POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAJA DE COMPENSACIÓN FAMILIAR DE ARAUCA COMFIAR

TABLA DE CONTENIDO

1. OBJETIVO 4

2. ALCANCE 5

3. REVISIÓN DE LA POLÍTICA 6

4. DEFINICIONES 7

5. ENFOQUE BASADO EN PROCESOS 8

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9

7. PRINCIPIOS QUE SOPORTAN LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE COMFIAR
10

8. CLASIFICACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE COMFIAR.
11

8.1 Seguridad de los Recursos Humanos 11
8.1.1 Antes de la Contratación Laboral 11
8.1.2 Roles y responsables 11
8.1.3 Durante la Vigencia del Contrato Laboral 11
8.1.4 Terminación o Cambio de la Contratación Laboral 11

8.2 Gestión de Activos 12
8.2.1 Instalaciones de equipos de cómputos y comunicaciones 12
8.2.2 Dispositivos móviles, teletrabajo o trabajo remoto 13

8.3 Control de acceso a equipos de cómputo, de comunicaciones y plataformas. 14
8.3.1 Control de acceso con usuario y contraseña 14
8.3.2 Gestión de Contraseñas. 15
8.3.3 Control de acceso remoto 15
8.3.4 Control de acceso a la Web 15
8.3.5 Seguridad Física y del Entorno 16
8.3.5.1 Perímetro de Seguridad Física 16
8.3.5.2 Acceso a áreas críticas 16

8.3.5.3 Protección Contra Amenazas Externas y Ambientales..... 17
8.3.6 Mantenimientos de equipos de cómputo.....17

8.4 Gestión de Software 18
8.4.1 Adquisición de software 18
8.4.2 Instalación del Software 18
8.4.3 Actualización de Software 19
8.4.4 Auditoria de Software instalado..... 19
8.4.5 Software e información propiedad de COMFIAR 19
8.4.6 Supervisión y Evaluación. 20

8.5 Gestión de Comunicaciones y Operaciones 20
8.5.1 Respaldo 20
8.5.1.1 Respaldo de la Información..... 20

9. COMPROMISOS DE LA ALTA DIRECCIÓN..... 22

10. GENERALES..... 23

11. SANCIONES..... 24

12. RECOMENDACIONES 25

13. VIGENCIA..... 26

1. OBJETIVO

Establecer lineamientos para la adecuada gestión de la seguridad y privacidad de la información de la Caja de Compensación Familiar de Arauca COMFIAR, basado en la identificación y valoración de los riesgos de la información utilizada por la corporación, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio, donde se garantice el cumplimiento de la normatividad vigente en toda la organización.

2. ALCANCE

Los lineamientos contenidos en la presente política se aplican a la información circulante en el Mapa de Proceso (Tablas de Retención Documental) documentos y demás información que administre, proteja y preserve la Caja de Compensación Familiar de Arauca COMFIAR y cualquier entidad que ejerza en su nombre o a través de convenios, recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con el personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos

3. REVISIÓN DE LA POLÍTICA

La Política de Seguridad y Privacidad de la Información se debe revisar a intervalos planificados o cuando se produce cambios significativos para garantizar que sigue siendo adecuada, suficiente y eficaz.

La política de seguridad y privacidad de la información está a cargo como responsable el Jefe de Sección Tecnología y Programación el cual revisará y valorará dicha política. Dicha revisión incluye las oportunidades de evaluación para mejorar la política de seguridad y privacidad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias de la corporación, las condiciones legales o el entorno técnico.

Se debe tener en cuenta los resultados de la revisión por parte del responsable. Debe existir procedimientos definidos para la revisión por la Dirección Administrativa, incluyendo una programación o periodo de revisión.

las entradas para la revisión por la Dirección Administrativa incluyen información sobre:

- Retroalimentación de las partes interesadas.
- Resultados de las revisiones independientes.
- Estado de las acciones preventivas y correctivas.
- Resultado de las revisiones previas por parte de la dirección.
- Desempeño del proceso y cumplimiento de la política de seguridad y privacidad de la información.
- Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.
- Tendencias relacionadas con las amenazas y vulnerabilidades.
- Incidentes de seguridad de la información reportados.
- Recomendaciones de las autoridades pertinentes.

4. DEFINICIONES

Con el objetivo de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben algunas de las definiciones [**NTC-ISO7IEC 27001-27002**].

- COMFIAR: Caja de Compensación Familiar de Arauca
- Activo(s): Cualquier cosa que tiene valor para la organización. [NTC 5411- 1:2006]
- Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- Directriz: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en la política.
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad puede estar involucradas
- Política: Tú intención y directriz expresada formalmente por la dirección.
- Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
- Análisis de riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- Evaluación de riesgos: Todo proceso de análisis y valoración del riesgo.
- Amenazas: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
- Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.
- Open-Source: también llamado “Código Abierto” es un término que se utiliza para denominar a cierto tipo de software que se distribuye mediante una licencia que le permite al usuario final, si tiene los conocimientos necesarios, utilizar el código fuente del programa para estudiarlo, modificarlo y realizar mejoras en el mismo, pudiendo incluso hasta redistribuirlo
- GLPI: (acrónimo: en francés, Gestionnaire Libre de Parc Informatique), es un software que permite gestionar el área tecnológica de una organización.
- ERP (Planificación de Recursos Empresariales): es un conjunto

de aplicaciones de software integradas, que nos permiten automatizar la mayoría de las prácticas de Comfiar relacionadas con los aspectos operativos o productivos de nuestra empresa, facilitando y centralizando la información de todas las áreas que la componen: compras, producción, logística, finanzas, recursos humanos, marketing, servicios, proyectos y atención al cliente

- SGSI: Sistema de gestión de seguridad de la Información.

5. ENFOQUE BASADO EN PROCESOS

Basado en el enfoque de procesos adoptado por la Caja, la Sección de Desarrollo de TIC hace parte del Proceso de Gestión Administrativa, será la responsable de velar por el cumplimiento de la política y directrices en el manejo de seguridad de la información. De igual manera todos los procesos son responsables del cumplimiento de esta política.

- Planificar (establecer el SGSI)
- Hacer (Implementar y operar el SGSI)
- Verificar (Hacer Seguimiento y revisar el SGSI)
- Actuar (Mantener y mejorar el SGSI)

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección Administrativa de la CAJA DE COMPENSACIÓN FAMILIAR DE ARAUCA COMFIAR, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con 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. Para COMFIAR, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

COMFIAR orienta sus esfuerzos con el fin de proteger, asegurar, preservar, conservar y administrar la confidencialidad, integridad, autenticidad, no repudio y disponibilidad de la información, así como el buen uso de esta en medio magnético y/o físicos de los afiliados, beneficiarios, comunidad en general y partes interesadas, teniendo en cuenta el cumplimiento de los requisitos legales aplicables.

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

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.

- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de COMFIAR.
- Garantizar la continuidad de la corporación frente a incidentes.
- COMFIAR ha decidido definir, implementar, operar y mejorar de forma continua de un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros de acuerdo a las necesidades de la Caja, y a los requerimientos regulatorios.

7. PRINCIPIOS QUE SOPORTAN LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACIÓN DE COMFIAR

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los trabajadores, proveedores, socios de negocio o terceros.
- Proteger la información generada, procesada o resguardada por los procesos de Comfiar, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- Salvaguardar la información creada, procesada, transmitida o resguardada por sus procesos de la corporación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Aplicar las herramientas al alcance para proteger la información de las amenazas originadas por parte del personal.
- Proteger las instalaciones físicas de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de los procesos de la corporación garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar control de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Asegurar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Garantizar la disponibilidad de los procesos de Comfiar y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Cumplir con las obligaciones legales, regulatorias y contractuales establecidas.

8. CLASIFICACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACIÓN DE COMFIAR.

8.1 Seguridad de los Recursos Humanos

8.1.1 Antes de la Contratación Laboral

Se debe cumplir con el procedimiento PR-RH-01 “PROCEDIMIENTO DE SELECCIÓN Y CONTRATACIÓN DE PERSONAL”; además asegurar que los contratistas y usuarios externos, entiendan sus responsabilidades y que estos sean apropiados y se ajusten a los roles para los que se les considera, esto para reducir el riesgo de robo, fraude o uso de las instalaciones. Para los empleados de esta Corporación lo anterior se realizará una vez se haya suscrito el vínculo contractual.

8.1.2 Roles y responsables

Es responsabilidad de los empleados de Comfiar:

- Proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizada.
- Implementar y actuar de acuerdo con las políticas de seguridad de la información de la Corporación.
- Garantizar que se asigne la responsabilidad a la persona que tome las acciones.
- Informar los eventos de seguridad, los eventos potenciales u otros riesgos de seguridad.
- Cumplir con los acuerdos de confidencialidad

8.1.3 Durante la Vigencia del Contrato Laboral

- Asegurar que todos los empleados, contratistas y usuarios visitantes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados parar apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el error humano mediante concientización, educación y formación en los procedimientos de seguridad y el uso correcto de los servicios y de la información para minimizar los posibles riesgos de seguridad.

8.1.4 Terminación o Cambio de la Contratación Laboral

- Asegurar que los empleados, los contratistas y los usuarios visitantes salgan de la organización o cambien su contrato laboral de forma ordenada.

- En el momento que un empleado, contratista o usuario termine su contrato con esta entidad, se debe asegurar la completa devolución de todo el equipo y la cancelación de todos los derechos de acceso a estos, a la red, correos institucionales, a toda la información y a los aplicativos de la corporación.

8.2 Gestión de Activos

8.2.1 Instalaciones de equipos de cómputos y comunicaciones

- Todo equipo de cómputo y de comunicaciones (computadoras, servidores, estaciones de trabajo, equipos de acceso y de distribución) que sean propiedad de Comfiar, debe sujetarse a las normas y procedimientos de instalación que emite la Sección de Desarrollo de TIC.
- La Sección de Infraestructura y Activos elaborara cronograma de toma de inventarios anual, para la verificación y actualización de estos de acuerdo con el procedimiento PR-IA-02 “Procedimiento Inventario de Activos Fijos”.
- La Sección de Infraestructura y Activos es la responsable de mantener actualizados los inventarios y registros de activos tecnológicos (equipos de computación y de comunicaciones) en el módulo de Activos pertenecientes a Comfiar, los cuales están cedulados (inventariados) de tal manera que puedan ser ubicados, identificados y registrada su trazabilidad desde de su compra y deberá registrar toda actividad de este (trazabilidad y/o repotenciación).
- El custodio del activo responderá por su protección física, así como la información que allí almacene en caso de que sea un equipo de cómputo, dispositivo móvil o de almacenamiento resaltando que es obligación hacer buen uso de este.
- Los movimientos (traslado de activos) en caso de que existan, el responsable del activo deberá notificar a la Sección de Infraestructura y Activos mediante el diligenciamiento del respectivo formato de reintegro a Almacén.
- Mediante el diligenciamiento del formato FT-IA-03 “Reintegro a Almacén” los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo, contrato que se tenga con la entidad o un traslado interno a otra dependencia.
- Se ejecuta el proceso mediante el cual se realiza de forma segura y correcta la eliminación, retiro, traslado o re-uso cuando ya no se

requieran los activos.

- Mediante el procedimiento de copias de seguridad el cual determina la toma de backup de los activos evitando así el acceso o borrado no autorizado de la información, este procedimiento contiene las correspondientes autorizaciones y aplica tanto para medios removibles (todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores) como activos de procesamiento y/o almacenamiento de información.

8.2.2 Dispositivos móviles, teletrabajo o trabajo remoto.

- Todos los trabajadores, contratistas o terceros que tengan acceso a las redes inalámbricas deben cumplir con los lineamientos de control de acceso a la red contemplados en él; y que tengan acceso de la información propiedad de COMFIAR, tienen la obligación y responsabilidad de dar buen uso a la información cumpliendo con los controles de seguridad que protegen el buen uso de la tecnología y de la información así como como las revisiones de seguridad que la corporación utilice para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.
- Los dispositivos (hardware) que se quieran conectar a la red de Comfiar deberán ser autorizados por la Sección de Desarrollo de TIC mediante el registro en la lista ARP tanto para redes físicas e inalámbricas
- Los usuarios logueados a las diferentes redes inalámbricas deberán permitir el acceso a su equipo para verificación de dirección física de la tarjeta de red "MAC", y se le asignará usuario y contraseña válida para única conexión y exclusiva para el equipo registrado cumpliendo los parámetros de gestión de contraseñas.
- Si el equipo de cómputo portátil se conectará por cable está sujeto a la misma revisión anteriormente descrita.
- Los computadores portátiles y/o dispositivos móviles de propiedad de los trabajadores no se incluirán en el dominio ccfcomfiar.local o cualquiera que funcione dentro de las instalaciones de COMFIAR sin antes cumplir con los lineamientos referentes a seguridad de la información.
- Para la modalidad teletrabajo en caso de que se llegue a dar, la Sección de Desarrollo de TIC suministrará las herramientas tecnológicas (VPN, usuarios a plataformas, etc.) para acceder a la información, estableciendo las condiciones de seguridad y privacidad de la información, de acuerdo con la Resolución 2133 de 2018 y las enmarcadas en el Libro Blanco del Teletrabajo o cualquiera que la adicione, modifique o complemente.

- Para la modalidad de trabajo en casa o trabajo remoto la cual es improvisada por la circunstancia, se debe solicitar mediante la plataforma de mesa de ayuda GLPI, el acceso a las diferentes plataformas y conexiones remotas a la información, especificando las fechas en que se va a realizar las actividades de manera remota.
- La Sección de Desarrollo de TIC debe realizar monitoreo sobre las conexiones y los servicios tecnológicos a las que el teletrabajador tiene acceso

8.3 Control de acceso a equipos de cómputo, de comunicaciones y plataformas.

8.3.1 Control de acceso con usuario y contraseña

- La Sección de Recursos Humanos, notifica a la Sección de Desarrollo de TIC el ingreso de los colaboradores para que le sean creadas las credenciales de acceso a las plataformas GLPI y ORFEO; así mismo, cuando haya traslado para que le sea cambiado el perfil y/o dependencia; también cuando suspensión, vacaciones o terminación del contrato para que le sea suspendidos todas las credenciales de accesos a las plataformas que conforma la ERP.
- Los jefes inmediatos de los colaboradores contratados solicitan mediante la plataforma de mesa de ayuda GLPI, creación de las credenciales de registro a las diferentes plataformas que podrán acceder; así como a qué equipo de cómputo para acceder a la información y desarrollar sus funciones.
- Los usuarios y contraseñas son de uso personal e intransferibles; no se debe prestar ni compartir.
- Cada equipo de cómputo tiene dos inicios de sesión el cual uno pertenece a la sesión de Desarrollo de TIC o de algún colaborador de la Sección de Desarrollo de TIC que tienen todos los permisos de administrador el cual permita la instalación o desinstalación de hardware de ser necesario, y el otro usuario pertenece al responsable del activo que tiene permisos de invitado, lo cual lo limita a realizar cualquier tipo de instalación y modificación de software.
- Cada usuario al que se le haya asignado usuario y contraseña para loguearse a un equipo de cómputo tiene carpeta acceso a una compartida en el servidor de datos que se encuentran en el dominio ccfcomfiar.local.
  - Si algún equipo de cómputo está afectando el óptimo rendimiento de la red, la Sección de Desarrollo de TIC está en la facultad de desconectarlo y verificar en presencia del custodio del activo el problema o hecho presentado, con el fin de solucionar el

inconveniente.

- La Sección de Desarrollo de TIC es la responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
- La Sección de Desarrollo de TIC es la responsable de difundir el reglamento para el buen uso de la red y procurar su cumplimiento.
- Todo equipo de cómputo que esté o sea conectado a la red y que no sean propiedad de COMFIAR, debe tener licencia de sistema operativo y antivirus en caso de ser necesario (Sistema operativo Windows) y debe sujetarse a los procedimientos de acceso, restricciones y demás políticas de seguridad que emita le Sección de sistemas.
- El acceso lógico a equipos especializados de cómputos (servidores, enrutadores, bases de daos, etc.) conectado a la red es administrado por la Sección de Desarrollo de TIC.

8.3.2 Gestión de Contraseñas.

- El parámetro de contraseña debe contener como longitud mínima 8 caracteres, mínimo un número, una minúscula, una mayúscula, un símbolo.
- Para acceso a aplicaciones se adiciona un captcha de seguridad.
- La contraseña de acceso a la sesión se configura para que que tenga un ciclo de vida de 30 días; esto garantiza la protección del acceso de usuarios o terceros no autorizados.
- Se asigna una contraseña temporal al usuario para cuando realice su primer acceso, el sistema le solicite el cambio inmediato de la contraseña temporal cumpliendo con los parámetros de seguridad de contraseñas. Aplica para acceso al equipo de cómputo y para acceso a aplicaciones de ERP (Planificación de Recursos Empresariales) corporativo.
- Los manuales de configuración, contraseñas y documentación técnica los equipos de cómputo y servidores se manejará como documentos confidenciales, con acceso únicamente del personal autorizado para manipular esta información.

8.3.3 Control de acceso remoto

- La Sección de Sistemas es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
- Los puertos de acceso remotos a los servidores y sistemas de información tanto por la Web (externos) como por la red interna de la Corporación, se encuentran bloqueados; únicamente se podrá acceder de manera presencial a estos servidores.
- Si se establece algún tipo de soporte o mantenimiento remoto con algún tipo de proveedor, se debe reprogramar el acceso remoto a los puertos de acceso, fecha, duración del soporte.
- La empresa encargada del soporte deberá sujetarse a las políticas de seguridad y en concordancia con los lineamientos generales de uso de la Internet.

8.3.4 Control de acceso a la Web

- La Sección de Desarrollo de TIC emite y socializa las políticas de privacidad y condiciones de navegación web, uso de la Internet, páginas institucionales y demás permitidas para el acceso seguro.
- Los accesos a las páginas web a través de los navegadores se sujetan a las normas que previamente se establecieron en la Sección de Desarrollo de TIC la cuales están aprobadas por la alta dirección

- Se realizan seguimientos a las restricciones de navegación las cuales permiten el óptimo funcionamiento establecidas para cada funcionario.
- Toda página de navegación que no está permitida se niega el acceso.
- Toda información que se envíe vía Web y que tenga fines corporativos referentes a Comfiar, debe llevar como firma digital el nombre del propietario o administrador de la cuenta de correo, cargo, dirección, teléfono incluyendo la extensión, y el enunciado de confidencialidad de la Corporación.
- Toda aplicación Web corporativa cuenta con certificado SSL el cual permite la transferencia de datos cifrados entre un navegador y un servidor web.

8.3.5 Seguridad Física y del Entorno

Tiene como objetivo principal evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la Corporación.

Los servidores que prestan los diferentes servicios en la corporación están ubicados en la primera planta de la Sede Administrativa ubicada en la Calle 22 # 16-51.

Están aislados de todo contacto del personal no autorizado, daño e interferencia con cualquier otra señal que afecte el perfecto funcionamiento de los sistemas de información en el Data Center.

8.3.5.1 Perímetro de Seguridad Física

- Se utiliza un perímetro de seguridad (paredes, puertas con llaves) que protegen el área que contiene los servidores (Data Center) con la información de la corporación.
- El Data Center cuenta con puerta contra incendios, termómetro para control de temperatura, iluminación de emergencia, cámara de seguridad, alarmas visuales y de ruido según con el código local de incendios.

8.3.5.2 Acceso a áreas críticas.

- Se debe proteger la ubicación física de todo activo tecnológico y de información que permite brindar el óptimo rendimiento y funcionamiento de los sistemas de información.
- Los equipos de la corporación que sean de propósito específico y sirvan como herramienta para el desarrollo de las funciones, requiere

estar ubicado en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales, alimentación eléctrica (protección con estabilizador o ups), y su acceso.

- El personal de la Sección de Desarrollo de TIC y de la Sección de Infraestructura y Activos son los únicos facultados para

  adecuaciones físicas, reubicaciones y todo aquello que implique movimientos de equipos de cómputo.
- Las áreas donde se tienen equipos de cómputo como los equipos de las auxiliares de subsidio, auxiliar de aportes y atención al cliente, están sujetas a fácil vigilancia del personal de seguridad privada de COMFIAR y circuito cerrado de televisión CCTV.
- El acceso a servidores y al Data Center, es exclusivo del personal de la Sección de Sistemas. Si es necesario la instalación de algún equipo nuevo, mantenimiento, revisión, soporte técnico etc., éste se realiza bajo la supervisión y acompañamiento de cualquier colaborador de la Sección de Desarrollo de TIC. Si es personal externo, se debe diligenciar el formato FT-IA-04 Registro Control De Acceso A Personal Externo Para Soporte Técnico.
- Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las directivas de la corporación

8.3.5.3 Protección Contra Amenazas Externas y Ambientales

- Se tienen en cuenta todas las amenazas para la seguridad que presenta las instalaciones circundantes tales como: incendios, fuga de agua, atentados terroristas, explosiones, etc.
- Los materiales combustibles o peligrosos se almacenan a una distancia prudente del área de seguridad.
- Se cuenta con el suministro de equipo apropiado contra incendios (Extintores de los siguientes tipos: polvo químico seco ABC, dióxido de carbono, Solcaflan y de agua) y están ubicados adecuadamente según estudio.

8.3.6 Mantenimientos de equipos de cómputo.

- A la Sección de Desarrollo de TIC corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar.
- Todo mantenimiento de dispositivos de comunicación por parte de algún proveedor, personal externo o terceros, se debe verificar con la existencia de un contrato de soporte de mantenimiento, una solicitud,

orden de servicio u autorización realizada a dicha entidad o actividad programada; se debe validar y tomar nota de los datos del personal técnico antes que se lleve a cabo la actividad, si éstos deben tener acceso al data center de la Sede Administrativa, se debe diligenciar el formato FT-IA-04 (Registro Control De Acceso A Personal Externo Para Soporte Técnico).
La Sección de Desarrollo de TIC elaborará y ejecutará un cronograma de mantenimiento preventivo formato FT-IA-01 "Cronograma de Mantenimiento Preventivo de Equipo de Cómputo y

Planta Eléctrica" al inicio de cada año; aclarando que está sujeto a actualizaciones por novedades en adquisiciones o bajas de equipos; dicho mantenimiento se realiza a todos los equipos de cómputo de la Corporación y se registra en el formato Control de Mantenimiento Preventivo y Correctivo a equipos de Cómputo y Periféricos" código: FT-TI-02.

- No es permitido al personal de la Sección de Desarrollo de TIC realizar cualquier tipo de mantenimiento, manipulación de equipos de cómputo o de telecomunicaciones que no sea propiedad de Comfiar; excepto aquellos que estén autorizados mediante un convenio o contrato.

8.4 Gestión de Software

8.4.1 Adquisición de software

- La Sección de Desarrollo de TIC es la encargada de presupuestar anualmente la renovación y adquisición de programas como sistemas operativos, antivirus, etc. con sus respectivas licencias, en caso de que los programas no sean Open- Source.
- La Sección de Desarrollo de TIC es la encargada de instalar y en caso de que sea necesario distribuir los instaladores y licencias de los diferentes programas adquiridos para la Corporación.
- La Sección de Desarrollo de TIC promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
- La Sección de Desarrollo de TIC es la encargada de realizar mantenimiento preventivo y/o correctivo al software instalado en los equipos de cómputo de la Corporación.
- Cuando se adquiere nuevos sistemas de información se tiene en cuenta lo recibido cumpla con lo ofertado; cada proceso y/o reporte y

en caso de tener la aprobación de otra área, ésta se incluye para determinar si cumple con el objeto de la compra.

8.4.2 Instalación del Software

- Corresponde únicamente a la Sección de Desarrollo de TIC instalar software de cualquier aplicación, sistema operativo, o programas en cualquier equipo de la Corporación.
- En los equipos de cómputo, de telecomunicaciones y en dispositivos

  basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado, adquirido por compra y/o OpenSource.
- El personal de la Sección de Desarrollo de TIC son los únicos autorizados para la instalación, desinstalación de cualquier software, firmware o actualización en los equipos de cómputo y de comunicaciones lo cuales deben ser licenciados o con licenciamiento libre (OpenSource).
- La Sección de Desarrollo de TIC es la responsable de brindar asesoría y supervisión para la instalación de software informático.
- La instalación de software que desde el punto de vista pueda poner en riesgo los recursos informáticos o activos de corporación no está permitida.
- La protección lógica de los sistemas corresponde a quienes en un principio se les fue asignado y les compete notificar cualquier anomalía a la Sección de Desarrollo de TIC.

8.4.3 Actualización de Software

- La adquisición y actualización de software para cada equipo de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con las fechas de vencimientos de licencias o renovaciones de software.
- Corresponde a la Dirección Administrativa autorizar cualquier adquisición y actualización del software, con el visto bueno de la Sección de Desarrollo de TIC, de lo contrario esta Sección no se hará responsable de adquisiciones en cuanto a su calidad y buen funcionamiento.

8.4.4 Auditoria de Software instalado

- La Sección de Desarrollo de TIC es el responsable de realizar revisiones periódicas para asegurarse que sólo software con licencia

paga por Comfiar esté instalada en los equipos de cómputo.

- En caso de que haya algún tipo de violación por contraseña y se encuentre instalado algún tipo de software no autorizado, se debe generar un reporte a la Dirección Administrativa para que tome acciones al respecto.

8.4.5 Software e información propiedad de COMFIAR

- Todo software, licencias, bases de datos y lo referente a programación adquirida por la Corporación sea por compra, donación

o cesión es propiedad de COMFIAR, y mantendrá los derechos que la ley de propiedad y privacidad los permita.

- Las bases de datos propias de COMFIAR, no son de uso comercial, cualquier difusión de estas no autorizada, tendrá sanciones disciplinarias y legales de acuerdo con lo permitido por la ley para la protección de la información y de los datos, ya que, va en contra del patrimonio de la Corporación y la Ley Estatutaria 1581 de 2012, Ley de Habeas Data.
- Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces, aplicativo SYS) desarrollados o adquiridos con o a través de los recursos de la Corporación, se mantendrán como propiedad de COMFIAR respetando la propiedad intelectual del mismo.
- Cada funcionario tiene la responsabilidad de mantener asegurado y respaldada la información interna de la Corporación, para ello debe realizar copia a la unidad D.
- Los datos, bases de datos, y la información generada por el personal y los recursos informáticos de la Corporación están asegurados con copias de seguridad almacenados en un servidor local y otro en la nube.
- Corresponde a la Sección de Desarrollo de TIC difundir y promover los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos, como el periodo que se deben realizar.

8.4.6 Supervisión y Evaluación.

- Cada equipo de cómputo que esté en riesgo la seguridad u operatividad, los usuarios custodios de estos activos deberán comunicar en el menor tiempo posible a la Sección de Desarrollo de TIC para que actúen y tomen acciones preventivas o correctivas para el bien de estos activos y la información.

- Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física, es coordinada con la Sección de Desarrollo de TIC para que no afecte la operación ni la seguridad de la empresa.
- Para efectos de seguridad de la red, se realiza monitoreo constante sobre todos y cada uno de los servicios que disponga en ese momento Comfiar.
- Los sistemas considerados críticos, están bajo monitoreo permanente.

8.5 Gestión de Comunicaciones y Operaciones

Asegurar la operación correcta y segura de los servicios de procesamiento de información.

8.5.1 Respaldo

Se mantiene la integridad y disponibilidad de la información y los servicios de procesamiento de información.

8.5.1.1 Respaldo de la Información.

Se realizan diariamente copias de respaldo de la información y de software.

- Se tiene servidor de copias de seguridad (Backup) local, donde se guarda toda la información que es generada por los trabajadores (ofimáticos y otros) y las fuentes y datos de las diferentes plataformas que tiene Comfiar en propiedad y o terceros.

- Se tiene servicio en la Nube donde se envían en manera inmediata las copias generadas en el servidor local de Copias de Seguridad.

Las copias de seguridad tendrán como consideración los siguientes lineamientos:

- El respaldo de los datos del aplicativo interno de la Caja, se realiza diariamente de la base datos y cada viernes de las fuentes del software.
- Se Clasificó y definió los niveles necesarios para la información de respaldo. Con excepción a los funcionarios de recreación y deportes, publicidad y mercadeo, eventos y programas especiales, ningún otro funcionario tendrá derecho a realizar el respaldo de imágenes, música y videos (contenido multimedia), el restante de funcionarios solamente se les salvaguardará archivos tales como documentos con extensiones (doc, docx, docm, txt, pdf, ppt, pptx, ppsx, sldx, xls, xlsx, csv).

- No se debe guardar respaldo de archivos personales Se usará el siguiente método de copias de seguridad
- Primero se crea una carpeta dentro del disco local (D:) la cual contenga todo el contenido a realizar el proceso de copia de seguridad según las consideraciones y clasificaciones vistas anteriormente.
- La primera copia o Backup es completo. Se crea una copia de resguardo de todas las carpetas y archivos que contenga la carpeta

  del disco D en la herramienta para hacer el Backup. Es ideal para crear la primera copia de todo el contenido de una unidad o bien de sus archivos de datos solamente.
- Después procedemos a realizar el Backup diferencial el cual compara el contenido de los archivos a la hora de determinar cuáles se modificaron de manera tal que solamente copia aquéllos que hayan cambiado realmente y no se deja engañar por las fechas de modificación de los mismos.
- Esta copia de seguridad se realizará diariamente una vez sea creado el archivo o que registre alguna novedad.
- Ningún documento magnético que tenga información de interés institucional podrá ser difundido, distribuidos o comercializados.

9. COMPROMISOS DE LA ALTA DIRECCIÓN.

- La Dirección Administrativa acepta la Política de Seguridad y Privacidad de la información; así como la implementación, operación, seguimiento, revisión, mantenimiento y mejora.
- Establecer funciones y responsabilidades de la Seguridad de la Información.
- Hacer cumplir con los planes de capacitación y/o divulgación de la Política de Seguridad y Privacidad de la Información.
- Brindar los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisión, mantener y mejorar la Política de Seguridad y Privacidad de la Información.
- Asegurar la realización de auditorías internas a la Política de Seguridad y Privacidad de la Información.
- Revisar la eficacia de la implementación de la Política de Seguridad y Privacidad de la Información.

10. GENERALES

La Sección de Desarrollo de TIC debe emitir y dar a conocer el plan de contingencia de Sistemas.

11. SANCIONES

- Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo con el reglamento interno de COMFIAR y el código penal en los artículos que refiere a la protección de la información y de los datos.
- Las sanciones pueden ser desde una llamada de atención al empleado hasta la suspensión del servicio dependiendo de la gravedad de la falta que esta manifiesta.
- Cualquier acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso o no autorizado, violación de datos personales y corporativos, suplantación de sitio web para capturar datos personales, violación a las políticas de seguridad de la información, políticas de privacidad y condicione de navegación web, hurto por medios informáticos semejantes, transferencia no consentida de activos y demás delitos informáticos, puede ser sancionado de acuerdo al reglamento interno y código penal.

12. RECOMENDACIONES

Estas Políticas de Seguridad deberá seguir un proceso de actualización periódica, sujeta a los cambios organizacionales relevantes; crecimiento de la planta de personal, cambio de infraestructura computacional, implementación de nuevas tecnologías y servicios, etc.

Este documento debe ser difundido a todo el personal de COMFIAR.

13. VIGENCIA

Esta Política de seguridad y privacidad de la información que expide la Caja de Compensación Familiar de Arauca – COMFIAR, rige a partir de su publicación y deroga todas las disposiciones que le sean contrarias.

Finalmente, el presente documento fue aprobado por la Agente Especial de Intervención mediante Resolución AEI No. 066 de 27 de diciembre de 2024.

ADRIANA MERCEDES BONILLA M.
Agente Especial de Intervención.

YANCY ESTELLA HINOJOSA RUIZ
Directora Administrativa Segunda Suplente