RESOLUCIÓN AEI No. 084
(17 de julio de 2024)

"Por medio de la cual se aprueba el Modelo de Seguridad y Privacidad de la Información- MSPI y se dictan otras disposiciones"

EL AGENTE ESPECIAL DE INTERVENCIÓN DE LA CAJA DE COMPENSACIÓN FAMILIAR DEL CAQUETA "COMFACA"

En ejercicio de sus facultades legales y en especial de las que le confiere la Ley 21 de 1982, la Ley 789 de 2002, el Decreto 1072 de 2015 (Único Reglamentario del Sector Trabajo) el Decreto 2150 de 1992, y las Resoluciones 0629 del 19 de septiembre de 2018 y N° 0277 del 31 de marzo de 2023, proferidas por la Superintendencia del Subsidio Familiar y los Estatutos de la Corporación, y

CONSIDERANDO

Que de acuerdo con el artículo 39 de la Ley 21 de 1982, las Cajas de Compensación Familiar son personas jurídicas de derecho privado sin ánimo de lucro, organizadas como corporaciones en la forma prevista en el Código Civil, cumplen funciones de seguridad social y se encuentran sometidas al control y vigilancia del estado en la forma establecida por la Ley.

Que mediante la Resolución No. 629 del 19 de septiembre de 2018, emitida por la Superintendencia del Subsidio Familiar adecuó el proceso de medidas cautelares señaladas en los literales a y d del numeral 23 de artículo 7 del Decreto 2150 de 1992 y el numeral 16 del artículo 5 del Decreto 2595 de 2012.

Que en virtud de la Resolución N° 0277 del 31 de marzo de 2023, emanada de la Superintendencia del Subsidio Familiar, se adopta la medida cautelar de Intervención Administrativa parcial de la Caja de Compensación Familiar del Caquetá "COMFACA", por considerar que el Consejo Directivo de la Caja de Compensación generaba conflicto de gobernabilidad al interior de COMFACA, circunstancia que puede terminar afectando de manera importante y grave a los trabajadores afiliados a la Caja. Esta medida se dictó con fundamento en lo señalado por el inciso final del artículo 17 de la Ley 789 de 2002, que establece en los casos de Caja única departamental, la improcedencia de la liquidación de la Corporación, y en su lugar, la intervención administrativa hasta tanto se logre superar la respectiva causal.

Que mediante Resolución No 0277 del 31 de marzo de 2023, el Superintendente del Subsidio Familiar designó al Dr. IVAN EDUARDO GARCÍA DUQUE, como Agente Especial de intervención, estableciendo en el parágrafo primero del artículo tercero de la referida providencia, que cumplirá las funciones propias del Consejo Directivo establecidas en la Ley y los Estatutos.

Que mediante Resolución No 0277 del 31 de marzo de 2023, el Superintendente del Subsidio Familiar, en el artículo quinto, decidió no separar del cargo al Director Administrativo de la Caja de Compensación Familiar del Caquetá, COMFACA, el Dr. César Augusto Trujillo Barreto.

VIGILADO SuperSubsidio

comfaca.caqueta caquetacomfaca

Sede Administrativa, Cra. 11 No. 10-34 PBX (8) 436 6300
atencionalusuario@comfaca.com
gestiondoc@comfaca.com
notificaciones.judiciales@comfaca.com
Página Web: www.comfaca.com

RESOLUCIÓN AEI No. 084
(17 de julio de 2024)

"Por medio de la cual se aprueba el Modelo de Seguridad y Privacidad de la Información- MSPI y se dictan otras disposiciones"

Que es deber del Consejo Directivo de conformidad con los numerales 6 del artículo 54 de la Ley 21 de 1982, *"6. Visitar y controlar la ejecución de los programas, la presentación de los servicios y el manejo administrativo y financiero de la Caja"*, en concordancia con lo dispuesto en el literal C y demás aplicables del artículo 51 de los Estatutos de la Caja de Compensación Familiar del Caquetá — COMFACA.

Que es función del Director Administrativo en virtud del numeral 2 del artículo 55 de la Ley 21 de 1982, entre otras, la *de: "2. Cumplir y hacer cumplir la ley, los estatutos y reglamentos de la entidad, las directrices del Gobierno Nacional y los ordenamientos de la superintendencia del Subsidio Familiar*", Disposiciones concordantes con los literales B del artículo 55 de los Estatutos Vigentes de la Corporación.

Que el día 16 de julio del año en curso en visita especial del Agente Especial de Intervención de Comfaca en las instalaciones de la Sede Administrativa el equipo administrativo de la Caja de Compensación Familiar "Comfaca" sustentó el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI

Que el Director Administrativo Suplente de COMFACA, a través de oficio de fecha 17 de julio de 2024 presentó a consideración de esta Agencia Especial de Intervención, el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI, de la siguiente forma:

"(…)En cumplimiento del numeral 2 del artículo 55 de la Ley 21 de 1982, entre otras, la de: "2. Cumplir y hacer cumplir la ley, los estatutos y reglamentos de la entidad, las directrices del Gobierno Nacional y los ordenamientos de la superintendencia del Subsidio Familiar", Disposiciones concordantes con los literales B del artículo 55 de los Estatutos Vigentes de la Corporación, me permito presentar para su aprobación el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION -MSPI, de conformidad con las siguientes consideraciones:

La Caja de Compensación Familiar de Caquetá "COMFACA" no es ajena a los diferentes ciberataques que han aumentado en Colombia en los últimos años, de los cuales puede verse afectada en el cumplimiento de sus objetivos estratégicos si es impactada a futuro por estos u otros tipos de ataque informáticos o materialización de riesgos de seguridad y privacidad de la información.

Para mitigar estos riesgos se debe establecer y ejecutar una reglamentación interna de conformidad con la diferente normatividad y requisitos aplicables con respecto a la seguridad de la información, con la finalidad de contribuir al desarrollo transparente de la Corporación y la gestión del riesgo digital, como es el caso de la Ley 1581 de 2012, Ley 1266 de 2008 y Decreto 1074 de 2015, entre otras. El desarrollo e implementación del modelo de seguridad de la información de la Caja de Compensación Familiar del Caquetá está determinado por las

Sede Administrativa, Cra. 11 No. 10-34 PBX (8) 436 6300
atencionalusuario@comfaca.com
gestiondoc@comfaca.com
notificaciones.judiciales@comfaca.com
Página Web: www.comfaca.com
comfaca.caqueta caquetacomfaca

VIGILADO SuperSubsidio

RESOLUCIÓN AEI No. 084
(17 de julio de 2024)

"Por medio de la cual se aprueba el Modelo de Seguridad y Privacidad de la Información- MSPI y se dictan otras disposiciones"

necesidades, los objetivos, los requisitos de seguridad, los procesos misionales, el tamaño y estructura de la Corporación.

El modelo de seguridad de la información de la Caja de Compensación Familiar del Caquetá se encuentra alineado al modelo de arquitectura de control y promueve la preservación de los tres pilares fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad, permitiendo garantizar la privacidad de los datos, mediante la aplicación de una metodología basada en la gestión integral del riesgo.

En ese sentido, La Agencia Especial de Intervención a través de la Resolución AEI No. 033 del 26 de octubre de 2023, aprobó las políticas de seguridad y privacidad de la información para la Caja de Compensación Familiar del Caquetá, las cuales se incorporan al Modelo de Seguridad y Privacidad de la Información "MSPI", este modelo imparte los lineamientos en materia de implementación y adopción de buenas prácticas de seguridad de información tomando como referencias estándares internacionales, para el caso de COMFACA, el Modelo de seguridad y privacidad de la información se ha basado en las directrices de la norma ISO 27001:2022

Este modelo encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital, como objetivos y alcance de la implementación del Modelo de Seguridad y Privacidad de la Información "MSPI", se señalan los siguientes:

OBJETIVOS:
•Promover el uso de buenas prácticas de seguridad con el fin de proteger la información de la Caja de Compensación Familiar del Caquetá.
•Establecer la política general de seguridad de la información de la Caja de Compensación Familiar del Caquetá y las políticas específicas que soporten su cumplimiento mediante la aplicación de controles para gestionar el riesgo de seguridad de la información.
•Brindar los lineamientos y recursos necesarios para que todas las partes interesadas de la Caja de Compensación Familiar del Caquetá estén informadas y cumplan con las políticas de seguridad de la información.
•Contribuir a mejorar todos los procesos de intercambio y transferencia de información de la Caja de Compensación Familiar del Caquetá

ALCANCE
tiene como alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), gestionar los riesgos de seguridad de la información para contribuir al normal desarrollo de las actividades de la corporación, en él se incluyen políticas y controles que están soportados por procedimientos que apoyan los procesos de la organización en materia de seguridad informática.

Que contempla el MSPI

VIGILADO SuperSubsidio

Sede Administrativa, Cra. 11 No. 10-34 PBX (8) 436 6300
atencionalusuario@comfaca.com
gestiondoc@comfaca.com
notificaciones.judiciales@comfaca.com
Página Web: www.comfaca.com

comfaca.caqueta caquetacomfaca

RESOLUCIÓN AEI No. 084
(17 de julio de 2024)

"Por medio de la cual se aprueba el Modelo de Seguridad y Privacidad de la Información- MSPI y se dictan otras disposiciones"

Organización de la seguridad de la información: conformación del comité de seguridad de la información y protección de datos personales, que tiene como objetivo gestionar bajo un enfoque basado en riesgos, la seguridad y privacidad de la información de la organización.

Integrado por:

- *Subdirector Corporativo y Financiero, quien presidirá*
- *Jefe del Departamento de Auditoría Interna.*
- *Jefe del Departamento Tics*
- *Jefe del Departamento Jurídico y de Contratación*
- *Jefe del Departamento de Gestión Humana*
- *Profesional de calidad (Riesgos)*

La gestión de seguridad de la información en la Corporación está basada en la gestión de riesgos y su arquitectura de control para el cumplimiento de los objetivos trazados en el Modelo de Seguridad y Privacidad de la Información, la cual incluye medidas preventivas y reactivas para proteger la información manteniendo su confidencialidad, integridad y disponibilidad, por lo tanto, se han establecido quince (15) políticas:

1. *Política General de Seguridad y Privacidad de la Información*
2. *Política para los Dispositivos Móviles.*
3. *Política de Teletrabajo y Trabajo en Casa.*
4. *Política de Control de Acceso.*
5. *Políticas de Creación y Uso de Contraseñas.*
6. *Políticas de Uso de Controles Criptográficos y Cifrado de la Información*
7. *Política de Escritorio Limpio, Pantalla e Impresoras Limpias.*
8. *Política de Protección Contra Código Malicioso y Antimalware.*
9. *Política de Instalación de Software.*
10. *Política de Copia de Respaldo*
11. *Política de Seguridad para la Transferencia de Información.*
12. *Política de Seguridad de la Información para la Gestión y Relación con Proveedores.*
13. *Política de Desarrollo Seguro.*
14. *Política de Seguridad de la Información en Gestión de Proyectos.*
15. *Política de Seguridad de la Información para la reutilización o eliminación segura de equipos.*

El MSPI también contempla la GESTIÓN DE ACTIVOS DE INFORMACIÓN: se ha determinado un procedimiento formal para la gestión de activos, el cual busca asegurar la gestión eficaz de activos de información (así como aquellos de tipo tecnológico).

Dentro del manejo de activos se tiene dentro del modelo activos de información, y activos relacionados con información (infraestructura), también se adelanta el inventario de activos, su clasificación, medio de custodia, etc.

El MSPI también incluye la gestión de riesgos, se ha realizado el análisis para la corporación basado en la ISO:31000:2018, se elaboró el procedimiento para la gestión de riesgos de

Sede Administrativa, Cra. 11 No. 10-34 PBX (8) 436 6300
atencionalusuario@comfaca.com
gestiondoc@comfaca.com
notificaciones.judiciales@comfaca.com
Página Web: www.comfaca.com
comfaca.caqueta caquetacomfaca

VIGILADO SuperSubsidio

RESOLUCIÓN AEI No. 084
(17 de julio de 2024)

"Por medio de la cual se aprueba el Modelo de Seguridad y Privacidad de la Información- MSPI y se dictan otras disposiciones"

seguridad de la información, se tiene actualizada la matriz de riesgos y oportunidades del Departamento de las Tics.

A través de la Resolución DA-083 del 12 de febrero del 2018 se creó el comité de protección de datos personales, buscando reglamentar en la Corporación el correcto tratamiento de los datos personales de la población afiliada y dar cumplimiento a la Ley 1581 del 2012.

En aras de continuar implementando el cumplimiento de la norma ISO 27001, Ley 1581 del 2012 y Circular Externa No. 2023-00002 en su capítulo VI de seguridad de la información y respectivos anexos expedidos por la Superintendencia del Subsidio Familiar, desde el Departamento de las TICS se ha recomendado adicionar funciones al comité de protección de datos personales existente y crearse en su lugar el "Comité de Seguridad de la Información y Protección de Datos Personales", lo que permitirá una mejor y mayor funcionalidad. (..)

Que, revisados los soportes documentales allegados a este despacho, se concluye la pertinencia y necesidad de aprobar el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI con el fin de implementar lineamientos en materia de implementación y adopción de buenas prácticas de seguridad de información y protección de datos de COMFACA.

En mérito de lo expuesto, el Agente Especial de Intervención Parcial,

RESUELVE:

ARTÍCULO PRIMERO: Aprobar el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI de conformidad con la parte considerativa, el cual hace parte integral de la presente Resolución.

ARTÍCULO SEGUNDO: Crear el Comité de Seguridad de la Información y Protección de Datos Personales, el cual tiene como objetivo gestionar bajo un enfoque basado en riesgos, la seguridad y privacidad de la información de la organización conformado por:

Subdirector Corporativo y Financiero o quien haga sus veces quien lo presidirá,
Jefe del Departamento de Auditoría Interna,
Jefe del Departamento Tics,
Jefe del Departamento Jurídico y de Contratación,
Jefe del Departamento de Gestión Humana y
Profesional de calidad (Riesgos),

VIGILADO SuperSubsidio

comfaca.caqueta caquetacomfaca

Sede Administrativa, Cra. 11 No. 10-34 PBX (8) 436 6300
atencionalusuario@comfaca.com
gestiondoc@comfaca.com
notificaciones.judiciales@comfaca.com
Página Web: www.comfaca.com

RESOLUCIÓN AEI No. 084
(17 de julio de 2024)

"Por medio de la cual se aprueba el Modelo de Seguridad y Privacidad de la Información- MSPI y se dictan otras disposiciones"

Parágrafo: Este Comité deberá ejercer las funciones que se encuentran establecidas en el MSPI y adicionalmente, cumplirá las funciones del Comité de protección de datos personales, que a partir de la fecha se encuentra incorporado al Comité de Seguridad de la Información y Protección de Datos Personales.

ARTÍCULO SEGUNDO: Harán parte integral de esta Resolución, documento denominado "MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI", el cual se recomienda ser incluida en la información documentada del área de las TICS según políticas de gestión de la calidad de la Caja.

ARTICULO TERCERO: Corresponde al Área de las TICS de COMFACA socializar MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI con los trabajadores de la Caja y demás partes interesadas y velar por que su implementación y funcionamiento se realice en debida forma y de acuerdo con lo reglado.

ARTICULO CUARTO: La presente Resolución rige a partir de su expedición y deroga cualquier otra disposición que le sea contraria.

Dado, el día diecisiete (17) de julio de dos mil veinticuatro (2024).

COMUNÍQUESE Y CÚMPLASE

IVÁN EDUARDO GARCÍA DUQUE
Agente Especial de Intervención de COMFACA
Resolución No. 0277 del 31 de marzo de 2023

VIGILADO SuperSubsidio

comfaca.caqueta caquetacomfaca

Sede Administrativa, Cra. 11 No. 10-34 PBX (8) 436 6300
atencionalusuario@comfaca.com
gestiondoc@comfaca.com
notificacionesjudiciales@comfaca.com
Página Web: www.comfaca.com

COMFACA

CAJA DE COMPENSACIÓN FAMILIAR
DEL CAQUETÁ.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI

FLORENCIA
CAQUETÁ | **2024**

TABLA DE CONTENIDO.

1. DEFINICIONES 5
2. INTRODUCCIÓN 11
3. OBJETIVOS 13
   - **3.1. Objetivo General.** 13
   - **3.2. Objetivos Específicos.** 13
4. ALCANCE 14
5. REQUISITOS LEGALES Y/O REGLAMENTARIOS 15
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 18
7. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 24
   - **7.1. Política General de Seguridad y Privacidad de la Información** 24
     - **7.1.1 Objetivo de la política:** 24
     - **7.1.2 Alcance de la política:** 24
     - **7.1.3 Reglamentación:** 25
   - **7.2. Política para los Dispositivos Móviles.** 27
     - **7.2.1 Objetivo de la política:** 27
     - **7.2.2 Alcance de la política:** 27
     - **7.2.3 Lineamientos de la política:** 27
   - **7.3. Política de Teletrabajo y Trabajo en Casa.** 29
     - **7.3.1 Objetivo de la política:** 29
     - **7.3.2 Alcance de la política:** 29
     - **7.3.3 Lineamientos de la política:** 29
   - **7.4. Política de Control de Acceso.** 30
     - **7.4.1 Objetivo de la política:** 30
     - **7.4.2 Alcance de la política:** 31
     - **7.4.3 Lineamientos de la política:** 31
   - **7.5. Políticas de Creación y Uso de Contraseñas.** 33
     - **7.5.1 Objetivo de la política:** 33

7.5.2 Aplicabilidad de la política: 33

7.5.3 Lineamientos de la política: 33

7.6. Políticas de Uso de Controles Criptográficos y Cifrado de la Información. 35

7.6.1 Objetivo de la política: 35

7.6.2 Alcance de la política: 35

7.6.3 Lineamientos de la política: 35

7.7. Política de Escritorio Limpio, Pantalla e Impresoras Limpias. 36

7.7.1 Objetivo de la política: 36

7.7.2 Alcance de la política: 36

7.7.3 Lineamientos de la política: 36

7.8. Política de Protección Contra Código Malicioso y Antimalware. 37

7.8.1 Objetivo de la política: 37

7.8.2 Alcance de la política: 37

7.8.3 Lineamientos de la política: 38

7.9. Política de Instalación de Software. 40

7.9.1 Objetivo de la política: 40

7.9.2 Alcance de la política: 40

7.9.3 Lineamientos de la política: 40

7.10. Política de Copia de Respaldo 41

7.10.1 Objetivo de la política: 41

7.10.2 Alcance de la política: 41

7.10.3 Lineamientos de la política: 41

7.11. Política de Seguridad para la Transferencia de Información. 42

7.11.1 Objetivo de la política: 42

7.11.2 Alcance de la política: 43

7.11.3 Lineamientos de la política: 43

7.12. Política de Seguridad de la Información para la Gestión y Relación con Proveedores. 45

7.12.1 Objetivo de la política: 45

7.12.2 Alcance de la política: 45

7.12.3 Lineamientos de la política: 45

7.13. Política de Desarrollo Seguro. 46

7.13.1 Objetivo de la política: 46

7.13.2 Aplicabilidad de la política: 47

7.13.3 Lineamientos de la política: 47

7.14. Política de Seguridad de la Información en Gestión de Proyectos. 47

7.14.1 Objetivo de la política: 47

7.14.2 Alcance de la política: 48

7.14.3 Lineamientos de la política: 48

7.15. Política de Seguridad de la Información para la reutilización o eliminación segura de equipos. 48

7.15.1 Objetivo de la política: 48

7.15.2 Alcance de la política: 49

7.15.3 Lineamientos de la política: 49

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN 50

8.1. Clasificación de la información. 50

8.2. Manejo de activos: 52

8.2.1 Activos de información. 52

8.2.2 Activos relacionados con información (infraestructura). 56

8.3. Inventario de activos. 57

8.4. Gestión de medios y soportes. 60

8.4.1. Gestión de medios removibles 60

8.5. Gestión y remoción de equipos. 62

9. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 63

9.2. Apetito, tolerancia y capacidad del riesgo 66

10. SEGURIDAD DE RECURSOS HUMANOS 68

11. SEGURIDAD FÍSICA Y AMBIENTAL 69

12. GESTIÓN DE COMUNICACIONES Y OPERACIONES. 72

13. CONTROL DE ACCESO. 74
13.1. Requerimientos en el control de Acceso Físico. 74
13.2. Control de Acceso Lógico. 75
13.3. Seguridad de Oficinas, Recintos e Instalaciones. 75
13.4. Gestión de Acceso al usuario. 76
13.5. Responsabilidad del usuario. 76
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. 77
14.1. Requerimientos de seguridad de los sistemas de información. 77
14.2. Seguridad en los procesos de desarrollo y soportes 78
14.3. Gestión de la Vulnerabilidad técnica. 79
15. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. 79
15.1. Contacto con autoridades y grupos de interés. 81
16. CUMPLIMIENTO. 84
17. BIBLIOGRAFIA. 85
18. IDENTIFICACIÓN Y CONTROL DE CAMBIOS: 85

1. DEFINICIONES

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO 27000, s.f.)
- **Acceso a la Información Pública:** Derecho fundamental que consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a

la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014)

- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo (CONPES 3854, 2016).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO 27000, s.f.)
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo, analiza los peligros que plantean los eventos de causa natural y humana a los activos de una organización. (ISO 27000, s.f.)
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO 27000, s.f.)
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. (Ley 1581 de 2012)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701)

- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Comunicaciones, 2009)
- **Antivirus:** Es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.
- **Apetito al riesgo:** Es utilizado para que la Alta Gerencia, defina qué tipo y cantidad de riesgo está dispuesto a asumir y cual no.
- **Área Segura:** Espacio físico donde se almacena o procesa información crítica de la corporación.
- **Capacidad de riesgo:** Es el máximo riesgo que pueden asumir la empresa en determinada área.
- **Certificado SSL:** Autentica y verifica que los usuarios que envían sean quienes afirman ser, también proporciona confidencialidad para el receptor con los medios para cifrar una respuesta.
- **Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Consecuencia:** Impacto en los objetivos producto del evento.

- **Contexto empresarial:** Las tendencias, eventos, relaciones y otros factores que pueden influir, aclarar o cambiar la estrategia actual y futura de la entidad y los objetivos de negocio.
- **Control:** Medio para gestionar el riesgo, incluye políticas, procedimientos, guías, practicas o estructuras.
- **Control de Acceso:** describe la restricción de los derechos de acceso a las redes, los sistemas, las aplicaciones, las funciones y los datos.
- **Contrafuegos (Firewall):** es un dispositivo de seguridad de red que monitorea el tráfico hacia o desde su red. Permite o bloquea el tráfico según un conjunto definido de reglas de seguridad.
- **Confidencialidad:** Propiedad mediante la cual la información no se hace disponible o revelada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de protección de la exactitud, uniformidad, confiablidad y completitud de la información.
- **Disponibilidad:** Propiedad mediante la cual la información es accesible y utilizable por solicitud de una entidad autorizada.
- **Dato:** Información amplia o concreta que permite una deducción o conocimiento exacto.

- **DoS:** Ataque de Negación de Servicios; es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **DDoS:** Es similar al DoS, pero este se origina desde múltiples y coordinadas fuentes.
- **Entorno Interno:** Cualquier elemento de dentro de la entidad que influya en la capacidad para lograr la estrategia y los objetivos de negocio.
- **Entorno Externo:** Cualquier elemento ajeno a la entidad que influya en la capacidad para lograr la estrategia y los objetivos de negocio.
- **Estrategia:** El plan de la organización para lograr su misión y visión, y aplicar sus valores clave.
- **Información:** Conjunto de datos sobre una materia determinada, además es un activo esencial para los negocios de una organización y por tanto debe ser protegida de forma adecuada.
- **Incidente:** La consecuencia de la materialización de una amenaza, la cual modifica el estado del activo de información.
- **Gestión de Activos:** Es el inventario y el esquema de clasificación para los recursos de información.
- **Malware:** Es un software malicioso que tiene como objetivo infiltrarse o dañar una computadora o sistema de información

- **Mapa de riesgos:** Es una herramienta que permite organizar la información sobre los riesgos de las empresas y visualizar su magnitud, con el fin de establecer las estrategias adecuadas para su manejo. Los mapas de riesgos pueden representarse con gráficos o datos.
- **Matriz de riesgos:** Es una herramienta de análisis de riesgos que sirve para evaluar la probabilidad y la gravedad del riesgo durante el proceso de planificación del proyecto
- **Plan de acción:** Sirve para organizar un proyecto por actividades y fases con los tiempos y responsables; estas se describen en un documento que servirá como guía para lograr los objetivos definidos.
- **Política de seguridad:** Documento que aborda las restricciones y los comportamientos de los miembros de una organización y específica a menudo como se puede acceder a los datos y la forma de acceso.
- **Riesgo:** Posibilidad (probabilidad) que suceda algún evento que impacte (consecuencia) sobre los objetivos de negocio (AS/NZS 4360) y se expresa como la combinación de probabilidad e impacto (ISO 31000).
- **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

- **Tolerancia al riesgo:** Es el rango aceptable de variación que puede haber en torno al apetito, es decir, es el rango donde se puede mover la compañía estando en un margen aceptable si bien no optimo, porque hay tres tipos de apetito, el apetito óptimo, el apetito tolerable y el apetito actual.
- **Virus:** Es un software malicioso que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario.
- **Vulnerabilidad:** Deficiencia, debilidad del activo, sistema de información, aplicación, software y hardware que puede ser explotada para causar daño o mal funcionamiento de este.
- **VPN:** Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

2. INTRODUCCIÓN

El modelo de seguridad y privacidad de la información para La Caja de Compensación Familiar del Caquetá, se elaboró con base en las mejores prácticas definidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma técnica ISO/IEC 27001:2022, los cuales, especifican los requisitos para establecer, implementar,

mantener y mejorar de forma continua el sistema de gestión de seguridad de la información dentro del contexto de la organización.

La Caja de Compensación Familiar del Caquetá es una entidad autónoma que proporciona servicios integrales y competitivos para contribuir al mejoramiento de la calidad de vida de los afiliados y la comunidad, con responsabilidad social. COMFACA tiene un compromiso con el cumplimento de las leyes, normas y requisitos aplicables con respecto a la seguridad de la información, con la finalidad de contribuir al desarrollo transparente de la corporación y la gestión del riesgo digital.

El desarrollo e implementación del modelo de seguridad de la información de la Caja de Compensación Familiar del Caquetá está determinado por las necesidades, los objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Corporación.

El modelo de seguridad de la información de la Caja de Compensación Familiar del Caquetá se encuentra alineado al modelo de arquitectura de control y promueve la preservación de los tres pilares fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad, permitiendo garantizar la privacidad de los datos, mediante la aplicación de una metodología basada en la gestión integral del riesgo.

Este modelo se deberá actualizar periódicamente para cumplir con los cambios en el contexto, normas y requisitos legales aplicables con respecto a la seguridad de la información.

Finalmente, el modelo de seguridad de la información de la Caja de Compensación Familiar del Caquetá, pretende dar un enfoque de compromiso hacia la seguridad de la información desde el alto nivel de la corporación pasando por todos los procesos de la organización con el fin de que cada funcionario tenga claridad de los objetivos que se deben cumplir.

3. OBJETIVOS

3.1. Objetivo General.

Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Caja de Compensación Familiar del Caquetá – COMFACA para soportar los procesos en los cuales se cree, transfiera, almacene y procese información, de esta manera, garantizar su confidencialidad, integridad y disponibilidad.

3.2. Objetivos Específicos.

- Promover el uso de buenas prácticas de seguridad con el fin de proteger la información de la Caja de Compensación Familiar del Caquetá.

- Establecer la política general de seguridad de la información de la Caja de Compensación Familiar del Caquetá y las políticas específicas que soporten su cumplimiento mediante la aplicación de controles para gestionar el riesgo de seguridad de la información.
- Brindar los lineamientos y recursos necesarios para que todas las partes interesadas de la Caja de Compensación Familiar del Caquetá estén informadas y cumplan con las políticas de seguridad de la información.
- Contribuir a mejorar todos los procesos de intercambio y transferencia de información de la Caja de Compensación Familiar del Caquetá.

4. ALCANCE

La Caja de Compensación Familiar del Caquetá tiene como alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), gestionar los riesgos de seguridad de la información para contribuir al normal desarrollo de las actividades de la corporación, en él se incluyen políticas y controles que están soportados por procedimientos que apoyan los procesos de la organización en materia de seguridad informática.

El presente modelo es adoptado y sus políticas aplican para todos los funcionarios en todos los niveles de la Caja de Compensación Familiar del Caquetá, que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación.

Todos los funcionarios, afiliados, clientes, proveedores, contratistas y visitantes deben acoger y cumplir lo dispuesto en el presente modelo, así mismo, cumplir con las políticas generadas desde el Comité de Seguridad de la Información y Protección de Datos Personales de la Caja de Compensación Familiar del Caquetá – COMFACA que soportan el modelo de seguridad y privacidad de la información.

5. REQUISITOS LEGALES Y/O REGLAMENTARIOS

- **Constitución Política de Colombia. Artículo 15**. Reconoce como derecho Fundamental el Habeas Data; **Artículo 20**. Libertad de Información.
- **Ley 527 de 1999.** "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- **Ley 1266 de 2008.** "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".
- **Ley 1273 de 2009.** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- **Ley 1341 de 2009.** "Tecnologías de la Información y aplicación de seguridad".
- **Ley 1437 de 2011.** "Procedimiento Administrativo y aplicación de criterios de seguridad".
- **Ley 1581 de 2012**. "Por la cual se dictan disposiciones generales para la Protección de Datos Personales".
- **Ley 1712 de 2014.** "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- **Decreto 2952 de 2010.** "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- **Decreto 1377 de 2013.** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
- **Decreto 886 de 2014.** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **Decreto 1083 de 2015.** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **Decreto 415 de 2016.** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

- **Resolución 76434 de 2012. "**Por la cual se deroga el contenido del título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reporte de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado título".
- **Circular 02 de 1997.** Parámetros a tener en cuenta para la implementación de nuevas tecnologías en los archivos públicos.

Políticas Públicas:

- **CONPES 3701 de 2011** Lineamientos de Política para ciberseguridad y ciberdefensa.
- **CONPES 3854 de 2016** Política Nacional de Seguridad digital, CONPES 3866 de 2016 Política Nacional de desarrollo Productivo.
- **CONPES 4069 de 2021** Política Nacional de Ciencia, Tecnología E Innovación 2022-2031.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La Caja de Compensación Familiar del Caquetá demostrando liderazgo y compromiso con la seguridad de la información, ha organizado un Comité de Seguridad de la Información y Protección de Datos Personales, el cual, tiene como objetivo gestionar bajo un enfoque basado en riesgos la seguridad y privacidad de la información de la organización.

El Comité de Seguridad de la Información y Protección de Datos Personales de la Caja de Compensación Familiar del Caquetá está integrado por los siguientes directivos:

- Subdirector Corporativo y Financiero
- Auditoría Interna.
- Jefe del departamento TIC's
- Jefe del departamento Jurídico
- Jefe de Gestión Humana
- Profesional de calidad (Riesgos)

Las funciones y responsabilidades del Comité de Seguridad de la Información y Protección de Datos Personales de la Caja de Compensación Familiar del Caquetá son:

- Constituir el gobierno del Programa Integral de Protección de Datos Personales.
- Monitorear el programa integral de protección de datos personales.

- Gestionar los cambios y actualizaciones de acuerdo con la normatividad vigente relacionada con la protección y el tratamiento de los datos personales.
- Gestionar el principio de responsabilidad demostrada (accountability).
- Definir los recursos necesarios para la implementación de los controles del Programa Integral de Protección de Datos Personales.
- Analizar las responsabilidades de cada cargo o área en función de la protección de datos personales.
- Definir el programa de entrenamiento en protección de datos personales específico y general.
- Integrar las políticas de Protección de Datos Personales dentro de las actividades de las demás áreas de la organización.
- Servir de enlace y coordinar con las demás áreas de la organización para garantizar una implementación transversal del Programa Integral de Protección de Datos Personales.
- Desarrollar de análisis de riesgos asociados al tratamiento de datos personales.
- Gestionar los incidentes o eventos que puedan presentarse en la organización y que involucren datos personales.
- Atender dentro de los tiempos establecidos todas aquellas consultas o reclamos

relacionados con el tratamiento de la información personal.

- Asegurar el cumplimiento de las políticas internas de protección de datos personales por parte del recurso humano interno y externo.
- Velar por una constante, adecuada y oportuna disposición de los avisos de privacidad y autorización de acuerdo con lo requerido por Ley.
- Asegurar la inclusión de cláusulas de confidencialidad y protección de datos en los contratos celebrados por el responsable, así como el uso o aplicación de contratos de transmisión y transferencia de datos cuando sea necesario.
- Impulsar la cultura de Protección de Datos Personales dentro de la organización.
- Realizar entrenamientos generales y capacitaciones relacionados con la privacidad y la protección de los datos personales.
- Mantener el inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
- Registrar las bases de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte de acuerdo con las instrucciones impartidas por la Superintendencia de Industria y Comercio (SIC).
- Asesorar a las áreas internas en temas relacionados con el cumplimiento de la Ley 1581 del 2012 de Protección de datos Personales y las políticas internas.
- Definir y promover la dirección estratégica para la seguridad de la información.

- Velar y apoyar la implementación del Sistema de Seguridad de la Información.
- Autorizar, facilitar e integrar la puesta en operación del Sistema de Seguridad de la Información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.
- Velar por el cumplimiento de las obligaciones regulatorias en materia de Seguridad de la Información.
- Velar por la disponibilidad de los recursos y su uso apropiado para que la corporación cumpla con el Modelo de Seguridad y Privacidad de la Información.
- Designar los responsables de la implementación del Sistema de Seguridad de la Información.
- Pronunciarse y hacer seguimiento a los informes que se presenten dejando constancia en las actas de las reuniones respectivas.
- Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.
- Revisar que la estrategia de Seguridad de la Información se encuentre alineada con los objetivos de negocio de la corporación.
- Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.
- Establecer las prioridades de los proyectos e iniciativas relacionadas con la Seguridad de la Información.
- Revisar y evaluar los incidentes de seguridad de la información y monitorear el proceso de respuesta.

- Aprobar la implementación de las nuevas iniciativas para la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Promover la concientización y formación de los empleados en materia de Seguridad de la Información.

Con el fin de ejercer el liderazgo necesario para el éxito del Modelo de Seguridad y Privacidad de la Información el presidente del comité tiene las siguientes funciones:

- Velar por el desarrollo de los objetivos estratégicos para la seguridad de la información, definidos al interior de la corporación.
- Velar por la implementación de la política de seguridad de la información.
- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Velar por la designación de los responsables de la implementación de la política de seguridad de la información.
- Citar por intermedio de la secretaria técnica a los integrantes del comité, a las sesiones ordinarias que se llevarán a cabo cada 3 meses y a las sesiones extraordinarias cuando la corporación lo demande.

De igual manera el secretario técnico del comité tendrá las siguientes responsabilidades:

- Elaborar un informe periódico, como mínimo trimestral, al presidente del Comité de Seguridad de la Información y Protección de Datos Personales para notificar aspectos relevantes de la seguridad de la información incluyendo las acciones preventivas y correctivas implementadas o por implementar, el seguimiento y resultados del cumplimiento de objetivos de seguridad de la información.
- Convocar a los integrantes del Comité de Seguridad de la Información a las sesiones ordinarias y extraordinarias según lo determinado por el presidente del comité.
- Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información.
- Elaborar las actas de reunión del Comité oportunamente.
- Llevar y custodiar el archivo de las actas y demás documentos soporte del Comité.
- Verificar el quórum al inicio de las sesiones.
- Recibir y preparar la respuesta a los documentos que sean de competencia del Comité.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité de Seguridad de la Información y Protección de Datos Personales.
- Las demás que le sean asignadas por el Comité y su presidente.

Fecha: 01 – diciembre – 2023	Fecha: 15 – diciembre – 2023	Fecha: 18 – diciembre - 2023

7. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Las Políticas de Seguridad de la Información, General y Específicas, fueron aprobadas Mediante la resolución AEI 033 de 2023 del 26 de octubre de 2023 por el agente especial de intervención de la Caja de Compensación Familiar del Caquetá COMFACA.

La gestión de seguridad de la información en la corporación está basada en la gestión de riesgos y su arquitectura de control para el cumplimiento de los objetivos trazados en el Modelo de Seguridad y Privacidad de la Información, la cual incluye medidas preventivas y reactivas para proteger la información manteniendo su confidencialidad, integridad y disponibilidad.

7.1. Política General de Seguridad y Privacidad de la Información

7.1.1 Objetivo de la política:

Establecer los lineamientos generales sobre la gestión integral de la seguridad y privacidad de información como directriz del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Caja de Compensación Familiar del Caquetá – COMFACA.

7.1.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá, que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la Corporación.

7.1.3 Reglamentación:

La Caja de Compensación Familiar del Caquetá COMFACA como entidad autónoma que proporciona servicios integrales y competitivos con el fin de contribuir al mejoramiento de la calidad de vida de los afiliados y la comunidad, y entendiendo la importancia que tiene una adecuada gestión de la información, tiene un compromiso decidido hacia la seguridad y la protección de la información propia y de terceros, incluyendo la información de carácter personal, deber que incluye a todas las partes interesadas internas y externas que pueda tener acceso a dicha información.

Es importante definir los principios de la protección y privacidad de la información:

- **Principio de confidencialidad de la información:** consiste en que todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan carácter público, están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar el suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas (Comercio, s.f.).

- **Principio de integridad de la información:** hace referencia a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación no ha sido manipulada por terceros de manera

malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.

- **Principio de disponibilidad de la información:** se refiere a que la información debe estar disponible siempre para que las personas autorizadas paran accederla y tratarla, y además se pueda recuperar en caso de que ocurra un incidente de seguridad que cause su pérdida o eliminación. Es decir; permite que la información esté disponible cuando sea necesario.

El compromiso de la entidad se encamina a la gestión del cumplimiento y va de conformidad con los requisitos aplicables a nuestra Corporación, tanto del ordenamiento jurídico pertinente, como contractual y técnico, haciendo especial énfasis en los aspectos de privacidad, transparencia y nivel de servicio, así como de la protección adecuada de información de carácter reservado.

Para asegurar la continua pertinencia de la gestión integral de la seguridad de la información frente a posibles cambios en el contexto, especialmente en partes interesadas, requisitos aplicables, y la dinámica del mercado, la Caja de Compensación Familiar del Caquetá COMFACA se compromete a mantener y mejorar de forma continua el MSPI y los riesgos asociados por medio del aprovechamiento de la tecnología, innovación y gestión del conocimiento con el fin de mantener el ciclo de mejora continua

y la correcta y oportuna gestión de los riesgos de tecnología y seguridad de la información.

A continuación, se describen las políticas específicas necesarias para garantizar la privacidad y seguridad de la información dentro de la empresa.

7.2. Política para los Dispositivos Móviles.

7.2.1 Objetivo de la política:

Establecer lineamientos para proteger la información corporativa transmitida, procesada y almacenada en los dispositivos móviles.

7.2.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación y terceros contratistas con asistencia permanente que desarrollen cualquier tipo actividad dentro de las instalaciones de la corporación.

7.2.3 Lineamientos de la política:

- Para la trasmisión, procesamiento, almacenamiento y consulta de cualquier tipo de información de la corporación no está autorizado el uso de dispositivos móviles tales como: Discos duros externos, dispositivos USB, celulares, entre otros.

- La trasmisión, procesamiento, almacenamiento y consulta de cualquier tipo de información de la corporación por medio de computadores portátiles debe hacerse desde las instalaciones de la corporación, en caso de hacerse fuera de las instalaciones se debe hacer a través de canales y protocolos seguros de comunicaciones tales cómo redes VPN.

- La información corporativa almacenada y procesada en los dispositivos móviles autorizados es propiedad de la Caja de Compensación Familiar del Caquetá, por lo cual la corporación tiene la potestad de restringir el acceso, modificar, copiar y eliminar la información según el caso sin dar previo aviso al usuario custodio del equipo móvil o portátil.
- La Caja de Compensación Familiar del Caquetá debe disponer de una póliza que asegure los equipos portátiles de su propiedad cuando estos son retirados de las instalaciones de la corporación por sus funcionarios para cumplir funciones propias de su trabajo y/o teletrabajo.
- La transmisión y consulta de cualquier tipo de información de la Caja de Compensación por medio de dispositivos móviles fuera de las instalaciones de la corporación, se deben hacer solo si se está conectado a una red segura, no está autorizado conectarse a redes wifi-públicas, por ejemplo; redes wifi de aeropuertos, hoteles, restaurantes, bares y otros establecimientos que tengan redes wifi abiertas.

- Los dispositivos móviles como celulares o tabletas propiedad de la Caja de Compensación Familiar del Caquetá deben tener configurada la contraseña de acceso.

7.3. Política de Teletrabajo y Trabajo en Casa.

7.3.1 Objetivo de la política:

Establecer lineamientos sobre el acceso y procesamiento de la información de la corporación o entregada a ésta para sus actividades misionales, desde la óptica del teletrabajo y trabajo en casa, es decir, cuando las actividades se realizan fuera de las instalaciones de la corporación.

7.3.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la Caja de Compensación y para terceros que desarrollen actividades relacionadas con trabajo en casa o teletrabajo.

7.3.3 Lineamientos de la política:

- En principio la ejecución de teletrabajo y/o el trabajo no está autorizado en la corporación, sin embargo, el teletrabajo en casa será autorizado ante la materialización de cualquier riesgo que afecte la salud física y/o mental de los funcionarios, en caso pandemia, evento que afecte la salud pública, disturbios y/o

manifestaciones que afecten el orden público, desastres naturales tales como terremotos, inundaciones, incendios y otros que a criterio de la gerencia de la corporación ameriten que se realicen las actividades laborales desde casa.

- Para que un funcionario ejecute labores de trabajo en casa deberá existir una comunicación formal emitida desde el área de talento humano, enviada vía correo electrónico y por medio de un formato de memorando en donde se estipula el periodo que se autoriza a realizar trabajo en casa; teniendo en cuenta que el periodo máximo de teletrabajo es un mes.
- Los funcionarios que tengan que realizar actividades que impliquen teletrabajo y/o trabajo en casa deberán hacerlo utilizando protocolos seguros de conexión tales como redes VPN (SSL, IPSec), para establecer las conexiones y acceder a la información corporativa de la Caja de Compensación Familiar del Caquetá.
- Está prohibido el uso de herramientas de escritorio remoto diferentes a la propia del sistema operativo, para acceder al computador de trabajo asignado y conectado dentro de la red interna corporativa de la corporación.

7.4. Política de Control de Acceso.

7.4.1 Objetivo de la política:

Establecer lineamientos generales e integrales para el control de acceso como elemento central de la seguridad de la información.

7.4.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá y para terceros contratistas que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación.

7.4.3 Lineamientos de la política:

- La asignación de derechos de acceso operará exclusivamente sobre una base contractual, de forma que será requisito la existencia de una relación contractual vigente entre las partes que determine específicamente que tipo de información va a estar en el dominio de quien suscribe el acuerdo, que acciones realizará sobre esa información y las razones de esta.
- El administrador de los sistemas de información de la Caja de Compensación Familiar del Caquetá de acuerdo a la matriz de roles y perfiles establecida asignará los permisos para el acceso a los usuarios y contratistas.
- El acceso lógico a la red corporativa y a los sistemas de información de la Caja de Compensación Familiar del Caquetá se hará mediante autenticación de usuario y contraseña.
- El usuario y la contraseña de cada funcionario es personal e intransferible, no está autorizado a ningún funcionario a prestar, difundir o entregar dicha información de acceso.

- En el caso de medios externos y considerando su movilidad, el acceso incluirá responsabilidades sobre la posible pérdida y robo del medio externo.
- En el caso de archivo físico, el acceso será dado en las instalaciones donde resida dicho archivo, y no estará permitida la extracción parcial o total.
- Sin importar los posibles derechos de acceso aplicables, está prohibida la copia, parcial o total, de datos, documentos y demás relacionados.
- Cuando los datos sobre los cuales se esté brindando acceso sean de carácter personal, se deberá adicionalmente suscribir la autorización expresa del titular del caso, un acuerdo de transferencia y responsabilidad sobre los datos personales entre el responsable de la información y el encargado de tratamiento de datos personales.
- El ajuste y remoción de derechos de acceso será realizado inmediatamente finalice la relación contractual, entre el funcionario y la corporación y si es necesaria una etapa de transferencia, tales derechos de acceso estarán a cargo de quien recibe la información.

- El líder del departamento de gestión humana o el departamento administrativo a cargo deberá notificar al departamento de TIC'S las novedades de ingreso o retiro del personal, funcionarios y terceros contratistas, con el fin de garantizar o remover los accesos a los sistemas de información y a la red corporativa de dichos

usuarios, llevando a cabo el formato de paz y salvo con el jefe de área y de este modo proteger la confidencialidad e integridad de la información.

- Ante cambios en el contexto (requisitos y contratos) se realizarán las actividades de revisión de derechos de acceso, de ser necesario aplicar algún tipo de ajuste, éstos serán realizados de forma inmediata.

7.5. Políticas de Creación y Uso de Contraseñas.

7.5.1 Objetivo de la política:

Establecer los parámetros para la creación y administración de las contraseñas de los sistemas de información y de acceso a la red de la corporación.

7.5.2 Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación y para terceros que tengan asignadas credenciales de acceso a los sistemas de información de COMFACA.

7.5.3 Lineamientos de la política:

- Las contraseñas son personales e intransferibles, ningún funcionario o contratista debe prestar ni compartir las credenciales de acceso a ninguno de los sistemas de información.

- Las contraseñas de los sistemas de información, plataformas de colaboración en la nube, servicios de red y usuarios de las estaciones de trabajo deben cumplir con los siguientes requerimientos:
    - Tener como mínimo 8 caracteres.
    - Mínimo una letra mayúscula.
    - Mínimo un número.
    - Mínimo un carácter especial.
- Los usuarios pueden cambiar en cualquier momento su contraseña, cumpliendo con los parámetros establecidos.
- Las cuentas consideradas cómo críticas deberán tener habilitado el múltiple factor de autenticación – MFA, siempre y cuando esté disponible en el sistema de información o servicio.
- Los administradores de la Infraestructura de TI, administradores de bases de datos, administradores de sistemas de información y quienes asignan recursos informáticos, deberán utilizar herramientas de gestión de contraseñas cifrados y/o protegidos por contraseña.

7.6. Políticas de Uso de Controles Criptográficos y Cifrado de la Información.

7.6.1 Objetivo de la política:

Establecer lineamientos en cuanto al uso de controles de cifrado (o criptográficos) y la gestión asociada de llaves, en cualquier escenario de transferencia o almacenamiento de información.

7.6.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación.

7.6.3 Lineamientos de la política:

- Los portales web https://www.comfaca.com/ y sus sitios web asociados, deben contar con certificados SSL para garantizar la autenticidad del sitio y la seguridad en la transferencia de los datos.
- Para el caso del acceso por parte de los administradores de la Infraestructura de TI, sistemas de comunicaciones y administradores de base de datos que realicen actividades de teletrabajo, el acceso se realiza a través de VPN utilizando protocolos seguros (SSL, IPSec) para establecer la conexión.
- Los equipos de cómputo de usuario final que procesen y almacenen información crítica para la corporación deberán estar cifrados para evitar la pérdida de la

confidencialidad de la información en caso de pérdida o robo del activo de información.

7.7. Política de Escritorio Limpio, Pantalla e Impresoras Limpias.

7.7.1 Objetivo de la política:

Establecer lineamientos para gestionar la seguridad de la información desde la óptica del acceso irrestricto a información en escritorios y pantallas de equipos de cómputo.

7.7.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación y para terceros con asistencia permanente que desarrollen cualquier tipo actividad en las instalaciones de la corporación.

7.7.3 Lineamientos de la política:

- En los equipos de cómputo, se debe mantener únicamente el ícono de papelera de reciclaje, el de sistema (cuando éste sea el caso) y las aplicaciones que por funcionalidad o configuración determinada deban estar allí ubicados.
- Sobre los archivos físicos, solo se pueden mantener ejemplares en el escritorio mientras son procesados y deben ser archivados donde corresponde cuando

finalice su procesamiento o sea necesario que la persona a cargo se retire de su sitio de trabajo, así sea solo momentáneamente.

- No está permitido dejar archivos impresos en las bandejas de las impresoras, todo archivo impreso debe ser gestionado o almacenado inmediatamente.
- Para los archivos digitales y físicos, se deberán aplicar los principios archivísticos de procedencia y de orden original para asegurar una adecuada organización de los datos.
- Se debe asegurar el bloqueo de sesión del equipo cada vez que se retire del puesto de trabajo, con el fin de que las pantallas de los equipos de cómputo queden protegidas contra el acceso no autorizado.

7.8. Política de Protección Contra Código Malicioso y Antimalware.

7.8.1 Objetivo de la política:

Establecer lineamientos para proteger la información ante posibles infecciones de los sistemas informáticos con código malicioso y establecer los controles antimalware en la corporación.

7.8.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación y para contratistas

con asistencia permanente que desarrollen cualquier tipo actividad en equipos de cómputo y sistemas informáticos de la corporación.

7.8.3 Lineamientos de la política:

- La Caja de Compensación Familiar del Caquetá administra el antivirus con funciones de antimalware, anti spam, antispyware, entre otras, como herramienta para reducir el riesgo de infección de software malicioso, y la copia de seguridad "Backup" respalda la información gestionada y almacenada en la infraestructura tecnológica de la corporación.
- El departamento de Tecnologías de la Información y las Comunicaciones debe programar y automatizar escaneos periódicos a los equipos de cómputo y servidores de la Caja de Compensación Familiar del Caquetá por medio del software de antivirus con el fin de detectar las amenazas que pueden comprometer la información de la corporación.
- El departamento de Tecnologías de la Información y las Comunicaciones valida que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- Los usuarios no pueden realizar cambios en la configuración del software de antivirus, antispyware, anti spam, antimalware.

- El departamento de Tecnologías de la Información y las Comunicaciones debe certificar que el software de antivirus, antispyware, anti spam, antimalware, posea las últimas actualizaciones y parches de seguridad, con el fin de proteger la información almacenada y procesada en los sistemas informáticos.
- Es deber de los usuarios de la Caja de Compensación Familiar del Caquetá ejecutar el software de antivirus, antispyware, anti spam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Es deber de los usuarios de la Caja de Compensación Familiar del Caquetá asegurarse que los archivos adjuntos de correos electrónicos descargados de internet o copiados de medios de almacenamiento, vienen de fuentes conocidas y seguras para evitar virus informáticos y/o software malicioso en recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al personal del departamento de TIC's quien es el encargado de esta revisión, para que se tomen las medidas de control correspondientes.

7.9. Política de Instalación de Software.

7.9.1 Objetivo de la política:

Establecer lineamientos para la gestión segura de software a partir del control de su instalación.

7.9.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación y para terceros con asistencia permanente que desarrollen cualquier tipo actividad en las instalaciones de la corporación.

7.9.3 Lineamientos de la política:

- Toda instalación de software, incluidas actualizaciones, será realizada por personal de soporte de sistemas y TI.
- Antes de realizar cualquier instalación, se evaluará la necesidad del requerimiento y en caso de afectar un proceso crítico de negocio se deberán realizar pruebas para determinar la compatibilidad y el nuevo nivel de riesgo asociado al nuevo software.
- Todo equipo de cómputo propiedad de la corporación o alquilado, deberá tener deshabilitada la opción de instalación de software.

- Toda instalación o actualización de software se debe hacer con permisos de administrador previo entendimiento de los acuerdos de licencia de usuario final (EULA).
- Cada computador tendrá usuario de administrador y solo este contará con permisos para instalación de software.
- El personal de contratistas debe hacer uso de software legal para procesar, transferir y almacenar información de la Caja de Compensación Familiar del Caquetá, no está permitido el uso de software ilegal dentro de la red corporativa de COMFACA.

7.10. Política de Copia de Respaldo

7.10.1 Objetivo de la política:

Establecer lineamientos para asegurar la disponibilidad de la información ante situaciones de afectación de la información crítica de la corporación.

7.10.2 Alcance de la política:

La presente política aplica para todas las partes interesadas (funcionarios y contratistas), en todos los niveles de la Caja de Compensación Familiar del Caquetá.

7.10.3 Lineamientos de la política:

- Es responsabilidad de cada funcionario de la Caja de Compensación Familiar del Caquetá salvaguardar la información corporativa que está bajo su custodia, para

ello dicha información deberá ser almacenada y compartida en las herramientas que la corporación ha dispuesto para ello como el correo electrónico corporativo, Google Workspace y Kaspersky para las cuentas criticas ruta C:\Documentos y escritorio.

- El período mínimo para la ejecución de copias de seguridad estará alineado al procedimiento de copias de seguridad.
- Para el caso de las copias de seguridad de los servidores se programan copias incrementales diarias, copias completas semanales. Se pueden mezclar estrategias de copia incremental (agregando los archivos nuevos o mejorados) o total (copiando totalmente la información objetivo).
- Las copias completas de los servidores se almacenan semanalmente en dos medios diferentes y uno de ellos se almacena en un lugar externo a las instalaciones de procesamiento de la Caja de Compensación Familiar del Caquetá. Igualmente, se realizan copias diarias en la nube.

7.11. Política de Seguridad para la Transferencia de Información.

7.11.1 Objetivo de la política:

Establecer lineamientos para asegurar la transferencia de información en los diversos escenarios pertinentes dentro y fuera de la corporación.

7.11.2 Alcance de la política:

La presente política aplica para todas las partes interesadas (funcionarios y contratistas), en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación.

7.11.3 Lineamientos de la política:

- Se deben establecer acuerdos de transferencia de información entre la corporación y partes externas las cuales deben estar soportadas como mínimo por cláusula de confidencialidad, no divulgación y responsabilidad en el tratamiento de datos personales.
- Se deben revisar regularmente y documentar, los requisitos para los acuerdos de confidencialidad y no divulgación de la información para la trasferencia de información entre la Caja de Compensación Familiar del Caquetá y partes externas, de acuerdo al contexto y dando cumplimiento a la normatividad vigente aplicable.
- La transferencia de información de carácter reservado y confidencial debe estar acompañada por el aviso de privacidad, confidencialidad y tratamiento de datos personales.
- No está permitido que ningún funcionario o contratista de la Caja de Compensación Familiar del Caquetá circule con información de propiedad de la

corporación en medios de almacenamiento externos (memorias USB, CD, DVD, discos duros externos, etc.).

- El transporte de la información física y de medios magnéticos la debe hacer una organización especializada en la custodia, transporte y guarda de documentos, para asegurar su confidencialidad e integridad.
- La transferencia de información digital entre funcionarios, contratistas y en general con los terceros se debe hacer solo por los medios ofrecidos por la Caja de Compensación Familiar del Caquetá para tal fin, tales como Google Workspace.
- No está permitida la transferencia de información por medio de software o herramientas de chat no Corporativos.
- Toda transferencia de información (interna o externa, desde o hacia la corporación) debe estar identificada contemplando como mínimo conjunto de datos, remitente, destinatario, medio de transferencia y justificación de la misma. Para el caso de transferencias sucesivas, este elemento solo será identificado una única vez a menos que cambie el conjunto de datos.
- Para mantener la integridad de la información la transferencia de datos entre sistemas de información propios y de terceros se debe hacer mediante protocolos seguros, por ejemplo (Web Service).
- Toda transferencia de información debe generar su respectivo registro para asegurar trazabilidad.

- No está permitida la transferencia de información reservada, confidencial o de carácter privado fuera del territorio colombiano, lo cual incluye el uso de herramientas de uso libre para compartir información, ejemplo (we transfer).
- Todos los equipos de cómputo de escritorio deberán tener deshabilitados los puertos USB, y la unidad óptica solo cumplirá la función de lectura.

7.12. Política de Seguridad de la Información para la Gestión y Relación con Proveedores.

7.12.1 Objetivo de la política:

Establecer lineamientos para que los proveedores de la corporación tengan un rol activo en la seguridad de la información.

7.12.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso o manipulen cualquier tipo de información de la corporación.

7.12.3 Lineamientos de la política:

- Todo proveedor crítico, es decir, que tenga a su cargo la delegación de uno o más procesos de la corporación o la gestión de información (incluida la captura, recepción, procesamiento, digitación y digitalización, almacenamiento,

reproducción y/o conservación y/o eliminación) deberá contar con políticas de Seguridad y Privacidad de la Información implementadas.

- Todo acuerdo, contrato o similar, propuesta comercial, deberá incorporar requisitos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.
- Todo acuerdo, contrato o similar, deberá incorporar requisitos de control y audibilidad, según el riesgo, para poder conocer la aplicación de los lineamientos y controles de seguridad de la información.
- Se realizarán auditorías de segunda parte a proveedores críticos lo cual plantea la necesidad de identificar y calificar la criticidad de los proveedores considerando el manejo directo (o indirecto) de la información y/o su participación en la cadena de valor de la corporación.

7.13. Política de Desarrollo Seguro.

7.13.1 Objetivo de la política:

Asegurar la incorporación de buenas prácticas y estándares en las fases del desarrollo de software de la corporación.

7.13.2 Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que participe de forma activa en ciclo de vida de desarrollo de sistemas.

7.13.3 Lineamientos de la política:

- Todo desarrollo, mantenimiento, prueba, implementación o cambio de software debe incluir la definición o aplicación de requisitos de seguridad según los riesgos identificados.
- Para cada desarrollo de software, cambio, o funcionalidad la corporación debe especificar los requisitos de seguridad en el software, basado en un estándar mínimo de requisitos de seguridad y buenas prácticas basada en el S-SDLC (Ciclo de Vida de desarrollo Seguro de Sistemas).

7.14. Política de Seguridad de la Información en Gestión de Proyectos.

7.14.1 Objetivo de la política:

Asegurar la incorporación de la seguridad de la información y sus elementos funcionales en los proyectos que tengan o puedan tener alguna incidencia en la información.

7.14.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación.

7.14.3 Lineamientos de la política:

- Todo proyecto deberá incorporar requisitos y riesgos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.
- Todo proyecto deberá incorporar mecanismos de seguimiento, medición y control para poder conocer la aplicación de los lineamientos generales y específicos en seguridad de la información.

7.15. Política de Seguridad de la Información para la reutilización o eliminación segura de equipos.

7.15.1 Objetivo de la política:

Asegurar la incorporación de procedimientos para la reutilización o eliminación segura de los equipos de cómputo donde se almacene y procese información crítica y confidencial.

7.15.2 Alcance de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de la Caja de Compensación Familiar del Caquetá que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la corporación.

7.15.3 Lineamientos de la política:

- De acuerdo con el ciclo de vida de la información, la Caja de Compensación Familiar del Caquetá y relacionados se compromete a asegurar el borrado seguro de la información almacenada en los equipos de cómputo y unidades de almacenamiento que van a ser reasignados, reubicados, reutilizados por otro usuario o entregado al proveedor.
- Los equipos de cómputo y unidades de almacenamiento que por su obsolescencia sean dados de baja se les debe ejecutar el procedimiento de borrado seguro de modo que los residuos de información original, copias y respaldos de seguridad en medio magnético, electrónico o cualquier otra presentación sean borrados y no sean recuperables.
- Se deberá utilizar métodos de borrado seguro que permita garantizar que la información eliminada no sea recuperada, para esto se seguirá el procedimiento de borrado seguro para tal fin de acuerdo con la tecnología y clasificación de la información a eliminar.

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Caja de Compensación Familiar del Caquetá – COMFACA, ha determinado un procedimiento formal para la gestión de activos, el cual busca asegurar la gestión eficaz de activos de información (así como aquellos de tipo tecnológico) considerando el actual marco normativo nacional.

8.1. Clasificación de la información.

La información se clasificará [según control 5.12 de ISO/IEC 27001:2022 y los lineamientos normativos aplicables, y considerará la guía 5 del MSPI] en términos de requisitos[1], valor[2], criticidad[3] y sensibilidad[4] a su divulgación (confidencialidad) o modificación no autorizados, considerando la siguiente tabla:

[1] Los requisitos se describen de la siguiente forma:
- Habilitantes: aquellos que deben cumplirse para que la organización pueda operar, desde la fecha misma de su inicio.
- Fundamentales: Refieren a derechos fundamentales establecidos constitucionalmente y su desarrollo normativo.
- Funcionales: corresponden a las funciones específicas que realiza la organización, tanto de orden misional como de apoyo, y que deben cumplirse para que sus productos o servicios sean adecuados.
- Contractuales: Surge de acuerdos, pactos y en general contratos que la organización ha suscrito con sus partes interesadas.

[2] La clasificación de valor se describe de la siguiente forma:
- Esencial: Información que sin ella la organización no puede realizar sus actividades misionales.
- Misional: Información recolectada, procesada o producida en ejercicio de su misión organizacional (o jurídica)
- Reemplazable: Información que puede ser reemplazada (o volver a ser generada)
- Bajo: Información que no representa valor para la organización, pero igualmente debe ser gestionada.

[3] La clasificación de criticidad se da según el siguiente listado:
- Alta: Tiene un impacto significativo sobre los objetivos de la organización (afectación de objetivos de negocio)
- Media: Considera un impacto significativo a nivel de proceso (afectación de objetivos de proceso)
- Baja: Considera un impacto mejor (a nivel de funcionario) sin repercusiones organizacionales.

[4] La clasificación de sensibilidad se presenta según la siguiente estructura:

Requisitos	Valor	Criticidad	Sensibilidad divulgación (confidencialidad)	Sensibilidad completitud, exactitud y modificación (integridad)	Disponibilidad
1-Habilitante	1-Esencial	1-Alta	1-Reservado	1-Alta	1-Alta
2-Fundamental	2-Misional	2-Media	2-Clasificada/de negocio	2-Media	2-Media
3-Funcional	3-Reemplazable	3-Baja	3-Confidencial/personal	3-Baja	3-Baja
4-Contractual	4-Bajo		4-Pública (transparencia)		
5-Soporte			5-Pública		

- Reservado: Información de negocio delimitada como "Información Pública Reservada" según el Cap. II "Información Pública Reservada" del Título IV "Gestión de información clasificada y reservada" de la Parte VIII "Patrimonio bibliográfico, hemerográfico, documental y archivístico" del decreto 1080/2015. La clasificación como confidencial o reservada sigue las directrices del capítulo III "Directrices para la Calificación de Información Pública como Clasificada o Reservada" del Título IV "Gestión de información clasificada y reservada" de la Parte VIII "Patrimonio bibliográfico, hemerográfico, documental y archivístico" del decreto 1080/2015 y los lineamientos que sean aplicables.
  Según el MSPI, la clasificación de reservado aplica para los casos donde la información solo está disponible para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
- Confidencial/personal: Además de lo anterior, esta información es confidencial considerando los lineamientos de la Ley 1581/2012 y el decreto compilatorio (reglamentario) 1074/2015 en sus capítulos
- Clasificada/de negocio: Información de negocio delimitada como "Información Pública Clasificada" en Cap. I "Información Pública Clasificada" Título IV "Gestión de la información clasificada y reservada" de la Parte VIII "Patrimonio bibliográfico, hemerográfico, documental y archivístico" del decreto 1080/2015.
  Según el MSPI, la información pública clasificada está disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
- Pública (transparencia): Corresponde, cuando aplique, a lo establecido en la Ley de Transparencia (Ley 1712/2014), según lo dispuesto en Art. 9 "Información mínima obligatoria respecto a la estructura del sujeto obligado" y Art. 11 "Información mínima obligatoria respecto a servicios, procedimientos y funcionamiento del sujeto obligado" y las excepciones del título III "Excepciones acceso a la información", asegurando la disponibilidad de la información según los Art. 7 "Disponibilidad de la Información" y Art. 12 "Adopción de esquemas de publicación".
  Según el MSPI, es Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad
- Pública: Información que la organización ha decidido (o debe normativamente) hacer pública (Ley 1712/2014)

Complementariamente, se tienen parámetros definidos para integridad[5] y disponibilidad[6]. En los casos en los cuales no exista clasificación de la información, en cualquiera de sus parámetros, por regla de prudencia, se deberá utilizar el mayor valor de escala en cada caso.

8.2. Manejo de activos:

Manejo de activos [control 5.10 de la norma ISO/IEC 27001:2022]: según el tipo de activos, se tiene el siguiente enfoque:

8.2.1 Activos de información.

- La gestión de activos de información será integral (documentos en soporte físico o digital)[7].

[5] Según el MSPI, se tiene la siguiente escala de clasificación de integridad con su respectiva explicación:
- Alta: Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
- Media: Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
- Baja: Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.

[6] Según el MSPI, se tiene la siguiente escala de clasificación de disponibilidad con su respectiva explicación:
- Alta: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, generar daño antijurídico, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
- Media: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
- Baja: La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

[7] Según lo establecido en la Ley General de Archivo (Ley 594/2000) Art. 19 "Soporte documental" desarrollado en el decreto 2609/2012 posteriormente compilado en el decreto 1080/2015 sobre la convergencia de los archivos (en soporte físico o digital) y su tratamiento unificado, así como lo referente a documentos y mensajes de datos electrónicos

- La gestión de activos incluirá al área de gestión documental[8] como instrumento formal para la gestión de activos de información (documentos en cualquier medio de soporte) y como medio de articulación con los instrumentos de gestión de información[9].
- Los mecanismos de gestión de información, incluyendo los sistemas de información, deberán estar alineados frente a este procedimiento y los del área de gestión documental[10]
- Los activos de información estarán sujetos a la clasificación de activos de información, así como con el cuadro de clasificación documental, y las tablas de retención documental (o de valoración documental, según aplique)[11], las cuales deberán estar conciliadas, de forma tal que el activo de información cuente con su correspondiente en el ámbito documental a manera de series y subseries, y describa, cuando sea aplicable, las tipologías documentales que le sean pertinentes.

(Ley 527/1999) en especial el Título II "Patrimonio archivístico" Cap. V "Gestión de documentos" y Cap. VII "La Gestión de Documentos Electrónicos de Archivo".

[8] Tal como lo establece la Ley General de Archivo (Ley 594/2000) Art. 21 "Programas de gestión documental", el decreto compilatorio (reglamentario) 1080/2015 en los artículos Art. 2.8.2.5.10 al 13 sobre el programa de gestión documental, la Ley 1712/2014 Art. 15 "Programa de Gestión Documental" y de la Parte VIII "Patrimonio bibliográfico, hemerográfico, documental y archivístico" del decreto 1080/2015 Título V "Instrumentos de gestión de información pública" Cap. IV "Programa de Gestión Documental".

[9] de acuerdo con el decreto 1080/2015 Art. Artículo 2.8.5.4.2. "Articulación y/o integración del Programa de Gestión Documental con los instrumentos de gestión de información"

[10] Según Ley 1712/2014 Título II "de la publicidad y del contenido de la información" Art. 17 "Sistemas de información"

[11] Según la Ley 594/2000 Art. 24 "Obligatoriedad de las tablas de retención", Acuerdo Archivo General de la Nación 39 de 2002 y decreto 1080/2015 Art. 2.8.2.2.2. "Elaboración y aprobación de las tablas de retención documental y las tablas de valoración documental".

- El etiquetado de información [control 5.13 de la norma ISO/IEC 27001:2022] seguirá los esquemas de clasificación de la información adoptados por la organización, es decir:
  - Los archivos en soporte físico, se aplicarán rótulos definidos por la corporación para sus unidades documentales, aplicados sobre unidades de conservación (cajas y carpetas) que deberán incluir los elementos indicados por el archivo general de la nación;
  - En archivos de soporte digital se tienen las siguientes situaciones:

    Datos estructurados (como bases de datos): El etiquetado corresponderá a la estructura principal (ejemplo, instancia de la base de datos).

    - Datos no estructurados (como archivos independientes): La corporación de los documentos deberá ser realizado en carpetas (en el sistema operativo correspondiente) con el menor nivel de anidación y con nombres (tanto en la carpeta como en archivos) que tengan longitudes de texto cortas que, combinados (anidadas y nombres de archivo) no generen riesgos de acceso a documentos. La organización de documentos en carpetas aplica el principio archivístico de procedencia. El etiquetado (y registro en el inventario de activos)

corresponderá a la carpeta, en el nivel pertinente, que asegure integridad documental y principio de procedencia.

- La consulta, acceso y préstamo deberá contar siempre con un registro[12].
- La transformación (cambio en el soporte documental, por ejemplo, por digitalización), eliminación y/o transferencias de documentos (en cualquier formato) deberá estar definida en el programa de gestión documental y seguir los requisitos pertinentes[13] [14].
- Todos los empleados y usuarios de partes externas, incluyendo contratistas, deben devolver los activos de la corporación que estén en su posesión al cambiar o terminar su empleo, contrato o acuerdo [control 5.11 de la norma ISO/IEC 27001:2022] como requisito para la liquidación y finalización del contrato, y de ello será evidencia de cumplimiento el inventario documental (de información).

[12] Ley 594/2000 Art. 27 "Acceso y consulta de los documentos"

[13] Ley 594/2000 Art. 46 "Conservación de documentos", Art. 48 "Conservación de documentos en nuevos soportes" y Art. 49 "Reproducción de documentos", así como el decreto 1080/2015 Art 2.8.2.2.5. "Eliminación de documentos". Las transferencias documentales son reglamentadas en el decreto 1080/2015 Título II "Patrimonio archivístico" Cap. IX "Transferencias Secundarias", Capítulo X "Transferencia de documentos de las demás ramas del poder público y de los órganos autónomos y de control", Capítulo XI "Procedimiento para realizar las transferencias de documentos de conservación Permanente". La custodia fue incluida en la misma norma Título II "Patrimonio archivístico" Cap. XII "Contratación del Servicio de Custodia de Documentos de Archivo por Parte de Entidades Públicas y Privadas que cumplen Funciones Públicas". Adicionalmente, se cuentan diversas circulares del Archivo General de la Nación.

[14] Ley 527/1999, en lo referente a la integridad de documentos

8.2.2 Activos relacionados con información (infraestructura).

La gestión de activos relacionados con información, en especial infraestructura, incluirá, además de lo establecido por la corporación en materia de activos físicos lo indicado en procedimientos complementarios a éste en materia de desarrollo, adquisición y mantenimiento de sistemas, de comunicaciones, operacionales y áreas físicas.

El uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de datos [control 5.10 de la norma técnica ISO/IEC 27001:2022] estará basado en las siguientes reglas:

- Todo uso de activos y de información, será permitido siempre y cuando esté orientado a la consecución de los objetivos del negocio y se dará a partir de la autoridad, roles y responsabilidades otorgados a la persona que realiza dicho uso.
- No estará permitido el uso de activos, tanto de información como los relacionados con la información, en el caso de actividades de captura, procesamiento, almacenamiento, reproducción y/o eliminación de información de datos personales.
- No estará permitido el uso de activos, tanto de información como los relacionados con la información, en el caso de actividades de cualquier índole que vayan en contravía del marco de requisitos al cual está sujeta la corporación y en general que puedan constituir incumplimiento o violación a las normas en general, la realización de delitos o apoyar su ejecución, o la afectación de derechos fundamentales.

- No estará permitido el uso de activos, de información como los relacionados con la información, orientados al proselitismo político, la promoción de tendencias religiosas o espirituales, tendencias filosóficas, o todo aquello que promueve o incite a la violencia, discriminación o inseguridad.
- La corporación podrá establecer lineamientos específicos relacionados con activos específicos.

8.3. Inventario de activos.

El inventario de activos [control 5.9 de ISO/IEC 27001:2022] identifica y mantiene actualizada la información y activos asociados con la información, incluyendo elementos de transparencia[15] así como su relación con gestión documental y archivo[16]. Este inventario de activos incluye el índice de "Información Clasificada y Reservada"[17]

Dentro del inventario de activos se incluye información sobre:

- Identificador: Número consecutivo único que identifica al activo en el inventario.
- Proceso: Nombre del proceso al que pertenece el activo.

[15] Según lo establecido en la Ley 1712/2014 Art. 13 "Registros de Activos de Información" y el Cap. I "Registro de Activos de Información" del Título V "Instrumentos de la gestión de información pública" de la Parte VIII "Patrimonio bibliográfico, hemerográfico, documental y archivístico" del decreto 1080/2015.

[16] El inventario documental se exige en la Ley General de Archivo Art. 26 "Inventario Documental" así como en su decreto compilatorio Art. 2.8.2.2.4. "Inventarios de documentos".

[17] Según Cap. II "Índice de Información Clasificada y Reservada" del Título V "Instrumentos de la gestión de información pública" de la Parte VIII "Patrimonio bibliográfico, hemerográfico, documental y archivístico" del decreto 1080/2015.

- Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.
- Descripción/Observaciones: describe el activo de forma clara para los miembros del proceso.
- Serie y subserie documental: Para los casos de activos de información (información y conocimiento representado como procedimientos y software) se debe indicar la serie y subserie (si aplica) en la cual se cataloga el activo de información.
- Tipo: define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:
    - Información: Datos e información almacenada o procesada de forma física o digital.
    - Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas, tanto comercial (como activo genérico) como software desarrollado a la medida (conocimiento representado – activo de información)
    - Hardware e infraestructura: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos.
- Clasificación de activos:

- Criticidad: Contempla dos subcategorías, una con un enfoque interno (de operaciones) como de servicios a terceros;
    - Sensibilidad (confidencialidad): Registra el parámetro de clasificación del activo desde la óptica de sensibilidad por divulgación (confidencialidad);
    - Valor organizacional: Registra el parámetro de clasificación según valor organizacional;
    - Valor de requisito: Registra el parámetro de clasificación según valor según requisitos;
    - Integridad: Registra el parámetro de clasificación del activo desde la óptica de sensibilidad por modificación/alteración, completitud y exactitud;
    - Disponibilidad: Registra el parámetro de clasificación según disponibilidad de los activos;

- Propietario: Es una parte designada de la corporación, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
- Custodio: Parte designada de la corporación, un cargo, proceso, o grupo de trabajo encargado de aplicar las restricciones y clasificaciones de acceso definidos por el

propietario. (Para sistemas de información o información, es TI, y para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio se define donde reposa el activo original).

- Localización: describe la ubicación tanto física como electrónica del activo de información.

Cada uno de los activos identificados en el inventario de activos debe indicar el propietario del activo [Control 5.9 de la norma ISO/IEC 27001:2022] que corresponde a aquella persona con responsabilidad demostrada sobre el activo. Sobre un mismo activo pueden existir varias personas propietarias o que tienen responsabilidad demostrada.

8.4. Gestión de medios y soportes.

8.4.1. Gestión de medios removibles

- Los medios removibles serán permitidos, según la clasificación de activos de información.
- Está prohibido el uso de medios removibles salvo autorización expresa por parte de la persona autorizada.
- No está permitido el transporte de información de tipo Confidencial/de negocio, Confidencial/personal o Reservado (ver clasificación de activos) sin el uso de medios seguros de transporte.

- Siempre que se usen medios removibles (debidamente autorizados) deberán considerar las políticas de transferencia de información, uso de cifrado y llaves de cifrado, y en general la política de seguridad de la información [Control 8.12 de la norma ISO/IEC 27001:2022].
- Siembre que se empleen medios removibles (debidamente autorizados) deberá dejarse registro para asegurar la trazabilidad de la consulta, acceso y préstamo de la información.
- Cuando el medio removible deje de utilizarse definitivamente por capacidad, daño o cualquier otra razón, deberá ser entregado a persona formalmente autorizada, quien procederá a su eliminación [Control 7.14 de la norma ISO/IEC 27001:2022] de forma segura.
- No está permitido la reutilización de medios removibles o su obsequio a otras partes interesadas.
- Se deben establecer normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes (Transferencia de información [Control 5.14 de la norma técnica ISO/IEC 27001:2022]).
- Si llegase a ocurrir la pérdida o robo de un medio removible con información de la corporación deberá ser inmediatamente reportado y aplicadas las medidas que se hayan definido para tal fin.

- En general todos los registros deberán estar protegidos de su pérdida, destrucción, falsificación, acceso no autorizado y liberación o divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio [Control 5.33 de la norma ISO/IEC 27001:2022].

8.5. Gestión y remoción de equipos.

- Los equipos asociados a Tecnologías de la Información y Comunicaciones (tales como equipos de cómputo, servidores, unidades de almacenamiento, unidades de procesamiento, infraestructura de red) tendrán mantenimiento de forma exclusiva por las personas delegadas para tal fin, quienes tendrán autorización única para acceder, desensamblar, transportar, cambiar piezas, y retirar.
- Una vez los equipos asociados a Tecnologías de la Información y Comunicaciones finalicen su ciclo de vida, o presenten falla que impida su operación, deberán ser removidos; La remoción de tales equipos será realizado de forma exclusiva por las personas delegadas para tal fin quienes deberán realizar el desensamble seguro de sus piezas y borrado seguro de aquellos elementos que pudiesen contener información, en especial discos duros; Una vez finalizada esta etapa, se deberá proceder a su reciclado.

9. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Caja de Compensación Familiar del Caquetá. COMFACA, gestiona los riesgos de seguridad de la información de todos los procesos que se desarrollan dentro de las áreas de la Corporación a través del programa de gestión de riesgo empresarial el cual está basado en la norma ISO:31000:2018.

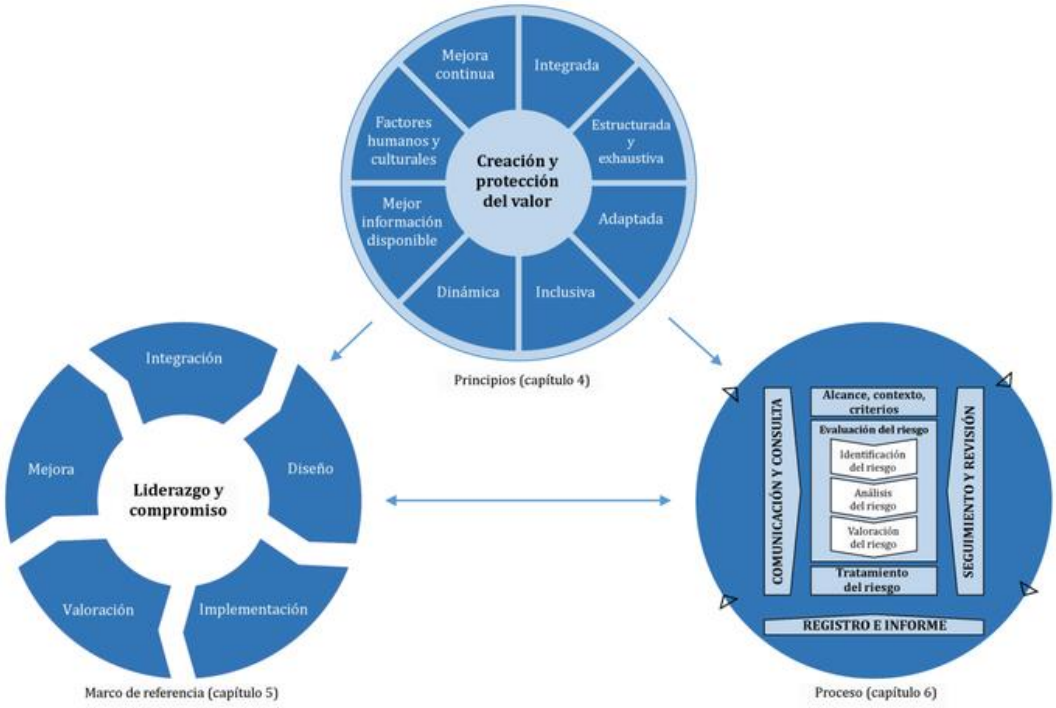


Figura. 1 Principios, marco de referencia y proceso de la gestión de riesgos. ISO 31000:2018.

La Caja de Compensación Familiar del Caquetá se ejecuta de acuerdo con el procedimiento para la Gestión de Riesgos de Seguridad de la Información en el cual, se identifican por parte de los jefes de departamentos los riesgos que se pueden llegar a materializar en cada uno de los procesos, registrando la información solicitada en el formato PE-PGC-FT-06-RIESGOS Y OPORTUNIDADES con cada equipo de trabajo. A su vez estas matrices deben ser socializadas y revisadas por el profesional de Calidad y posteriormente aprobadas por la Dirección Administrativa.

9.1. Matriz de Riesgos

MATRIZ		**Amenazas**					Oportunidades				
		Impacto									
Probabilidad		Muy Bajo	Bajo	Medio	Alto	Muy Alto	Muy Alto	Alto	Medio	Bajo	Muy Bajo
		1	2	3	4	5	5	4	3	2	1
Casi Seguro	5	5	10	15	20	25	25	20	15	10	5
Probable	4	4	8	12	16	20	20	16	12	8	4
Posible	3	3	6	9	12	15	15	12	9	6	3
Improbable	2	2	4	6	8	10	10	8	6	4	2
Rara Vez	1	1	2	3	4	5	5	4	3	2	1

MATRIZ		Amenazas					Oportunidades				
		Impacto									
Probabilidad		Muy Bajo	Bajo	Medio	Alto	Muy Alto	Muy Alto	Alto	Medio	Bajo	Muy Bajo
		1	2	3	4	5	5	4	3	2	1
Casi Seguro	5										
Probable	4										
Posible	3										
Improbable	2										
Rara Vez	1										

Tabla 1. Matriz de probabilidad e impacto.

Los riesgos son consolidados en un mapa de calor teniendo en cuenta la valoración del riesgo en estado residual con base a los controles existentes definidos en la matriz de riesgos. Este mapa de riesgos es presentado en el informe, de acuerdo al plan de trabajo del área de planeación, en cabeza del profesional de calidad, a fin de socializar los riesgos que se identificaron como inaceptables y así mismo, presentar los planes de acción con sus respectivas fechas de ejecución.

De igual manera, cada equipo de trabajo presenta evidencias sobre cada una de las acciones ejecutadas para gestionar el riesgo, demostrando avances o justificando la

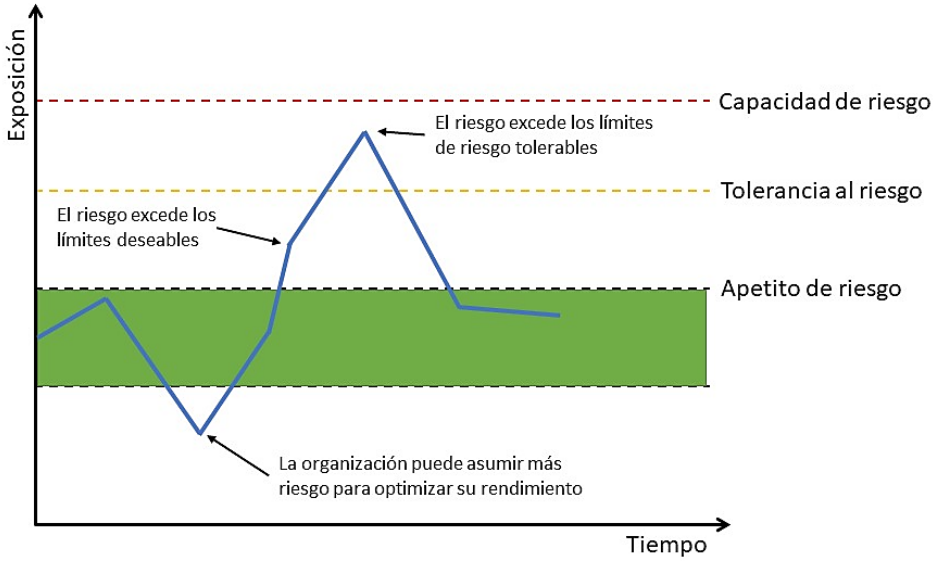
reprogramación de fechas si aplica; estos seguimientos serán consolidados en el formato de matriz de riesgo. Las reprogramaciones de los planes de acción deben estar soportadas y aprobadas por el Jefe de cada área, estableciendo nuevas fechas para ejecutar las acciones definidas de los planes establecidos.

Finalmente, cuando se han cumplido los planes de acción definidos en la matriz de riesgos, el equipo de calidad debe realizar la actualización del mapa de calor de los riesgos identificados y gestionados. El área presenta mediante un informe la matriz de riesgos, haciendo énfasis en la mitigación de los riesgos que habían sido identificados como inaceptables o de aquellos que no se lograron mitigar por falta de ejecución de los planes de acción y continúan en estado inaceptable, con el propósito de tomar las medidas correctivas por parte de la Dirección.

Cuando se presenten situaciones de impacto en los procesos y objetivos del negocio, en alguna de las unidades de la Caja de Compensación Familiar del Caquetá, el Jefe del departamento responsable debe actualizar la matriz de riesgos con la situación existente, identificándolo como "riesgo materializado" y aplicando así el análisis de riesgos.

9.2. Apetito, tolerancia y capacidad del riesgo

Una adecuada gestión de los riesgos permite el cumplimiento de los objetivos y la satisfacción de lograr los resultados esperados, por lo que la corporación cuenta con un sistema de gestión de riesgos administrado.



9.2.1. Apetito al riesgo: Indica que tipo y cantidad de riesgo una organización está dispuesta a asumir y cual no, para lograr sus objetivos. Es decir, ¿se está dispuesto a asumir riesgos que puedan tener un alto impacto en la reputación de la corporación?, ¿Qué tanto riesgo la organización desea asumir al ejecutar sus procesos?

9.2.2. Tolerancia al riesgo: La tolerancia es el rango aceptable de variación que puede haber en torno al apetito, es decir, el delta que hay entre el apetito y la capacidad. Por tanto, es el rango en el cual se puede mover la organización estando aún en un margen aceptable si bien no óptimo.

9.2.3. Capacidad de riesgo: Se entiende por la cantidad y tipo de riesgo que una organización es capaz de soportar en la persecución de sus objetivos. Es el

máximo riesgo que puede asumir la organización en determinada área. Es el límite. Si se excede la capacidad la empresa deja de ser viable.

9.2.4. Nivel de riesgo: Dentro del nivel de riesgo aceptable se encuentran aquellos riesgos que la corporación ha identificado y está dispuesta a asumir de acuerdo con el apetito de riesgo.

10. SEGURIDAD DE RECURSOS HUMANOS

La Caja de Compensación Familiar del Caquetá – COMFACA para controlar que sus empleados y contratistas entiendan sus responsabilidades y sean idóneos, realiza el proceso de selección de sus funcionarios a través de la agencia de empleo Comfaca.

De igual manera, el manual de funciones se establece para cada uno de los cargos, autoridades, roles y responsabilidades en materia de seguridad de la información, así como competencias esenciales en ese ámbito.

Adicionalmente, durante el tiempo del empleo o de la relación contractual, la Caja de Compensación Familiar del Caquetá asegura que los empleados y contratistas sean conscientes y cumplan sus responsabilidades en seguridad de la información.

11. SEGURIDAD FÍSICA Y AMBIENTAL

El presente objetivo de control busca prevenir el acceso físico no autorizado al igual que el daño e interferencia a la información e instalaciones de procesamiento de la Caja de Compensación Familiar del Caquetá – COMFACA.

Se han definido dentro de las instalaciones de la Caja de Compensación Familiar del Caquetá áreas seguras, estas áreas deberán estar protegidas por un perímetro de seguridad, y contar con controles ambientales y aquellas otras medidas necesarias para garantizar la confidencialidad, la integridad y disponibilidad de la información.

11.1. Áreas Seguras.

Se consideran áreas seguras físicas:

- Circuito Cerrado de Televisión.
- Centro de datos, de cómputo y de comunicaciones.
- Cuartos de centro de cableado.
- Área de almacenamiento de archivo, de gestión documental y radicación
- Cuartos y plantas eléctricas.
- Oficinas, subdirecciones y departamentos.

11.2. Perímetro de Seguridad Física.

Las instalaciones de la Caja de Compensación Familiar del Caquetá – COMFACA tienen definidas unas áreas de recepción a la entrada de los edificios, adicionalmente cuentan con el servicio de vigilancia privada; servicio que tiene un guarda de seguridad asignado 15 horas del día, los siete días de la semana y un CCTV. Para el control de acceso, los funcionarios deben identificarse mediante el carnet de la corporación.

El archivo central de la corporación está resguardado por acceso con cerradura de seguridad mecánica.

Los cuartos de comunicaciones, centros de cableado cuentan con un control de acceso con cerradura de seguridad digital, cámaras de seguridad y solo el personal de Infraestructura y Comunicaciones del departamento de TICS están autorizados a ingresar. En caso de ser necesario el ingreso de un proveedor de servicio se debe registrar la actividad y el tiempo de permanencia dentro de esta área en el formato establecido para tal fin.

11.3. Seguridad en Equipos de Cómputo

- Los equipos de cómputo sean de escritorio y/o portátil que son asignados a cada funcionario de La Caja de Compensación Familiar del Caquetá – COMFACA deben tener contraseña para la cuenta de usuario del Sistema Operativo y una

credencial de administrador del Sistema Operativo preinstalada por el personal del departamento de TIC's.

- La contraseña de ingreso al Sistema Operativo garantizara que personal no autorizado no pueda ingresar a la configuración y/o documentación que se encuentre en el equipo.
- Los equipos de cómputo asignados en cada sede no pueden ser transportados o movidos de su ubicación por inventario por ningún funcionario sin previa autorización por parte del área de servicios administrativos o departamento de TIC's de la corporación.
- Está prohibido la apertura de los equipos, cambio de partes o cualquier modificación física que se pueda realizar al hardware del equipo por parte de los funcionarios asignados. Esta responsabilidad es asumida únicamente por el personal del departamento de TIC's o el proveedor.
- Está prohibida la instalación de software No Licenciado.
- La instalación de Software libre debe presentar autorización previa del departamento de Tecnologías de la Información y las Comunicaciones dando cumplimiento a la Política de Instalación de Software en el ítem 7.9 del presente documento.

12. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

Para asegurar las operaciones que se realizan diariamente con respecto al procesamiento de la información en los sistemas de información, y en las instalaciones de la corporación, La Caja de Compensación Familiar del Caquetá tiene los siguientes controles:

- Todos los procedimientos operativos se encuentran debidamente documentados y están disponibles para los funcionarios que desempeñan dichos roles.
- Todas las estaciones de trabajo, computadores de la corporación cuentan con un antivirus licenciado para la detección, prevención y recuperación contra malware.
- La Caja de Compensación Familiar del Caquetá tiene la política de copias de respaldo (Backup) para la información de los funcionarios de la corporación, la cual esta enunciada en el numeral 7.10. de este documento.
- Se registran los eventos de actividad de usuario en los sistemas de información para tener la trazabilidad de la operación.
- La Caja de Compensación Familiar del Caquetá tiene una política de instalación de software enunciada en este documento en el numeral 7.9.

12.1. Procedimientos y Responsabilidades de operación.

Para asegurar las comunicaciones, La Caja de Compensación Familiar del Caquetá – COMFACA ha dispuesto los siguientes controles:

- A nivel de red, cuenta con firewall y listas de control de acceso para proteger la información y las aplicaciones.
- La Caja de Compensación Familiar del Caquetá, tiene una política de seguridad para la transferencia de información, la cual esta enunciada en este documento en el numeral 7.11 de este documento.
- La Caja de Compensación Familiar del Caquetá en toda propuesta comercial y contrato requiere una cláusula de confidencialidad y cláusula de protección de datos personales, para salvaguardar la información de la organización.
- La trasferencia de cualquier tipo de información de La Caja de Compensación Familiar del Caquetá – COMFACA debe realizarse a través de las herramientas colaborativas licenciadas para tal fin.

12.2. Monitoreo

La Caja de Compensación Familiar del Caquetá cuenta con sistemas de identificación del riesgo que permiten monitorear en tiempo real la supervisión de seguridad de la información y de la red que permiten la detección de los cambios en la red que indiquen una violación de seguridad.

13. CONTROL DE ACCESO.

13.1. Requerimientos en el control de Acceso Físico.

El acceso físico a las instalaciones de La Caja de Compensación Familiar del Caquetá por parte de funcionarios y visitantes debe cumplir con lo siguiente:

- Para ingresar a las sedes de La Caja de Compensación Familiar del Caquetá los funcionarios deben portar el carnet en un lugar visible y es de uso obligatorio dentro de las instalaciones de la corporación.
- No está permitido prestar el carnet de identificación, se considera suplantación de identidad por parte de la persona que lo utiliza.
- La pérdida del carnet de identificación debe ser reportado de inmediato al área de Gestión Humana.
- En caso de los visitantes, se deben registrar al ingresar en el formato de control de acceso de personal operado por el guarda de seguridad, previa autorización del funcionario de la Caja de Compensación Familiar del Caquetá que los acompaña.
- El ingreso de computadores que no sean propiedad de la Caja de Compensación Familiar del Caquetá debe ser debidamente registradas al ingresar, indicando la fecha, hora de entrada, hora de salida, nombre y apellido, marca, serial y firma; de

igual manera a la hora de salida se debe verificar que el equipo que está saliendo sea el mismo número de serie del que entró con la persona responsable.

13.2. Control de Acceso Lógico.

El control de acceso lógico se rige por la Política de Control de Acceso que se encuentra en el numeral 7.4. del presente documento.

13.3. Seguridad de Oficinas, Recintos e Instalaciones.

La Caja de Compensación Familiar del Caquetá – COMFACA para mitigar el riesgo de pérdida de información de sus instalaciones adopta las siguientes medidas:

- El personal de vigilancia debe revisar todo bolso o paquete del personal al ingresar o salir de las instalaciones.
- Todo ingreso de contratistas o visitantes para los fines de semana deberá ser solicitado previamente al jefe de área, indicando el motivo del requerimiento, en caso de ser autorizado se informará el día anterior a la vigilancia del edificio el ingreso del personal y su ingreso se dará solo a través de un documento aprobado por el jefe inmediato en el que conste el permiso o necesidad para ingresar a las instalaciones.
- El ingreso del personal en los días no hábiles deberá ser registrado en el formato de control de acceso del personal operado por el guarda de seguridad.

13.4. Gestión de Acceso al usuario.

La gestión de acceso al usuario se encuentra en el presente documento en el ítem Política de Control de Acceso numeral 7.4.

13.5. Responsabilidad del usuario.

- Es responsabilidad de los funcionarios el uso o las acciones que se realice sobre la cuenta de acceso (usuario) a los sistemas de información y servicios de red de la corporación.
- No está autorizado ceder o prestar el usuario de ingreso o las credenciales de acceso.
- El funcionario no deberá almacenar en ningún sitio visible o documento físico las contraseñas de ingreso al equipo o sistemas de información de la corporación.
- Es responsabilidad de los funcionarios reportar cualquier daño, falla, riesgo o amenaza detectada en los sistemas de información, computadores o componentes físicos al personal técnico calificado de soporte y al área TIC's.
- Reportar todas las anomalías, fallas o incidentes que afecten la seguridad física o de software tecnológico de la corporación.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

La adquisición, desarrollo y mantenimiento de los sistemas de información de La Caja de Compensación Familiar del Caquetá, están contratados con terceros los cuales deben cumplir las políticas de seguridad en relación con proveedores, desarrollo de software y gestión de proyectos enunciadas en los numerales 7.12, 7.13 y 7.14. del presente documento.

Para cada proyecto nuevo, mejora sustancial o cambio a los sistemas de información de la Caja de Compensación Familiar del Caquetá se debe ejecutar un análisis de riesgo antes de iniciar.

14.1. Requerimientos de seguridad de los sistemas de información.

- **Objetivo**

Garantizar que la seguridad de la información sea una parte integral de los sistemas de información a través del ciclo de vida completo e incluir los requisitos para sistemas de información que proporcionan servicios sobre redes públicas o privadas.

- **Análisis y especificación de los requisitos de seguridad de la información.**

Los requisitos relacionados a la seguridad de la información están incluidos dentro de los requerimientos para el desarrollo de nuevos sistemas de información o mejoras a los sistemas existentes.

- **Protección de transacciones en servicios de aplicación.**

La información involucrada en las transacciones de los servicios de aplicación está protegida para prevenir la transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.

14.2. Seguridad en los procesos de desarrollo y soportes

- **Objetivo**

Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

- **Política de desarrollo seguro de software**

Los desarrollos de software y sistemas dentro de la corporación cuentan con reglas establecidas para realizar la estandarización de los procesos de desarrollo.

- **Pruebas de aceptación del sistema**

Los nuevos sistemas de información, actualizaciones y nuevas versiones cuentan con programas de pruebas y criterios de aceptación, según actas de aprobación por el solicitante del desarrollo.

14.3. Gestión de la Vulnerabilidad técnica.

Se deben realizar las pruebas de intrusión o evaluaciones de vulnerabilidad (Ethical Hacking, entre otros) contempladas dentro del marco de la revisión del cumplimiento técnico de los requerimientos establecidos para la gestión de la seguridad de los sistemas de información.

Dichas pruebas se deben ejecutar de forma periódica al menos una vez por año o cuando se implemente un cambio significativo en la funcionalidad de los sistemas.

15. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

La Caja de Compensación Familiar del Caquetá gestiona los incidentes y eventos de seguridad de la información mediante el reporte oportuno de todo el personal de COMFACA, funcionarios y terceros, en todos los niveles de la corporación y el análisis de la información recolectada del suceso para reducir la afectación negativa de la continuidad de las operaciones.

Para asegurar un enfoque consistente y eficaz de la comunicación de un incidente de seguridad de la información se debe seguir el procedimiento de gestión de incidentes del MSPI.

El reporte de cada evento de seguridad de la información se realizará a través de los canales establecidos por la corporación para la atención y soporte a los sistemas de información, en este caso el correo electrónico sistemas@comfaca.com o por medio de la extensión del área de sistemas.

Cada evento será evaluado por el departamento de TIC's, para decidir si se clasifica como incidente de seguridad.

La respuesta de incidentes se debe realizar según el procedimiento de gestión de incidentes.

Cada incidente deberá ser socializado para mitigar la probabilidad de impacto e incidente futuro asegurando aprendizaje del mismo.

La evidencia recolectada por cada incidente será salvaguardada por el departamento de Tecnologías de la Información y las comunicaciones y el Oficial de seguridad para darle manejo según normatividad vigente.

15.1. Contacto con autoridades y grupos de interés.

Las siguientes autoridades listadas corresponden a las entidades competentes en caso de que se presente un incidente de cualquier índole que pusiera en riesgo la confidencialidad, integridad y disponibilidad de la información, en caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo los funcionarios encargados.

Descripción	Organización	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	https://caivirtual.policia.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Phishing		
Ingeniería Social		
Respuesta a Emergencias Cibernéticas de Colombia	COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano	CSIRT-CCIT – Centro de Coordinación	https://cc-csirt.policia.gov.co/

	Seguridad Informática Colombia	
Emergencia por Incendio	Bomberos	119
Robo	Policía Nacional	112
Antisecuestro y Antiextorsión	Gaula	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja	132
Incidentes laborales	Centro Toxicológico	136
Robo	Dijin	157
Comando de Policía del departamento de Caquetá	Comando de Policía	(608) 4348941 y 4358919

ELABORÓ:	REVISÓ:	APROBÓ:
Cargo: Profesional 2 – Tic's	Cargo: Jefe depto. 3 – Tic's	Cargo: Director Administrativo
Fecha:14 - diciembre - 2023	Fecha: 15 - diciembre - 2023	Fecha: 08 - febrero - 2024

El encargado de Seguridad de la Información en la corporación coordinará la entrega oportuna de la información recolectada, a fin de brindar ayuda en la toma de decisiones en materia de seguridad, éste podrá obtener asesoramiento de otros organismos.

Se debe mantener contacto permanente con las Universidades, los grupos de investigación, entidades del gobierno, proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones.

Grupo de interés	Contacto	Teléfono
ACIS	https://www.acis.org.co/	Cel.: 3015530540 Tel: 6161407-09 / 6104842
Ministerio de Tecnologías de la Información y las comunicaciones	https://www.mintic.gov.co/portal/inicio/	
CSIRT ASOBANCARIA	https://csirtasobancaria.com/	
INFO SECURITY	https://isec-infosecurity.com/	
SEGU.INFO	https://www.segu-info.com.ar/	

16. CUMPLIMIENTO.

La Caja de Compensación Familiar del Caquetá – COMFACA para dar cumplimiento a las obligaciones legales, estatutarias, regulatorias y contractuales, relacionadas con la seguridad de la información, cuenta con un procedimiento para la gestión del cumplimiento y la conformidad conforme a la norma técnica ISO 19600:2014, que acredita la adopción del modelo de seguridad de la información.

El propósito que persigue la corporación con el cumplimiento del Modelo de Seguridad y Privacidad de la Información es generar una garantía de que los procesos se desarrollan bajo los lineamientos dados en las políticas de seguridad de la información y cumplen con a lo establecido en la ley 1581 de 2012 y el decreto 1377 de 2013.

El Comité de Seguridad de la Información y Protección de Datos Personales de La Caja de Compensación Familiar del Caquetá está encargado de supervisar el cumplimento de todas las políticas de seguridad de la información dentro de la organización, revisando de manera independiente los cambios generados por el contexto en el que se desempeña la organización.

Igualmente, el Comité de Seguridad de la Información y Protección de Datos Personales de La Caja de Compensación Familiar del Caquetá se reunirá periódicamente para revisar los controles aplicados a los procesos de la corporación, y para realizar la

evaluación de los objetivos de control del modelo de seguridad y privacidad de la información.

17. BIBLIOGRAFIA.

Comercio, S. d. (s.f.). Obtenido de https://www.sic.gov.co/manejo-de-informacion-personal

Comunicaciones, C. d. (2009). Resolución Comision de Regulacion de Comunicaciones 2258.

CONPES 3701, L. d. (s.f.).

CONPES 3854, P. n. (2016).

ISO 27000. (s.f.). ISO27000.ES. Obtenido de https://www.iso27000.es/glosario.html

Ley 1581 de 2012, L. d. (s.f.).

Ley 1712 de 2014, a. 4. (s.f.). Ley de transparencia y del derecho de acceso a la información publica nacional.

18. IDENTIFICACIÓN Y CONTROL DE CAMBIOS:

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN