

PRESENTACIÓN

Director

Juan Eduardo Zuluaga Perna

Secretaria General

Ines Adriana Valencia Galeano

Auditora

Angela Medina Casas

Gerente Productividad y Desarrollo

Héctor Andrés Abadía García

Gerente de Tecnología

Carlos Andrés Duque Quintero

Gerencia de datos

Carlos Andres Bastidas Silvera

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Publicación Corporativa

Manizales, mayo de 2026

CONTENIDO

1. INTRODUCCIÓN.

- 1.1 Política de SGI
- 1.2 Objetivo
- 1.3 Alcance
- 1.4 Documentos de referencia
- 1.5 Terminología básica sobre seguridad de la información
- 1.6 Adaptación y estructura de la norma

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- 2.1 Organización interna
- 2.2 Roles y responsabilidades

3. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

- 3.1 Antes de asumir el empleo
- 3.2 Durante la ejecución del empleo
- 3.3 Terminación y cambio de área

4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN TECNOLÓGICOS

- 4.1 Responsabilidad sobre los activos de información tecnológicos de Confa por parte de las Áreas
- 4.2 Uso aceptable de los activos de información tecnológicos
- 4.3 Devolución de los activos de información tecnológicos
- 4.4 Manejo de los medios de Almacenamiento

5. CONTROL DE ACCESOS

- 5.1 Requisitos de acceso a zonas sensibles
- 5.2 Requisitos de las áreas para el control de acceso a los sistemas de información
- 5.3 Gestión de acceso de usuario de Confa
- 5.4. Control de acceso a plataforma, bases de datos y sistemas de información de Confa
- 5.5 Responsabilidades de los usuarios

6. CIFRADO/CRİPTOGRAFÍA

- 6.1 Controles Criptográficos

7. CONTROLES FÍSICOS

- 7.1 Áreas Seguras
- 7.2 Seguridad de los equipos
- 7.3 Puestos de trabajo despejado y bloqueo de pantalla

8. CONTROLES TECNOLÓGICOS

- 8.1 Protección contra el código Malicioso
- 8.2 Copias de seguridad
- 8.3 Control del software en explotación
- 8.4 Registro y seguimiento
- 8.5 Gestión de vulnerabilidades
- 8.6 Consideraciones sobre auditorías de sistemas de información

9. SEGURIDAD DE LAS TELECOMUNICACIONES

- 9.1 Gestión de seguridad en las redes de datos
- 9.2 Segmentación o separación de las redes
- 9.3 Intercambio de información con terceros
- 9.4 Políticas de uso de internet
- 9.5 Uso del correo electrónico corporativo
- 9.6 Política de transferencia de información

10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- 10.1 Requerimientos de seguridad de los sistemas de información
- 10.2 Seguridad en los procesos de desarrollo y de soporte
- 10.3 Datos de prueba

11. SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- 12.1 Proceso de gestión de incidentes de seguridad de la información con mejoras constantes

13. TRABAJO AUTÓNOMO

- 13.1 Política de trabajo autónomo

14. SEGURIDAD Y USO DE DISPOSITIVOS MÓVILES

- 14.1 Política de seguridad y uso de dispositivos móviles

15. SOPORTE REMOTO DE LOS ACTIVOS DE LA ORGANIZACIÓN

- 15.1 Política de soporte remoto de los activos de la organización.
- 15.2 Responsabilidades del auxiliar mesa de ayuda
- 15.3 Responsabilidades del usuario colaborador
- 15.4 Responsabilidades del supervisor administrativo/técnico del contrato

16. BORRADO/FORMATEO SEGURO

- 16.1 Activos de información en Confa
- 16.2 Metodología de entrega del proveedor/contratista/prestador de servicios y/o tercero

17.POLÍTICA DE USO DE INTELIGENCIA ARTIFICIAL (IA) EN LA ORGANIZACIÓN

17.1 Propósito

17.2 Ámbito de aplicación

18.CUMPLIMIENTO LEGAL

18.1 Cumplimiento de los requisitos legales y contractuales

18.2 Protección de los registros

18.3 Revisiones de la seguridad de la información.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Fecha de la versión:	Mayo 6 de 2026
Creado por:	Profesional de Auditoría TIC Profesional de Datos e Informes Profesional Seguridad de la Información Profesional de Tecnología
Nivel de confidencialidad:	Medio sólo corporativo

HISTORIAL DE CAMBIOS

Fecha	Versión	Creado por	Descripción de la modificación
	1.0	Analista de Seguridad	Descripción básica del documento
15/03/2016	1.0	Analista de Seguridad	Cambios dados por un abogado laboral.
05/05/2020	2.0	Profesional de Gestión organizacional	Revisión y concepto seguridad de la información
11/05/2020	2.0	Profesional Seguridad de la información	Cambio general al documento
11/05/2020	2.0	Profesional Auditora TIC	Revisión y Cambios políticas seguridad de la información
22/05/2020	2.0	Comité de Licencia y Seguridad de la Información	Revisión, concepto y cambios en la Política de Seguridad de la Información
06/06/2020	2.0	Auditora	Revisión y concepto seguridad de la información
14/08/2020	2.0	Profesionales Auditoría	Revisión y concepto seguridad de la información
07/09/2020	2.1	Profesional de Seguridad	Adecuación de políticas en la Organización de la seguridad de la información, Seguridad de recursos humanos, Seguridad de las operaciones y Adquisición, desarrollo y mantenimiento de sistemas

08/09/2020	2.1	Jefe de Soluciones de Tecnológicas	Revisión y Cambios políticas seguridad de la información
27/01/2021	2.1	Gerente Tecnología	Revisión y Cambios políticas seguridad de la información
27/01/2021	2.1	Jefe de Soluciones de Tecnológicas	Revisión y Cambios políticas seguridad de la información
27/01/2021	2.1	Profesional de Seguridad	Revisión y Cambios políticas seguridad de la información
28/01/2021	2.1	Abogada - Secretaría General	Revisión políticas seguridad de la información
29/01/2021	2.1	Coordinador de Gestión Organizacional	Revisión políticas seguridad de la información
23/02/2021	2.1	Jefe de Relaciones Laborales	Revisión políticas seguridad de la información
02/03/2021	2.1	Gerente Productividad y Desarrollo	Revisión políticas seguridad de la información
15/03/2021	2.2	Jefe de Soluciones de Tecnológicas	Revisión y modificación políticas seguridad de la información
15/03/2021	2.2	Profesional de Seguridad	Revisión y modificación políticas seguridad de la información
06/04/2021	2.2	Comunicaciones Internas	Socialización Política de Seguridad de la Información
07/10/2022	3.0	Profesionales Auditoría TIC	Actualización de Política de Seguridad de la Información
07/10/2022	3.0	Profesional de Seguridad de la	Actualización de Política de Seguridad de la Información

		Información	
07/10/2022	3.0	Oficial de Protección de Datos	Actualización de Política de Seguridad de la Información
09/11/2022	3.0	Auditoría	Revisión de documento
03/02/2023	3.0	Auditoría	Revisión de documento
03/02/2023	3.0	Oficial de Protección de Datos	Actualización de Política de Seguridad de la Información
03/02/2023	3.0	Profesional de Seguridad de la Información	Actualización de Política de Seguridad de la Información
10/02/2024	3.1	Profesional de Seguridad de la Información	Actualización de Política de Seguridad de la Información.
04/07/2024	3.1	Profesional de Seguridad de la Información Auditoría Oficial de Protección de Datos	Se encuentra en modificación la Política de Seguridad basado en la ISO27001:2022
15/09/2024	3.2	Profesional de Seguridad de la Información	Se hace cambio de nombre de Auditor.
07/07/2025	3.2	Profesional de Seguridad de la Información Auditoría Oficial de Protección de Datos	Se encuentra en modificación la Política de Seguridad basado en la ISO27001:2022
17/09/2025	3.2	Profesional de Seguridad de la Información	Se encuentra en modificación la Política de Seguridad basado en la ISO27001:2022

		Profesional Tecnología	
25/02/2026	3.2	Profesional de Seguridad de la Información Profesional Tecnología	Se hace última revisión para envío a diferentes áreas de la organización
27/02/2026	3.2	Auditora	Revisión y concepto seguridad de la información
03/03/2026	3.2	Profesional de Soluciones tecnológicas	Se revisa gramática
04/03/2026	3.2	Mesa de ayuda	Revisión y concepto seguridad de la información
04/03/2026	3.2	Jefe Gestión Integral de Riesgos	Revisión y concepto seguridad de la información
11/03/206	3.2	Jefe de Gestión Humana	Revisión y concepto seguridad de la información
21/03/2026	3.2	Coordinadora de Relaciones Laborales	Revisión y concepto seguridad de la información
06/05/2026	4	Auditoría Gerencia de inteligencia de datos Gerencia de Tecnología	Última revisión para publicación

1. INTRODUCCIÓN

La Caja de Compensación Familiar de Caldas - Confa tiene en cuenta la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la organización, razón por la cual es necesario que se establezca un marco en el cual se gestione y proteja la información de una manera adecuada independientemente de la forma en que se accede, maneja, procesa, transporta o almacena.

Este documento describe las políticas de la organización y normas de seguridad de la información. Para la elaboración del mismo, se toman como base la norma ISO 27001:2022, Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, términos y condiciones de Amazon AWS y Google Workspace y demás regulaciones aplicables,.

Las políticas incluidas en este documento se constituyen como parte fundamental del modelo de seguridad de la información adoptado por Confa y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. La seguridad de la información es una prioridad para Confa y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradicen la esencia y el espíritu de cada una de estas políticas.

1.1 POLÍTICA SGI

Somos una Caja de Compensación Familiar del departamento de Caldas que facilita el acceso a soluciones de bienestar para apoyar a las familias en el mejoramiento de su calidad de vida.

Enmarcado en los valores sostenibilidad, servicio, bienestar, innovación y excelencia, Confa trabaja por lograr el crecimiento y la sostenibilidad de su sistema de gestión integrado, a través de:

- Cumplir con la propuesta de valor para los diferentes grupos de interés, según sus requisitos, el marco legal y organizacional, promoviendo la mejora continua en el sistema de gestión integral.
- Incorporar la gestión del riesgo como eje del sistema, orientando la continuidad

de los servicios y negocios.

- Propiciar un ambiente laboral seguro y saludable en todas las modalidades de trabajo.
- Proteger la confidencialidad, integridad, disponibilidad y autenticidad de la información
- Ser responsable con el medio ambiente, controlando los aspectos e impactos ambientales significativos en el área de influencia y previniendo la contaminación.

1.2 OBJETIVO

Definir las directrices, principios y buenas prácticas para disminuir los riesgos a los que está expuesta la información, de manera que permita a la organización mantener el monitoreo, control, gestión de herramientas de seguridad, medición de las amenazas y vulnerabilidades, aplicando procedimientos que salvaguarden la confidencialidad, integridad, disponibilidad y privacidad de la misma.

1.3 ALCANCE

La política de seguridad de la información es aplicable a los activos de información tecnológicos entre los cuales están los sistemas de información, bases de datos, dispositivos de telecomunicaciones, equipos de cómputo, dispositivos móviles, documentación digital, dispositivos biométricos, impresoras, dispositivos IoT, todos los recursos en AWS (instancias EC2, RDS, S3, IAM, etc.) y aplica a los siguientes grupos de interés: la Asamblea General, Consejo Directivo, Director Administrativo, Revisor Fiscal, Gerencias y Coordinaciones que componen la estructura organizacional de Confa; así mismo, aplica para los colaboradores cualquiera que sea su situación contractual, convenios, proveedores, contratistas y/o terceros, acreedores, afiliados, pacientes, clientes, entidades públicas, organismos de vigilancia y control.

Lo anterior, con el fin de conseguir un adecuado nivel de protección del sistema de gestión de calidad y modelo de seguridad de la información, aportando acciones

preventivas y correctivas, siendo un punto clave para el logro del objetivo y su finalidad. Es de anotar que los grupos de interés antes enunciados deben dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección, La Gerencia de Tecnología, Comité de licenciamiento y Seguridad de la información, Secretaría General, Gerencia Inteligencia de Datos, Auditoría y Gestión Humana.

1.4 Documentos de referencia

- Norma ISO/IEC 27001:2022
- Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013 Protección de Datos Personales
- Lista de obligaciones legales, normativas y contractuales.
- Términos y condiciones de Amazon AWS
- Términos y condiciones de Google

1.5 Terminología básica sobre seguridad de la información

- **Activos de Información Tecnológicos:** Son el resultado de la construcción de un inventario y clasificación de los activos usados por Tecnología, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los colaboradores de Tecnología sobre los mismos.
- **Almacenamiento externo:** Cualquier dispositivo de hardware que no está fijo o de modo permanente dentro del equipo y que sirve para copiar, transportar y/o resguardar información. Las ventajas residen en su facilidad de transporte derivadas de su rápido acceso, larga vida útil, poco tamaño y peso.
- **Aplicaciones:** Interfaz o pantalla que se le muestra al usuario para interactuar con un sistema de información y/o base de datos.
- **Base de datos:** Banco de información que relaciona datos relativos a diversas temáticas y categorizados de distinta manera, que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto.
- **Conexión VPN:** Conexión tecnológica privada entre el origen y el destino.
- **Confidencialidad:** Característica de la información que está disponible solo para personas o sistemas autorizados.
- **Encriptación:** Proceso tecnológico por medio del cual se oculta la información para evitar que sea descubierta o interceptada, para ser modificada con fines delictivos.

- **Disponibilidad:** La capacidad de garantizar que tanto el sistema como los datos van a estar disponibles para el usuario o titular de la información en todo momento.
- **Documentación digital:** Documento en formato electrónico que puede ser tratado en computadores, servidores, dispositivos móviles, entre otros.
- **Información clasificada:** Es un tipo de información sensible que está restringida por las leyes o regulada para clases particulares de personas.
- **Integridad:** Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros
- **IoT:** Internet de las cosas, se refiere a la red colectiva de dispositivos conectados y a la tecnología que facilita la comunicación entre los dispositivos y la nube, así como entre los propios dispositivos.
- **MSPI:** El Modelo de Seguridad y Privacidad de la Información
- **Políticas de seguridad y privacidad de la información:** Es la declaración o lineamientos generales de Confa que representa la posición de la organización con respecto a la protección de la información.
- **Política de tratamiento de la información:** La presente Política tiene como objeto dar la información necesaria y suficiente a los diferentes grupos de interés, así como establecer los lineamientos que garanticen la protección de los datos personales que son objeto de tratamiento de datos personales a través de los procedimientos de LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, para de esta forma, dar cumplimiento de la ley, políticas y procedimientos de atención de derechos de los titulares, criterios de recolección, almacenamiento, uso, circulación y supresión que se dará a los datos personales.
- **Seguridad de la información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Servidor:** Equipo ubicado en la red, que funciona como almacenamiento de los sistemas de información y de las bases de datos, al cual se conectan los usuarios para realizar procesamiento de información.
- **Sistema de gestión de seguridad de la información(SGSI):** Se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.
- **Sistema de Información:** es un conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información para

apoyar la toma de decisiones. Además apoyan la coordinación, control, análisis y visualización de una organización.

- **Responsable de activo de información:** Son las personas que tienen a cargo recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades. Puede ser que le interese leer este artículo ISO 27001:2022
- **RNBD:** El Registro Nacional de Bases de Datos – RNBD - es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos
- **Token:** Es un dispositivo físico utilizado para acceder a un recurso restringido electrónicamente, se utiliza como complemento o en lugar de una contraseña y actúa como una llave electrónica para acceder.
- **Usuarios ROOT:** Usuarios con permisos de edición, borrado y actualización.
- **Virus:** Son programas creados para infectar sistemas y otros programas, generando modificaciones y daños que hacen que éstos funcionen incorrectamente.
- **Invitado:** usuario o sistema con acceso temporal, restringido o externo, que puede interactuar en un entorno sin los privilegios completos de un administrador.
- **Shared Responsibility Model:** Modelo de Responsabilidad Compartida, que define qué parte de la seguridad y el cumplimiento es responsabilidad del proveedor de la nube (AWS) y qué parte corresponde al cliente/usuario.
- **OT:** Orden de trabajo que debe ingresar un usuario por medio del sistema JDE para alguna solicitud o requerimiento específico.
- **MGSI:** Modelo de Gestión de Seguridad de la Información

1.6 Adaptación y estructura de la norma

Confa adapta la norma ISO 27001:2022 de acuerdo con la estructura organizacional, tomando de dicha norma las mejores prácticas en seguridad de la información con el objetivo de mantener la integridad, disponibilidad y confiabilidad de la misma.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

[ISO/IEC 27001:2022 A.5.2]

2.1 Organización Interna

Las políticas deben ser revisadas y/o modificadas en el momento que se presente un riesgo, cuando se produzca un cambio relevante en la operación y o servicios que implique realizar ajustes en el entorno y/o de las necesidades de la operación; a corto plazo cuando se encuentren hallazgos de auditoría o cambio de leyes o normas colombianas y a largo plazo cuando se presente un cambio de fondo de la política.

Los roles y responsabilidades descritos más adelante se definen siguiendo los lineamientos de seguridad de la información en Confa y las directrices dadas por el comité de licenciamiento y seguridad de la información o quien haga sus veces y del Profesional de Seguridad de la Información, normas, leyes Colombianas y estándares de seguridad de la información tales como ISO, Cobit, ITIL, entre otros.

2.2 Roles y Responsabilidades

2.2.1 Apoyo de la alta dirección

2.2.1.1 El Director de Confa, debe apoyar activamente la seguridad de la información dentro de la entidad, definir un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

- Mantener dentro de sus colaboradores un funcionario con el perfil de Profesional de Seguridad de la Información, quien será el encargado de todo lo relacionado con la seguridad de la información y cuyas funciones estarán caracterizadas y definidas en la presente política.
- Velar por el cumplimiento de las políticas de seguridad de la información.
- Asignar responsabilidades a las áreas y personas asociadas a temas de la seguridad de la información.
- En la administración de la seguridad de la información participan todos los colaboradores de la Caja de Compensación Familiar de Caldas - Confa.

- Aprobar los recursos necesarios para la gestión de herramientas de seguridad de la información

2.2.2 Auditoría

2.2.2.1. El área de Auditoría de Confa, disponiendo de sus profesionales internos o a través de contratistas, deberá practicar auditorías a los sistemas de información y toda la plataforma tecnológica instalada y en operación (software y hardware) de la Corporación, determinando su periodicidad con base en los riesgos y cuando se presenten cambios sustanciales en los recursos tecnológicos de Confa, debiendo informar respecto al estado, especificaciones y medidas de seguridad de la información establecidas por esta Política, por las normas que rigen la materia, procedimientos y políticas internas.

2.2.3 Secretaría General

2.2.3.1 Debe incluir y tener en cuenta los lineamientos y políticas de seguridad de la información en la gestión de la contratación con convenios, proveedores, contratistas y/o terceros.

2.2.3.2 Es responsabilidad de esta dependencia velar por el cumplimiento de la política de seguridad de la información en el desarrollo de sus funciones, con sus colaboradores, convenios, proveedores, contratistas y/o terceros. Así mismo, asesorar en materia legal a la Caja de Compensación Familiar de Caldas - Confa en lo que se refiere a la seguridad de la información. Para lo anterior, se definirá un normograma donde se identifiquen las disposiciones legales aplicables a la entidad con relación a la seguridad de la información.

2.2.3.3 Secretaría General debe exigir en toda relación contractual que requiera alguna gestión y acceso a la información de Confa, la firma del acuerdo de confidencialidad y en los contratos que no especifiquen este alcance incluir una cláusula de confidencialidad. Igualmente, deberá apoyar la supervisión del cumplimiento de las políticas de seguridad de la información.

2.2.4 Gerencia de Productividad y Desarrollo

Esta dependencia debe cumplir las funciones de:

2.2.4.1 Asegurar que los colaboradores durante el proceso de selección, comprendan sus responsabilidades, los términos y las condiciones de contratación, así como verificar la idoneidad de éstos para ejercer los roles para los que se contratan.

2.2.4.2 Ejecutar los planes de formación en seguridad de la información a los colaboradores de Confa, previo plan anual enviado por el Profesional de Seguridad de la información.

2.2.4.3. Contar con un procedimiento formal, para iniciar procesos disciplinarios a los colaboradores que no hayan cumplido con la política de a la seguridad de la información y garantizar su divulgación.

2.2.4.4 Garantizar que desde Gestión Organizacional se realice el acompañamiento en los procesos de cambio en cuanto a Seguridad de la Información de la organización.

2.2.4.5 Dar a conocer mediante la inducción general a todos los colaboradores de Confa, sus obligaciones respecto del cumplimiento de las políticas de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella se deriven, así mismo, notificar, divulgar y socializar la presente Política a todo el personal, los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad, entre otros y las tareas de capacitación continua en materia de seguridad de la información de acuerdo con las necesidades y coordinadas previamente con el Profesional de Seguridad de la Información.

2.2.5. Gerencia de Tecnología

2.2.5.1 La Gerencia de Tecnología debe cumplir la función de cubrir los requerimientos de seguridad de la información definidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Caja de Compensación Familiar de Caldas - Confa.

Todo lo anterior dentro de los marcos de operación, desarrollo, gobierno, cumplimiento y de buenas prácticas que sean establecidas en la entidad.

2.2.5.2 La Gerencia de Tecnología debe dar el visto bueno, concepto técnico y acondicionamiento a todas las nuevas instalaciones de procesamiento de la información, soluciones o plataformas tecnológicas (Hardware o Software) incluyendo todos los recursos en AWS (instancias EC2, RDS, S3, IAM, etc.), en donde se evalúen los aspectos de viabilidad técnica, compatibilidad y capacidad.

2.2.5.3 Los nuevos recursos de procesamiento de información serán autorizados por la Gerencia de Tecnología, según aplique, considerando su propósito y uso, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad de la información, así como los lineamientos de arquitectura tecnológica.

2.2.5.4 Todas las nuevas adquisiciones e instalaciones de soluciones o plataformas tecnológicas (Hardware o software) incluyendo todos los recursos en AWS (instancias EC2, RDS, S3, IAM, etc.) de la Caja de Compensación Familiar de Caldas - Confa, deben contar con el visto bueno y concepto técnico de la Gerencia de Tecnología y del Profesional de Seguridad de la Información, en donde se evalúen los aspectos de viabilidad técnica (estudios, diseño, arquitectura), compatibilidad, capacidad, integridad, disponibilidad y confidencialidad.

2.2.5.5 Cuando aplique, el Administrador Funcional del Sistema de Información con el asesoramiento de los Profesionales de Tecnología, deben verificar el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas que ya están en operación o en producción.

2.2.5.6 Trabajar en conjunto con el Profesional de Seguridad de la Información para alinear las iniciativas de seguridad de la información y ciberseguridad en toda la organización.

2.2.5.7 Velar por la seguridad física de las instalaciones en donde se localiza el procesamiento de la información.

2.2.5.8 Administrar la infraestructura tecnológica(hardware, software, comunicaciones y redes) que da soporte a los distintos servicios y resguardo de la información.

2.2.5.9 Monitorear los riesgos de Tecnológicos y planes de acción necesarios para tener un adecuado control sobre los activos informáticos de la infraestructura y sistemas de información.

2.2.5.10 Apoyar, aprobar y monitorear la elaboración Planes de Recuperación de Desastres tecnológicos (DRP) que permitan dar continuidad operativa a la infraestructura crítica de tecnología ante la materialización de un evento de impacto mayor.

2.2.5.11 Identificar los riesgos relacionados a la seguridad de la información, gestionar y tomar las acciones necesarias para minimizar la materialización de los posibles riesgos.

2.2.6 Gerencia de Inteligencia de Datos

Esta dependencia es responsable de definir la estrategia, el gobierno y la analítica de los datos de la organización, asegurando que su tratamiento se realice bajo estándares de seguridad y cumplimiento legal. Sus funciones principales son:

2.2.6.1 Gobierno de datos: Definir los lineamientos y políticas para garantizar la protección de la información utilizada en los procesos de toma de decisiones.

2.2.6.2 Autorización de Uso de Información: Autorizar, junto con los líderes de área, el acceso, divulgación o uso de información que contenga datos personales de propiedad de Confa.

2.2.6.3 Conceptos Técnicos de Privacidad: Emitir conceptos técnicos y avalar el intercambio de información personal de afiliados, beneficiarios o colaboradores con terceros, convenios o entes de control.

2.2.6.4 Gestión del Riesgo de Datos: Trabajar en conjunto con la Gerencia de Tecnología y el Profesional de Seguridad de la Información para identificar y mitigar riesgos asociados al ciclo de vida del dato.

2.2.6.5 Capacitación y Concientización: Participar en la gestión, creación y ejecución del plan de capacitación en protección de datos personales para fomentar la conciencia colectiva en la organización.

2.2.6.6 Apoyar en el Registro Nacional de Bases de Datos (RNBD): Colaborar con la Secretaría General y el Oficial de Protección de Datos en la identificación de bases de datos nuevas o modificadas que deban ser reportadas ante los entes de control.

2.2.7 Todas las gerencias, áreas y servicios de Confa

Todas las gerencias, áreas y servicios de Confa deben tener en cuenta y cumplir los siguientes lineamientos:

2.2.7.1 Toda adquisición e implementación de una solución o plataforma tecnológica (hardware o software), debe contar con el visto bueno, concepto técnico y acompañamiento de Tecnología y el Profesional de Seguridad de la Información, donde se evalúen los requisitos funcionales y no funcionales, aspectos de viabilidad técnica previos a la liberación del requerimiento, compatibilidad, capacidad, integridad y disponibilidad, tanto desde la óptica de infraestructura de tecnología, como de seguridad de la información.

2.2.7.2 Todo requerimiento, incidente, problema o cambio tecnológico debe ser reportado a Tecnología mediante el uso de las herramientas de comunicación de la organización.

2.2.7.3 Incluir y tener en cuenta los lineamientos, políticas de seguridad de la información y política de tratamiento de datos en la gestión de la contratación con colaboradores de Confa, convenios, proveedores, contratistas y/o terceros.

2.2.7.4 Hacer cumplir y facilitar el acceso a sus colaboradores de todas las políticas, normas, manuales y procedimientos de seguridad de la información y de protección de datos personales.

2.2.7.5 Deben notificar las bases de datos nuevas que contengan datos personales al Oficial de Protección de Datos.

2.2.7.6 Trabajar en conjunto con el profesional de seguridad de la información con el fin de salvaguardar la información de la organización.

2.2.8 Profesional de Seguridad de la Información.

2.2.8.1 El Profesional de Seguridad de la Información debe desarrollar todas las actividades de coordinación de la seguridad de la información. La Caja de Compensación Familiar de Caldas - Confa debe contar con un colaborador que cumpla con la función de Profesional de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol:

2.2.8.2 Formular, definir y actualizar políticas, normas, procedimientos y estándares definidos en el MGSI, junto con el comité de licenciamiento y seguridad de la información o quien haga sus veces.

2.2.8.3 Mantener actualizado el análisis, control y evaluación del riesgo sobre los Activos de Información Tecnológicos de Confa. Dentro de este propósito se debe mantener definida y actualizada una metodología e instrumentos de levantamiento de Activos de Información Tecnológicos y una política y metodología de gestión de riesgos.

2.2.8.4 Evaluar, apoyar, dar visto bueno y emitir conceptos técnicos, sobre nuevas soluciones o plataformas tecnológicas a adquirir o implementar en la organización.

2.2.8.5 Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y planes de recuperación de desastres.

2.2.8.6 Evaluar, seleccionar e implementar herramientas que faciliten la labor de seguridad de la información.

2.2.8.7 Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios.

2.2.8.8 Promover en la Caja de Compensación Familiar de Caldas - Confa la formación, educación y el entrenamiento en seguridad de la información.

2.2.8.9 Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.

2.2.8.10 Recibir y dar capacitación en el tema de seguridad de la información.

2.2.8.11 Realizar estudios o consultas de pruebas de seguridad en todos los ambientes informáticos de la entidad, previa autorización de Auditoría, Secretaría General, Tecnología o Gestión Humana, según sea el caso.

2.2.8.12 Proyectar, proponer, presentar y someter a consideración del Comité de Gerencia, las políticas, normas, acciones o buenas prácticas necesarias para incorporar y/o aplicar en la Gestión de la Seguridad de la Información de la entidad.

2.2.8.13 Crear y revisar los acuerdos de confidencialidad con colaboradores, convenios, proveedores, contratistas y/o terceros.

2.2.8.14 El Profesional de Seguridad de la Información podrá convocar a diferentes colaboradores para formar grupos interdisciplinarios que apoyen la definición e implementación de los diferentes temas de seguridad de la información, a través del conocimiento y la experiencia de éstos.

2.2.8.15 Este profesional podrá obtener asesoramiento de otros organismos o entidades, con el objeto de optimizar su gestión y habilitar el contacto con todas las áreas o servicios internos.

2.2.8.16 Verificar la aceptación y aprobación de los riesgos identificados en ciberseguridad; y de sus respectivos planes de tratamiento.

2.2.8.17 Comprometerse para que los colaboradores de Confa, conozcan y apliquen las políticas de seguridad de la información.

2.2.8.18 El Profesional de Seguridad de la Información, debe apoyar, facilitar y mantener cuando se requiera relaciones con empresas, entidades u organismos que presten asesoría especializada en seguridad de la información.

2.2.8.19 Elaborar Planes de Recuperación de Desastres tecnológicos (DRP) que permitan dar continuidad operativa a la infraestructura críticas de tecnología ante la materialización de un evento de impacto mayor

2.2.8.20 Identificar los riesgos relacionados a la seguridad de la información, gestionar y tomar las acciones necesarias para minimizar la materialización de los posibles riesgos.

2.2.8.21 Debe exponer cuando sea requerido los incidentes de seguridad al Comité de Conciliación.

2.2.8.22 Se debe mantener actualizado el texto contenido en los acuerdos de confidencialidad, de modo que reflejen las necesidades de la entidad para la protección y seguridad de la información.

2.2.9 Oficial de protección de datos personales.

El oficial de protección de datos, será la persona encargada de dar trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013 y el responsable de hacer cumplir el sistema de protección de datos personales al interior de la Organización como lo indica el Artículo 23 del Decreto 1377 de 2013.

El oficial de protección de datos deberá liderar el sistema de protección de datos personales adoptado por la organización y alineado con la política de seguridad de la información, a través de las siguientes funciones:

2.2.9.1 La planeación, ejecución y seguimiento de los elementos que hacen parte del sistema de protección de datos personales.

2.2.9.2 Asesorar, sensibilizar y emitir conceptos en relación con el sistema, las políticas, normas, leyes colombianas y las principales obligaciones en materia de protección de datos y manejo de información personal.

2.2.9.3 Mantener actualizada la política de protección de datos personales y aviso de privacidad gestionando su efectiva divulgación.

2.2.9.4 En compañía del área de Secretaria General realizar el seguimiento de las normas sobre protección de datos personales y realizar las adecuaciones pertinentes al programa para procurar su cumplimiento.

2.2.9.5 Gestionar y liderar el proceso de actualización de bases de datos ante el Registro Nacional de Bases de Datos y realizar los reportes legales que los entes de control soliciten.

2.2.9.6 Elaborar y gestionar el registro de incidentes ante el Registro Nacional de Bases de Datos.

2.2.9.7 Debe exponer cuando sea requerido los incidentes de seguridad al Comité de Conciliación.

2.2.9.8 Participar y proporcionar evidencias y soportes en auditorías internas o externas.

2.2.9.9 Se debe mantener actualizado el texto contenido en los acuerdos de confidencialidad, de modo que reflejen las necesidades de la entidad para la protección y seguridad de la información.

2.2.10 Soluciones tecnológicas

2.2.10.1 Deben realizar en compañía del Profesional de Seguridad de la Información las pruebas de seguridad de los sistemas de información antes de salir a producción.

2.2.10.2 Deben notificar al administrador funcional las bases de datos nuevas que contengan datos personales al Oficial de Protección de Datos.

2.2.10.3 Deben implementar controles basados en desarrollo seguro sobre los accesos a los sistemas de información.

2.2.10.4 Participar en la elaboración, pruebas y ejecución del Plan de Recuperación de Desastres tecnológicos (DRP) que permitan dar continuidad operativa a la infraestructura crítica de tecnología ante la materialización de un evento de impacto mayor.

2.2.10.5 Participar y proporcionar evidencias y soportes en auditorías internas o externas.

2.2.11 Profesionales infraestructura tecnológica

2.2.11.1 Diseñar, implementar y mantener la infraestructura de red (on-premise, híbrida o en la nube).

2.2.11.2 Garantizar la segmentación de redes (producción, pruebas, desarrollo, usuarios).

2.2.11.3 Asegurar la aplicación del principio de mínimo privilegio en accesos a red y a recursos en AWS (Security Groups, NACLs, IAM).

2.2.11.4 Supervisar el tráfico de red, identificar patrones anómalos y reportar incidentes.

2.2.11.5 Asegurar que toda comunicación use cifrado robusto (TLS 1.2/1.3, VPN, IPSec).

2.2.11.6 Evitar uso de protocolos inseguros (ej. Telnet, FTP sin cifrado)

2.2.11.7 Revisar y asegurar la configuración de conectividad con AWS (Direct Connect, VPN Site-to-Site).

2.2.11.8 Validar que los servicios de red de terceros cumplan con los requisitos de seguridad.

2.2.11.9 Deben realizar en compañía del Profesional de Seguridad de la Información las pruebas de seguridad de la infraestructura tecnológica incluyendo todos los recursos en AWS (instancias EC2, RDS, S3, IAM, etc.).

2.2.11.10 Participar y proporcionar evidencias y soportes en auditorías internas o externas.

2.2.11.11 Reportar incidentes, vulnerabilidades o malas configuraciones detectadas.

2.2.12 Colaboradores

Los colaboradores de Confa que hacen uso de los sistemas de información para la ejecución de sus labores, son responsables de cumplir la política de seguridad de la Información vigente en los siguientes términos:

2.2.12.1 Conocer, comprender y aplicar la política de seguridad de la información de Confa en los procedimientos que ejecute en el marco de sus labores.

2.2.12.2 Asegurarse de no generar ninguna infracción de seguridad de la información en el desarrollo de las actividades propias de su cargo.

2.2.12.3 Comunicar al Profesional de Seguridad de la Información las incidencias y/o anomalías de seguridad de la información que detecte.

2.2.12.4 Hacer uso de las buenas prácticas definidas en Confa para todos los temas relacionados con la seguridad de la información.

2.2.12.5 Cumplir con el acuerdo de confidencialidad suscrito con Confa.

2.2.12.6 Todos los colaboradores de la Caja de Compensación Familiar de Caldas - Confa deben ser parte activa del Sistema de Gestión de Seguridad de la Información.

2.2.13 Responsables de Activos de Información Tecnológicos

El propietario de un activo de información, entendiéndose como tal, aquel que es el responsable de dicho activo, tendrá las siguientes obligaciones:

2.2.13.1 Informar al Profesional de Seguridad de la Información cuando detecte cualquier incidente de seguridad de la información, para tratarlo y corregirlo mediante la aplicación de controles.

2.2.13.2 Implementar las medidas de seguridad de la información necesarias en su área o servicio para evitar fraudes, robos o interrupción en los servicios.

2.2.13.3 Todos los responsables de activos de información deben suscribir en sus contratos la cláusula de confidencialidad, donde se indican sus responsabilidades.

2.2.13.4 Deben implementar controles seguros sobre los accesos a los Activos de Información Tecnológicos.

2.2.13.5 Participar en la elaboración, pruebas y ejecución del Plan de Recuperación de Desastres tecnológicos (DRP) que permitan dar continuidad operativa a la infraestructura crítica de tecnología ante la materialización de un evento de impacto mayor.

2.2.14 Administradores Funcionales de los sistemas de información de Confa

Los administradores de los sistemas de información de las diferentes plataformas de Confa, deben implementar las políticas, normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información. En este sentido, deberán:

2.2.14.1 Conocer y cumplir la política de seguridad de la información.

2.2.14.2 Aplicar los lineamientos y políticas de seguridad de la información que le sean impartidas por Confa y apliquen a la administración del sistema de información a cargo

2.2.14.3 Informar al Profesional de Seguridad de la Información cuando detecte cualquier incidente de seguridad de la información y sugerir controles o contramedidas para su tratamiento.

2.2.14.4 Documentar los aspectos de seguridad de la información aplicados dentro de su línea de gestión y su respectivo control de cambios.

2.2.14.5 Reportar al oficial de protección de datos personales sobre el acceso de terceros al sistema de información, con el fin de hacer el registro en el RNBD.

2.2.14.6 Deben notificar las bases de datos nuevas que contengan datos personales al Oficial de Protección de Datos.

2.2.14.7 Participar en las pruebas del Plan de Recuperación de Desastres tecnológicos (DRP) que permitan dar continuidad operativa a la infraestructura crítica de tecnología ante la materialización de un evento de impacto mayor.

2.2.15 Convenios, proveedores, contratistas y/o terceros

Confa debe establecer para los convenios, proveedores, contratistas y/o terceros restricciones de acceso a la información, además, el acceso a la información debe limitarse a lo mínimo indispensable para cumplir con la actividad asignada o contratada. Las excepciones a los accesos deben ser analizadas y aprobadas por el Administrador Funcional, Responsable del Activo de Información, el Profesional de Seguridad de la Información, el Gerente, Líder o Coordinador de la organización. Esto incluye tanto acceso físico como lógico a los Activos de Información Tecnológicos.

2.2.15.1 Los convenios, proveedores, contratistas y/o terceros que tengan acceso a los Activos de Información Tecnológicos, están obligados a cumplir las políticas de seguridad de la información de Confa.

2.2.15.2 Todo acceso por parte de personal externo debe ser autorizado por el administrador funcional o supervisor técnico del contrato, quien asume la responsabilidad por las acciones que pueda realizar el usuario dentro del sistema de información.

2.2.15.3 Los contratistas o proveedores deben firmar un acuerdo de confidencialidad antes de obtener acceso a sistemas de información de Confa.

2.2.15.4 A los convenios, proveedores, contratistas y/o terceros, se les dará acceso a los sistemas de información de la organización, únicamente bajo un requerimiento formal y previa aprobación del Administrador Funcional o responsable del activo de información previo análisis de pertinencia..

2.2.15.5 Todas las conexiones que se originan desde redes o equipos externos hacia la Caja de Compensación Familiar de Caldas - Confa, deben limitarse únicamente a los servidores y aplicaciones necesarios.

2.2.15.6 En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a tomar en caso de violación de dichos contratos.

2.2.15.7 Los convenios, proveedores, contratistas y/o terceros deben comunicar al respectivo supervisor del contrato, los incidentes de seguridad de la información que

detecten, para que éste siga el conducto regular y se adelanten las acciones tendientes a resolver dicho incidente.

2.2.15.8 El área de Compras o el área contratante y el Supervisor Administrativo deben asegurar que los convenios, proveedores, contratistas y/o terceros durante el proceso de selección, comprendan sus responsabilidades, los términos y las condiciones de contratación respecto de la seguridad de la información en Confa.

2.2.16 Cooperación Interinstitucional

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, el Profesional de Seguridad de la Información podrá mantener contactos con entidades, organismos o empresas especializados en temas relativos a la seguridad de la Información, como por ejemplo:

- Ministerio de Tecnologías de Información y comunicaciones
- Alta Consejería TIC
- CSIRT de la Policía Nacional
- ColCert
- Instituto Colombiano de Normas Técnicas ICONTEC
- Empresas especializadas del sector privado
- Academia
- Registraduría
- Otros Organismos

2.2.16.1 Cuando se presente intercambio de información de seguridad en las actividades de asesoramiento, no se divulgará información confidencial de la Caja de Compensación Familiar de Caldas - Confa.

2.2.16.2 El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, solo se permite cuando previamente se haya firmado un Acuerdo de Confidencialidad, el cual debe ser de obligatorio cumplimiento para el personal que participe en los temas que se tratan.

2.2.17 Comité de licencias

2.2.17.1 Definir políticas internas de adquisición, uso y renovación de licencias.

2.2.17.2 Verificar que todo software usado en la organización esté legalmente licenciado.

2.2.17.3 Asegurar cumplimiento con leyes de propiedad intelectual y contratos con proveedores.

2.2.17.4 Establecer criterios de auditoría interna para detectar software no autorizado.

2.2.17.5 Analizar el uso real de licencias para evitar pagos innecesarios (licencias infrautilizadas).

2.2.17.6 Aprobar la adquisición de nuevas licencias según justificación técnica y presupuestal.

2.2.18 Grupo de contención emergencias incidentes de ciberseguridad

2.2.18.1 Deben adoptar las medidas inmediatas para limitar esa falla y evitar cualquier compromiso adicional a la información .

2.2.18.2 Deben participar de forma activa cuando sean requeridos por la organización.

2.2.18.3 Deben contribuir en la toma de decisiones frente a un incidente de ciberseguridad

2.2.18.4 Deben evaluar la severidad e impacto del incidente de ciberseguridad.

2.2.19 Comité de conciliación

2.2.19.1 Toman decisiones de tipo organizacional frente al incidente de ciberseguridad y protección de datos, junto con los riesgos con sus causas, efectos e impactos.

2.2.19.2 Emiten recomendaciones a nivel organizacional sobre los planes de acción frente a los incidentes de ciberseguridad y protección de datos.

2.2.20 Amazon AWS

2.2.20.1 Amazon AWS es responsable de la seguridad de la nube (infraestructura física), y Confa de la seguridad en la nube (configuración, datos, accesos).

3. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

[ISO/IEC 27001:2022 A.6.1]

3.1 Antes de asumir el empleo

La Gerencia Productividad y Desarrollo es la encargada de realizar las siguientes actividades relacionadas con la selección de nuevos colaboradores para la organización y que son fundamentales para la seguridad de la información:

3.1.1 Verificar los antecedentes de todos los candidatos a un empleo, de acuerdo con:

- El código de ética y buen gobierno de Confa y las disposiciones legales y reglamentarias vigentes en el territorio nacional.
- La clasificación de la información a la cual se va a tener acceso.
- Verificación de antecedentes por mal manejo de información o de datos personales.

3.1.2 Confirmar la información de referencias personales, familiares y comerciales, para los casos en los que el candidato vaya a tener acceso a información considerada sensible.

3.1.3 Realizar todas las verificaciones necesarias para confirmar la veracidad de la información suministrada por el candidato a ocupar un cargo antes de su vinculación definitiva.

3.1.4 Asegurar que todos los colaboradores de Confa, firmen en calidad de aceptación un acuerdo de confidencialidad, cláusula de protección tratamiento de datos personales y que se les ha informado de la existencia de las políticas de seguridad de la información y políticas del tratamiento de la información, junto con el sitio o ubicación donde reposa dicha información.

3.1.5 El área de compras o el área contratante, la Secretaría General, el administrador funcional, y/o el supervisor Administrativo, serán los encargados de garantizar que los

convenios, proveedores, contratistas y/o terceros, que en razón de sus funciones deban tener acceso a información de Confa, firmen en calidad de aceptación un acuerdo de confidencialidad, las cláusulas de protección tratamiento de datos, el conocimiento de las políticas de seguridad de la información, políticas del tratamiento de la información y el cumplimiento de los requisitos de la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013.

3.2 Durante la ejecución del empleo

3.2.1 Responsabilidades de los colaboradores de Confa

3.2.1.1 Todos los colaboradores de la Caja de Compensación Familiar de Caldas - Confa, cualquiera sea su vinculación contractual, el área o gerencia en la cual desarrolle sus actividades y el nivel de las tareas que desempeñe, debe tener asignado un perfil de uso de los recursos de red, incluyendo el hardware y software asociado; para el efecto, el área de Tecnología debe mantener un directorio completo y actualizado de los usuarios asignados en la red, los administradores funcionales y los perfiles asignados en sus sistemas de información.

3.2.1.2 La responsabilidad de custodia o copia de seguridad de cualquier información almacenada, usada o producida por los colaboradores de Confa que se retiran de la Corporación o cambian de cargo, recae en el jefe inmediato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

3.2.1.3 Todo colaborador de Confa, cualquiera sea su vinculación contractual, el área o gerencia en la cual desarrolle sus actividades y el nivel de las tareas que desempeñe, debe conocer las políticas de seguridad de la información y las políticas del tratamiento de la información.

3.2.1.4 Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada Administrador Funcional de los Sistemas de Información, de acuerdo a los lineamientos dados por Tecnología en cuanto a los dispositivos hardware y los elementos software.

3.2.1.5 El reglamento de trabajo debe contemplar procesos y sanciones disciplinarias para los casos en que se presenten usos inadecuados de información y de los recursos

de tecnología que violen las políticas de seguridad de la información, las políticas del tratamiento de la información o los lineamientos dados por la organización.

3.2.1.6 Las gerencias de Productividad y Desarrollo, Gerencia Inteligencia de datos y Tecnología se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información y protección de datos personales, que propendan por el crecimiento continuo de la conciencia individual y colectiva en temas de dicha materia.

3.2.1.7 Las gerencias de Productividad y Desarrollo y Tecnología se encargarán de crear y mantener centralizada la información relacionada con temas de seguridad de la información tales como responsabilidad en las buenas prácticas, amenazas de seguridad, entre otros.

3.2.2 Responsabilidades de Usuarios Externos

3.2.2.1 Todos los usuarios externos, empresas contratistas, convenios, proveedores y/o terceros, deberán suscribir un acuerdo de confidencialidad y cláusula de protección tratamiento de datos personales a cargo de su representante legal y cumplir con los lineamientos de la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, así mismo, los accesos a las herramientas tecnológicas o a la información de Confa deben ser aprobados por el jefe inmediato del Administrador funcional y por la gerencia de Tecnología.

3.2.2.2 Los supervisores del contrato será responsable del control y vigilancia del uso y acceso adecuado de la información y los recursos asignados a los convenios, proveedores, contratistas y/o terceros, así mismo, velará por el cumplimiento de las normas Colombianas y políticas de la organización en materia de seguridad y tratamiento de datos personales.

3.2.2.3 La creación y mantenimiento de los usuarios en la red de Confa para los convenios, proveedores, contratistas y/o terceros, estará a cargo de la gerencia de Tecnología, los supervisores del contrato y el administrador funcional.

3.2.2.4 Los usuarios creados para las actividades de los convenios, proveedores, contratistas y/o terceros deben aceptar las políticas de seguridad de la información, acuerdos de confidencialidad, cláusula de protección tratamiento de datos personales,

política de tratamiento de datos y las obligaciones dispuestas por la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013.

3.2.2.5 La solicitud de creación y retiros de los usuarios de los convenios, proveedores, contratistas y/o terceros en los sistemas de información deben ser informados al Administrador funcional, él debe revocar los permisos en el Sistema de Información asignado y notificará al área de Tecnología.

3.2.2.6 El Administrador funcional del Sistema de Información debe gestionar los permisos necesarios para el acceso a una base de datos nueva y notificar a Secretaría General para realizar su diligenciamiento frente al Registro Nacional de Base de Datos de la SIC.

3.2.3 Usuarios invitados y servicios de acceso público.

3.2.3.1 El acceso de usuarios no registrados solo debe ser permitido a la redes inalámbricas libres de Confa, usadas para brindar conexión a Internet y sus actividades pueden ser monitoreadas desde Tecnología.

3.2.3.2 El acceso y uso a cualquier otro tipo de recurso de información y/o sistemas de información, Red Local (LAN) no es permitido a usuarios invitados o no registrados.

3.2.3.3 El adecuado uso de los recursos permitidos a las redes inalámbricas libres de Confa, será responsabilidad del usuario invitado.

3.2.3.4 El acceso a la información de Confa a usuarios invitados no será suministrada sin previa autorización de los coordinadores, jefes, líderes o gerentes de las diferentes áreas.

3.2.3.5 Para CONFA se considera como uso no aceptable el envío o intercambio de mensajes que pongan en riesgo la reputación de CONFA y/o actividades que promuevan la discriminación social o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

3.3 Terminación y cambio de área

La Caja de Compensación Familiar de Caldas - Confa asegurará que sus colaboradores serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura, por lo tanto, define lo siguiente:

3.3.1 El área de Relaciones Laborales debe realizar el procedimiento de desvinculación de colaboradores que terminan su relación contractual con Confa, en el cual se gestione la inactivación de los usuarios y perfiles en los sistemas de información internos a través de un RPA y externos por medio de una notificación por correo electrónico, así mismo, el jefe inmediato es quien debe reportar oportunamente la novedad de licencias, incapacidades y vacaciones al área de Relaciones Laborales para proceder al respectivo reporte de desactivación de las cuentas si se requiere.

3.3.2 El jefe inmediato debe notificar al profesional de seguridad de la información cuando hay un caso de terminación de la relación laboral (despidos, renunciaciones, incapacidades prolongadas, licencias no remuneradas, vacaciones, entre otros) con el objetivo de salvaguardar la información de la organización que se encuentre en poder del colaborador.

3.3.3 Ante el retiro inmediato o inesperado (despidos, renunciaciones, incapacidades prolongadas, licencias no remuneradas, vacaciones, entre otros) de un colaborador, el profesional de seguridad de la información notifica a los administradores funcionales, al administrador técnico del sistema de información y al profesional de infraestructura tecnológica para que desactiven el usuario en los respectivos sistemas de información donde tenga una cuenta activa

3.3.4 Cada gerente, líder o coordinador debe reportar de manera inmediata al área de Relaciones Laborales, la desvinculación o cambio de labores de sus colaboradores, con el fin de que se tomen las medidas pertinentes y a su vez se informe a las áreas o servicios interesados.

3.3.5 Cuando hay un cambio de área, el auxiliar de contratación notifica al auxiliar técnico de mesa de ayuda, administrador técnico del sistema de información o al profesional de infraestructura tecnológica por OT para el cambio de prefijo en el correo electrónico y en red.

4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN TECNOLÓGICOS

[ISO/IEC 27001:2022 A.5.9 al 5.13]

4.1. Responsabilidad sobre los Activos de Información Tecnológicos de Confa por parte de las Áreas

4.1.1 Confa es el dueño de la propiedad intelectual de los avances tecnológicos, documentos estratégicos, documentos que contengan: configuración de planos, diagramas, archivos con información confidencial y personal, correos(e-mails), drive, chats, agendas, documentos compartidos e intelectuales desarrollados por los colaboradores de la organización y convenios, proveedores, contratistas y/o terceros, derivadas del cumplimiento de funciones y/o tareas asignadas o contratadas, como las necesarias para el cumplimiento del objeto del contrato.

Confa es el responsable de la gestión de la información suministrada por los Afiliados, usuarios, colaboradores, beneficiarios, convenios, proveedores, contratistas y/o terceros y es responsabilidad de los colaboradores mantener la confidencialidad respecto de dicha información, como se estipulan en el acuerdo de confidencialidad, cláusula de protección tratamiento de datos personales en los contratos laborales y en las políticas de seguridad de la información y políticas del tratamiento de la información.

4.1.2 Confa es propietario de los Activos de Información Tecnológicos y los administradores de estos activos son los colaboradores, convenios, proveedores, contratistas y/o terceros (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware e infraestructura tecnológica de la Caja.

4.1.3 En Confa es fundamental la protección de los Activos de Información Tecnológicos, por eso cada área debe hacerse responsable de la correcta gestión, uso, administración, salvaguardado, otorgamiento de acceso a los mismos y revocación de permisos al momento del retiro de un colaborador.

4.1.4 La vigencia de los derechos de acceso y su revocatoria debe estar estrechamente relacionada con la terminación del contrato laboral o con el cambio de cargo, siguiendo el manual de administración de usuarios en el punto 3.3.3 de esta política. Y los

colaboradores, convenios, proveedores, contratistas y/o terceros al momento de su retiro no podrán realizar eliminación, copiado, modificación y/o asignación de permisos de todos los activos de la información pertenecientes a Confa, tampoco podrá acceder a ninguno de los sistemas de información, llegado el caso de ser requerido el ingreso debe contar con el acompañamiento del administrador funcional, gerente, líder, coordinar y/o jefe.

4.1.5 En caso de pérdida o robo de cualquier activo de Información Tecnológico que contenga información de Confa, tales como acceso a los aplicativos o sistemas de información de la organización o estén configurados con cuentas corporativas, debe ser reportada de inmediato al Profesional de Seguridad de la información, el cual activará la revisión y gestión del incidente.

4.1.6 Por seguridad y disponibilidad, es responsabilidad de los colaboradores, usar la suite colaborativa de Confa como primer medio de almacenamiento de los archivos que contengan información corporativa.

4.1.7 Cualquier verificación, análisis, monitoreo, consulta que se deba realizar a un activo de información de la organización, debe contar con previa autorización del jefe de Gestión Humana por medio de correo electrónico.

4.1.8 Los activos de Confa deben ser utilizados sólo para fines laborales de la organización.

4.1.9 Confa bajo el Modelo de Responsabilidad Compartida(Shared Responsibility Model), será el responsable de la seguridad en la nube (configuración datos, accesos) y AWS es responsable de la seguridad de la nube (infraestructura física).

4.2. Uso Aceptable de los Activos de Información Tecnológicos

4.2.1 Todos los Activos de Información Tecnológicos que sean susceptibles de intercambio entre áreas, con convenios, proveedores, contratistas y/o terceros deben ser compartidos, enviados o transmitidos por un medio de comunicación o canal seguro, en el caso de correos electrónicos se debe usar o realizar desde las cuentas organizacionales.

4.2.2 Un colaborador de Confa puede acceder, divulgar, usar o compartir información de propiedad de Confa en la medida en que esté autorizado por escrito por parte del líder, coordinador, gerente y si la información contiene datos personales se debe gestionar con Gerencia de Datos,. (ver también el Capítulo 6 del Código de Buen Gobierno y Ética).

4.2.3 En caso de transferencia de archivos con entidades financieras, estos deben ser encriptados con sus respectivas llaves privadas y públicas.

4.2.4 Los colaboradores de Confa deben usar las herramientas habilitadas por la organización para hacer la conversión de formatos de archivos o de lo contrario se debe autorizar su uso o compra por el Comité de Licencias.

4.3. Devolución de los Activos de Información Tecnológicos

4.3.1 Todos los colaboradores, practicantes, convenios, proveedores, contratistas y/o terceros están en la obligación de devolver a Confa los activos fijos, dispositivos móviles, token, llaves, usuarios, contraseña y de información, a la terminación de su contrato, acuerdo de servicios o solicitud hecha por el gerente, líder y/o coordinador, teniendo en cuenta que son propiedad de Confa.

4.4. Manejo de los medios de almacenamiento

4.4.1 En Confa los colaboradores, convenios, proveedores, contratistas y/o terceros deben gestionar los medios de almacenamiento existentes para evitar la divulgación no autorizada, modificación, eliminación de la información almacenada en los medios físicos o electrónicos y en caso de requerir la destrucción se debe solicitar el acompañamiento del Profesional de Seguridad de la Información y Auditoría.

4.4.2 Cuando se imprima o se requiera información física de tipo confidencial estipulada por la ley de habeas data o Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, debe garantizar su:

- Debida autorización por parte del líder, coordinador o gerente.
- Autorización para transferencia o préstamo del documento impreso o físico.
- Correcta protección del documento físico.

- Almacenamiento seguro de documento físico.
- Destrucción de forma segura del documento físico.
- Solicitar la debida autorización a Gestión Documental y Comité de Archivo según sea el requerimiento.

4.4.3 Los colaboradores que manejan medios de almacenamiento externo asignados a sus funciones, deben asegurar la protección de éstos y de los equipos de cómputo en donde se requiera acceder a dicho medio, cumpliendo los siguientes requisitos:

- Los medios de almacenamiento existentes y asignados a los colaboradores deben ser usados únicamente en los equipos de la organización, en caso de ser requerido el uso en equipos que no sean de la organización se debe de informar al Profesional de Seguridad de la Información, para revisar la viabilidad y evitar algún riesgo en la información de la organización.
- Se debe garantizar que la información transferida o copiada desde los medios de almacenamiento será destruida de los mismos al finalizar la actividad, utilizando los procedimientos de borrado seguro de información o formateando el medio.
- En caso de pérdida o robo de un medio de almacenamiento que contenga información de Confa, debe ser reportada de inmediato al Profesional Seguridad de la información, el cual activará el proceso de Gestión de Incidentes.
- En caso de daño que implique restauración de información, debe ser reportada de inmediato al personal de Mesa de Ayuda.
- Los colaboradores de Confa deben garantizar el uso adecuado de las herramientas tecnológicas de la Organización, evitando situaciones que pongan en riesgo el funcionamiento e información del activo.
- Los colaboradores de Confa deben garantizar que las herramientas de almacenamiento solo deberán ser usadas para salvaguardar la información de la organización.
- Los archivos que requieran ser enviados o transmitidos entre las partes, en el marco de convenios, proveedores, contratistas y/o terceros, deben tener implementados controles criptográficos siempre y cuando la información de los activos esté clasificada como privada, con previo acuerdo de la confidencialidad de la información y siguiendo lo estipulado por la Ley 1581 del 2012.
- Tecnología debe garantizar que las estaciones de trabajo como PC's, portátiles y dispositivos móviles que van a ser dados de baja, se formateen o se destruyan con el fin de mitigar el riesgo de recuperación de información sin la debida autorización previa, al sustraer partes como los discos duros.

5. CONTROL DE ACCESOS

[ISO/IEC 27001:2013 A.5.15 a 5.18]

5.1. Requisitos de acceso a zonas sensibles

5.1.1 Confa debe asegurar todos los centros de procesamiento de información.

5.1.2 Los Líderes, Gerentes, Jefes y/o Coordinadores de las áreas de Confa o las personas encargadas de las áreas seguridad y/o responsables de los centros de cableado, tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- El acceso a las áreas donde se maneja información clasificada es limitada únicamente a personas autorizadas.
- El acceso a las áreas seguras como Tesorería, Créditos, Preescolar, Centros de Cómputo, Centros de Cableado y monitoreo de CCTV debe controlarse.
- Los colaboradores y convenios, proveedores, contratistas y/o terceros no deben hacer uso de dispositivos como puntos de acceso inalámbricos (Access Point), routers y cables de red, que no hayan sido asignados para el cumplimiento de sus actividades.

5.2. Requisitos de las áreas para el control de acceso a los sistemas de información

5.2.1 En Confa cada área con su administrador funcional es responsable de gestionar los requerimientos para brindar los accesos y privilegios de los usuarios a las respectivas herramientas tecnológicas de la caja, con el fin de asignar los perfiles adecuados en los sistemas de información. Por eso los usuarios que dispongan de acceso a los sistemas de información y servicios de la red son los que han sido específicamente autorizados para su uso.

5.2.2 Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de Confa, es por eso que se prohíbe el préstamo de los usuarios y contraseñas.

5.3. Gestión de acceso de usuario de Confa

5.3.1 La creación de los usuarios en la red debe ser solicitada a la Gerencia de Tecnología según el procedimiento.

5.3.2 La creación, asignación de roles y permisos en los sistemas de información debe ser solicitada al área y Administrador Funcional correspondiente.

5.3.3 El jefe inmediato es quien debe reportar oportunamente la novedad de licencias, incapacidades y vacaciones al área de Relaciones Laborales para proceder al respectivo reporte de desactivación de las cuentas si se requiere.

5.3.4 Es responsabilidad de los administradores funcionales validar la desactivación automática de usuarios de los aplicativos desde el RPA y/o desde sus propios sistemas de información.

5.4. Control de acceso a plataforma, bases de datos y sistemas de información de Confa

5.4.1 En Confa la asignación y utilización de los derechos de acceso preferente se deberá restringir y controlar como se menciona en la siguiente directriz:

- Los usuarios administradores deben ser controlados y usados únicamente por personas autorizadas y llevar una relación sobre los seguimientos realizados.
- Los usuarios administradores no deben ser compartidos con personas ajenas al proceso.

5.4.1.1 Los administradores de bases de datos, administradores de aplicaciones, administradores funcionales y usuarios con controles de acceso avanzados en los sistemas de información de Confa, seguirán los siguientes términos:

- Propiedad de la información
- La información que se encuentre almacenada en bases de datos físicas o electrónicas (estaciones de trabajo, medios de almacenamiento externo, herramientas colaborativas, servidores de versionamientos, servidores de aplicaciones, aplicaciones y bases de datos) son de propiedad de la organización y no puede ser copiada, compartida, divulgada sin autorización del coordinador, líder o gerente; excepto para las auditorías o

solicitudes formales hechas por entes de control gubernamentales o de revisoría fiscal.

- Creación de usuarios funcionales y bases de datos

La creación y capacitación de un usuario, administrador funcional o tercero debe ser aprobado por el líder, coordinador o gerente y su gestión a cargo del área. Así mismo y por la privacidad de los datos, el nuevo usuario debe diligenciar y firmar el formato de confidencialidad de la información.

Los administradores funcionales de los activos de Información Tecnológicos deben revisar periódicamente los derechos de acceso, frente a las actividades actuales del colaborador en el sistema, cualquier desviación debe ser tratada como un incidente de seguridad. Los responsables deben dejar trazas del ejercicio de esta actividad, las que serán objeto de revisiones por parte del área de Auditoría de Confa.

Los derechos de acceso de los colaboradores, convenios, proveedores, contratistas y/o terceros en los Activos de Información Tecnológicos, deben ser retirados por los administradores funcionales en el momento de la terminación de la relación contractual o cuando la organización lo considere pertinente.

- Uso de usuarios administradores con acceso a servidores.
 - Solo el usuario root tendrá el permiso total a los servidores.
 - Solo se creará un usuario para el soporte a las aplicaciones y tendrá acceso restringido por los Profesionales de Infraestructura Tecnológica.
 - Para los convenios, proveedores, contratistas y/o terceros que requieran acceso a los servidores deben de cumplir con el acuerdo de confidencialidad y con las cláusulas de protección de datos personales. La creación del usuario debe ser previamente aprobada por el líder del área y Gerente de Tecnología.
- Procesos u operaciones en la plataforma tecnológica y bases de datos

Por la criticidad de los servicios de Confa, se debe tener en cuenta que para la realización de procesos u operaciones que impliquen la modificación y actualización de la información sobre las bases de datos, las aplicaciones (sistemas de información), configuraciones de hardware y software (Sistemas Operativos) de los servidores o elementos que conforman la plataforma tecnológica que soportan la operación de los servicios, deberán efectuarse en horarios en los que no haya interrupción de la operación y con previa solicitud por orden de trabajo o correo electrónico, además de contar con la aprobación de los gerentes, líderes, coordinador del servicio y/o de Tecnología.

En el caso específico de Salud se deben acordar estos tiempos con las partes, debido a que su operación es 7x24.

Para garantizar la continuidad de la operación, los procesos (desarrollos, actualizaciones, configuraciones y parametrizaciones) que se hagan en el Hardware, Software, Sistemas Operativos, bases de datos y Aplicaciones, se debe verificar en un ambiente de pruebas (que nunca se apunte a bases de datos de producción) y una vez se validen exitosamente, se debe notificar a todos los colaboradores involucrados y/o administradores funcionales en las áreas correspondientes, para migrar los cambios al servidor de producción con su respectivo visto bueno.

Antes de realizar salida en vivo o producción, se debe verificar que todas las aplicaciones queden apuntando al ambiente de producción.

Antes de la realización de alguna migración de desarrollos, configuración o modificación de aplicaciones, sistemas operativos o modificaciones de bases de datos, se debe elaborar y validar la existencia de una copia de seguridad actualizada de la base de datos y del software (Sistema o aplicación).

Para realizar operaciones masivas (Inserción, borrado y/o actualización mediante script o archivo plano), sobre cualquier base de datos por un medio diferente a la interfaz de usuario final, se debe contar con el análisis previo, solicitud formal mediante orden de trabajo por el Administrador Funcional del sistema de información comprometido y cuando aplique, notificación a Auditoría mediante el flujo diseñado en la herramienta tecnológica.

El Profesional de Tecnología y/o los colaboradores que tengan acceso a cualquier base de datos por una interfaz diferente a la de usuario final, debe asegurar que se cuenta con todas las condiciones y conocimientos suficientes en la ejecución de órdenes por comandos, SQL, Scripts, entre otras para no afectar la prestación del servicio.

Con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información, se deben realizar bajo la responsabilidad de Tecnología, copias de seguridad diaria, semanal, mensual y anual de las bases de datos y de las aplicaciones con sus respectivos archivos anexos (cuando aplique), según el Instructivo de copias de seguridad, a cargo de las personas responsables de la infraestructura tecnológica. Los Profesionales de Soluciones Tecnológicas y/o Administrador Funcional deben comunicar a Tecnología sobre la información de las bases de datos, aplicaciones nuevas o actualizadas que requieran ser incorporadas en los procesos de copias de seguridad.

En caso tal de que el área de Tecnología no tenga acceso a una copia de seguridad en sitio y de necesitarla con urgencia, se debe solicitar al convenio, proveedor, contratista y/o tercero encargado de la custodia externa para que se lleve a las instalaciones de Confa.

Cuando se realicen desarrollos o pruebas fuera de la ubicación física de Confa, o mediante el uso de la VPN, sobre bases de datos o aplicaciones, será obligatorio contar con la autorización previa del administrador funcional. Esta autorización también aplica para el uso y acceso a las fuentes de datos involucradas.

Se recuerda que toda la información intercambiada durante estos procesos es confidencial y debe ser tratada conforme a lo establecido en la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, relacionados con la protección de datos personales.

- Soluciones de tecnología y telecomunicaciones (hardware y Software)

Los colaboradores de Confa, convenios, proveedores, contratistas y/o terceros que tienen acceso a las bases de datos y a los sistemas de información, fuera de infraestructura de la red de la organización o que usen equipos portátiles

personales, deben acceder remotamente por medio de una conexión VPN y contar con antivirus como mínimo requerimiento de seguridad, previa autorización del líder, coordinador o gerente.

Los terceros que se encuentren en las instalaciones y que necesiten hacer uso de las redes de Confa, no podrán tener instalado o hacer uso de ningún software analizador de tráfico y así mismo deben cumplir con: las cláusulas de los contrato o minutas, las políticas de Confa y la normatividad Colombiana.

El ingreso para los servicios de soporte, mantenimiento y administración de los equipos como servidores, dispositivos de red y cableados, debe ser controlado con las respectivas identificaciones tanto corporativas como del convenio, proveedor, contratista y/o tercero, notificando vía correo electrónico al Profesional de Tecnología en el proceso.

Cualquier cambio de ubicación de elementos (rack, dispositivos de red) dentro de los cuartos de servidores o en las instalaciones de Confa, por Profesionales de Tecnología o terceros autorizados, debe ser avalado por parte del Profesional de Infraestructura Tecnológica, Jefe de Soluciones Tecnológicas o Gerente Tecnología y se deberá realizar en una ventana de mantenimiento programada.

- Servicios tercerizados

Cualquier acceso para consultas, modificaciones, actualizaciones, suspensiones o acciones que impliquen la interrupción en el servicio de los sistemas de información tercerizados, debe ser comunicado y autorizado al administrador funcional, líder, coordinador o gerente del área y el gerente de Tecnología.

Cualquier solicitud de reunión, conferencia, videoconferencia, asistencia técnica, donde se involucre información clasificada como confidencial debe ser notificada y autorizada vía correo electrónico por el administrador funcional, el líder, coordinador o gerente del área.

Cualquier solicitud de información física y electrónica que involucre información clasificada como confidencial y de criticidad alta, debe ser solicitada directamente por el líder, coordinador o gerente del área y con la documentación y normatividad que especifique tal requerimiento e informar al oficial de

protección de datos personales para reportar al ente de control la respectiva consulta en habeas data.

5.5 Responsabilidades de los usuarios.

5.5.1 Con el fin de garantizar la integridad de nuestros sistemas y prevenir la pérdida de datos, queda restringido en Confa el uso de dispositivos de almacenamiento físico (como memorias USB, discos duros externos o tarjetas SD) en los equipos de la organización. Toda la información corporativa debe ser gestionada a través de las plataformas de almacenamiento en la nube facilitadas por la organización para el cumplimiento de las actividades contratadas. Cualquier excepción por necesidades operativas críticas deberá ser evaluada y aprobada previamente por el profesional de seguridad de la información y el coordinador de mesa de ayuda.

5.5.2 El colaborador de Confa tendrá un usuario y contraseña para acceder a los sistemas de información de la organización y estaciones de trabajo. Las cuales deben ser salvaguardadas y gestionadas por el colaborador y es responsabilidad del mismo todas las acciones que se hagan con ellas.

Las credenciales al ser activos de la organización podrán ser controladas, auditadas y monitoreadas por auditoría, secretaria general, productividad y desarrollo y tecnología.

5.5.3 Los colaboradores de Confa que acceden a las bases de datos y a los sistemas de información deben salvaguardar los usuarios y/o claves en medios diferentes a los físicos como agendas, libretas o papel sobre sus puestos de trabajo.

5.5.4 Los colaboradores de Confa que acceden a las bases de datos y a los sistemas de información deben guardar usuarios y/o claves en distintos formatos a los automáticos brindados por la configuración de los navegadores.

5.5.5 Los colaboradores de Confa, no deben realizar suscripciones con las cuentas corporativas a páginas de dudosa procedencia y/o plataformas que no cumplan con el objetivo de las funciones asignadas.

5.5.6 Los usuarios con acceso a datos sensibles (Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013) de Confa, deben tener en cuenta la confidencialidad y tratamiento de ellos, no se debe divulgar información a terceros o a otros colaboradores que no tengan relación con ella.

5.5.7 Es responsabilidad de los colaboradores controlar, gestionar y velar por la protección de las credenciales de los usuarios suministrados durante la actividad de supervisión técnica o administrativa a los convenios, proveedores, contratistas y/o terceros.

5.5.8 Los colaboradores de Confa, deben seguir los lineamientos dados por la organización frente al tiempo de cambio de contraseñas y uso de contraseñas seguras.

6. CIFRADO/CRIPTOGRAFÍA

[ISO/IEC 27001:2022 A.8.24]

6.1. Controles criptográficos

6.1.1 Los tokens de seguridad deben ser usados y salvaguardados dentro de las áreas asignadas por el usuario responsable. Debe permanecer en un sitio seguro, seco, evitando su exposición a campos magnéticos, a líquidos y a temperaturas extremas, manteniéndolos preferiblemente siempre fuera del alcance de terceros no autorizados. Se recomienda un sitio con un nivel de seguridad apropiado, llave, candado, clave o caja fuerte. Evitando que sean golpeados o sometidos a esfuerzo físico.

6.1.2 Los tokens de seguridad nunca deben salir del perímetro del área responsable, solo en caso de extrema urgencia se podrá hacer con previa autorización del líder del área. Sus usuarios no deben permitir que terceras personas observen la clave que genera el Token y no deben aceptar ayuda de terceros para su utilización.

6.1.3 Cualquier incidente de seguridad presentado con el token de Confa que contiene firmas digitales por deterioro, mal funcionamiento, robo, pérdida o caducidad, deberá ser informado al Profesional de Seguridad de la Información.

6.1.4 Cualquier incidente de seguridad presentado con el token de los bancos por deterioro, mal funcionamiento, robo, pérdida o caducidad, deberá ser informado al Banco de inmediato para seguir el conducto regular estipulado por la entidad y también debe ser reportado al Profesional de Seguridad de la Información.

6.1.5 Para realizar las transacciones bancarias, los tokens de seguridad deben ser extraídos de su sitio de custodia y deben ser llevados al puesto o sitio de trabajo por sus usuarios. Se deben realizar las transacciones electrónicas sin perder de vista los Tokens y sin que el responsable pueda ausentarse del puesto de trabajo durante este proceso. En caso de que ocurra algún evento irregular con los Tokens, los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

6.1.6 En el momento que se termina la transacción con los Tokens de seguridad, estos deben ser colocados nuevamente en su lugar de custodia directamente por el usuario asignado de la custodia y sin ayuda de terceros, en ningún caso.

6.1.7 No puede divulgarse la información sobre el proceso de custodia a ninguna persona ajena al proceso, dentro y fuera del área de operación.

6.1.8 Los usuarios no deben abrir los Tokens, retirar su batería o placa de circuitos, toda vez que puede alterar su funcionamiento.

6.1.9 Los tokens de seguridad única y exclusivamente pueden ser usados por las personas responsables de los mismos, asignados por cada área.

6.1.10 Los tokens de seguridad única y exclusivamente pueden ser usados en los equipos de cómputo asignados a los usuarios responsables de los tokens.

6.1.11 No se deben realizar transacciones electrónicas en presencia de otra persona del área, ni externa a la misma, cuando se involucren los Tokens de seguridad.

6.1.12 No utilizar las claves en otro portal de los bancos que no tenga los mínimos requerimientos de seguridad, protocolo de conexión https, candado de seguridad en la parte superior de la página.

6.1.13 El usuario solo debe hacer uso de las claves en el portal de los bancos únicamente del computador asignado para tal actividad, así mismo no se debe acceder a los portales haciendo uso de un buscador como Google o a través de un link enviado o recibido vía correo electrónico, solo es permitido el ingreso desde el sitio oficial de la entidad bancaria.

6.1.14 Confa cifra la información de los datos en tránsito mediante SSL, con huellas digitales SHA-256 con longitud de clave RSA a 2048, lo que permite cifrar comunicaciones entre cliente y servidor, garantizar la autenticidad del dominio, proteger datos en tránsito y evitar que la información sea interceptada para los dominios contratados por Confa.

6.1.15 La organización para el cifrado de datos en las instancia de Veeam en los datos en tránsito usa TLS 1.2 y 1.3 y para los datos en reposo usa AES-256 (Advanced Encryption Standard, clave de 256 bits) en modo CBC o GCM.

6.1.16 La inmutabilidad para las copias de las instancias en veeam usa Cifrado de AES-256. SSE-KMS

7. CONTROLES FÍSICOS

[ISO/IEC 27001:2022 A.7.1 A 7.9]

7.1 Áreas Seguras

7.1.1 El perímetro de las áreas que contienen información de los usuarios sensibles o clasificados como privados, deberán estar protegidas de accesos no autorizados mediante los controles de entrada adecuados y deben tener sistemas de vigilancia y monitoreo, lo que mitigue el riesgo de robo de Activos de Información Tecnológicos; además los colaboradores que se encuentre en estas áreas tendrán todo el derecho de solicitar identificación de Confa a las personas desconocidas.

7.1.2 El acceso a las áreas consideradas como sensibles por Confa o que manejan o procesan información confidencial, sólo pueden ser usados por los colaboradores y/o contratistas autorizados, salvo en caso de emergencias el líder, coordinador, director o gerente pueden autorizar ingreso a personas ajenas a dichos sitios.

7.1.3 En el ingreso a los centros de cómputo o centros de cableado, las puertas deben permanecer cerradas y aseguradas en el momento que se haga uso de los mismos; esto con el fin de garantizar la adecuada temperatura dentro del sitio.

7.1.4 Las instalaciones de centro de cómputo y de cableado deben cumplir con las mínimas normas o estándares de calidad y funcionamiento y su mantenimiento preventivo y correctivo debe ser llevado a cabo por las personas encargadas y capacitadas para dicha tarea.

7.1.5 Todo personal que ingrese a las áreas consideradas como sensibles por Confa o que manejan o procesan información confidencial, deberán estar debidamente identificadas y con las protecciones exigidas por el Sistema de Seguridad y Salud en el Trabajo.

7.2 Seguridad de los Equipos

7.2.1 Los equipos de cómputo deben tener un correcto mantenimiento, con el fin de garantizar y asegurar la integridad y disponibilidad de los mismos.

7.2.2 La reutilización de equipos de cómputo o de partes de equipos de cómputo debe ser controlada por Tecnología, con el fin de evitar el robo de hardware o de información privada, siguiendo los lineamientos del ítem 16 borrado/formateo seguro.

7.2.3 La salida de los equipos de cómputo de las instalaciones de Confa debe ser registrada en las estaciones de los guardas de seguridad y deberán cumplir con el procedimiento establecido por el área de activos fijos, así mismo, se debe tener en cuenta la seguridad de estos equipos fuera de las sedes y oficinas de la Organización quedando bajo la responsabilidad y custodia de quien lo retira.

7.2.4 Toda estación de trabajo, servidor, base de datos, aplicación, dispositivo móvil y dispositivo de red, debe contar con un usuario y contraseña segura.

7.3 Puestos de trabajo despejado y bloqueo de pantalla

7.3.1 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que desarrollen actividades en las instalaciones de Confa, deben conservar su escritorio libre de información de la Organización o restringiendo el acceso a personas inescrupulosas que puedan hacer uso indebido de la misma o que por su perfil no tengan autorización.

7.3.2 Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se debe reutilizar papel que contenga información confidencial, este deberá ser destruido.

7.3.3 La información confidencial y crítica debe estar asegurada en cajas fuertes, al igual que los Activos de Información Tecnológicos como computadoras portátiles, dispositivos de almacenamiento en los que se guarde información confidencial y con los que se hacen transferencias, transacciones y/o operaciones críticas para la organización.

7.3.4 Los colaboradores de Confa deben ser responsables de la sesión en los sistemas de información y en la estación de trabajo donde haya ingresado con su usuario y contraseña asignadas para sus actividades, es decir, deben bloquear o cerrar la sesión cuando se ausentan de su puesto de trabajo ya sea en teletrabajo, trabajo autónomo o en oficina, como mínimo requerimiento de seguridad para proteger la información.

7.3.5 Al finalizar sus actividades diarias, todos los colaboradores, convenios, proveedores, contratistas y/o terceros que hagan uso de los recursos tecnológicos, deben cerrar las sesiones y apagar las estaciones de trabajo.

7.3.6 Los colaboradores deben garantizar la conexión de las estaciones de trabajo en redes de confianza, conocidas o seguras, se recomienda no hacer uso de redes públicas.

8. CONTROLES TECNOLÓGICOS

[ISO/IEC 27001:2022 A.8 a 8.13]

8.1 Protección contra el código Malicioso

8.1.1 Los colaboradores, convenios, proveedores, contratistas y/o terceros que accedan a los sistemas de información y a la red de datos de Confa y que sospechen de alguna infección por virus deben dejar de usar inmediatamente el equipo de cómputo y notificar a Tecnología para la revisión y eliminación del virus.

8.1.2 Las herramientas de seguridad adquiridas por Confa, podrán analizar automáticamente todo tipo de documento electrónico o medio removible y eliminar cualquier virus que se encuentre en estos Activos de Información Tecnológicos; si no se puede eliminar el virus el Profesional de Seguridad de la Información solicitará un espacio para la revisión manual del activo.

8.1.3 Confa no se hace responsable de los archivos eliminados por la existencia o detección de un virus en la información recibida o existente en medios externos.

8.1.4 Las licencias de antivirus adquiridas por Confa, sólo deben ser instaladas por los responsables de Tecnología.

8.1.5 Cualquier equipo o dispositivo móvil conectado a la red de Confa puede ser monitoreado y supervisado para la detección de código malicioso únicamente por Tecnología y al encontrar cualquier riesgo, se realizará la debida gestión del incidente de seguridad por parte de Profesional de Seguridad de la Información.

8.1.6 El único servicio de antivirus autorizado en la organización es el licenciado en Confa y gestionado por Tecnología, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso.

8.1.7 Es responsabilidad de Tecnología la ejecución de los procesos de actualización del antivirus de manera periódica y segura.

8.1.8 En algunas excepciones, Tecnología podrá realizar la ejecución de otro programa antivirus, a efectos de reforzar el control de presencia de virus o código malicioso.

8.1.9 Se deben hacer revisiones y análisis periódicos del uso de software malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de Tecnología.

8.1.10 Se deben hacer campañas de sensibilización a todos los colaboradores, convenios, proveedores, contratistas y/o terceros, con el fin de generar una cultura de seguridad de la información.

8.1.11 Los colaboradores, convenios, proveedores, contratistas y/o terceros de Confa no deben abrir archivos o link adjuntos de correo electrónico recibidos de remitentes desconocidos, de dudosa procedencia o archivos contenidos en dispositivos externos, que puedan contener software malicioso.

8.1.12 Los colaboradores, convenios, proveedores, contratistas y/o terceros no deben deshabilitar el antivirus, el firewall, los congeladores de discos y cualquier otro recurso informático que preserve la seguridad de la Información en la organización, esta labor es exclusiva del personal técnico autorizado.

8.1.13 Se recomienda el uso de las redes asignadas por Confa, redes seguras o conocidas, el uso de redes no seguras puede permitir que un atacante intercepte el tráfico de red de un dispositivo y obtenga acceso a información confidencial y/o personal.

8.1.14 Todo colaborador es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio a Confa y cuyo origen le sea desconocido o sospechoso. Así mismo el colaborador será responsable de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos. El colaborador deberá informar cuando se presente alguno de estos casos a la cuenta de correo oficial.seguridad@confaco.co.

8.1.15 Toda instalación de software en la organización debe ser autorizada y realizada por Tecnología y la descarga de algún tipo de instalador se debe hacer desde las páginas oficiales.

8.1.16 En el momento que Tecnología requiera una ventana para la revisión del equipo frente al riesgo de seguridad, el colaborador debe facilitar el espacio para la ejecución de la misma.

8.1.17 Todo equipo que no pertenezca a la organización y requiera acceder a la red de Confa, debe contar con la autorización solicitada por el Gerente/Líder/Coordinador y aprobada por el profesional de seguridad de la información, adicional todo el software que tenga el equipo debe ser licenciado y contar con un antivirus.

8.2. Copias de Seguridad

8.2.1 Cada uno de los colaboradores debe hacerse responsable de la generación de copias de respaldo de su información ubicada en las herramientas tecnológicas (Suite colaborativa, estaciones de trabajo, entre otras) asignadas para su actividad; Confa como prioridad le brinda una herramienta de almacenamiento en la nube para realizar las copias.

8.2.2 Tecnología debe actualizar periódicamente las configuraciones de los servidores para la correcta ejecución de las copias de respaldo de las bases de datos, servidores de aplicaciones, configuración de sistemas operativos de servidores, archivos adjuntos cuando sea necesario y Web Services.

8.2.3 Tecnología debe planear la restauración de las copias de seguridad para verificar su correcto funcionamiento.

8.3 Control de software en explotación

8.3.1 Se debe asegurar que en los sistemas operativos no se instalará software diferente al que servirá para el desempeño de las funciones de los colaboradores. Cualquier tipo de instalación de aplicaciones requerida por un colaborador debe ser gestionada por el Comité de Licencias.

8.3.2 La gerencia de Tecnología es la única responsable de monitorear las actividades de red, es por ello que ningún colaborador debe instalar programas que escanean las redes en estaciones de trabajo como en dispositivos móviles.

8.3.3 Cualquier equipo o dispositivo móvil conectado a la red de Confa puede ser monitoreado y supervisado únicamente por Tecnología y al encontrar cualquier riesgo, se realizará la debida gestión del incidente de seguridad por parte de Profesional de Seguridad de la Información.

8.3.4 Tecnología debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, entre otros.

8.3.5 Para el desarrollo de contenidos de carácter laboral, se prohíbe el uso de software no licenciado en equipos personales, de lo contrario se debe gestionar los recursos necesarios para el desarrollo de la actividad.

8.4 Registro y seguimiento

8.4.1 La Caja de Compensación Familiar de Caldas - Confa, realizará monitoreo permanente del uso que dan los colaboradores a los recursos de la plataforma tecnológica y los sistemas de información de la organización.

8.4.2 Los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la institución.

8.4.3 Los servicios, deben determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.

8.4.4 La Gerencia de Tecnología en conjunto con los responsables de los servicios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada y de los sistemas de información, acorde con los eventos a auditar establecidos.

8.4.5 La Gerencia de Tecnología y los Administradores Funcionales, deben certificar la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información, estos registros deben ser almacenados y sólo deben ser accedidos por personal autorizado.

8.5. Gestión de Vulnerabilidades

8.5.1 Confa, por intermedio del Profesional de Seguridad de la Información, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica, por medio de la realización de pruebas de vulnerabilidades (cada año), y aplicará los correctivos sobre los hallazgos arrojados por dichas pruebas.

8.5.2 El Profesional de Seguridad de la Información debe revisar según se requiera, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los Administradores

Funcionales y a los Profesionales de Tecnología involucrados, con el fin de prevenir la exposición a riesgos.

8.5.3 El Profesional de Seguridad de la Información debe gestionar los planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

8.6 Consideraciones sobre auditorías de sistemas de información

8.6.1 Confa, apoyada en la Gerencia de Tecnología y en el Procedimiento de Auditoría Interna, verificará el cumplimiento de las directrices organizacionales, de las normas ISO aplicables y la normatividad vigente, cada año o según sea necesario.

8.6.2 Tecnología y/o los Administradores Funcionales deben verificar que las auditorías concluyan sin afectar la disponibilidad y los datos de los sistemas de información implementados en la Organización.

8.6.3 Los Administradores Funcionales deben planificar las actividades (pruebas, apagados, modificaciones al sistema de información, monitoreo a roles y perfiles, entre otras) para reducir al mínimo las interrupciones de los procesos, de acuerdo con los requisitos de auditoría, seguridad de la información (análisis de vulnerabilidades internas y externas) y las actividades relacionadas con la verificación de los sistemas de información.

8.6.4 El Profesional de Seguridad de la Información debe velar por el cumplimiento del Modelo de Gestión de Seguridad de la Información con seguimientos continuos a los sistemas de información, adquisición de herramientas de seguridad de la información, monitoreo con herramientas de seguridad de la información, licenciamientos, foros de seguridad de la información, planes de acción y recomendaciones.

8.6.5 El Profesional de Seguridad de la Información debe gestionar lo solicitado por las auditorías internas, externas o de cualquier ente de control en lo referente a temas tecnológicos, cumpliendo los reglamentos internos y normativa vigente.

9. SEGURIDAD DE LAS TELECOMUNICACIONES

[ISO/IEC 27001:2022 A.8.20 a 8.23]

9.1. Gestión de seguridad en las redes de datos

9.1.1 Tecnología debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red, con el fin de disminuir la afectación en tiempo de la prestación de los servicios a los grupos de interés.

9.1.2 Tecnología debe gestionar e implementar los controles necesarios para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

9.1.3 Tecnología debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos en la red de datos de Confa e inhabilitar o eliminar el resto de los servicios, protocolos y puertos que no sean necesarios.

9.1.4 Tecnología y la organización como responsable y encargados de los datos personales, debe velar por la confidencialidad y disposición de la información en el direccionamiento y el enrutamiento de las redes de datos.

9.1.5 Por razones de seguridad y mantenimiento de la infraestructura de red y herramientas tecnológicas, la Gerencia de Tecnología o a quien se asigne está facultada para monitorear todos los equipos, dispositivos móviles, sistemas a los que los colaboradores, usuarios, convenios, proveedores, contratistas y/o terceros se les haya permitido el acceso para el cumplimiento de sus funciones y filtrar el contenido que se transmitan en la red en cualquier momento.

9.1.6 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que son autorizados para acceder a la red de datos y los componentes tecnológicos, son responsables de todas las actividades que se ejecuten con los usuarios de acceso.

9.1.7 Los colaboradores, los convenios, proveedores, contratistas y/o terceros, proveedores, no deben retirar los cables de estaciones de trabajo o dispositivos de red para ser usados con otros fines, cuando sea necesario se debe contar con la autorización de redes o mesa de ayuda de Tecnología.

9.1.8 En las sedes de la organización, se proporciona a los colaboradores, convenios, proveedores, contratistas y/o terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar sus funciones o actividades, por lo cual no es permitido conectar elementos de red (Switches, enrutadores, módems, entre otros) a las estaciones de trabajo o a los puntos de red corporativa que no sean autorizados por Tecnología.

9.1.9 El trabajo a través de accesos remotos o VPN a la red de datos de Confa, sólo se permitirá de acuerdo a la política de trabajo autónomo e instructivo para soporte remoto de equipos de cómputo, cláusulas de confidencialidad y/o acuerdos pactados con la organización; para usuarios creados en la VPN de convenios, proveedores, contratistas y/o terceros, entre otros, se debe informar a Secretaría General para que sean registrados como encargados de la información.

9.1.10 Para los colaboradores que usen medios remotos como VPN, software de control remoto, modalidad de trabajo autónomo, entre otras, deben conocer y cumplir las medidas de seguridad informática, tratamiento de datos personales y disposiciones de ley que permitan la confidencialidad, integridad, disponibilidad y no repudio de la información.

9.1.11 Para el caso de que el proveedor, tercero y/o contratista finalice su relación contractual con Confa, es responsabilidad del supervisor administrativo del contrato y del Administrador Funcional de informar la inactivación del uso de la VPN a Tecnología.

9.1.12 Para garantizar el correcto funcionamiento del fluido eléctrico y de la red corporativa, se debe hacer un adecuado uso de las conexiones de red, dispositivos activos de red (switches, cámaras, chapas biométricas, access point, entre otras) y eléctricas. Así mismo, se prohíbe la manipulación del cableado eléctrico y de red sin la debida autorización o acompañamiento de las áreas encargadas o especializadas.

9.2 Segmentación o separación de las redes

9.2.1 Confa debe establecer un esquema de segregación, separación de las redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

9.2.2 Se debe realizar solicitud al área de tecnología para los controles de acceso a los servicios de red.

9.2.3 Tecnología debe retirar periódicamente los activos fijos que se den de baja y que tengan acceso a la red de Confa.

9.2.4 Se deben establecer parámetros técnicos (usuarios, contraseñas, accesos a sitios web, accesos a dispositivos USB, entre otros) para la conexión segura con los servicios de red.

9.2.5 Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

9.2.6 Se deben separar las redes inalámbricas de acceso a visitantes de las redes internas, para garantizar los principios de la seguridad de la información.

9.2.7 Se debe implementar el doble factor de autenticación donde aplique.

9.3 Intercambio de información con terceros

9.3.1 El intercambio de información entre colaboradores y usuarios externos, debe hacerse por medio de las cuentas corporativas del correo electrónico como medio de comunicación oficial y haciendo uso de las herramientas de seguridad que éste contiene. Se prohíbe el uso de otros medios no corporativos u oficiales para enviar información perteneciente a Confa.

9.3.2 Confa velará por la protección de la información, sin embargo, el contenido de los archivos enviados a través del canal de internet será responsabilidad de los colaboradores. Dejar lo de IA en el capítulo de política de IA

9.3.3 Para la transmisión de información sensible, privada o confidencial, el colaborador debe asegurar que esta, se realice desde una red confiable que cuente con las protecciones necesarias para dicho fin.

9.3.4 Antes de ser enviada la información sensible, privada o confidencial a convenios, proveedores, contratistas y/o terceros, entre otros, el colaborador debe informar a la Gerencia de Inteligencia de Datos sobre la información solicitada.

9.3.5 Es deber de la Secretaria General registrar los convenios, proveedor, contratista y/o tercero nuevo, donde se expongan datos personales, con el fin de poder realizar su inscripción en el Registro Nacional de Base de Datos.

9.4 Políticas de uso de Internet

Confa, consciente de la importancia de internet como una herramienta para el desempeño de las labores diarias, proporcionará los recursos necesarios para asegurar su disponibilidad a los colaboradores que así lo requieran para el desarrollo de sus actividades dentro de la organización y el tráfico de Internet podrá ser registrado y revisado con fines de seguridad, auditoría y cumplimiento normativo, de acuerdo con las leyes vigentes de protección de datos y reglamentos internos..

9.4.1 Usos aceptables del servicio

9.4.1.1 Tecnología debe proporcionar los recursos necesarios para la implementación, administración y mantenimientos requeridos para la prestación segura del servicio de internet en las sedes de Confa, bajo las restricciones de los perfiles de acceso establecidos.

9.4.1.2 Tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna en las sedes de Confa.

9.4.1.3 Todas las comunicaciones establecidas mediante los servicios de Internet de Confa pueden ser revisadas y/o monitoreadas por Tecnología o cualquier instancia de vigilancia y control, incluyendo la carga y tráfico.

9.4.1.4 Tecnología debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.

9.4.1.5 Tecnología debe generar y proporcionar cuando sean solicitados a Productividad y Desarrollo, Auditoría y Secretaría General registros de la navegación y los accesos de los usuarios a internet en las sedes de Confa, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.

9.4.1.6 Los colaboradores, convenios, proveedores, contratistas y/o terceros a los que se les habilite el servicio de internet de Confa, deben utilizarlo exclusivamente para la ejecución de sus funciones o actividades contratadas por Confa y no debe utilizarse para ningún otro fin.

9.4.1.7 Los colaboradores, convenios, proveedores, contratistas y demás terceros autorizados para acceder al servicio de internet de Confa son responsables de su uso adecuado y de evitar cualquier práctica que comprometa los recursos tecnológicos, que afecte la seguridad de la información o cause daños reputacionales a la organización. Bajo ninguna circunstancia podrán realizar actividades ilícitas o malintencionadas que atenten contra terceros, vulneren la legislación vigente o pongan en riesgo la seguridad de la información.

9.4.2 Usos no aceptables del servicio

9.4.2.1 Los colaboradores, convenios, proveedores, contratistas y/o terceros deben abstenerse de descargar software no autorizado desde internet, así como su instalación en las estaciones de trabajo asignadas para el desempeño de sus labores, a menos que sean autorizados por el comité de licencias.

9.4.2.2 Evitar el envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red de Confa, a menos que el desempeño de las funciones lo amerite.

9.4.2.3 Cualquier otro propósito diferente al considerado en el apartado de usos aceptables del servicio de la presente política.

9.4.2.4 Todos los usuarios invitados que tengan acceso al servicio de internet de Confa, deben cumplir estrictamente con las normas colombianas.

9.4.2.5 No se permite el acceso desde la red de Confa a páginas con contenido restringido como pornografía, proxy's anónimos, redes sociales, actividades criminales

y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware o páginas catalogadas como de alto riesgo.

9.4.2.6 En las estaciones de trabajo asignadas para el desempeño de sus labores, no se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking.

9.4.2.7 El acceso a Internet se gestionará mediante herramientas tecnológicas de filtrado web, bloqueando categorías de sitios y servicios que representen riesgo para la organización, la productividad y el cumplimiento legal.

9.4.2.8 Se bloquearán sitios maliciosos, de phishing, distribución de malware o que puedan comprometer la confidencialidad, integridad y disponibilidad de la información de Confa.

9.4.2.9 Cualquier acceso a categorías restringidas deberá ser solicitado y aprobado mediante el procedimiento de excepciones establecido por el área de Seguridad de la Información.

9.5 Uso del correo electrónico corporativo

9.5.1 Usos aceptables del servicio del correo electrónico

9.5.1.1 Los colaboradores, convenios, proveedores, contratistas y/o terceros que les sea asignada una cuenta de correo del dominio de Confa, deben autenticarse mediante verificación en dos pasos (2FA) para acceder a los servicios.

9.5.1.2 Los colaboradores, convenios, proveedores, contratistas y/o terceros que les sea asignada una cuenta de correo del dominio de Confa se les prohíbe compartir documentos fuera del dominio corporativo sin autorización previa. Google Drive está configurado para restringir el acceso externo por defecto.

9.5.1.3 Los mensajes y la información contenida en las cuentas de correo son de propiedad de Confa y pueden ser revisadas por cualquier instancia de vigilancia y

control, en caso de una investigación o incidentes de seguridad de la información de acuerdo con instructivo copia de Google Workspace.

9.5.1.4 Los colaboradores, convenios, proveedores, contratistas y/o terceros que les sea asignada una cuenta de correo del dominio de Confa, deben utilizarse exclusivamente para la ejecución de las actividades contratadas por Confa y no se debe utilizar para otros fines, así mismo, se prohíbe el uso de cuentas personales para actividades laborales.

9.5.1.5 Se deben utilizar las cuentas de correo corporativo de manera ética, razonable, eficiente, responsable, no abusiva, dando cumplimiento a las normas colombianas, sin generar riesgos para la operación de equipos o sistemas de información y la imagen de Confa.

9.5.1.6 Los colaboradores, convenios, proveedores, contratistas y/o terceros que son autorizados para acceder a las cuentas de correo corporativas son responsables de todas las actividades que se ejecuten con sus usuarios.

9.5.1.7 Cuando un área o gerencia tenga información de interés institucional para divulgar, lo debe hacer a través de Comunicaciones Internas y/o Corporativas de Confa o el medio formal autorizado para realizar esta actividad.

9.5.1.8 Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por Confa y deberán conservar en todos los casos el mensaje legal de la organización.

9.5.1.9 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros serán responsables de generar las copias de seguridad de sus buzones de correo y documentos almacenados en dicha plataforma.

9.5.1.10 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros son responsables de informar sobre accesos no autorizados en: correos electrónicos, agendas, accesos a los documentos de drive, grupos de chat y aplicaciones o extensiones de Chrome, entre otros y que no correspondan a sus funciones o actividades designadas dentro de Confa, con el fin de que se realicen los ajustes de permisos requeridos. Con lo anterior también es obligación del líder, coordinador, supervisor del contrato, administrador funcional hacer seguimiento, reportar novedades

del personal a cargo con el propósito de contribuir al aseguramiento de la administración de usuarios.

9.5.1.11 El usuario debe reportar cuando reciba correos no deseados, maliciosos, no solicitados, con adjuntos sospechosos, correos de dudosa procedencia o con virus al Profesional de Seguridad de la Información, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos y debe asumir la responsabilidad de las consecuencias al no reportar este tipo de eventos.

9.5.1.12 Confa se reserva el derecho de filtrar los tipos de archivo, remitentes, asuntos de correo para evitar amenazas de virus y otros programas destructivos. En caso de que un colaborador detecte el no ingreso remitentes de correos externos debe reportar al profesional de infraestructura y/ o profesional de seguridad de la información para su respectiva revisión.

9.5.1.13 Los colaboradores, convenios, proveedores, contratistas y/o terceros de Confa que tengan acceso a la suite colaborativa, deben habilitar la verificación en dos pasos o doble factor de autenticación.

9.5.1.14 Los colaboradores, convenios, proveedores, contratistas y/o terceros de Confa que tengan acceso a cuentas de la suite colaborativa, no deben hacer uso de la cuenta corporativa en redes sociales, plataformas web no autorizadas, sitios de compras y/o comercio electrónico, entre otras.

9.5.1.15 Todos los correos masivos en la organización deben ser gestionados con el área de relaciones corporativas y usando las plataformas adecuadas para dicho fin, cumpliendo con los estándares establecidos por la organización.

9.5.1.16 Se considera como uso no aceptable del correo electrónico el envío o intercambio de mensajes que pongan en riesgo la reputación de Confa y que promuevan la discriminación social o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

9.5.1.17 Los colaboradores, convenios, proveedores, contratistas y/o terceros de Confa terminada su relación laboral, no podrán enviar información masiva a las cuentas de la organización y/o aquellas recolectadas de las base de datos de Confa para fines de envío de correos masivos de tipo publicitario o temas distintos a las actividad de Confa.

9.5.2 Uso no aceptable del servicio del correo electrónico

9.5.2.1 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que envíen correos masivos que no hayan sido previamente autorizados por las áreas encargadas.

9.5.2.2 Envío o intercambio de mensajes que pongan en riesgo la reputación de Confa y que promuevan la discriminación o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

9.5.2.3 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que envíen mensajes que contengan amenazas, ciberdelincuencia o inciten a la violencia.

9.5.2.4 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que divulguen información de propiedad de Confa sin autorización.

9.5.2.5 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que abran o hagan uso y revisión de la cuenta de correo electrónico de otro usuario.

9.5.2.6 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que envíen correos electrónicos masivos sin usar la copia oculta de los destinatarios.

9.5.2.7 Todos los colaboradores, convenios, proveedores, contratistas y/o terceros que hagan uso del correo electrónico para fines personales, inscripción a plataformas de ventas online o plataformas que no se requieran para el desarrollo de las actividades contratadas por Confa.

9.5.2.8 El uso de correos electrónicos diferentes a los del dominio de Confa para el desarrollo de las actividades contratadas por ésta. Lo anterior aplica para los colaboradores y todos aquellos terceros que por la naturaleza de sus servicios cuenten con un correo de la Organización.

9.5.2.9 No cumplir con los términos y condiciones de la plataforma de correo.

9.5.2.10 Todo correo que contenga virus será bloqueado o rechazado por las herramientas de seguridad.

9.6 Política de transferencia de información

9.6.1 El área de Secretaría General debe establecer en las relaciones contractuales que se constituyan con terceras partes, los acuerdos de confidencialidad, políticas de protección de datos, metodología de entrega dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de Confa.

9.6.2 El área de Tecnología y/o los Administradores Funcionales deben velar porque el intercambio de información con entidades externas se realice en cumplimiento de las políticas de seguridad de la información, política de tratamiento de la información, acuerdos de confidencialidad y normas colombianas.

9.6.3 Los colaboradores de Confa no deben revelar o intercambiar información confidencial de la Organización por ningún medio, sin contar con la debida autorización del gerente, coordinador, líder y/o jefe.

9.6.4 Si las áreas de la organización requieren compartir información de tipo personal de los afiliados, beneficiarios, colaboradores, usuarios y menores de edad, con convenios, proveedores, contratistas, entidades de vigilancia y control, y/o terceros, deberán solicitar el concepto al oficial de protección de datos y/o Gerencia de Inteligencia de Datos.

10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

[ISO/IEC 27001:2022 A.8.25 a 8.33]

10.1 Requerimientos de seguridad de los sistemas de información

La Caja de Compensación Familiar de Caldas - Confa, asegurará que el software adquirido y/o desarrollado tanto al interior de la Corporación como por terceras partes, incluirá buenas prácticas de seguridad y calidad. Las áreas y/o servicios propietarios de sistemas de información y Tecnología, incluirán requisitos de seguridad en la definición de requerimientos y posteriormente se asegurará que éstos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

10.1.1 Con el fin de evitar riesgos en la arquitectura TIC, Administración de la plataforma y cibernéticos, la Gerencia de Tecnología debe aprobar la compra, desarrollo, implementación, mejora, entre otros, de los aplicativos, sistemas de información o el software requerido por los servicios.

10.1.2 Tecnología debe establecer metodologías para el desarrollo, mejoras, implementación y pruebas de software, que incluya la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.

10.1.3 Las gerencias, áreas y/o servicios, propietarias de los sistemas de información, en acompañamiento de Tecnología, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando los requerimientos de seguridad de la información.

10.1.4 Las gerencias, áreas, servicios y/o Administradores Funcionales propietarias de los sistemas de información deben definir qué información confidencial puede ser eliminada de sus sistemas y solicitar que éstos soporten la **eliminación** de dicha información, como es el caso de los datos personales o financieros cuando ya no son requeridos, siguiendo las tablas de retención documental y las normas colombianas.

10.1.5 Los profesionales de tecnología deben documentar los requerimientos establecidos, y definir la arquitectura de software más conveniente para cada sistema de información que se requiera desarrollar o implementar, de acuerdo con los requerimientos de seguridad y los controles deseados.

10.1.6 Los profesionales de soluciones tecnológicas deben verificar y asegurar que todo sistema de información adquirido a través de un tercero o desarrollado en Confa, utilice herramientas de desarrollo licenciadas, seguras, conocidas y actuales en el mercado y siguiendo la Política de Uso de Inteligencia Artificial (IA) en la Organización.

10.1.7 Los profesionales de soluciones tecnológicas y/o proveedores deben deshabilitar las funcionalidades de “completar automáticamente” en formularios de solicitud de datos que requieran información sensible, con el fin de garantizar la seguridad de la información.

10.1.8 Los profesionales de soluciones tecnológicas y/o proveedores, deben garantizar en sus desarrollos el cerrar las sesiones activas de las aplicaciones cuando se presente inactividad por un tiempo establecido.

10.1.9 Los profesionales de soluciones tecnológicas y/o proveedores, deben utilizar los protocolos de red sugeridos por los profesionales de infraestructura tecnológica en los aplicativos desarrollados y adquiridos por Confa.

10.1.10. Los profesionales de soluciones tecnológicas y/o proveedores deben realizar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros y utilizando mecanismos o herramientas de cifrado.

10.2 Seguridad en los procesos de desarrollo y de soporte

10.2.1 La Caja de Compensación Familiar de Caldas - Confa velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado, además, se asegurará que todo software desarrollado o adquirido cuente con el nivel de soporte requerido por la Organización.

10.2.2 Tecnología en conjunto con el administrador funcional o quien designe el servicio, deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad necesarios para dar paso a producción.

10.2.3 Tecnología en conjunto con el administrador funcional o quien designe el servicio, deben realizar las pruebas de los sistemas de información, ajustes y/o entrega de funcionalidades nuevas, cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos (Instructivo para definir el plan de pruebas de desarrollo) establecidas para este fin, documentando dichas pruebas y de ser satisfactorias el servicio debe realizar la aprobación para el respectivo despliegue en producción y formalizar la notificación de la puesta en producción mediante un correo electrónico dirigido a las áreas funcionales, confirmando la fecha y hora del despliegue

10.2.4 Tecnología en conjunto con el administrador funcional o quien designe el servicio deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos, de cambios y/o nuevas funcionalidades.

10.2.5 Tecnología debe implantar los controles necesarios de acuerdo con el instructivo de gestión de cambios de emergencia e instructivo gestión de cambios soluciones tecnológicas, para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción, han sido aprobadas de acuerdo con el procedimiento de control de cambios.

10.2.6 Tecnología debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.

10.2.7 Tecnología y Secretaría General deben asegurarse que los sistemas de información adquiridos o desarrollados por terceros, cuenten con políticas, procedimientos, estándares y/o metodologías de seguridad de la información, riesgos y continuidad del negocio implementadas y monitoreadas, con un acuerdo de licenciamiento, acuerdo de confidencialidad, acuerdo de protección de datos personales, metodologías de gestión de cambios, metodología de entrega y custodia de la información al terminar el contrato, así mismo, se debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

10.2.8 Tecnología en sus desarrollos propios debe cumplir con los procedimientos, estándares, políticas, metodología de gestión de cambios, metodologías de pruebas y paso a producción.

10.2.9 Los profesionales de soluciones tecnológicas deben considerar las buenas prácticas y lineamientos de desarrollo seguro (Instructivo para el desarrollo de software y de sistemas de información), durante el ciclo de vida de desarrollo (Metodología de referencia para el Ciclo de vida de desarrollo de sistemas de información) de los mismos, pasando desde el diseño hasta la puesta en marcha.

10.2.10 Tecnología debe proporcionar un canal de comunicación y un nivel adecuado de soporte para solucionar los problemas que se presenten en el aplicativo.

10.2.11 Todos los colaboradores pertenecientes al área de Tecnología deben garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles

del sistema, identificadores de sesión o información de las cuentas de usuarios, así mismo, deben implementar mensajes de error genéricos.

10.2.12 Los profesionales de soluciones tecnológicas deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

10.2.13 Los profesionales de soluciones tecnológicas deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

10.3 Datos de prueba

10.3.1 Protección de datos de prueba

10.3.1.1 Tecnología y el administrador funcional o quien designe el servicio, debe verificar que los ambientes productivos apuntan a las bases de datos de producción.

10.3.1.2 Tecnología y el administrador funcional o quien designe el servicio, deben verificar y garantizar que las bases de datos usadas en pruebas, sean eliminadas una vez culminada la actividad.

10.3.1.3 El administrador funcional y quien designe el servicio debe informar a Tecnología y a Gerencia de Inteligencia de Datos sobre pruebas en los sistemas de información contratados externamente, con el fin de gestionar y revocar los datos de prueba usados.

10.3.1.4 Tecnología, el administrador funcional o quien designe el servicio y convenios, proveedores, contratistas y/o terceros de desarrollo, deben cumplir con los lineamientos de Confa y las normas colombianas frente al uso de datos para ambientes de prueba.

10.3.1.5 El administrador funcional, supervisor administrativo o técnico de los contratos o quien designe el servicio, deben informar a la Secretaría General sobre la entrega de base de datos que incluya información sensible para fines de pruebas a un convenio, proveedor, contratista y/o tercero, con el fin de establecer los encargados de la información previo a la celebración de dichos contratos.

11. SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES

[ISO/IEC 27001:2022 A.5.19 a 5.22]

La Caja de Compensación Familiar de Caldas - Confa, establecerá mecanismos de control en sus relaciones con los convenios, proveedores, contratistas y/o terceros, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

11.1 Los supervisores de los contratos con convenios, proveedores, contratistas y/o terceros deben asegurar la divulgación de las políticas internas, normas y procedimientos que apliquen a ambas partes.

11.2 Los convenios, proveedores, contratistas, entidades externas y/o terceros que requieran acceso a la información de Confa, deben cumplir con el acuerdo de confidencialidad, acuerdo de protección de datos personales, cláusulas de seguridad de la información y metodología de entrega y custodia de la información según sea determinado en el contrato. Estos aspectos deben ser incluidos en las cláusulas de cualquier proceso de contratación y cumplir con lo establecido en la ley de habeas data o ley 1581. Así mismo, el administrador funcional, supervisor administrativo o técnico del contrato debe reportar al oficial de tratamiento de datos, para que hagan sus modificaciones en el RNBD como encargado de la información.

11.3 Al terminar los contratos, los acuerdos de confidencialidad, acuerdos de protección de datos personales, metodología de entrega y custodia de la información deben hacer parte integral de los mismos o documentos que legalicen la relación de las negociaciones.

11.4 Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

11.5 Los convenios, proveedores, contratistas y/o terceros, deben contar con una política de copias de seguridad que incluya: los soportes en las que se deben realizar, la periodicidad(diaria, semanal, mensual y anual, según corresponda), tiempo de conservación y las ubicaciones de los centros de respaldo.

11.6 Secretaría General debe entregar al oficial de protección de datos personales los documentos de las relaciones contractuales con terceros, para su debida legitimación de datos personales para ser registrados ante la Superintendencia de Industria y Comercio.

11.7 El convenio, proveedor, contratista y/o tercero debe reportar al supervisor administrativo, administrador funcional, oficial de protección de datos (proteccion.datos@confa.co) y/o profesional de seguridad de la información (oficial.seguridad@confa.co) cualquier vulnerabilidad en la información detectada y que ponga en riesgo la información de la organización.

11.8 Los convenios, proveedores, contratistas y/o terceros que sean encargados o responsables de la información personal de los grupos de interés de Confa, deberán notificar ante la Superintendencia de Industria y Comercio y los titulares cualquier incidente que afecte dicha información.

11.9 Confa debe informar a los convenios, proveedores, contratistas y/o terceros cualquier incidente, cambio o acciones preventivas o correctivas en la seguridad de la información que representen un riesgo para ellos.

11.10 Los supervisores de los contratos y Secretaría General deben garantizar que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento, acuerdo de confidencialidad, acuerdo de protección de datos personales, planes de la ejecución y custodia de copias de seguridad, metodología de entrega y custodia de la información al terminar el contrato, así mismo, se deben especificar las condiciones de uso del software y los derechos de propiedad intelectual.

11.11 Los convenios, proveedores, contratistas y/o terceros, administradores funcionales, supervisor técnico, supervisor administrativo, gerentes, coordinadores, líderes o jefes, deben involucrar o informar a Tecnología y Gerencia de Inteligencia de Datos de cualquier prueba de funcionalidad o entrega.

11.12 Tecnología, el administrador funcional o quien designe el servicio y los convenios, proveedores, contratistas y/o terceros que ejecuten desarrollos deben cumplir con los lineamientos de Confa y normas colombianas frente a la ejecución de pruebas y el uso de datos para dichos ambientes.

11.13 El Contratista, proveedor, prestador de servicio y/o tercero terminada su relación laboral con CONFA no podrá seguir haciendo uso los usuarios, contraseñas, credenciales y/o token asignados para la realización de las actividades objeto del contrato finalizada la relación contractual, si es necesario el acceso se debe solicitar su autorización con el supervisor administrativo del contrato o con el gerente o líder o coordinador o jefe.

11.14 El Contratista, proveedor, prestador de servicio y/o tercero terminada su relación laboral con CONFA no podrá manipular la infraestructura de CONFA, crear, modificar, eliminar archivos o documentos asignados para la realización de las actividades objeto del contrato finalizada la relación contractual, si es necesario el acceso se debe solicitar su autorización con el supervisor administrativo del contrato o con el gerente o líder o coordinador o jefe.

11.15 Confa en contratos con proveedores globales de tecnología (ej. AWS, Google Workspace, Google Cloud), adoptará el Modelo de Responsabilidad Compartida. Esto implica la aceptación de las políticas de seguridad, acuerdos de nivel de servicio (SLA) y políticas de tratamiento de datos del proveedor, asegurando que el uso de sus servicios cumpla con los estándares de protección de datos de la organización.

11.16 Los contratistas, proveedores y terceros que realicen desarrollos o suministren servicios de nube, deben garantizar la continuidad de la operación mediante un Plan de Recuperación ante Desastres (DRP) documentado y una estrategia de copias de seguridad verificables. Estos mecanismos deben asegurar que, ante un fallo crítico, la restauración de los servicios y la integridad de la información de Confa se realicen dentro de los tiempos acordados.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

[ISO/IEC 27001:2022 A.5.24 a 5.28]

12.1 Proceso de gestión de incidentes de seguridad de la información con mejoras constantes

El proceso de gestión de seguridad de la información se activa de la siguiente manera:

12.1.1 Todos los usuarios, convenios, proveedores, contratistas y/o terceros y colaboradores de Confa, tienen la responsabilidad de reportar cualquier violación a las políticas establecidas en este documento, evento, incidente o debilidad en cuanto a la seguridad de la información que identifique o se presente. Para los proveedores, contratistas y/o terceros que identifique cualquier riesgo de vulnerabilidad en las bases de datos que tienen a su cargo y que contengan datos personales, lo deben reportar ante la superintendencia de industria y comercio y ante la organización.

12.1.2 Por parte de las personas involucradas se debe dar un tratamiento de confidencialidad y adecuado a todos los incidentes de seguridad de la información reportados, hasta que la organización lo considere.

12.1.3 Se debe divulgar periódicamente a los colaboradores, el procedimiento de atención de incidentes de seguridad de la información de la organización.

12.1.4 Es responsabilidad de la gerencia de Tecnología realizar sensibilización a todos los colaboradores sobre incidentes de seguridad de la información detectados.

12.1.5 Los incidentes de seguridad resultantes del incumplimiento de la Política de Seguridad de la Información Corporativa y/o Política de tratamiento de la Información, serán direccionados a las áreas correspondientes donde se activará el proceso disciplinario respectivo.

12.1.6 El profesional de seguridad de la información debe gestionar cualquier recomendación dada por entes auditores frente a la seguridad de la información.

12.1.7 El profesional de seguridad de la información debe gestionar los riesgos y sus controles frente a la seguridad de la información.

12.1.8 El profesional de seguridad de la información debe notificar o informar al oficial de protección de datos frente a cualquier incidente reportado y que afecte los datos personales de los grupos de interés de Confa, para que proceda con el registro frente a los órganos de control.

13. TRABAJO AUTÓNOMO

[ISO/IEC 27001:2022 A.6.7]

13.1 Política de trabajo autónomo

13.1.1 Solo los colaboradores, convenios, proveedores, contratistas y/o terceros previamente autorizados por el coordinador, líder o gerente, podrán utilizar los beneficios del sistema VPN y/o permisos por IP's desde el portal seguro de aplicaciones.

13.1.2 Es responsabilidad del usuario con VPN y/o permisos por IP's desde el portal seguro de aplicaciones, garantizar que ninguna otra persona utilice su cuenta de acceso y no dar en préstamo el usuario y la contraseña asignada para tal fin, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

13.1.3 En caso de pérdida de una estación de trabajo con VPN instalada y configurada, el colaborador debe reportar inmediatamente al profesional de seguridad oficial.seguridad@confaco.co de la información, con el fin de tomar las acciones necesarias.

13.1.4 El uso del sistema VPN, está ligado y controlado con la contraseña asociada al usuario de red (LDAP) la cual debe cumplir con los estándares según el instructivo para crear contraseñas seguras.

13.1.5 Cuando un colaborador esté conectado a la red de Confa haciendo uso de la VPN, el sistema permitirá el acceso a las aplicaciones de acuerdo con lo solicitado por el coordinador, líder, jefe y/o gerente, del usuario creado en la VPN.

13.1.6 Para cada usuario de VPN solo se permite una conexión simultánea desde la red externa hacia la red de Confa.

13.1.7 Los acceso a las aplicaciones por VPN serán configuradas y administradas por Tecnología. Todos los computadores dispuestos por Confa conectados a la red interna de la organización mediante VPN, deberán utilizar el software antivirus actualizado definido por Tecnología.

13.1.8 Para los equipos personales de los colaboradores que requieran de VPN se debe contar con la previa autorización del coordinador, jefe y/o líder para su respectiva instalación, así mismo, se recomienda que los equipos personales que se conecten a la red interna de la organización, cuenten con un sistema operativo original y actualizado, adicional que el usuario tenga instalado y actualizado un software antivirus en su equipo.

13.1.9 Las conexiones establecidas desde la redes externas hacia la red interna de Confa vía VPN, deben ser generadas desde servicios de internet conocidos y seguros. Se recomienda no realizar conexiones desde Café internet, Wifi's libres, centros comerciales o toda red pública.

13.1.10 Mediante el uso de la tecnología VPN, los usuarios deben alinear sus actividades acorde con las políticas de seguridad de la información, normas, leyes y reglamentaciones colombianas, y los lineamientos establecidos por la organización, así mismo, los accesos y actividades realizadas por conexión VPN pueden ser auditados cuando sea requerido por la organización.

13.1.11 Para las conexiones establecidas desde la redes externas hacia la red interna de Confa vía VPN, los usuarios deben dar cumplimiento a lo establecido por la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013 y los lineamientos y políticas organizacionales frente a la protección de datos personales.

14. SEGURIDAD Y USO DE DISPOSITIVOS MÓVILES

[ISO/IEC 27001:2022 A.8.1]

Esta política aplica para los dispositivos móviles que son activos fijos de Confa, es decir se excluyen dispositivos móviles personales.

14.1 Política de seguridad y uso de dispositivos móviles

14.1.1 La configuración y actualización inicial de los dispositivos móviles pertenecientes y sus respectivas aplicaciones pertenecientes a Confa, cualquiera que sea su fabricante, serán ejecutados por el personal de Mesa de Ayuda adscrito a la Gerencia de Tecnología.

14.1.2 El área de Tecnología configurará los accesos solicitados por las áreas a las aplicaciones de los dispositivos móviles de Confa que procesan información crítica.

14.1.3 Confa es el dueño del dispositivo móvil y será asignado a un colaborador, el cual se hará responsable del mismo, tanto de su protección física como lógica. En caso de renuncia y/o terminación de la relación laboral, el colaborador debe realizar la devolución de dicho dispositivo a su respectivo coordinador, jefe y/o líder del área correspondiente y no podrá realizar eliminación de datos, desinstalación de aplicaciones o restauración de fábrica del dispositivo.

14.1.4 Fuera de las actividades laborales, está prohibido a los colaboradores prestar o dejar desatendido el dispositivo móvil a su cargo, el cual contiene acceso a la información de Confa.

14.1.5 Todo colaborador, convenio, proveedor, contratista y/o tercero, en caso de pérdida o robo de un dispositivo móvil ya sea personal o activo fijo de la organización con el que acceda a los recursos o servicios Tecnológicos de Confa, debe reportar de inmediato vía correo electrónico al profesional de seguridad de la información, oficial de protección de datos y/o área de Seguridad, con el fin de revocar los accesos o permisos a la red.

14.1.6 Todos los dispositivos móviles asignados a los colaboradores, convenios, proveedores, contratistas y/o terceros de Confa deben tener instalado un software de antivirus.

14.1.7 Las áreas de la organización serán responsables de efectuar y salvaguardar las copias de seguridad de los equipos móviles.

14.1.8 El área de Tecnología protegerá el acceso a los dispositivos móviles como mínimo con una contraseña o con el dibujo de un patrón.

14.1.9 Los colaboradores no deben prestar los usuarios y contraseñas que les han sido otorgados para el cumplimiento de sus funciones, además deben ser responsables de la información que almacenan en su dispositivo móvil y de las acciones que se ejecuten con dichos usuarios y contraseñas.

14.1.10 Está prohibida la instalación de aplicaciones y el cambio o la manipulación de configuraciones en los dispositivos móviles asignados por Confa, salvo expresa autorización del área de Tecnología.

14.1.11 Todos los dispositivos móviles de Confa deben tener la última o la más segura versión de las aplicaciones.

14.1.12 Los dispositivos móviles de Confa serán solo para el uso y almacenamiento de información de tipo laboral.

14.1.13 La información de los dispositivos móviles será de propiedad de Confa, incluso luego de la remoción del acceso personal, la información crítica debe ser respaldada con copias de seguridad periódicamente.

14.1.14 Todos los dispositivos móviles que son propiedad de Confa pueden estar monitoreados y ser sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrán limitar las conexiones hacia ciertos servicios de información que sean considerados maliciosos.

14.1.15 Los colaboradores, convenios, proveedores, contratistas y/o terceros de Confa, deben adoptar las precauciones necesarias y apropiadas para salvaguardar la confidencialidad de la información que tenga en cualquier medio (dispositivos móviles, correo, usb, discos duros, estaciones de trabajo, portátiles, entre otros), así mismo, los responsables de los dispositivos deben dar cumplimiento a lo establecido por la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013 y los lineamientos, políticas organizacionales y normatividad vigente frente a la protección de datos personales.

15. SOPORTE REMOTO DE LOS ACTIVOS DE LA ORGANIZACIÓN

[ISO/IEC 27001:2022 A.5.37]

15.1 Política de soporte remoto de los activos de la organización.

Para el soporte de acceso remoto a los dispositivos de la organización, Confa cuenta con la herramienta “**TeamViewer**” la cual es la única que está autorizada y licenciada por la organización para dicho fin.

15.1.1 El acceso para soporte remoto solo puede ser realizado por el personal autorizado por la Gerencia de Tecnología previa solicitud de servicio. Se considera riesgo a la seguridad de la información y de los recursos de Confa cuando un colaborador incurre en cualquiera de las conductas mencionadas a continuación:

- Facilitar el acceso remoto(credenciales de acceso) a quien no tenga autorización para su uso.
- Utilizar el acceso remoto con el fin de obtener beneficio propio o de terceros.
- Ingresar sin previo aviso y hacer uso del acceso remoto maliciosamente, buscando causar cualquier perjuicio u obtención de información.
- Instalar otro software de acceso remoto sin la debida autorización.
- Intentar sustraer, copiar, modificar o eliminar información en los equipos de cómputo que se acceda remotamente sin la autorización del usuario o personal responsable.
- Capturar sin autorización la información de los accesos de otros usuarios (contraseñas, aplicaciones, carpetas, documentos, entre otros.) .
- El acceso no autorizado a colaboradores, convenios, proveedores, contratistas y/o terceros al área de Mesa de Ayuda donde se brinda el soporte remoto.
- Realizar una conexión remota sin informar previamente al colaborador.
- Incumplir las leyes y normas colombianas.

15.1.2 Los colaboradores que hagan uso del software de acceso remoto, deben conocer y aplicar la política de seguridad de la información de Confa en el desarrollo de actividades de soporte remoto y trabajo autónomo.

15.2 Responsabilidades del auxiliar de mesa de ayuda

- Deben garantizar la adecuada descarga, instalación y funcionamiento del software usado para el soporte remoto.
- Debe mantener la confidencialidad e integridad de la información a la que accede al momento del soporte remoto.

- Debe establecer una comunicación con el colaborador previo al soporte remoto haciendo uso de las herramientas oficiales suministradas por Confa.
- El software usado para soporte remoto solamente podrá ser utilizado con el fin de brindar soporte técnico a los usuarios.
- Utilizar únicamente el software para soporte remoto autorizado por la organización.
- Debe verificar que el colaborador permanezca frente a su equipo, visualizando las acciones de soporte durante todo el tiempo que dure la atención, salvo que el colaborador exprese su autorización para realizar la sesión sin su permanencia frente al equipo, en este caso, aunque no permanezca en frente de este, debe contar con disponibilidad para atender a las indicaciones del Auxiliar de la Mesa de Ayuda. Dicha autorización debe registrarse en el chat corporativo como respaldo ante cualquier eventualidad en ausencia del usuario.
- Deben informar a los colaboradores sobre la herramienta de soporte remoto instalada en las estaciones de trabajo de la organización.
- Deben hacer una revisión y actualización al software de antivirus, dejándolo siempre en su última versión.
- Verificar e informar la finalización de la sesión remota y hacer cambio de contraseña del software usado para el soporte remoto cuando sea requerido, siguiendo el instructivo contraseñas seguras.

15.3 Responsabilidades del usuario colaborador

- Debe suministrar la información necesaria antes y durante el soporte remoto.
- Cada usuario que recibe soporte remoto debe permanecer frente a su equipo, visualizando las acciones de soporte durante todo el tiempo que dure la atención, salvo que el colaborador exprese su autorización para realizar la sesión sin su presencia frente al equipo, en este caso, aunque no permanezca en frente de este, debe contar con disponibilidad para atender a las indicaciones del Auxiliar de la Mesa de Ayuda.
- Es responsabilidad del colaborador garantizar la adecuada conexión a internet para poder acceder remotamente al equipo.

15.4 Responsabilidades del supervisor administrativo/técnico del contrato.

- Recibir la solicitud de soporte remoto por parte del tercero y generar la Orden de Trabajo a Mesa de Ayuda.
- Garantizar el cumplimiento de los Acuerdos de Nivel del Servicio (ANS'S) establecidos para el soporte remoto y facilitar la comunicación entre el convenio, proveedor, contratista o tercero y la Mesa de Ayuda.
- Verificar e informar la finalización de la sesión remota, revocar los permisos de acceso dados al convenio, proveedor, contratista y/o tercero y hacer cambio de contraseña del software usado para el soporte remoto, siguiendo el instructivo contraseñas seguras.

16. BORRADO/FORMATEO SEGURO

[ISO/IEC 27001:2022 A.8.10]

16.1 Activos de información en Confa

- Para garantizar la protección de los datos personales y de cualquier activo de información de Confa, la organización cuenta con una medida de seguridad de borrado seguro que permitirá minimizar el efecto de cualquier tipo de recuperación de información no autorizada sobre los medios de almacenamiento físicos y electrónicos, siempre que el activo de información almacene datos personales e información confidencial que desecha una organización.
- Es responsabilidad de las áreas tener controlados y documentados los dispositivos (USB, CD, DVD, Discos Duros Externos, estaciones de trabajo, móviles entre otros) que contienen datos de los grupos de interés de Confa. Incluidos los discos duros de servidores y almacenamientos centrales, pero también los dispositivos de copias de seguridad.
- El área que requiera elaborar un borrado seguro o destrucción de cualquier dispositivo de almacenamiento, debe solicitar mediante orden de trabajo a Mesa de Ayuda la ejecución de la actividad, indicando el tipo de medio o activo fijo.
- Mesa de ayuda cuando se solicite mediante orden de trabajo, realizará un borrado seguro de cualquier medio de almacenamiento en las estaciones de trabajo que contenga o haya contenido información clave, estratégica o datos

personales, usando una herramienta que permita el borrado seguro en caso de reasignación, reutilización o dado de baja.

- Mesa de ayuda cuando se solicite mediante orden de trabajo, realizará la destrucción de cualquier medio de almacenamiento en las estaciones de trabajo con información clave, estratégica o datos personales, usando una herramienta que permita el borrado seguro en caso de reasignación, reutilización o dado de baja, en compañía del profesional de Seguridad de la Información y Auditoría.
- Mesa de Ayuda cuando haga el traslado de activo fijo o cambio de disco duro o medios de almacenamientos, se debe realizar el formateo estándar de dicho elemento.

16.2 Metodología de entrega del proveedor/contratista/prestador de servicios y/o tercero

- El Contratista, proveedor, prestador de servicio y/o tercero se compromete a entregar a Confa los usuarios, contraseñas, credenciales, llaves, token y toda la información que posea de manera previa, al momento y posterior a la firma del presente documento de acuerdo a las estructuras definidas, los formatos, lineamientos, directrices e indicaciones realizadas por Confa para tales efectos, sin embargo esta entrega se hará de la siguiente manera:
 - a. Una vez terminado el vínculo contrato se debe notificar la fecha de entrega de la información y custodia en un tiempo máximo de 2 meses para la entrega.
 - b. En la entrega de la información, la entidad debe revisar y dar el visto bueno en un tiempo límite de máximo 30 días calendario.
 - c. Una vez la entidad nos da el recibo a satisfacción de la misma se procede a la eliminación total.
 - d. Entrega final por medio de documento formal acta de entrega a satisfacción.

Nota: Las entregas corresponden a: Estructura de tablas principales de documentos generados, Metadatos, archivos electrónicos generados en el sistema en unidades lógicas.

17. Política de Uso de Inteligencia Artificial (IA) en la Organización

[ISO/IEC 27001:2022 A.5.10]

17.1 Propósito

Teniendo en cuenta el contexto de la transformación digital constante y el creciente uso de tecnologías disruptivas como la inteligencia artificial (IA), a nivel nacional e internacional, este documento busca establecer lineamientos, principios y pautas claras para la adquisición, el desarrollo y uso responsable de herramientas de inteligencia artificial en Confa, garantizando el cumplimiento de la legislación aplicable, principios éticos, buenas prácticas corporativas, la protección de la privacidad y las demás normas que forman parte de la estrategia de la Organización. Así mismo se propende el fomento de una cultura organizacional que promueva el uso responsable de la IA, incluyendo programas de capacitación continua y campañas de sensibilización y por otro lado con este documento se fijarán las bases para un equilibrio entre la innovación tecnológica y la responsabilidad ética, asegurando que las mejoras o avances en estas herramientas no comprometan los derechos humanos, regulaciones legales existentes o los valores y principios corporativos que son nuestra razón de ser.

De igual manera, cabe anotar que este documento no solo responde a un mandato legal, sino que se rige como un pilar estratégico para la consecución de los siguientes objetivos: a) Fortalecer la gobernanza corporativa, asegurando que las decisiones basadas en IA estén alineados con la misión, visión, código de ética y buen gobierno, PTEE y demás documentos relacionados. b) Promover y alinear el uso de IA con objetivos organizacionales sostenibles y estándares internacionales (ejemplo: como los lineamientos de la UNESCO en ética de IA). c) Generar y sostener la confianza, así como el buen relacionamiento que caracteriza a Confa con sus grupos de interés, desde colaboradores hasta clientes, garantizando transparencia en procesos automatizados y seguridad en el manejo de su información."

17.2 Ámbito de aplicación

Esta política aplica a todos los colaboradores, contratistas, proveedores y/o terceros que desarrollen y/o usen herramientas de inteligencia artificial para los procesos de la

Organización. Donde se prohíbe introducir datos sensibles o propiedad intelectual de Confa en modelos de IA públicos sin su previa autorización.

La política queda publicada en la intranet o confanet de la organización

18. CUMPLIMIENTO LEGAL

[ISO/IEC 27001:2022 A.5.36]

18.1. Cumplimiento de los requisitos legales y contractuales

18.1.1 En Confa todos sus colaboradores tienen la responsabilidad de conocer y velar por el cumplimiento de las políticas establecidas en este documento, con el objetivo de preservar la integridad, confidencialidad, buena reputación y disponibilidad de la información.

18.1.2 Los colaboradores tienen la responsabilidad de cumplir las normas, regulaciones o leyes colombianas que a derechos de autor se refiere, entendiendo las restricciones de carácter legal en el uso de contenidos como software, aplicaciones, vídeos, fotografías, documentos, presentaciones, audios, entre otros.

18.1.3 Se obliga al cumplimiento de las directrices técnicas sobre seguridad de la información y ciberseguridad emitidas por estos entes de control específicos.

18.2. Protección de los registros

18.2.1 Los registros y/o información de la organización deben estar protegidos contra pérdida, destrucción, falsificación, acceso y divulgación no autorizados, de conformidad con los requisitos legales, reglamentarios, contractuales y comerciales.

18.3. Revisiones de la seguridad de la información

18.3.1 Confa tiene como objetivo garantizar el proceso de implementación de la seguridad de la información alineada a los objetivos estratégicos de la organización.

Se harán revisiones a los aspectos de seguridad de la información de forma periódica o cuando por cambios significativos se hagan necesarios.

Anexos

Disposiciones Legales.

- I. Ley 1273 del 5 de enero 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". Ésta ley, creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.
- II. Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- III. Terminos y condiciones Amazon AWS
- IV. Terminos y condiciones Google Workspace
- V. Hoja de ruta IA para Colombia
- VI. Marco ético para la inteligencia artificial en Colombia
- VII. Ley 23 de 1982 y la Ley 44 de 1993, que regulan la propiedad intelectual en Colombia, asegurando que todo desarrollo realizado por colaboradores o terceros sea propiedad de Confa.
- VIII. Circular 007 de 2018 (SFC) Estándar de gestión de riesgos tecnológicos en el sector.
- IX. ISO/IEC 27001:2022 Aunque se menciona en el documento, debe ratificarse como el marco de control principal.
- X. Circular externa única No 00004-2024 Su objetivo principal es la implementación obligatoria del Sistema de Control Interno del Subsidio Familiar (SCISF).

Juan Eduardo Zuluaga Perna

Juan Eduardo Zuluaga Perna
Director

Inés Adriana Valencia G.

Ines Adriana Valencia Galeano
Secretaria General

Angela Medina Casas

Angela Medina Casas
Auditora

Héctor A. Abadía G.

Héctor Andrés Abadía García
Gerente Productividad y Desarrollo

Carlos A Duque Q

Carlos Andrés Duque Quintero
Gerente de Tecnología

Bastidas Silvera

Bastidas Silvera
Gerencia de Datos

Visto Bueno

Diana Ma Serna Garcia

Diana Maria Serna Garcia

Diana Alexandra Hernández

Diana Alexandra Hernandez Ríos

paolaandrea.cardona

Paola Andrea Cardona Hincapié

Oscar Edo Alzate

Oscar Eduardo Alzate Romero

Víctor

Víctor Alejandro Caicedo Quiceno