MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO DEL MANUAL

Determinar el establecimiento e implementación del Sistema de Gestión de Seguridad de la Información (SGSI); garantizando la cobertura total de los requisitos obligatorios de la norma ISO 27001:2013, considerando para ello el alcance del Sistema de Gestión de Seguridad de la Información, sus objetivos y responsabilidades del personal en general para alcanzar las metas de la seguridad de la información en la Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE.

2. ALCANCE DEL MANUAL

Este documento especifica los requisitos para el establecimiento e implementación del Sistema de Gestión de seguridad de la Información (SGSI) para la Caja de Compensación Familiar del Oriente Colombiano en adelante COMFAORIENTE.

3. REFERENCIAS NORMATIVAS

El siguiente documento, parte o en su totalidad, constituyen referencias expuestas en la normativa ISO 27001:2013 para la constitución del Sistema de Gestión de Seguridad de la Información (SGSI).

G

Guía de Normatividad de Seguridad de La Información G-TEC-04

4. TÉRMINOS Y CONDICIONES

Para el propósito del presente documento, aplica los términos y definiciones dados en la normativa ISO 27001:2013 para la constitución de Sistema de Gestión de Seguridad de la Información (SGSI).

- **Acción correctiva:** Remediación de los requisitos o acciones que dieron origen a la organización de no una conformidad, de tal forma que no se vuelva a presentar.

- **Acción preventiva:** Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

- **Activo:** Según [ISO IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos de COMFAORIENTE. Se pueden clasificar de la siguiente manera:

- Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en COMFAORIENTE. Ejemplo: archivo de Word, "listado de personal.docx".

- **Software/Aplicaciones:** Es todo el software que se utiliza para la gestión de la información.

- **Personal:** Es todo el personal COMFAORIENTE, el personal subcontratado, los afiliados, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información COMFAORIENTE.

- Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

-**Tecnología**: Son todos los equipos tecnológicos utilizados para gestionar la información y las comunicaciones.
Ejemplo: equipo de cómputo, teléfonos, impresoras.

- Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Tesorería

- **Administración de incidentes de seguridad**: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

  - Detectar cualquier alteración en los servicios TI.
  - Registrar y clasificar estas alteraciones.

- Asignar el personal encargado de restaurar el servicio.

- **Almacenamiento en la Nube**: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

- **Amenaza:** Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Análisis de riesgos**: A partir del riesgo definido, se determinan las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular o en la corporación en general.

- **Auditoría:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Autenticación**: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Autenticidad**: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

- **Base de datos**: Contiene toda la información pertinente acerca de los componentes de uno o varios sistemas de información utilizado en la organización.

- **Características de la Información**: Las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

- **Cifrar:** Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.

- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización,

revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.

- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **Control**: Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

- **Declaración de aplicabilidad (SOA - Statement of Applicability):** Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

- **Denegación de servicios**: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

- **Directiva:** Según [ISO IEC 13335-1: 2004): Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad:** Según [ISO IEC 13335-1: 2004): Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Evento:** Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de

seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

- **FTP: (File Transfer Protocol)** es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.

- **Gestión de claves**: Controles referidos a la gestión de claves criptográficas.

- **Gestión de riesgos**: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Gusano (Worm):** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

- **Impacto:** Resultado de un incidente de seguridad de la información.

- **Incidente:** Según [ISO IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- **Información pública clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

- **Información pública reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.

- **Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior.

  En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **Inventario de activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

- **ISO 27001**: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

- **ITIL IT Infrastructure Library**: Un marco de gestión de los servicios de tecnologías de la información.

- **Keyloggers:** Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano.

  Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

- **Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **No conformidad grave**: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- **No repudio**: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

- **PDCA Plan-Do-Check-Act**: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

- **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Política de seguridad:** Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- **Ransomware**: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

- **Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad de la información**: Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

- **SGSI Sistema de Gestión de la Seguridad de la Información**: Según [ISO IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

- **Spamming:** Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

- **Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

- **Spoofing:** Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

- **Tratamiento de riesgos**: A partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

- **Trazabilidad:** Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

- **Usuario:** En el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de COMFAORIENTE, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del DAPRE y a quienes se les otorga un nombre de usuario y una clave de acceso.

- **Valoración de riesgos:** Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

- **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

- **VPN (Virtual Private Network):** Es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

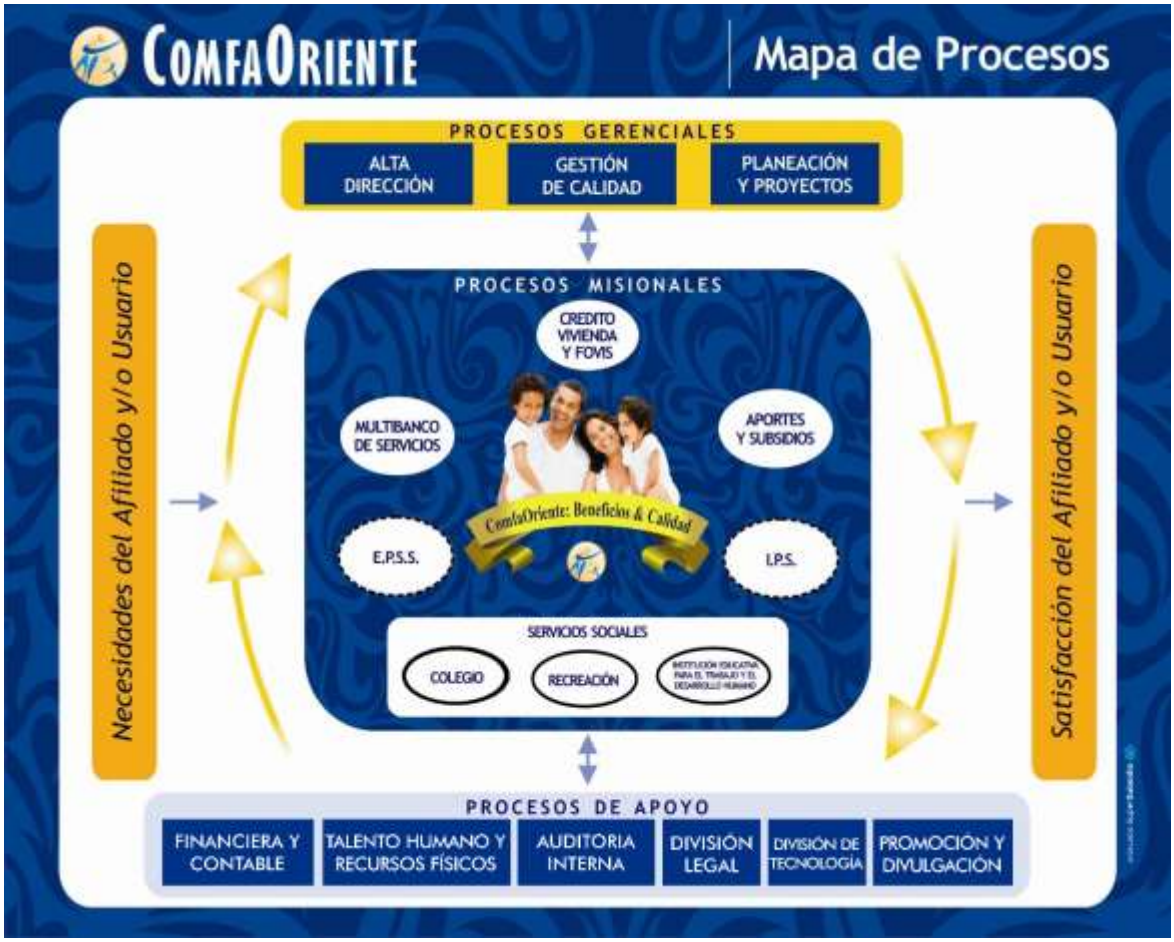
Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. CONTEXTO DE LA ORGANIZACIÓN

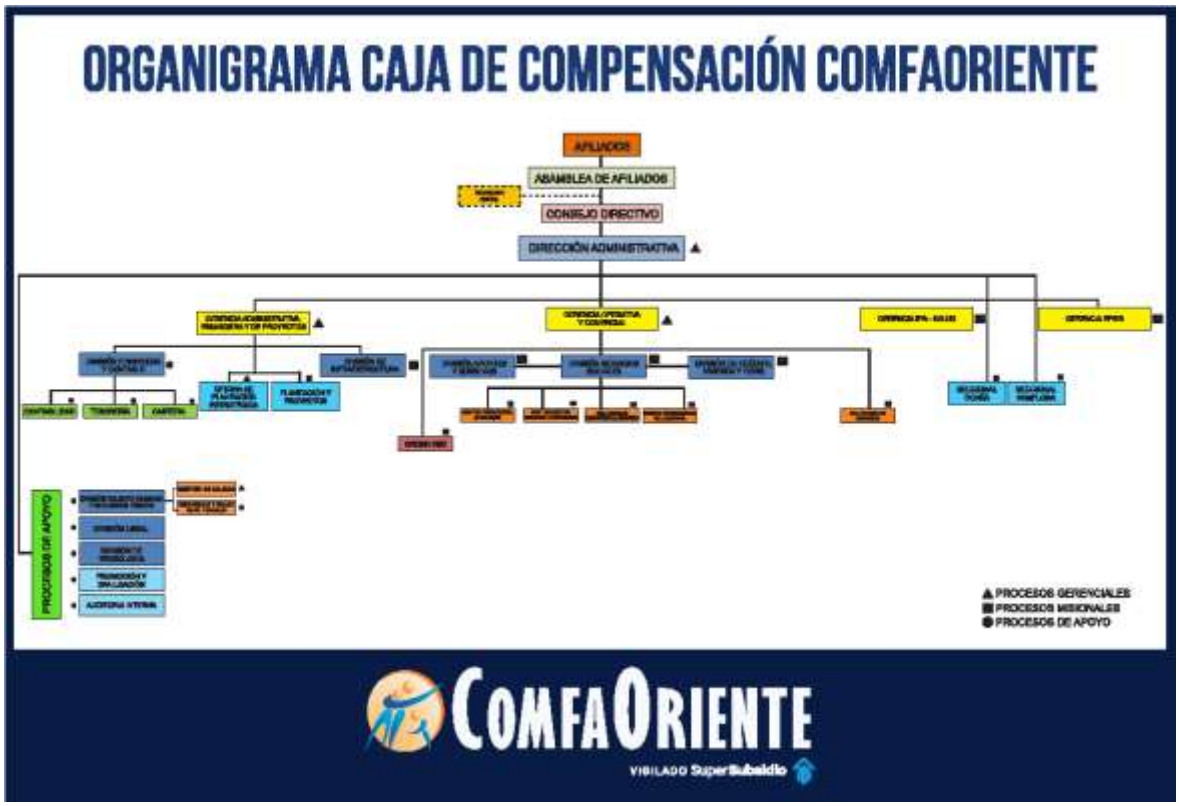
5.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO

La Caja de Compensación Familiar del Oriente Colombiano - COMFAORIENTE, es una corporación de carácter privado, sin ánimo de lucro, que cumple funciones de Seguridad Social para el mejoramiento de las condiciones de vida de trabajadores afiliados, sus núcleos familiares y la comunidad general, sometida al control del Estado a través de la Superintendencia del Subsidio Familiar, organismo creado mediante la Ley 25 de 1981 quien asesora, vigila y supervisa las actuaciones de las Cajas de Compensación y que garantiza que los recursos del 4% que aportan los empresarios con destino al pago del subsidio familiar, se administren con austeridad, eficiencia y transparencia.

Los procesos establecidos son:



La estructura organizacional está organizada de forma jerárquica, de la siguiente forma:



La empresa cuenta con una red de datos con infraestructura local, con un Data Center propio ubicado en las instalaciones físicas de la Caja de Compensación.

5.2. MISIÓN

Somos la Caja de Compensación Familiar comprometida en mejorar la calidad de vida de los trabajadores y comunidad del Oriente Colombiano, ofreciendo beneficios a través de su red de servicios integrales.

5.3. VISIÓN

Ser reconocida en el oriente colombiano como empresa líder en responsabilidad social, apoyada en talento humano con tecnología y un portafolio de servicios de alto impacto.

5.4. POLÍTICA DE CALIDAD

Mantener una actitud proactiva comprometida con el mejoramiento continuo de la organización, ofreciendo servicios integrales óptimos, asegurando la fidelidad y satisfacción de nuestros clientes.

5.5. CONOCIMIENTO DE LAS NECESIDADES DE LAS PARTES INTERESADAS

Mejorar la prestación de los servicios a los diferentes clientes (internos o externos), fortaleciendo la protección de la información en las diferentes etapas de los procesos o servicios que son entregados. Poder medir la efectividad y eficacia de los controles implementados como parte del SGSI, garantizando la seguridad y calidad de todas las partes interesadas.

Las partes interesadas están distribuidas en partes internas y externas:

- Partes interesadas internas
    - Toma de decisiones
        - Consejo Directivo
        - Dirección administrativa
    - Aplicación y ejecución de acciones de control
        - Personal interno
- Partes interesadas externas
    - Proveedores de servicio
    - Afiliados
    - Particulares
    - Entidades de control

5.6. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, establece, implementa, opera, verifica el Sistema de Gestión de Seguridad de la Información (SGSI) de estará compuesto por procesos gerenciales, misionales y de apoyo.

El proceso en el alcance es de apoyo y corresponde a:

- División de Tecnología

Así mismo, las ubicaciones del alcance son:

- Sede administrativa y de servicios: Avenida 2 #13-75 Barrio La Playa Cúcuta - Norte de Santander.

- EPS: Avenida 2 #13-55 Barrio La Playa - Cúcuta, Norte de Santander
- IPS ComfaOriente Cúcuta: Calle 16 # 1-21 Barrio la Playa - Cúcuta, Norte de Santander
- IPS ComfaOriente Sede Atalaya: Manzana 12 Lote 1 Primera etapa Atalaya - Cúcuta, Norte de Santander
- Centro Recreacional Villa Silvania: Kilómetro 4 Vía Boconó - Cúcuta, Norte de Santander
- Institución Educativa Gimnasio Campestre ComfaOriente: Kilómetro 4 Vía Boconó - Villa del Rosario, Norte de Santander
- Seccional ComfaOriente Ocaña: Calle 7 # 33-123 Barrio la Primavera - Ocaña, Norte de Santander
- Centro Recreacional ComfaOriente Ocaña: Calle 7 # 41-80 Barrio la Gloria - Ocaña, Norte de Santander
- Seccional ComfaOriente Pamplona: Carrera 7 # 5-67 Centro - Pamplona, Norte de Santander
- EPS´S ComfaOriente Pamplona: Calle 5 #6-80 Centro – Pamplona – Norte de Santander
- Seccional Tibú : Calle 8 N 5-33 El Carmen, Tibú, Norte de Santander
- Villa Chirama: K 4 NRO 26-329 Lote 2 urbanización la Italia

Finalmente, la infraestructura de Tecnología de Información en el alcance será:

- Red local COMFAORIENTE: Considera dispositivos de red, servidores, equipos de usuario y servicios que se encuentran en las ubicaciones físicas.

5.7. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

COMFAORIENTE, establece, implementa, mantiene y mejora de manera continua el Sistema de Gestión de Seguridad de la Información, de acuerdo con los requisitos de la norma ISO 27001.

6. LIDERAZGO

6.1. LIDERAZGO Y COMPROMISO

La Alta Dirección de COMFAORIENTE, declara estar comprometida con la información, como uno de sus activos más importantes, por lo tanto, manifiesta su total compromiso con el establecimiento, implementación y gestión de un Sistema de Seguridad de la Información que incluye el diseño e implementación de un plan de continuidad y recuperación ante desastres.

El Consejo Directivo y la Dirección Administrativa se encuentran en conocimiento y con interés de apoyar al cumplimiento de la implementación del SGSI, ha destinado el recurso humano y financiero para la gestión e implementación del sistema de gestión de seguridad de la información de acuerdo con su alcance definido en el punto 5.3 de este documento.

La Alta Dirección demostrará su compromiso a través de:

- La revisión y aprobación de la política contenida en este documento.
- Que las políticas y objetivos del SGSI están establecidos he integrados con los procesos de la organización.
- Que el SGSI cuenta con los recursos necesarios para lograr los resultados esperados.
- Que las personas entiendan cuán importante es realmente la seguridad de la información. Demostrar su liderazgo y compromiso con la seguridad de la información dentro de sus propias áreas.
- La divulgación de esta política a todos los funcionarios de la Caja de Compensación.

6.2. POLÍTICA GLOBAL DEL SGSI

Para COMFAORIENTE la información es un activo relevante, por lo cual existe el compromiso de protección con esta y por ende la Alta Dirección de la Caja de Compensación del Oriente Colombiano COMFAORIENTE se compromete a la implementación y mejora de un Sistema de Gestión de Seguridad de la Información, con el objetivo de minimizar riesgos, fortalecer la cultura de seguridad y garantizar el cumplimiento de los requerimientos internos o externos.

Todo el personal que tenga acceso a la información de COMFAORIENTE debe adoptar las definiciones en el marco del Sistema de Gestión de Seguridad de la Información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. La Política Global del Sistema de Gestión de Seguridad de la Información se encuentra apoyada por información documentada que da directrices sobre el manejo de la información y activos de la caja.

6.2.1. Políticas de Seguridad de la Información

Se cuenta con políticas específicas las cuales se encuentran en el documento **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PL-TEC-01**:

- Políticas de uso dispositivos móviles
- Política de uso de conexiones remotas
- Política de Seguridad del Personal
- Política de Gestión de Activos
- Política de Gestión de Control de Acceso
- Política de controles criptográficos
- Política de Seguridad física y medioambiental
- Política de Seguridad en las Operaciones
- Política de Seguridad en las Comunicaciones
- Políticas de Adquisición, Desarrollo y Mantenimiento De Sistemas De Información
- Políticas que rigen la Relación con Terceras Partes
- Políticas que Gestión de Incidentes de Seguridad

6.3. ACUERDO DE CONFIDENCIALIDAD

Todos los funcionarios y contratistas deben firmar el **ACUERDO DE CONFIDENCIALIDAD F-THR-42** que debe ser parte integral de los contratos laborales y de prestación de servicios utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplica para los casos de contratación temporal o cuando se permita el acceso a información y/o a los recursos a personas o Entidades externas.

6.4. FUNCIONES, RESPONSABILIDADES Y AUTORIDAD DE LA ORGANIZACIÓN

Dentro del Sistema de Gestión de Seguridad de la Información SGSI, está identificada la **MATRIZ DE ROLES Y RESPONSABILIDES F-TEC-16**

La Dirección Administrativa ha asignado al personal competente para la implementación y gestión del Sistema de Gestión de Seguridad de la Información, la cual se concentrará principalmente en:

- División de Tecnología
- Oficial de Seguridad de la información
- Comité de Seguridad de la información conformado por:

6.4.1. Comité de Seguridad

El comité de seguridad de COMFAORIENTE está conformado por los siguientes directivos:

- Director Administrativo
- Gerente Financiero y de Proyectos
- Jefe de División de Talento Humano y Recursos Físicos
- Jefe de División de Tecnología
- Jefe Oficina Legal
- Jefe Oficina Auditoría Interna
- Jefe Oficina Gestión de Calidad
- Profesional de Dirección
- Oficial de seguridad de la información (Ingeniero de Soporte)

Las funciones y responsabilidades del Comité de Seguridad son:

- El Comité debe asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

- Definir y aprobar las directrices, políticas y mecanismos de control y seguimiento de la Información de la Entidad de conformidad con el marco normativo vigente.

- Dentro del flujo de aprobación de las Políticas de Seguridad de la Información, el Comité de Seguridad de la Información es el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de éstas;

- Prevenir pérdidas patrimoniales o que comprometan los activos de información.

- Por medio del Comité de Seguridad de la Información se supervisa y controla el Plan de Seguridad de la Información para analizar temas tales como:

    - Revisar el avance del plan y dar directrices en caso de atrasos;

- Establecer recursos para administrar los incidentes de seguridad u otras vulnerabilidades;

- Definir proyectos de tecnología que impliquen la aplicación de Seguridad de la Información en el contexto del negocio (Servicio, Producto e Información);

- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Organización frente a posibles amenazas, sean internas o externas.

- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la Organización.

- Proveer dirección y experiencia técnica para asegurar que los activos de información se encuentren protegidos apropiadamente, sobre bajo los principios de la confidencialidad, integridad y disponibilidad.

- Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios de la Organización, sean preexistente o nuevos.

- Acompañar e impulsar el desarrollo de proyectos de seguridad.

- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Caja.

- Velar por el cumplimiento de la legislación y regulación vigente relacionada con seguridad de la información.

- Promover la concientización y formación de los empleados en materia de seguridad de la información.
- Aprobar el uso de lineamientos para el Sistema de Gestión de seguridad de la Información.

- Apoyar las revisiones anuales a Sistema de Gestión de Seguridad de la Información.

- Apoyar la definición de acciones de mejora con el Sistema de Gestión de Seguridad de Información.

- Las demás funciones inherentes a la naturaleza del Comité.

7. PLANIFICACIÓN

7.1. ACCIONES PARA ENFRENTAR LOS RIESGOS Y LAS OPORTUNIDADES

Para la identificación, categorización, valoración y tratamiento de los riesgos se definió una metodología, misma que se encuentra vigente.

7.2. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN Y LA PLANIFICACIÓN PARA ALCANZARLOS

A continuación, se detalla los objetivos de la seguridad de la información mismos que serán articulados mediante la implementación del SGSI:

- Implementar el Sistema de Gestión de Seguridad de la Información, con el objeto de disminuir los riesgos de seguridad de la Caja de Compensación Familiar Oriente Colombiano COMFAORIENTE.

- Sensibilizar a todo el personal en temas de seguridad de la información mediante el uso de herramientas digitales.

- Fortalecer las responsabilidades del personal respecto al Sistema de Gestión de Seguridad de la Información (SGSI).

8. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos es la columna vertebral de la gestión de seguridad de la información y permite a la corporación identificar sus necesidades para proteger sus activos de información y establecer los controles adecuados para mitigar dichos riesgos.

Los activos de información del SGSI de COMFAORIENTE se encuentran identificados en el inventario de activos de información de cada proceso. Por lo tanto, los procesos de la Caja de Compensación, son sometidos a un proceso de análisis y valoración de riesgos de seguridad de la información, que incluye su tratamiento y los criterios de aceptación del riesgo para identificar los niveles de riesgo aceptable. La gestión de riesgos de seguridad de la información, se lleva a cabo de acuerdo a la **GUÍA PARA LA ADMINISTRACIÓN INTEGRAL DE RIESGOS EN LOS PROCESOS**

COMFAORIENTE realiza la evaluación de los riesgos de seguridad teniendo en cuenta los numerales presentados a continuación:

8.1. RECURSOS

La Dirección Administrativa determina y proporciona los recursos necesarios para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad la Información.

8.2. COMPETENCIAS

COMFAORIENTE, mediante la División de Talento Humano y Recursos Físicos, tiene establecidas las competencias necesarias para el personal que desempeña los distintos cargos que apoyan la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información SGSI.

8.3. CONCIENTIZACIÓN

COMFAORIENTE, ha proporcionado lineamientos para definir la estrategia, medios, temas y fases de desarrollo para la sensibilización y capacitación en seguridad de la información para su personal, según **Guía del Programa de Capacitación G-TEC-02**

8.4. COMUNICACIÓN

Los lineamientos para la comunicación dependerán de la sensibilidad de la información:

- La información debe acoger los lineamientos de manejo que se establezcan acorde a la clasificación de información.

- La información que no sea de carácter público se transmitirá de forma segura.

- Si es información para terceros deberá cumplir con las definiciones de seguridad de la información considerando su entrega de manera segura y con las advertencias de seguridad.

8.5. DOCUMENTACIÓN DE LA INFORMACIÓN

La documentación de la información debe cumplir con las definiciones de manejo documental definidos en la Caja de Compensación, el cual considera lineamientos de formato, control de cambios, almacenamiento, aprobación y difusión. Algunos documentos en el marco del Sistema de Gestión de Seguridad de la Información son:

- Procedimiento de control de cambios
- Procedimiento de gestión de vulnerabilidades
- Procedimiento de gestión de medios
- Procedimiento de control de control de acceso
- Metodología de análisis y evaluación de riesgos

9. OPERACIÓN

9.1. PLANIFICACIÓN Y CONTROL OPERACIONAL

Se aplicarán las definiciones para el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información y se acogerán las prácticas necesarias para integrar las mejores prácticas aplicables a la Caja de Compensación.

9.2. EVALUACIÓN Y TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La evaluación y tratamiento de riesgos será acorde al método, métricas y zonas de riesgo definidas por COMFAORIENTE.

La evaluación de riesgo es el proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de importancia del riesgo.

El objetivo de esta evaluación es la de identificar y evaluar los riesgos. Los riesgos son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad.

El riesgo se evalúa contemplando tres elementos básicos:

a) **Estimado del valor de los activos de riesgos**: El objetivo es determinar el daño económico que el riesgo pudiera causar a los activos evaluados.

b) Probabilidad de ocurrencia del riesgo: Se lleva a cabo reuniones con los jefes del proceso con el fin de visualizar por cada activo sus impactos, amenazas y posibilidad de ocurrencia, así como las vulnerabilidades y su posibilidad de ser explotadas, determinándose la posibilidad de ocurrencia del riesgo por cada activo de información perteneciente.

c) Valoración del riesgo de los activos: Por último, se llevó a cabo la valoración del riesgo de los activos.

10. EVALUACIÓN DE DESEMPEÑO

10.1. MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUCIÓN

COMFAORIENTE ha proporcionado lineamientos para definir las necesidades que deben ser monitoreas, métodos, medición, análisis y evaluación según corresponda, con la finalidad de garantizar los resultados; además se considera también la frecuencia de monitoreo, medición, análisis y evaluación.

COMFAORIENTE evalúa el desempeño de la seriedad de la información y la eficacia del Sistema de Gestión de Seguridad de la Información.

Donde se determina:

a) A qué es necesario hacer seguimiento y qué es necesario medir, incluido los procesos y controles de la seguridad de la información.

b) Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos.

c) Cuándo se debe lleva a cabo el seguimiento y la medición.

d) Quién debe llevar a cabo el seguimiento y la medición.

e) Cuándo se deben analizar y evaluar todos los resultados del seguimiento y la medición.

f) Quien debe analizar y evaluar todos los resultados.

COMFAORIENTE conserva la información documentada apropiada como evidencia de los resultados del monitoreo y la medición.

10.2. AUDITORIAS INTERNAS

COMFAORIENTE, mediante el plan de auditoría anual articula la planificación y ejecución de la auditoría interna que apoya a la identificación del cumplimiento del SGSI de acuerdo con la norma y que contribuye a asegurar la eficiencia, eficacia y efectividad del SGSI

10.3. REVISIÓN POR PARTE DE LA DIRECCIÓN

La Dirección Administrativa revisará el Sistema de Gestión de Seguridad de la Información mediante los resultados de las auditorías internas, externas, y los seguimientos realizados por el Comité de Seguridad de la Información. Los temas para considerar son:

- Estatus de las acciones de las anteriores revisiones de la Dirección Administrativa.
- Cambios significativos que afectaron al SGSI.
- No conformidades identificadas por las auditorias.
- Indicadores de cumplimiento del SGSI.
- Evaluaciones de Riesgos.
- Oportunidades de mejora.
- Resultados de las decisiones tomadas.

11. MEJORA

Este Manual es de aplicación inmediata y continua, desde el momento de su divulgación y socialización dentro de la Caja de Compensación. Este documento se actualizará por lo menos una (1) vez cada dos (2) años o cuando se presenten cambios significativos en la organización o las directrices gubernamentales que sean aplicables en cada caso.

COMFAORIENTE, mediante el tratamiento de riesgos garantizará las acciones necesarias para mitigar riesgos y no conformidades obtenidas de las auditorias, así como también la mejora continua de los controles de seguridad y del SGSI en general.

El proceso de mejora significa integrar de manera sistemática los procesos de mejora del SGSI dentro de los procesos normales de revisión de la Caja de Compensación. Se trata de que en las reuniones de revisión el SGSI tenga también un papel importante para demostrar el liderazgo efectivo sobre el mismo y su preocupación en la mejora del sistema y de la seguridad de la información.

En el proceso de mejora continua también están involucrados los procesos de comunicación y establecimiento de la cultura de la seguridad ya que la participación activa de todo el personal es un factor crucial en la mejora de un SGSI.