TABLA DE CONTENIDO

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. INTRODUCCIÓN

La información de la Caja de Compensación Familiar de Boyacá - COMFABOY, 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 políticas de seguridad de la información que garanticen la

confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio de la información de COMFABOY, 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, y los demás derechos, libertades y garantías constitucionales, de conformidad con la Ley 1581 de 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; éstas 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 y privacidad de la 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.

4. ALCANCE

Las Políticas de Seguridad de la Información y tratamiento de datos personales, aplican a todos los funcionarios, 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.

5. 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 estrategias 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: 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 (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.
- 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 encripta 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.
- SGSI 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 computador 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.

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.
. Norma Técnica NTC-ISO/IEC 27000 y 27001, tecnologías de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información con los respectivos requisitos.

7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Caja de Compensación Familiar de Boyacá - COMFABOY, tiene el 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.

Directrices

. Verificar periódicamente que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
. Todos los funcionarios, contratistas, terceros y/o usuarios de las Tecnologías de la Información y Comunicaciones 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.
. 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 funcionarios, contratistas y usuarios de los sistemas de información de la Caja de Compensación Familiar de Boyacá.
. Los jefes de cada dependencia 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 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.

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

8.2 Políticas de Seguridad de los Recursos Humanos

Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.

Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información, mediante el cual se compromete a realizar un adecuado uso de estos.

Todos los funcionarios, contratistas y terceros, luego del proceso de vinculación deberán recibir una inducción o instrucción de lectura de las políticas y lineamientos de Seguridad y Privacidad de la Información como de las políticas de tratamiento y protección de datos, bajo la coordinación del grupo de Gestión Humana con el apoyo del Departamento de Sistemas; lo anterior 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.

8.3 Políticas de Gestión de Activos

Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de la Caja de Compensación Familiar de Boyacá - COMFABOY.

El uso de los activos dispuestos por COMFABOY para el apoyo de las labores desempeñadas por los funcionarios, contratistas o proveedores, se permitirá únicamente para ejecución de tareas establecidas en el ámbito laboral.

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

Se realizará una visita periódica según el cronograma anual de mantenimiento a las diferentes dependencias de la entidad por parte del equipo de profesionales del Departamento de Sistemas, para verificar si los programas utilizados e instalados son los autorizados y licenciados por Comfaboy.

No es permitido 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.

Los trabajadores de la Caja al usar los equipos de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en los discos duros o medios magnéticos.

Los bienes informáticos serán cargados al inventario del trabajador responsable y su movilización no se podrá realizar sin la aprobación de la dependencia que administre los bienes.

8.4 Política de Uso Adecuado de Internet y Redes Sociales

La Caja de Compensación Familiar de Boyacá - 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 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, portales de juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud al jefe del Departamento de Sistemas, para que sea autorizado y será objeto de auditorías de seguridad

mediante el módulo de seguridad web de la entidad.

Todos los funcionarios 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.

Toda información que sea publicada por las redes sociales como Facebook®, Twitter®, YouTube® LinkedIn® o blogs, entre otras, en un ambiente diferente al del departamento de mercadeo y comunicaciones, no se considera oficial, por consiguiente, no se podrá garantizar su confiabilidad, integridad y disponibilidad de la información.

El Departamento de Sistemas podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

8.5 Política de Uso Adecuado de Correo Electrónico

Las cuentas de correo asignados a los funcionarios, contratistas o terceros pertenecen a la Caja de Compensación Familiar de Boyacá - COMFABOY, por lo tanto, su contenido también es propiedad de la Entidad.

El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.

El Departamento de Sistemas podrá verificar el contenido de los buzones de los correos electrónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

8.6 Política de Manejo Disposición de Información, Medios y Equipos

La Caja de Compensación Familiar de Boyacá - COMFABOY, 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.

El soporte, instalación, mantenimiento y actualización de hardware sólo lo realizará el personal del Departamento 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 dependencia.

Los diferentes equipos tecnológicos se deben mantener libres de posters, papeles, fotos, calcomanías, artesanías, entre otros elementos que los puedan deteriorar o acortar su vida útil.

El Departamento de Sistemas de Comfaboy, contará 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.

Comfaboy posee un Software Antivirus licenciado y activo, el cual debe ser el único antivirus instalado y en uso en todos los equipos de cómputo propiedad de la entidad.

Los funcionarios de la caja, 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.

En el uso de impresoras de Comfaboy, se deben tener en cuenta los siguientes lineamientos:

. No tendrán acceso directo a internet sin pasar por el cortafuegos de red corporativo, ni siquiera para tareas de mantenimiento por parte del servicio de soporte.
. Se mantendrá actualizado el firmware para solucionar las posibles vulnerabilidades de seguridad detectadas; si la impresora es muy antigua y no dispone de soporte, se debe sustituir por otra más segura o desconectarla de la red.
. Si la impresora se conecta a la wifi, se extremarán las precauciones en la configuración de la wifi para proteger el acceso inalámbrico.
. Se cifrará el contenido de sus discos duros internos para proteger la información almacenada en ellos, y se procederá a realizar un borrado seguro del mismo cuando se sustituya o deseche el dispositivo o su disco duro de almacenamiento.

Comfaboy se reserva el derecho de monitorear los recursos tecnológicos (equipos de cómputo, portátiles, tablets entre otros), que estén conectados a su red de datos, y de los cuales se tenga sospecha que están poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información.

Las demás políticas incorporadas en la gestión de activos de información de la entidad, se encuentran definidas en las Políticas generales gestión tecnológica_v4 D-21-014.

8.7 Políticas de Uso de Dispositivos Móviles

El departamento logístico de Comfaboy, deberá llevar un registro y control de todos los dispositivos móviles que posee la Caja de Compensación y que están asignados a los determinados funcionarios (entrega y recibido de los dispositivos), los cuales deberán hacer buen uso de los dispositivos y destinarlos únicamente para el desempeño de sus funciones laborales u obligaciones contractuales.

Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para todos los dispositivos móviles, a cargo del departamento de logística.

Utilizar en los dispositivos móviles únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

El departamento de logística deberá asegurarse que los dispositivos puestos en servicios de los funcionarios cuenten con copias de seguridad periódicas, usen mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos como OneDrive, Dive, entre otros y cifrado de la información.

La Caja de Compensación Familiar de Boyacá - COMFABOY, tendrá el derecho a revisar la utilización del dispositivo móvil ante cualquier indicio de un uso inapropiado del mismo, inspeccionarlo o disponer de el de cualquier forma, dado que tanto el dispositivo móvil como la información almacenada es propiedad de Comfaboy.

8.8 Políticas de Seguridad Física y del Entorno

La Caja de Compensación Familiar de Boyacá - COMFABOY, cuenta con medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

Comfaboy definirá áreas seguras en sus instalaciones, junto con controles de acceso físico correspondientes para la protección de la información que allí se resguarda.

El área de sistemas tendrá acceso restringido a personas no autorizadas, según el responsable del área, al igual que los cuartos de equipos y cuartos de UPS.

La información es de acceso público e interno está protegida por Firewalls, con esquema de seguridad, además de contar con medidas básicas de control del perímetro y también debe contar con sistemas de detección de intrusos.

Todos los Trabajadores, deberán portar el carnet en un lugar visible, permitiendo con esto una mejor identificación y control de las personas que ingresan a las áreas de cómputo restringidas.

En los tomacorrientes donde se alimenten los equipos de cómputo, no se deben conectar otros equipos que interfieran con el consumo de energía.
Se debe propender por el uso de unidades ininterrumpidas de potencia UPS, para prevenir daños en los equipos ante ausencia de corriente.

Debe existir medidas contra fuego, agua, y otras similares.

8.9 Política de Control de Acceso Presencial y Remoto

Todos los funcionarios, contratistas y terceros de la Caja de Compensación Familiar de Boyacá - COMFABOY, deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información, considerándolas como importantes para el SGSI; dicho acceso será una única e intransferible identidad personal, ya sea carnet o documento de identificación, como credenciales para los distintos sistemas de información. El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Las acciones que involucren accesos desautorizados, impropios o el mal uso de recursos informáticos de la red están sujeto a sanciones disciplinarias.

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 Departamento de Sistemas.

El Servicio de acceso remoto a la red de datos de la entidad para funcionarios, contratistas y terceros, debe ser autorizada por el jefe de la dependencia, con el visto bueno y solicitud por correo electrónico 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.

8.10 Política de Establecimiento, Uso y Protección de Claves de Acceso

El Departamento de 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.

El usuario deberá cambiar periódicamente su clave de acceso de acuerdo a la criticidad de los sistemas de información que maneje.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose al Departamento 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.

Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

El administrador de la red y el administrador de la base de datos cambiará inmediatamente la clave de acceso a los empleados o contratistas que tengan ausencias definitivas de sus cargos o terminación de sus contratos; para que esto sea posible, cada jefe de área o dependencia debe informar por escrito al Departamento de Sistemas de Comfaboy sobre la novedad de personal, relacionando claramente los datos de los Trabajadores entrantes y salientes.

8.11 Políticas de Seguridad del Centro de Datos y Centros De Cableado.

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 o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
. Extraer información de los equipos en dispositivos externos.

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

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.

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.

Es indispensable que todos los cuartos de equipo tengan alimentación de corriente ininterrumpida (UPS) con capacidad de alimentar todos los equipos que se conectarán al centro de cableado, con el fin de mantener los servicios de red aún en casos de falla del fluido eléctrico.

8.12 Política de Respaldo y Restauración de Información

El objetivo de sacar las copias de respaldo es el de restituir la operación 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.

El Departamento de Sistemas de la Caja de Compensación Familiar de Boyacá - COMFABOY, debe resguardar con copias de seguridad la información sensible y critica de la entidad.

El lugar de almacenamiento para las copias mensuales y anuales deberá ser un sitio externo a la entidad, este sitio debe asegurar condiciones óptimas ambientales y de seguridad.

8.13 Políticas de Gestión de Incidentes

El Departamento de Sistemas de la Caja de Compensación Familiar de Boyacá - COMFABOY, se encargará de 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, como el formato f211076_Reporte_incidente_seguridad_informacion, con el fin de tomar oportunamente las acciones correctivas.

Toda la información relativa a los incidentes reportados al Departamento de Sistemas, debe ser manejada con total confidencialidad, que, a su vez reportará ante la autoridad competente los incidentes de seguridad que estén considerados como un delito informático.

8.14 Política de Escritorio Limpio

No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el escritorio virtual que puedan llegar a ser copiados, sustraídos o utilizados por terceros o por personal ajeno que no tenga autorización para su uso, su conocimiento o su divulgación.

Los funcionarios y contratistas de la Caja de Compensación Familiar de Boyacá - COMFABOY, que estén ubicados en puestos de atención al público, al momento de ausentarse de su puesto de trabajo deberán guardar la documentación y los medios magnéticos que estén al alcance de personas externas.

Cada vez que los funcionarios se ausenten de su lugar de trabajo deben bloquear los equipos de cómputo, para proteger el acceso a las aplicaciones y servicios de la institución de personal no autorizado.

Se deberán emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica

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 anualmente, 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.

10. 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.
- El Departamento de Sistemas será el encargado de recopilar y entregar a la Oficina de Auditoria 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 de seguridad derivado con el incumplimiento de las políticas.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	20/Mar/2024	Actualización General de Políticas

ELABORÓ	REVISÓ	APROBÓ
Nombre: Carlos Andrés Reyes Ramos **Cargo:** Analista I- Planeación y Calidad **Fecha:** 20/Mar/2024	**Nombre:** Orlando Rodriguez Castillo **Cargo:** Jefe Grupo Sistemas **Fecha:** 20/Mar/2024	**Nombre:** Jaime Fernando Diaz Molina **Cargo:** Jefe Departamento de Planeación e Informática **Fecha:** 20/Mar/2024