá acceso a la información solicitada.
Derechos de Autor:
Está prohibido por las normas de derechos de autor y por Comfaboy, hacer copias integrales o parciales de la información de la entidad, en cualquier formato físico y/o digital, hacer copias no autorizadas de software adquirido o desarrollado por la entidad.
Comfaboy, no efectuará copias de seguridad de software que no le esté autorizado o permitido por el autor.
Propietario de la Información:
La entidad es propietaria de sistemas de información, bases de datos, videos, fotos, folletos, revistas, entre otros, y pueden ser Diseñados, creados, manejados y administrados por los trabajadores, contratistas y tercero, sin que se transfieran los derechos de autor a estos.
Los Trabajadores, contratistas y terceros no podrán propagar o difundir comunicados o cadenas de mensajes de tipo político, religioso, comercial entre otros, que puedan contener contenidos ofensivos para el personal, terceros de la Entidad, usuarios o la comunidad en general.
La cuenta de correo electrónico institucional es para uso exclusivo del desarrollo y desempeño de las funciones asignadas por la entidad, de igual forma no podrán ser utilizadas para el uso personal.

- Administradores de equipos tipo servidor:
Es deber de los trabajadores, contratistas y terceros sin excepción, que sean administradores de equipos servidores, bases de datos, sistemas de información que manejen información clasificada como, sensible, privada, y semiprivada garantizar la absoluta confidencialidad, reserva y seguridad de la información, así como del uso de credenciales de administración usuario y contraseña.
La administración de equipos tipo servidor en los que se alojan y/o procesan la información de tipo institucional debe ser realizada por el personal (trabajadores, contratistas y terceros) autorizados por el Departamento de Sistemas.
Los equipos servidores que no sean administrados directamente por el Depto. de sistemas, así como el responsable o los responsables del activo de información que reposen en estos, deberán presentar por escrito al jefe del departamento de sistemas la matriz de activos de información (inventario de información) que reposen o se tramiten, además el motivos y justificación de cambios o solicitud de requerimientos especiales.
Los trabajadores, contratistas y terceros deben cumplir cabalmente y con fidelidad sus funciones y/o tareas que les fueron asignadas, y deben guardar reserva de toda la información que utilicen, creen, salvaguarden dentro de sus funciones o por contacto con otros trabajadores de la caja o terceros que sea propiedad de la entidad.



**8.2 Organización de la gestión SI (A6)**

**8.2.1 Política de Escritorio y Pantalla Limpia.**

El objetivo de esta política es aumentar la disponibilidad de los servicios y la calidad del servicio, y disminuir el tiempo atención al usuario, al mantener sus labores al día y sin tener documentos represados o procesos en equipos de cómputo o en el escritorio. Además de reducir los riesgos de acceso no autorizado, de pérdida, daño y/o robo de información durante y fuera del horario laboral, en los equipos de cómputo y de los escritorios de los trabajadores de la entidad.

Directrices
✓ Todos los equipos de cómputo de la entidad deben usar el papel tapiz Institucional y contar con bloqueo de sesión automática pasados 5 minutos de inactividad, debe mostrar la pantalla de inicio de sesión solicitando el ingreso del usuario y contraseña para reanudar la sesión.
✓ Todo el personal de la Caja De Compensación Familiar de Boyacá debe conservar su escritorio libre de documentación e información de propiedad de la entidad, que pueda llegar hacer copiada, sustraída o utilizada por terceros o por personal ajeno que no tenga autorización para su uso, su conocimiento o su divulgación.
✓ Los trabajadores y contratistas de la entidad que estén ubicado en puestos de atención al público, al momento de ausentarse de su puesto de trabajo deberán guardar la documentación y los medios magnéticos que contengan, en especial la información sensible.
✓ Todos los equipos de reproducción de información de la entidad, (impresoras, fotocopiadoras, escáneres, entre otros), se deben ubicar en sitios o lugares de acceso controlado y toda la documentación con información sensible (pública clasificada o pública reservada), se debe retirar de forma inmediata del equipo y puesta en un lugar seguro. De igual forma, No se deberá reutilizar papel que contenga información confidencial o sensible
✓ Una vez se ausente de su lugar o puesto de trabajo debe bloquear su equipo, para proteger el acceso a las aplicaciones y servicios de la institución de personal no autorizado. tecla WINDOW +L

✓ Los datos sensibles almacenados en los equipos de cómputo, o en sistemas de información, o en carpetas compartidas deberán encontrarse ubicados en rutas que NO sean de fácil acceso o que no cuenten con contraseña.
✓ Todos los trabajadores de la entidad, al finalizar la jornada laboral, o en horas no laborales o cuando el sitio de trabajo se encuentre desatendido, deberán dejar la información CONFIDENCIAL física o en extraíbles, protegida bajo llave. Lo anterior incluye documentación impresa, en medios ópticos, medios magnéticos, en dispositivos de almacenamiento USB y en cualquier medio removible en general.
✓ Todos los trabajadores, contratistas y terceros de la entidad, al finalizar la jornada laboral deben cerrar la sesión o salir de todas las aplicaciones correctamente y dejar los equipos apagados (no sólo el monitor). excepto los trabajadores, contratistas y terceros que tengan manejo de equipos tipo servidor.

**8.2.2. Política Clasificación de la información**

✓ Comfaboy deberá garantizar que la información es tratada y protegida adecuadamente de acuerdo con el nivel de clasificación otorgado. Por lo tanto, la información física y digital se clasificará según las Tablas de Clasificación Documental de la entidad y siguiendo los lineamientos de la superintendencia de subsidio familiar y los internos de archivo y administración documental.
✓ Cada trabajador, contratista y los terceros deberán clasificar la información y entregar al archivo de gestión (cada oficina) organizado, y cada jefe de área igualmente se encarga de la entrega clasificada al archivo Central, según la tabla de valoración documental o la tabla de retención documental.

**8.2.3 Política de retención y archivo de datos.**

Esta política tiene como propósito: Conservar la integridad de los activos de información, garantizando la disponibilidad, los servicios y el tratamiento de la información, los datos, documentos, sistemas físicos y digitales de todos los procesos y áreas de la entidad.

Directrices:

✓ Implementar las Tablas de Retención y Conservación de los archivos de Comfaboy, para establecer en donde reposa y que tiempo deben permanecer almacenada la información de la organización en el archivo de Gestión, en el archivo Central o el archivo Histórico.
✓ Reglamentar e Implementar políticas de archivística, según los lineamientos de la superintendencia de subsidio Familiar y/o lo definidos por la ley 594 del 2000 de archivística nacional y las políticas institucionales.
✓ Adoptar el Programa de Gestión Documental PGD y el Sistema Integrado de Conservación SIC.
✓ Utilizar bases de datos, sistemas de información para la administración, conservación de archivos e implantación del programa de gestión documental.
8.2.4. Política Esquema de clasificación
✓ Toda Información perteneciente a COMFABOY deberá ser identificada y clasificada de acuerdo con los siguientes niveles:
. Público
. Uso Interno
. Confidencial
. Reservado
✓ El departamento logístico, en su área de archivo y administración es la responsable de definir los lineamientos de clasificación, tratamiento y/o manejo de la información de acuerdo con el nivel de clasificación al que pertenecen.
Cada área debe tener en cuenta los siguientes ítems:
✓ Restringir el acceso a la información solo al personal debidamente autorizado (confidencialidad).
✓ Se debe llevar un registro actualizado de los funcionarios, contratistas y terceros autorizados para realizar el manejo de datos y/o información de la entidad (roles y responsabilidades).
✓ Cada área de la entidad debe conservar la información en medios de almacenamiento seguro y tener una estrategia de conservación, integridad, disponibilidad y confidencialidad .



**8.2.5. Política Etiquetado y manejo de la información**

✓ se debe etiquetar el nivel de confidencialidad de la información tratada por la entidad (marcada y/o evidenciada) en todos los folios que contengan información confidencial y/o sensible de forma fácil y legible.
✓ Es responsabilidad de cada uno de los trabajadores de todos los niveles, y contratistas de la entidad mantener etiquetado y organizado la información, datos, documentos producidos y el archivo de gestión (de cada oficina), bajo los lineamientos establecidos por archivo y administración documental del área y/o la entidad.
✓ Los jefes de cada área deberán establecer los lineamientos para el control de la reprografía de documentos (autenticidad o fiabilidad de la información, sobre todo digitalización), con el fin de mantener la integridad, confidencialidad y confiabilidad de la información de la entidad.

**8.3 Recursos Humanos (A7)**

✓ Esta política tiene como propósito garantizar la protección, disponibilidad, integridad y confidencialidad de la información que producen, salvaguardan, utilizan, editan los trabajadores, contratistas y terceros de Comfaboy; también busca alfabetizar digitalmente, aportar lineamientos en roles y en responsabilidades en las áreas, procesos y procedimientos.
✓A su vez validar y concientizar el recurso humano de la entidad continuamente en materia de gestión de riesgos, manejo de la información, amenazas de seguridad existentes, control de acceso y protección de datos (ingeniería social, phishing, vishing,

business email compromise, entre otros), el uso aceptable de la intranet y la seguridad de la red.

**8.3.1 Recurso humano y buenas prácticas**

✓ Todo el personal de la entidad debe tener en cuenta el manual de políticas de seguridad y privacidad de la información para el desarrollo de todas y cada una de las labores, funciones, procesos y procedimientos misionales de la entidad.
✓ Deben ser incorporados los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los funcionarios, contratistas y terceros.
✓ La entidad debe contar con un acuerdo y/o cláusula de confidencialidad, tratamiento y protección de datos para todos los Trabajadores, contratistas y terceros que ingresen o trabajen con Comfaboy. Deben firmar como parte de sus términos y condiciones iniciales de trabajo, un acuerdo de confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el acta de posesión del trabajador, contratista o terceros. Este acuerdo debe incluir la aceptación de las políticas de Seguridad y Privacidad de la Información, así como las políticas de Tratamiento y Protección de Datos de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen tales como el Decreto 1377 de 2013, decreto 255 del 2022. Este acuerdo debe ser archivado de forma segura, por parte de la Gestión Humana y áreas interesadas según sea el caso.
✓ Dentro del mismo acuerdo los funcionarios, contratistas y terceros deben declarar conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo, estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad, ni los derechos de los Trabajadores, contratistas y terceros.
✓ La selección de contratistas y terceros (pasantes, judicantes entre otros) dentro de los procesos de contratación, debe realizarse previa verificación de antecedentes, de acuerdo con la reglamentación vigente.
8.3.2 Recurso humano y el conocimiento en sus labores
✓ Se deben aplicar los controles establecidos por Comfaboy para conceder el acceso a la información CONFIDENCIAL y/o RESERVADA por parte del personal que resulte vinculado a la Entidad. La oficina de Gestión humana y/o contratación será responsable de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y de anexar la documentación requerida para la contratación, términos y condiciones laborales
✓ Para el caso puntual de terceros, proveedores y subcontratistas de la entidad, el departamento de Gestión humana, departamento de logística y/o contratación será responsable de realizar la verificación de la hoja de vida, idoneidad y experiencia requerida para realizar la actividad contratada por la entidad, en especial en seguridad de los activos de información (leyes, normas, lineamientos, políticas y buenas prácticas) y demás requisitos legales vigentes.
✓ Todos los trabajadores, contratistas y terceros deben dar cumplimiento a las normas vigentes como a las políticas, lineamientos de seguridad y privacidad de la información, como a las políticas de tratamiento y protección de datos y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.
✓ Todos los trabajadores, contratistas y terceros, durante el proceso de vinculación deberán recibir una inducción sobre las políticas y lineamientos de Seguridad y Privacidad de la Información como de las políticas de tratamiento y protección de datos, bajo la coordinación de la Gestión Humana, con el apoyo del Departamento de sistemas, con el propósito de sensibilizar y capacitar el recurso humano de la entidad, sobre la protección adecuada de los recursos tecnológicos, el manejo de la información y las responsabilidades legales en el manejo y administración de los activos de la entidad, para el buen desempeño de sus funciones laborales y contractuales.
✓ Cada área capacitará a los nuevos integrantes y mantendrá el conocimiento de los antiguos trabajadores, en cuanto al funcionamiento del archivo de gestión de cada área, así como de los lineamientos, roles y responsabilidades, y políticas aplicables en la administración de los activos de información.



**8.4 Política gestión de activos (A8)**

**8.4.1 Política de gestión de activos de información.**

El propósito de esta política es plantear la forma como salvaguardar adecuadamente los activos de información, para este fin se debe mantener actualizada la matriz de activos de información, para identificar el propietario y custodio designado por la entidad para cada uno de los activos de información.
Directrices.
✓ Se generará y conservará un inventario actualizado y centralizado de todos los activos de información en cada área, en especial cada persona estará asignada como responsable propietario de la información que genere. El original con la totalidad de la matriz reposará en el Departamento de logística y, se enviará copia al Departamento de Sistemas.
✓ Reglamentar e Implementar políticas de información, datos y documentos, según los lineamientos definidos por La Superintendencia de subsidio familiar, la Ley 594 del 2000 de archivística nacional, la Ley 1712 de 2014 y las políticas institucionales. Además de deben guiar por el Programa de Gestión Documental PGD y el Sistema Integrado de Conservación SIC y los lineamientos para el Registro de Activos de Información
✓ Los propietarios de los activos de información son responsables de crear y revisar periódicamente las prohibiciones y privilegios de acceso físico y lógico de los funcionarios, contratistas y terceros.
✓ El Propietario o encargado de un activo de información de la entidad, es el único responsable de validar que los activos bajo su custodia cuenten con los controles necesarios para preservar los objetivos de legalidad, integridad, confidencialidad y disponibilidad de la información.
✓ La información, los sistemas de información, las bases de datos, las aplicaciones que reposen en los servidores del data center de la entidad, así como la infraestructura y recursos tecnológicos para las comunicaciones, o backup, es responsabilidad mantenerlos activos, disponibles y protegidos por el departamento de sistemas. Aunque los dueños de los activos de información y su organización son cada uno de los procesos propios de cada área.

**8.4.2. Política de uso de los activos.**

El propósito de esta política es salvaguardar todos los activos de información de la entidad, mediante la asignación de responsabilidades a los trabajadores y contratistas de Comfaboy, según el rol y las funciones que desempeñe.
Directrices.
✓ Los activos de información son propiedad única y exclusivamente de Comfaboy y deben emplearse para tal fin.
✓ Los activos de Información de la entidad NO se pueden emplear para propósitos diferentes para los cuales fueron definidos o utilizarlos para fines personales.
✓ Se realizará una visita periódica según el cronograma anual de mantenimiento, a las diferentes áreas de la entidad por parte del Depto. de Sistemas y/o auditoría interna, para verificar si los programas utilizados e instalados son los autorizados y licenciados por la institución.
✓ El personal de Comfaboy deberá hacer un uso óptimo tanto de los recursos tecnológicos como de los sistemas de información.
✓ El trabajado, contratistas y terceros, NO podrán compartir las contraseñas o permitir el acceso a los recursos tecnológicos (sistemas de información, bases datos, correos electrónicos entre otros) de la Entidad, igualmente es responsable del manejo apropiado de la información.
✓ No se realizará Instalación de software o programas en ningún equipo de Comfaboy, sin previa autorización del Departamento de Sistemas.
✓ Queda prohibido realizar modificaciones de hardware y software, en los equipos de cómputo o de comunicaciones de propiedad de Comfaboy, sin previa autorización del Departamento de Sistemas.
✓ Todas las acciones efectuadas desde la "cuenta de usuario", es responsabilidad única y exclusiva del propietario de la cuenta.
✓ Toda la información o archivo en formato digital o descargada de la Internet, debe ser examinado por el antivirus contratado por Comfaboy.
✓ Todos los activos de propiedad de la entidad, asignados para el desarrollo de sus funciones a los trabajadores, contratistas o terceros, deberá ser devueltos y/o entregados al momento de retirarse, cambio de cargo o finalización del contrato. Esto incluye la información corporativa (física y/o digital), Recursos tecnológicos (equipos de cómputo, escáner, Software, dispositivos móviles, tarjetas de acceso, manuales, en general), códigos y en general.

**8.5 Política Controles de Acceso (A9)**

**8.5.1. Políticas de acceso remoto.**

La presente política va dirigida a definir el uso de los recursos y las restricciones que se deben tener para hacer las comunicaciones y conexiones de accesos remotos de los recursos tecnológicos de la entidad, manteniendo la seguridad de la información.



**Directrices.**
✓ El Servicio de acceso remoto a la red de datos de la entidad, para Trabajadores, contratistas y terceros, debe ser autorizada por el jefe de área, departamento, unidad y/o secretaria, con el visto bueno y solicitud por correo electrónico o GLPI al Departamento de Sistemas, el acceso a la conexión desde una red interna o externa, están sujetas a la autenticación con un nivel adecuado de protección.
✓ Para el servicio de accesos remoto se realizará la conexión solo con los equipos tipo servidor y de comunicaciones. Para la conexión de acceso remoto con los equipos tipo cliente quedan sujetos a la previa autorización e identificaciones de estos (TeamViewer).
✓ Los funcionarios o contratistas que necesiten el servicio de acceso remoto a los computadores y/o servidores de la entidad, deben hacer la solicitud a la mesa de ayuda (GLPI) del departamento de Sistemas, esta se realizara dependiendo el tipo de actividades y el tipo de activo que el usuario gestione.
✓ El Departamento de Sistemas, será el encargado de realizar la instalación y adecuación de los recursos tecnológicos para conexión de acceso remoto, es prohibido que lo realice personal ajeno a esta dependencia.
✓ Las anteriores directrices aplican para el trabajo en casa según los lineamientos dados por el estado colombiano de trabajo desde casa.
8.5.2 Política De Control De Acceso a sistema de información
Esta política busca coordinar y regular el acceso y uso de sistema de información de la entidad donde las directrices debe ser trazadas por el dueño del proceso o área y el depto. de sistema en caso de que el sistema contenga sistemas, datos o información electrónicamente; y si es información física directamente con el depto. de logística, archivo y administración documental.
Directrices
✓ Cada uno de los sistemas en cabeza del jefe del área y coordinación del área de sistemas establecen los lineamientos, procedimientos, responsabilidades y mecanismos de control de acceso de forma segura y controlada a la información, de forma física o de forma lógica, en los sistemas de procesamiento de información de acuerdo con los niveles de clasificación de los activos de información y los lineamientos trazados por gestión documental de la entidad, con el fin de protegerlos de accesos no autorizados.
✓ Los trabajadores y contratistas de la entidad, para tener acceso a los Sistemas de Información de la entidad, bases de datos y en general cualquier servicio de los recursos de la Tecnologías de Información y las comunicaciones TIC, se debe realizar por medio de Credenciales de Acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.
✓ Para la asignación, eliminación y restauración de credenciales de acceso a los usuarios (funcionarios y contratistas), deben colocar una incidencia en la mesa de ayuda (GLPI) del Departamento de sistemas.
✓ El acceso a los equipos especializados de comunicaciones alojados en el data center como: servidores, enrutadores, entre otros, conectado a la red de datos, siempre serán controlados y administrado por el departamento de sistemas.

✓ Cada uno de los trabajadores y contratistas de la entidad, es responsable de todas las actividades, llevadas a cabo con su identificación de usuario y contraseña.
✓ La asignación de la contraseña para tener acceso a la red o a sistemas de información de la entidad, se debe realizar de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
✓cualquier trabajador, contratista o tercero al revelar o compartir la contraseña el usuario autorizado se expone a responsabilizarse de acciones que otras personas hagan con su contraseña.
✓ Está prohibido imprimir y colocar de forma visible, en el área de trabajo el usuario y contraseña, de tal forma que personas ajenas tenga acceso a la información.
✓ Está prohibido que los trabajadores o contratistas o usuarios, de los recursos Tecnológicos de la entidad, puedan almacenar y/o guardar las contraseñas en programa o sistema que proporcione esta facilidad.
✓ El Administrador del Sistema entregará una clave de ingreso al sistema al usuario (trabajador y/o contratista), la cual será válida solamente para el ingreso la primera conexión del usuario, quien debe cambiarla antes de realizar cualquier actividad en el sistema.
✓ El acceso a los sistemas de información y en general cualquier aplicación y/o recurso de tecnológico de la entidad. Será asignado previa solicitud escrita o por correo electrónico del jefe del departamento de sistemas.
✓ Los usuarios deben tener en cuenta el siguiente lineamiento para la construcción de sus contraseñas, deben estar compuesta al momento de su construcción de al menos ocho (8) caracteres. Estos caracteres deben ser caracteres alfabéticos (mayúsculas y minúsculas), numéricos (Base de 10 dígitos (0 a 9)) y símbolos o caracteres especiales. ( ¡,$,%,&).
✓ El administrador de dominio de red debe configurar y/o programar el servidor para que se realice cambio de contraseña cada tres meses, para poder ingresar su equipo a la red de la entidad
✓ El usuario tiene la libertad de cambiar su contraseña cuantas veces lo crea necesario.
✓ Cuando el fabricante proporciona (contraseñas por defecto), es obligación de los trabajadores o contratistas realizar el cambio de claves antes de poner en producción cualquier activo de información en la entidad.
✓ Para restaurar la contraseña de la cuenta de correo institucional, se debe hacer la solicitud de la nueva contraseña por GLPI.
✓ Los trabajadores o contratistas que tenga la sospecha que su contraseña es conocida por otra persona, está en la obligación de cambiarla inmediatamente.

**8.6 Política de criptografía (A10)**

**8.6.1 Política de uso de controles criptográficos**

Establecer los lineamientos para el uso correcto y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de acuerdo con la evaluación de riesgos realizada por el propietario de la Información y encargados.
Directrices.

✓ el Depto. de sistemas debe establecer los lineamientos para uso de los controles criptográficos en los siguientes ítems:
. Para toda la información digital con clasificación reservada y/o clasificada.
. Para la protección de claves de acceso a los recursos tecnológicos de la entidad (sistemas de información, bases de datos, servicios entre otros).
. Para él envió y recepción de correos electrónico con información reservada y/o clasificada.
✓ el Depto. de sistemas es el encargado de verificar que todos los recursos tecnológicos de la entidad (sistemas de información, bases de datos, servicios entre otros), que requiera realizar intercambio (transmisión y recepción) de información clasificada o reservada cuente con mecanismos de cifrado de datos.
✓ El Depto. de sistemas debe establecer e implementar estándares para la aplicación de controles criptográficos en los servicios que lo requiera la entidad.
✓ El Depto. de sistemas debe asegurar y coordinar con los proveedores (compra y/o desarrollos) de los recursos tecnológicos (sistemas de información, bases de datos, servicios entre otros), que los controles criptográficos de los recursos adquiridos anteriormente mencionados cumplen con los estándares o lineamientos de la entidad.
✓ El depto. de sistema debe contar con herramientas necesarias para el cifrado de medios de almacenamiento interno de la información de la entidad.
✓ El Depto. de sistemas debe verificar el uso de herramientas de cifrado de la información almacenada y/o alojada en sitios externos al Datacenter a la entidad.
✓ El depto. de sistemas debe establecer lineamientos para el uso de las llaves criptográficas utilizadas para el cifrado de información clasificada como confidencial y debe ser protegidas contra: (divulgación, uso indebido, sustitución entre otras), es importante restringir al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.
✓ El depto. de sistemas debe establecer lineamientos de fechas de inicio y fechas de caducidad y/o vigencia del uso de las llaves, para reducir la probabilidad de fraude y aumentar la seguridad, confidencialidad e integridad de estas.

**8.7.Política seguridad física y del ambiente (A11)**

**8.7.1 Política De Uso De Los Recursos Tecnológicos**

✓ Recurso Tecnológico: La entidad cuenta con una serie recursos tecnológicos tales como (impresoras, portátiles, escáner, computadores, servidores, entre otros), que se utilizan única y exclusivamente por el personal autorizado para el desarrollo de sus funciones y/o actividades asignadas.
✓ Está totalmente prohibido a los trabajadores, contratistas y terceros realizar la instalación y configuración a los recursos tecnológicos (impresoras, portátiles, escáner, computadores, servidores, entre otros) cuando se realizan cambios de oficina, de

piso y/o edificio. Estos cambios deben ser informados a la oficina de logística con copia al depto. de Sistemas, para coordinar la instalación y configuración de los mismos en su nuevo sitio de trabajo.
✓ Soporte, Instalación, Mantenimiento y Actualización de Hardware:
Este tipo de servicio solo lo realizara por el personal (trabajadores, contratistas y terceros) del Depto. de Sistemas, es el único autorizado para instalar, desinstalar y actualizar aplicaciones y realizar el mantenimiento preventivo y correctivo de los recursos tecnológicos de la entidad. Para lo cual deberán solicitar el Servicio a la mesa de ayuda de la entidad.
✓ Responsabilidad del Recurso Tecnológico:
Es responsabilidad de todo el personal (trabajadores, contratistas y terceros), de la entidad el buen uso de los recursos tecnológicos que le sea asignados; el cual será incluido a su inventario personal, de acuerdo con el procedimiento de logística.
✓ Elementos de Decoración en los Recurso Tecnológico:
Estos recursos se deben mantener libres de: postic, papeles, fotos, calcomanías, artesanías entre otro elemento que lo pueda deteriorar o acortar su vida útil.
Software en los Recursos Tecnológicos:
El software que se maneje, utilice e instale en Comfaboy, será adquirido de acuerdo a sus necesidades y a las normas vigentes, siguiendo los procedimientos y/o lineamientos internos del departamento de logística, con visto bueno del Departamento de Sistemas.
✓ El departamento de Sistemas contara con un inventario de las licencias de software de la entidad que le permita su instalación, configuración, administración y control evitando así posibles sanciones por instalación de software no licenciado.
✓ El software con licencia de tipo (demo, trial, evaluación o de prueba), instalados en los recursos tecnológicos (computadores) de COMFABOY deberá desinstalarse una vez termine y/o caduque el periodo de prueba de la licencia.
✓ recuerde y tenga en cuenta que los recursos tecnológicos, así como el software y hardware son propiedad de la entidad, se instalará única y exclusivamente el software que cuente con licencia autorizadas o de propiedad de la entidad. Por lo anterior el software que no cumpla con estos lineamientos se debe desinstalar de forma inmediata para poder garantizar el cumplimiento de la Ley antipiratería por parte de la entidad.
✓ Está totalmente prohibido a los trabajadores, contratistas y terceros realizar cambios relacionados con la configuración de los equipos, como la conexión de la red de datos, el cambio de usuarios locales del equipo, en el papel tapiz y protector de pantalla corporativo. Estos cambios son realizados únicamente por el departamento de Sistemas.
✓ Todos los trabajadores, contratista y terceros de Comfaboy deben cumplir con la Normatividad vigente adoptada por la entidad, las leyes de derechos de autor, acuerdos de licenciamiento de software (sistema operativo, paquete ofimático y antivirus licenciado para el caso de los contratistas) y los acuerdos de confidencialidad.
✓ Software Antivirus: Se instalará única y exclusivamente el software antivirus establecido por el Departamento de sistemas, a todos los equipos de cómputo propiedad de la entidad.
El personal (trabajadores, contratistas y terceros), que debe realizar labores o funciones de escaneo de archivos y directorios, no deben por ningún motivo cambiar o eliminar la configuración del antivirus en los equipos de cómputo propiedad de la entidad.
✓ Los trabajadores, contratistas y terceros no deben descargar ningún tipo de archivo adjunto que procedan de fuentes desconocidas, para evitar contaminar con virus informáticos o la instalación de software malicioso en sus equipos terminales, estaciones de trabajo, equipos portátiles, o computadores.
✓ Comfaboy cuenta con un Data Center, como zona adecuada para alojar los equipos tipo servidor y otros equipos básicos de comunicación.
✓ La instalación, actualización y modernización de un nuevo componente y/o equipo activo o pasivo en la red de datos debe estar Autorizada, Coordinada y supervisada por el Departamento de Sistemas.
✓ Monitoreo de Equipos: La entidad se reserva el derecho de monitorear los recursos Tecnológicos (equipos de cómputo, portátiles, tablets entre otros), que estén conectados a la red de datos de Comfaboy, y de los cuales se tenga sospeche que está poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información.
✓ Aplicaciones de Ofimática: Solo está permitida la instalación de la suite de ofimática de Microsoft Office licenciada por la entidad.
✓ Sistemas de información de entes de control: El licenciamiento de los sistemas de información a través de los cuales se reporta información, es responsabilidad del ente de control respectivo.
✓ Acceso a Código Fuente de Aplicaciones: Está totalmente prohibido a los Trabajadores, contratistas y terceros manipular el código fuente de una aplicación sin la autorización del fabricante y/o Departamento de sistemas, para realizar cambios o mejoras a la misma. Si requiere tener acceso al código fuente de una aplicación desarrollada en la entidad, se debe solicitar permiso al Depto. de Sistemas. De igual forma si es una aplicación desarrolla por un proveedor externo, se deben revisar las cláusulas del contrato.



**8.7.2 Política de cambio de recursos Tecnológicos y desarrollo de sistemas de información**

Gestión de Cambios o adaptación de Recursos Tecnológicos y/o software:
✓ Al existir una solicitud de cambio de tecnología o el personal del departamento de sistemas emite un concepto técnico con la necesidad de cambio, se envía al departamento de logística las razones y los elementos que se van a incorporar o cambiar, para continuar con el proceso interno de almacén y el adecuado proceso de instalación o desinstalación.
Sistemas Propietarios Desarrollados en la Entidad.
✓ Los productos tecnológico desarrollados, recomendados y aprobados por el Departamento de Sistemas, realizará la instalación solo en los equipos de la entidad designados para este fin.
✓ Toda adopción, instalación, pruebas y uso de nuevas tecnologías de la información y las comunicaciones orientadas a la gestión de servicios de la entidad deben ser aprobados y coordinados por el departamento de sistemas.
✓ Sólo el personal autorizado por el jefe de área y con visto bueno y solicitud por GLPI al Depto. de sistemas podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la entidad; las conexiones establecidas para este fin utilizaran los esquemas de seguridad establecidos por la entidad.

✓ El software y/o paquetes ofimáticos de propiedad de la entidad, es para uso exclusivo de usuarios o trabajadores y contratistas de la entidad. Los Proveedores y/o contratistas no pueden instalar o hacer uso de las licencias de propiedad de la entidad.
✓ el departamento de sistemas: La entidad cuenta con este Departamento para gestionar y administrar, el soporte y mantenimiento periódico de los equipos activos y pasivos del Data Center, y poder garantizar la integridad, disponibilidad y confidencialidad de los activos de información de la entidad que se encuentran allí alojada.
✓ La información almacenada en los equipos de cómputo, cuentas de correo o medios de almacenamiento institucionales y clasificada como de uso personal, se debe guardar en su totalidad en el equipo que le ha sido asignado por la entidad, en una partición D (diferente a C) en una carpeta para este fin, la cual debe ser nombrada como "trabajo" y organizar internamente dentro de esta, según la tabla de retención documental a la que pertenezca el archivo, dato o documento.
✓ Todo activo de Información propiedad de la entidad, que haya sido asignado a un trabajador, un contratista o tercero, o lo haya utilizado, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, llaves, códigos y la información corporativa que tenga almacenada en dispositivos móviles o removibles.
✓ En caso de presentarse una falla o problema de hardware o software en un recurso tecnológico propiedad de la entidad, el usuario responsable del mismo deberá informarlo al jefe inmediato y al departamento de sistemas, a través de la mesa de ayuda, para una asistencia especializada y por ningún motivo, deberá intentar resolver el problema.
✓ Los equipos de cómputo que no requiere mantenimiento preventivo, si no mantenimiento correctivo (formateo o reinstalación de aplicaciones, por problema de infección de virus, o cambio de hardware haya sufrido un avería o daño), el personal de soporte del departamento de sistemas sacara copia de seguridad al disco duro de la unidad (D) o backup, si se puede, No se hace responsable a la perdida de información del disco C, Es Responsabilidad del funcionario o contratista tener su copia de seguridad en el ONE DRIVE de la entidad o en cualquier otro medio.
✓ Los trabajadores, contratista o terceros encargados de la mesa de ayuda del departamento de sistemas, contarán con un repositorio de software (drivers e instaladores) para el soporte y mantenimiento preventivo y correctivo de los recursos tecnológicos de la entidad.

**8.7.3 Política De Instalación De Cableado**

Esta política busca que la instalación del cableado estructurado de la entidad. Cuente con un diseño, con planeación, con administración y mantenimiento preventivo y correctivo.
El cableado estructurado de la red de telecomunicaciones de la entidad es responsabilidad del departamento de sistema, debe eta en funcionamiento y cumplir con las normas técnicas vigente, y con los estándares adoptados por la entidad, con el fin de garantizar la integridad, la seguridad, la confiabilidad de la información y conservar la estética, la arquitectura y la seguridad de la red.

**8.7.4 Políticas De Seguridad Del Datacenter Y Centros De Cableado**

Esta política debe garantizar la protección y seguridad de la información en los servidores y en la infraestructura tecnológica de la entidad, por parte del personal de Comfaboy, como de los terceros que ingresan a estas instalaciones.
Directrices.
✓ Se prohíbe fumar, comer o beber; en las instalaciones del Datacenter y los centros de cableado.
✓ Se prohíbe guardar en las instalaciones del Datacenter y centro de cableado papelería o materiales con alto riesgo de incendio o propagación de fuego, se debe eliminar periódicamente estos materiales, y se debe conservar el orden y la limpieza del Data center y los centros de cableado.
Se prohíbe el ingreso de personal extraño al Datacenter y centros de cableado, el personal externo que visite o necesite del departamento de sistemas debe estar autorizado y registrado. Y debe diligenciar el formato de ingreso y egreso del personal.
✓ Se prohíbe mover, desconectar y/o conectar equipo de cómputo sin autorización del Departamento de Sistemas.
✓ Se prohíbe modificar la configuración de cualquier equipo o intentarlo, sin autorización del departamento de Sistemas.
✓ Se prohíbe alterar software instalado en los equipos sin autorización del Departamento de sistemas.
✓ Se prohíbe alterar o dañar las etiquetas de identificación de los sistemas de comunicaciones, de información o sus conexiones físicas sin autorización del departamento de sistemas
✓ Se prohíbe extraer información de los equipos servidores en dispositivos externos sin autorización del departamento de sistemas.
✓ El control de ingreso del personal al Datacenter y centros de cableado, se realizará mediante dispositivos electrónicos de control de acceso con autenticación (por huella, por tarjeta y control biométrico).
✓ el departamento de sistemas y el departamento de logística, deberán garantizar a la Entidad, que todos los recursos o equipos tecnológicos del Datacenter y los centros de cableado deberán contar con U.P.S (sistema alterno de respaldo de energía).
✓ El Datacenter debe estar provisto de señalización, elementos y equipos de emergencia, luces de emergencia y guías de evacuación, siguiendo la normatividad vigente de seguridad industrial y de salud ocupacional.
✓ El Datacenter deben contar con pisos falsos, elaborados con materiales no combustibles.
✓ Deben estar acondicionados con sistemas de enfriamiento por aire acondicionado de precisión. Estos equipos deben ser redundantes para cuando este falle, se pueda continuar con la refrigeración, y no afecte los equipos tecnológicos del Datacenter.
✓ el sistema de extinción de fuego y las alarmas de detección de humo, deben ser automáticos y deben estar conectados al sistema central.
✓ Los sistemas contra incendios (extintores deben estar cargados y no deben estar despresurizado), deben ser adecuados, y estar adecuadamente, ensayados y con la capacidad ideal para detener el fuego generado al interior.
✓ El cableado estructurado de la red de datos debe estar certificado y cumplir con las normas y estándares internacionales.
✓ El mantenimiento preventivo y correctivo del Datacenter y los centros de cableado, deben estar supervisados y debidamente autorizados por el personal del departamento de sistemas.
✓ Los recursos o equipos tecnológicos del Datacenter y los centros de cableado que lo requieran, deben ser revisados

permanentemente para identificar a tiempo las fallas que se puedan presentar de forma inmediata.

**8.7.5 Política para uso de dispositivos móviles.**

✓ La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "Smart phones", cámaras de video, entre otros), suministrados por entidad y personales que hagan uso de los servicios de información de la Entidad.
✓ Para el caso de los equipos portátiles, tables entre otros, el departamento de sistemas será la encargada de suministrar las características técnicas de los equipos y estás serán definidos por las necesidades y el tipo información procesada y almacenada por cada usuario de la entidad.
✓ Los trabajadores, contratistas y terceros usuarios de estos equipos no están autorizados para cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles de la entidad, únicamente deben aceptar y aplicar las actualizaciones del fabricante.
✓ Todos los trabajadores, contratistas y terceros que utilicen dispositivos móviles institucionales que contengan información Confidencial o de Uso Interno deben usar la última versión del sistema, los parches o actualizaciones disponibles por los fabricantes.
✓ Los trabajadores, contratistas y terceros que utilicen dispositivos móviles deben mantener actualizado el software antivirus del dispositivo y/o informar al departamento de sistemas en el caso de que el dispositivo no tenga instalado y funcionando del antivirus institucional.

**8.8 Política Seguridad de las operaciones (A12)**

**8.8.1. Política De Gestión De Medios Removibles**

Esta política proporciona los lineamientos para la administración, protección y traslado de información, mediante el uso de los medios de almacenamiento removible.

Directrices.
✓ Los medios removibles, NO son una opción de respaldo de la información de forma permanente, es responsabilidad exclusiva de los trabajadores, contratistas y terceros, conservar y/o proteger la información en los servidores, o en el servicio de la nube contratada por la entidad para tal fin.
✓ Es responsabilidad exclusiva de los trabajadores, contratistas y terceros, dar buen uso y cuidado a los medios removibles asignados por la entidad.
✓ Se deben escanear y/o vacunar todos los medios removibles cada vez que sean conectados a los recursos tecnológicos de la red de datos de la entidad, con el propósito de eliminar los posibles códigos malicioso (virus) que puedan llegar a causar perdida de activos y daño en los equipos de la entidad.
✓ Es responsabilidad exclusiva de los trabajadores, contratistas y terceros, la custodia, el buen uso, la conservación y/o protección de la información guardada en los medios removibles asignados por la entidad.
✓ Toda la información sensible y/o confidencial de la entidad almacenada en medios removibles, deben ser almacenados en un lugar seguro, vigilado, ventilado y codificado según el nivel de información.
✓ No se debe almacenar por ningún motivo información confidencial en los teléfonos móviles empresariales o personales.
✓ Cuando se realice mantenimiento correctivo y/o formateo, a los medios removibles por perdida de información, por perdida de vigencia de la información, o por que se realiza el cambio del equipo de área, se debe realizar de eliminación segura de la información.



**8.8.2. Política De Desarrollo Seguro.**

✓ El Departamento de Sistemas debe revisar los lineamientos que permitan apoyar, actualizar y mejorar los diferentes procesos operativos y estratégicos de la entidad, por consiguiente, debe hacer uso intensivo de las Tecnologías de la Información y las comunicaciones. Los productos de software pueden ser adquiridos a través de terceros o desarrollados por personal de la entidad.
✓ El Departamento de sistemas debe revisar y/o elaborar, mantener y aplicar una metodología para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, procedimientos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.

**8.9 Política de comunicaciones (A13)**

**8.9.1. Política De Uso De Redes Sociales**

Garantizar la seguridad, la integridad y confidencialidad a la hora de utilizar servicios de redes sociales, página web y aplicaciones de mensajería instantánea en la entidad, por parte de los trabajadores y contratistas autorizados para este fin.

Directrices:
✓ El servicio de red sociales para proporcionar información de la entidad solo estará autorizado y administrado por el departamento de mercadeo y comunicaciones. según el proceso de divulgación y comunicaciones con código C-03-14, del 17/May/2024.
✓ Toda información que sea publicada por las redes sociales como Facebook®, Twitter®, YouTube® LinkedIn® o blogs, entre otras, en un ambiente diferente al departamento de mercadeo y comunicaciones, no se considera oficial, por consiguiente, no se

podrá garantizar su confiabilidad, integridad y disponibilidad de la información.
✓ Todos los funcionarios y contratistas autorizados para hacer uso de los servicios de Redes Sociales o aplicaciones de mensajería instantánea son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la entidad.
✓ Los Usuarios (trabajadores y contratistas), NO deben utilizar redes, ni aplicaciones de mensajería instantánea para descargar programas ejecutables o archivos que puedan contener software o código malicioso.
✓ No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales y aplicaciones de mensajería instantánea.
✓ No se debe acceder de forma no autorizada a los sistemas de seguridad de la red de datos de la entidad, o aprovechar el acceso a Redes Sociales y aplicaciones de mensajería instantánea para fines ilegales.
✓el departamento de Sistemas, será la encargada de establecer las normas y lineamientos para el uso de las diferentes herramientas o plataformas digitales, plataformas virtuales, plataformas de redes sociales y aplicaciones de mensajería instantánea para la entidad, previo acuerdo con la el departamento de mercadeo y comunicaciones.
✓ Es importante realizar el cambio o actualización de contraseña por lo menos una (1) vez por trimestre, y teniendo en cuenta las sugerencias dadas en este manual.

**8.10 Política de mantenimiento del sistema (A14)**

**8.10.1 Política Adquisición, desarrollo y mantenimiento de sistemas**

✓ En el levantamiento de requisitos y en el funcionamiento de los sistemas de información se debe tener en cuenta, que la seguridad de la información, sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información contratados con externos.
✓ Cada sistema debe realizar el análisis y especificación de requisitos de seguridad de la información Protección de transacciones de los servicios de las aplicaciones.

**8.10.2 Seguridad en los procesos de desarrollo y de soporte:**

✓ Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
✓Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
✓ Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
✓ El departamento de sistemas debe establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
✓ Desarrollo externo
La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente, también hacer cumplir los requisitos funcionales según necesidades y de acuerdo a la Inter operatividad de los datos.
Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.



**8.11 Política de proveedores (A15)**

**8.11.1 Política Relaciones con los Proveedores**

Esta política busca implementar requisitos de seguridad para protección de la información, e incluirlos dentro de los acuerdos con proveedores, que permita identificar riesgos asociados para implementar planes de acción dependiendo de las actividades a realizar, para establecer, aprobar y divulgar los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos posean.

Directrices.

Los proveedores deben aceptar y firmar los acuerdos de confidencialidad establecidos por Comfaboy.
✓ Los proveedores y/o terceros deben hacer llegar la hoja de vida de sus colaboradores y/o empleados a talento humano para verificar su idoneidad y en el caso particular de instalación y/o mantenimiento de recursos tecnológicos o sistemas digitales, se debe enviar copia al Departamento de Sistema para verificación del perfil y experiencia del personal.
✓ Se debe implementar para su diligenciamiento un documento que permita el registro y control de todo personal que ingrese a las instalaciones de la entidad con el fin de realizar servicios, soporte e instalación de recursos tecnológicos (equipos de cómputo, sistemas de información, bases de datos entre otros) y demás activos, el cual debe cumplir con los requisitos mínimos de seguridad y contar con la firma del personal que ingresa.
✓ Cuando se les conceda acceso a proveedores al centro de procesamiento, sistemas centrales, entre otros, se deberá hacer siempre con la participación y/o acompañamiento del personal autorizado del departamento de sistemas, previa evaluación de los riesgos, para identificar los requerimientos y controles específicos, teniendo en cuenta: El tipo de acceso requerido (físico, lógico y a qué recurso) y los motivos para los cuales solicita el acceso aprobado por el dueño de la Información.
✓ En ningún caso se dará acceso a los proveedores a la información, ni a las instalaciones de los centros de cableado, Datacenter, servidores entre otras áreas, hasta tanto no se haya firmado un contrato y/o acuerdo que definan las condiciones para el acceso remoto o el ingreso físico, y se hayan implementado los controles pertinentes para el desarrollo de este.
✓ Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, bases de

datos, redes de datos, computadores, contemplarán como mínimo los siguientes aspectos:
. La forma en los que se cumplirán los requisitos legales aplicables.
. El medio para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad de la información.
. La forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información. . La forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres. . Niveles de seguridad física que se asignará al equipamiento tercerizado.
✓ Todos los trabajadores y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o Entidades externas.
✓ Se deben establecer los acuerdos de servicio y los acuerdos de trasferencia y recibo de información con cada proveedor, dentro del contrato realizar acuerdo con los lineamientos establecidos por la entidad.
✓ El Departamento de sistemas, es el área encargada de los recursos tecnológicos de la entidad, se debe conciliar, con el proveedor, la verificación de las condiciones de trasferencia y recibo de información de forma segura.
✓ Se deben definir las cláusulas por incumplimiento en los contratos de los proveedores, para establecer las situaciones que puedan generar multas o penalizaciones, dentro de los cuales se contempla los acuerdos de confidencialidad y no divulgación de la información.

**8.12 Política de incidentes de seguridad de la información (A16)**

**8.12.1 Política de manejo de incidencias.**

✓ La entidad cuenta con el sistema de mesa de ayuda GLPI administrada por el Departamento de sistemas, para canalizar todos los incidentes y peticiones de los recursos tecnológicos solicitadas por los usuarios (trabajadores y contratistas) de la entidad.
✓ Toda la información relativa a los incidentes reportados a la mesa de ayuda, deben ser manejados con total confidencialidad, discreción y análisis para determinar el grado de riesgo o vulnerabilidades asociadas.
✓ El Departamento de sistemas y el departamento jurídico reportarán ante la autoridad competente los incidentes de seguridad de la información u otros que estén considerados como un delito o delito informático.
✓ Los incidentes de seguridad de información que se presenten en la entidad deben ser tratados según el plan de incidentes de seguridad y privacidad de la información G-21-094.
✓ Cada equipo de trabajo en cada área de la entidad deben procurar tener su propio plan de incidentes de seguridad de la información y protección de activos esenciales para la atención de usuarios internos y externos, para esto es necesario tener una lista de los responsables y responsabilidades para los diferentes escenarios que se presentan, donde se debe tener el control, detección, acción y reporte, para posteriormente organizar la retroalimentación y buscar prever acciones futuras ante el incidente.
✓ Todos los incidentes de seguridad de la información presentados en entidad deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.
✓Cuando se detecte un incidente de seguridad, se recomienda tener cuidado con las acciones que se generen, para evitar que se pueda perder la seguridad en la evidencia y para la posterior custodia
✓ De presentarse un incidente se debe proceder a proteger la cadena de custodia de la información.
✓ Se debe procurar: establecer seguridad de la evidencia, generar los roles y acciones de acceso, comunicación y salvaguarda.



**8.13 Política de continuidad del negocio (A17)**

**8.13.1. Política de respaldo y restauración de información.**

Esta política busca es garantizar la seguridad, la integridad y confiabilidad de la información de (bases de datos, sistemas de información y el software), en caso de sufrir fallas y/o perdida de información, mediante la implementación e instalación de sistemas de respaldo.

Directrices:

✓ Todos los sistemas de información, en especial los digitales, en conjunto con el departamento de sistemas deben crear el objetivo y la estrategia para sacar las copias de respaldo incremental o full, con el fin de restituir el sistema en caso de que sufra ataques por medio de virus informático, defectos o daño total en los discos de acopio, dificultades de hardware y software en los servidores o en los computadores personales, catástrofes, fallas eléctricas y por requerimiento legal.
✓ Al departamento de Sistemas se le recomienda mantener útil en el momento indicado, los sistemas digitales o la tecnología solicitada y acordada por cada área para el respaldo de los sistemas, y que resguardan con copias de seguridad, la información sensible, critica de la entidad o esencial y conservando la integridad, disponibilidad, confiabilidad y confidencialidad.
✓ El departamento de Sistemas debe garantizar las copias de la información de configuración contenida en la plataforma tecnológica; así como, de los recursos tecnológicos (imágenes del sistema, equipos tipo servidor, equipos activos de red y dispositivos de red inalámbricos, en general) para todos los sistemas de información aprobados en la entidad, y según los lineamientos tranzados con cada área y existentes en la entidad.
✓ El personal encargado de administrar los recursos tecnológicos (servidores, sistemas de información, bases de datos entre otros), serán los encargados de definir la periodicidad (semanalmente, diaria, mensual), para hacer las copias de respaldo y/o backup, y de verificar los requerimientos y/o necesidades técnicas y administrativas de seguridad para hacer las mismas. De igual forma deben verificar su correcto funcionamiento y ejecución de los procesos, según los lineamientos existentes para tal fin.

✓ Es responsabilidad exclusiva de los usuarios (trabajadores, contratista y terceros), de la creación de copias de seguridad de los archivos de información usados, producidos, custodiados o administrados en cada una de las funciones, utilizando los sistemas de salvaguarda acordado con su jefe inmediato.

**8.14 Política de Cumplimiento**

**8.14.1. Política De Cumplimiento**

✓ Las políticas de seguridad de la información contempladas en este manual son de obligatorio cumplimiento para todos los trabajadores, contratistas y terceros de la entidad; y la entidad, ante el incumplimiento o violación de estas, ya sea causada de forma intencional o por negligencia, tomará las acciones disciplinarias y/o legales correspondientes contra quien incumpla.
✓ Todos los trabajadores, contratista y terceros de COMFABOY deben cumplir con la Normatividad vigente adoptada por la Superintendencia de Subsidio Familiar de la República de Colombia, por la Caja de Compensación Familiar de Boyacá, las leyes nacionales e internacionales relacionadas, las leyes de derechos de autor, acuerdos de licenciamiento de software y los acuerdos de confidencialidad.
✓ El Departamento de Sistemas en cabeza del líder de seguridad de la información, tiene el compromiso de actualizar, socializar y divulgar los cambios en la reglamentación, referente a la seguridad y privacidad de la información y protección de datos que debe cumplir la entidad, de igual forma debe ser soporte en la interpretación y administración de la legislación en activos de Información.

**8.14.2. Política Procesos de Seguridad de la Información**

Esta política tiene como objeto calificar el grado de responsabilidad ante incidentes disruptivos que generen denegación de servicios, perdida de credibilidad en la entidad, problemas judiciales, suplantación, perdida parcial o total de datos, información, documentos, archivos, expedientes, así como temas que trasciendan las fronteras del país, u otros incidentes que repercutan en la inestabilidad de los sistemas de Información de Comfaboy.

Directrices

✓ En caso de materializarse un incidentes de seguridad de la información, y en el momento que se tenga el reporte del análisis de resultados con la causa, afectación y dependiendo del impacto generado en los activos de información de la entidad y las responsabilidades identificadas, se tomarán acciones de mitigación y/o se realizará el traslado al departamento de sistemas y/o al departamento de gestión humana, y al área propietaria de la Información, que es la encargada de investigar y de ser necesario iniciar el Proceso de acuerdo con la información recolectada del incidente de seguridad reportado.
✓ En lo pertinente a la violación de las políticas de seguridad de la información de la Entidad, a los Colaboradores y Terceros, se les aplicará lo establecido en ley 527 del 2009, 1273 del 2009, ley 1581 del 2012, ley 1712 del 2014 y demás leyes y normas que las adicionen, modifiquen, reglamenten o complementen a la fecha del incidente, siempre observando sean faltas a la ley.



**8.14.3. Incumplimiento de la Política**

El incumplimiento de la presente política en cualquiera de sus fases se dará por acción u omisión y en tal sentido, conllevará medidas de carácter administrativo o disciplinario necesarias para garantizar la normalización de la situación, subsanar el evento sucedido o eliminar la causa raíz del problema identificado.

**8.14.4 Política Sanciones**

La falta de conocimiento de los presentes lineamientos no libera al personal de la Caja de Compensación Familiar de Boyacá - COMFABOY, de las responsabilidades establecidas en ellos, por el mal uso que hagan de los activos de información o por el incumplimiento de los lineamientos aquí descritos.

- Se aplicarán sanciones de acuerdo con el reglamento interno de trabajo de Comfaboy.
- Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
- Ante un incidente disruptivo o con secuelas económicas o administrativas, el (las) área(s) involucrada y/o El Departamento de Sistemas será(n) el(los) encargado(s) de recopilar y entregar a la Oficina de Auditoría Interna y/o Departamento de Gestión Humana, las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno; así mismo.

El Departamento de Sistemas será el encargado de registrar y gestionar el Incidente que involucre la tecnología de las comunicaciones de seguridad de la Información derivado del incumplimiento de las políticas.

**8.15 Política Administración de seguridad**

**8.15.1 La evaluación de riesgos de seguridad en Recursos Informáticos en producción**

Se debe ejecutar al menos una vez cada año. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo. Los Trabajadores y contratistas de Comfaboy que realizan las labores de administración del recurso informático y de servicios son responsables por la implementación, permanencia y monitoreo de los controles sobre los recursos computacionales. La implementación debe ser consistente con las prácticas establecidas por el

Departamento de Sistemas.

**8.15.2 El Departamento de Sistemas divulgará, las políticas, estándares y procedimientos en materia de seguridad digital a través de un Programa de capacitación y sensibilización en Seguridad de la Información.**

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar a los usuarios que lo requieran, de acuerdo con su competencia según las actividades a desarrollar y los niveles de seguridad establecidos previamente. La Entidad efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará al Departamento de sistemas los casos de incumplimiento con copia área de auditoría Interna.

**8.15.3 En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información**

se deberá tramitar el cumplimiento de la ley 1273 del 2009, ley 1581 del 2012, ley 1712 del 2014, Ley 1437 de 2011, decreto 620 del 2020, así como, el cumplimiento de las normas que reglamenten a los trabajadores y el control fiscal.

**8.15.4 Directriz de Registros de auditoría:**

Todos los sistemas informáticos que operen y administren información sensible, valiosa o crítica para Comfaboy, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deberán generar pistas de auditoría o logs de registro de sucesos de la operación, las cuales deben proporcionar suficiente información para apoyar el monitoreo, control y las mismas auditorias.
Todos los archivos de logs de auditorías deben ser almacenados y custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que con razón justificada y autorizada por la sectorial correspondiente requieran los registros deberán solicitarlos ante dicha dependencia, quien a su vez deberá solicitar el soporte adecuado al Departamento de sistemas, encargada de su administración y custodia.
. El servidor de dominio deberá tener sincronizada la hora con servidores de hora de Windows o similares para que los equipos que estén configurados en el dominio también se sincronicen correctamente.
. No se permite la instalación, ni utilización de cualquier herramienta de auditoría ni de pruebas de seguridad informática, ni de Ethical Hacking sin previa autorización del Departamento de sistemas.

**8.15.5 Directriz de Derechos de vigilancia**

. La Administración se reserva el derecho de supervisar e inspeccionar los sistemas de información de la entidad en cualquier momento.
. Estas inspecciones pueden llevarse a cabo con o sin el consentimiento y/o la presencia de los empleados involucrados.
. Los sistemas de información que pueden ser objeto de inspección incluyen el registro de actividad de los usuarios, los archivos del disco duro y correo electrónico.
. La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico. Para este efecto, el trabajador o contratista autoriza a la entidad para realizar las revisiones y/o auditorías internas o a través de terceros.



**9. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS**

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos bianualmente, o cuando existan incidentes de seguridad de la información , o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la Caja de Compensación Familiar de Boyacá - COMFABOY.

| VERSIÓN | FECHA | RAZÓN DE LA ACTUALIZACIÓN |
|---|---|---|
| 1 | 20/Mar/2024 | Actualización General de Políticas |
| 2 | 22/Ago/2025 | Actualización Introducción, objetivo, alcance, términos y definiciones, normativa, políticas de seguridad y privacidad de la Información |

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| **Nombre:** Carlos Andrés Reyes Ramos<br>**Cargo:** Analista I- Planeación y Calidad<br>**Fecha:** 22/Ago/2025 | **Nombre:** Orlando Rodriguez Castillo<br>**Cargo:** Jefe Grupo Sistemas<br>**Fecha:** 03/Sep/2025 | **Nombre:** Jaime Fernando Diaz Molina<br>**Cargo:** Jefe Departamento de Planeación e Informática<br>**Fecha:** 03/Sep/2025 |