MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA CAJA DE COMPENSACIÓN FAMILIAR DEL ORIENTE COLOMBIANO.

COMFAORIENTE.

TABLA DE CONTENIDO.

1. INTRODUCCIÓN

El modelo de seguridad de la información de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE se elaboró con base en las mejores prácticas, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma técnica ISO/IEC 27001:2013, el cual especifica los requisitos para establecer, implementar, mantener y mejorar de una manera continua el sistema de gestión de seguridad de la información dentro del contexto de la Corporación.

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, la cual tiene un compromiso con el cumplimento de las leyes, normas y requisitos aplicables con respecto a la seguridad de la información, con el fin de contribuir a desarrollo transparente de la Corporación y la gestión del riesgo digital en el entorno del ciberespacio.

El desarrollo e implementación del modelo de seguridad de la información de COMFAORIENTE 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 MSPI de COMFAORIENTE se encuentra alineado modelo de arquitectura de control y promueve la preservación de los tres pilares fundamenta de la seguridad de la información; Confidencialidad, Integridad y Disponibilidad, permitien

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 lo información.

Finalmente, el MSPI de COMFAORIENTE pretende dar un enfoque de compromiso hacia la seguridad de la información desde del alto nivel de la Corporación pasando por todos los procesos de la cadena de valor para que cada funcionario tenga claridad de los objetivos que se deben cumplir.

2. OBJETIVOS

2.1. Objetivo General.

Implementar el Modelo de Seguridad Y Privacidad de La Información (MSPI) de La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, para soportar los procesos de la Corporación y la interacción con los proveedores críticos de la cadena de suministro en donde se cree, transfiera, almacene y procese información y así garantizar su confidencialidad, integridad y disponibilidad.

2.2. Objetivos Específicos.

- Promover el uso de buenas prácticas de seguridad de la información a nivel interno y externo para proteger la información de la Corporación.
- Establecer la política general de seguridad de la información de COMFAORIENTE y las políticas específicas que soporten su cumplimiento mediante la aplicación de controles para gestionar los riesgos de seguridad de la información.
- Gestionar de manera adecuada y monitorear continuamente los riesgos de seguridad de la información que se presenten tanto en el contexto interno como externo incluyendo los servicios prestados por proveedores críticos con el fin de proteger la información y los datos de la corporación.
- Dar los lineamientos y los recursos necesarios para que todos los funcionarios de COMFAORIENTE y sus partes interesadas estén capacitados y cumplan con las políticas de seguridad de la información.

3. ALCANCE

La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, define dentro del alcance de su Modelo de Seguridad Y Privacidad de La Información (MSPI): Gestionar integralmente los riesgos de seguridad de la información para contribuir al cumplimiento de los objetivos estratégicos y metas de la Corporación.

El MSPI de la COMFAORIENTE incluye políticas de seguridad de la información y controles que están soportados por procedimientos, los cuales apoyan los procesos de la Corporación en materia de seguridad informática.

El presente modelo es adoptado y sus políticas aplican para todos los funcionarios en todos los niveles y partes interesadas incluyendo proveedores de COMFAORIENTE 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 MSPI, así mismo, cumplir con las políticas establecidas desde el comité de seguridad de la información de COMFAORIENTE que soportan el presente modelo.

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Constitución Política. 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 20 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías 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 3995 DE 2020 Política Nacional de Confianza y Seguridad Digital.

CONPES 4069 de 2021 Política Nacional de Ciencia, Tecnología E Innovación 2022-2031.

5. TÉRMINOS Y DEFINICIONES.

Análisis de Riesgo: Proceso para analizar los peligros que plantean los eventos de causa natural y humana a los activos de una organización.

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.

Área Segura: Espacio físico donde se almacena o procesa información crítica de la Corporación.

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.

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 Corporación 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 q causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

DDoS: Es similar al DoS pero este se origina des múltiples y coordinadas fuentes.

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

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.

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 del mismo.

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

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, demostrando liderazgo y compromiso con la implementación de un SGSI basado en la norma ISO/IEC 27001 ha organizado un comité de seguridad de la información, el cual, tiene el objetivo de gestionar bajo un enfoque basado en riesgos la seguridad de la información de la organización.

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:

La Corporación con el fin de formalizar los roles y responsabilidad de seguridad de la información ha formalizado la **MATRIZ DE ROLES Y RESPONSABILIDADES F-TEC-16**

El comité de seguridad de la información de COMFAORIENTE está integrado por las siguientes personas, según sus cargos en la corporación:

- 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 e Ingeniero de Soporte Salud)

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 información a través de todo el organismo.
- Definir y aprobar las directrices, políticas y mecanismos de control y seguimiento 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;
- Proporcionar los recursos para la adecuada implementación de la seguridad de la información.
- Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de 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.
- Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de negocio de la Caja.
- Impulsar el desarrollo de proyectos de seguridad.
- Asegurar que las implementaciones de los diferentes controles cumplan con la función esperada en materia de seguridad de la información.
- 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 las obligaciones regulatorias en materia de seguridad de la información.
- Promover la concientización y formación de los empleados en materia de seguridad de la información.
- Aprobar la implementación de las nuevas iniciativas para la mejora continua del Sistema de Gestión de seguridad de la Información.
- Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.
- Revisar, evaluar los incidentes de seguridad de la información y monitorear el proceso de respuesta.
- Apoyar las revisiones anuales al Sistema de Gestión de Seguridad de la Información.
- Apoyar la definición de acciones de mejora con el Sistema de Gestión de Seguridad de Información.
- Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.
- Las demás funciones inherentes a la naturaleza del Comité.

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

- Velar por el desarrollo de los objetivos estratégicos para la seguridad de información, definidos por el consejo de administración.
- 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 correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información
- Designar los responsables de la implementación de la política de seguridad de la información.
- Presentar un informe periódico, como mínimo cuatrimestral, a la División Servicios Sociales sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.

El comité de seguridad de la información por intermedio de la secretaria técnica convocará a los integrantes del comité de seguridad de la información a las sesiones ordinarias que se llevaran a cabo cada 4 meses y a las sesiones extraordinarias cuando la corporación lo demande.

Funciones del secretario técnico:

- Elaborar un informe periódico, como mínimo cuatrimestral, al Jefe de División de Tecnología sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y 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.
- Elaborar las actas de reunión del Comité oportunamente.
- Enviar la agenda a los miembros 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.
- Firmar las actas que hayan sido aprobadas.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- Las demás que le sean asignadas por el Comité.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información, general y las específicas, fueron revisadas y aprobadas por el Comité de Seguridad de la Información del para su entrada en vigencia.

7.1. Política General de Seguridad de la Información

Objetivo de la política:

La presente política establece los lineamientos generales sobre la gestión integral de la seguridad y privacidad de información como directriz general del Modelo de Seguridad y Privacidad de la Información (MSPI) de La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE.

Aplicabilidad de la política:

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

Lineamientos:

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 continua de un Sistema de Gestión de Seguridad de la Información, con el objetivo de minimizar riesgos asociados, fortalecer la cultura de seguridad medio del aprovechamiento de la tecnología, innovación y gestión del conocimiento.

La Corporación incluye la gestión del cumplimiento y de la conformidad sobre los requisitos aplicables al sector, tanto del ordenamiento jurídico pertinente, como contractual y técnico, priorizando los aspectos de privacidad, transparencia y nivel de servicio, así como la protección adecuada de información de carácter personal y reservado.

Todo el personal que tenga acceso a la información de COMFAORIENTE debe adoptar los lineamientos establecidos en el marco del Sistema de Gestión de Seguridad de la Información, con el fin de proteger su confidencialidad, integridad y disponibilidad.

La Política General del Sistema de Gestión de Seguridad de la Información se encuen apoyada por información documentada que da directrices sobre el manejo de la informació activos de la Caja De Compensación Del Oriente Colombiano.

7.2. Política para los Dispositivos Móviles.

Objetivo de la política:

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

Aplicabilidad de la política:

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

Lineamientos:

- COMFAORIENTE, proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la caja; así mismo, velará porque el personal interno o externo haga un uso responsable de los servicios y equipos proporcionados
- Se debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la caja.
- No se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).
- Se debe contar con una opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Se debe contar con una solución de copias de seguridad para la información conteni en los dispositivos móviles de la caja.
- Se debe evitar la instalación de programas desde fuentes desconocidas.
- Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo manera automática y manual.

- Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la Corporación, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la Corporación.
- Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata a la División de Talento Humano y Recursos Físicos y a La División de Tecnología y continuar con el procedimiento administrativo por perdida de elementos establecido por la Corporación.
- Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).

Excepciones a la política: N/A

7.3. Política de Teletrabajo y Trabajo en Casa.

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.

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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 para la Corporación.

Lineamientos:

- COMFAORIENTE, definirá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.
- El trabajo 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, desastr naturales tales como terremotos, inundaciones, incendios y otros que a criterio de gerencia de la Corporación ameriten que se realicen las actividades laborales des casa.

- 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 COMFAORIENTE.
- Se debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Se deben establecer conexiones remotas solo en computadores previamente identificados y registrados.

Excepciones a la política: N/A

7.4. Política de Control de Acceso.

Objetivo de la política:

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

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, 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.

7.4.1. Acceso a Redes y Recursos de red.

Lineamientos:

- El acceso lógico para los usuarios internos y externos (incluidos contratistas) a la plataforma tecnológica, recursos de red y sistemas de información se garantizará de acuerdo a los roles y perfiles de cada usuario establecido por el jefe de la unidad solicitante y previa firma del contrato y cláusula de confidencialidad y no divulgación.
- Se establecen controles para proteger el acceso a las redes de datos y los recursos de red de la caja los cuales incluyen controles físicos y lógicos.
- Las redes inalámbricas de la corporación deben contar con métodos de autenticación y protocolos seguros para evitar accesos no autorizados.
- Se debe verificar periódicamente los controles de acceso para los usuarios internos y externos (incluidos contratistas), con el fin de revisar que estos tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- El personal interno y externo (incluidos contratistas) deben cumplir con todos los requisitos o controles para autenticarse en la red o en sus recursos y únicamente realizar las tareas para las que fueron autorizados.

7.4.2. Gestión de Accesos al Usuario.

Lineamientos:

- COMFAORIENTE, establece privilegios para el control de acceso lógico de cada usua o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas

información, a través de normas y procedimientos que limiten la asignación de derechos para velar porque el personal interno o externo tenga acceso únicamente a la información necesaria para el desarrollo de sus labores.

- Se establece un procedimiento formal para la administración de los usuarios en la red, los recursos tecnológicos y sistemas de información, el cual contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario. **Procedimiento de Control de Acceso a los Sistemas de Información P-TEC-05**.
- Se crea, modifica, bloquea o elimina cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- Se definen lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información; dichos lineamientos deben considerar por lo menos aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso.
- Se deben otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo al personal designado para dichas funciones.
- Se limita las conexiones remotas en los recursos de la plataforma tecnológica únicamente a personal autorizado, de acuerdo con las labores desempeñadas.
- Se asegura que los usuarios o perfiles por defecto de sistemas operativos, firmware y bases de datos sean suspendidos o renombrados y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- El personal interno o externo deben responsabilizarse de las acciones realizadas con los accesos asignados a los servicios de red y sistemas de información.
- Los funcionarios, contratistas y demás colaboradores, que tengan bajo su responsabilidad la custodia de la información física almacenada en los archivadores que se encuentra en las oficinas, deben mantener el control de acceso a esta información, considerándose está un área segura, por tanto, debe cumplir con el **Procedimiento para Áreas Seguras P-TEC-06**; Las llaves se deben guardar en un sitio seguro, bajo la custodia de las personas que la dependencia que se estime conveniente.
- El personal interno y externo (incluidos contratistas) NO puede compartir sus cuentas de usuario y contraseñas, estas son para uso personal e intransferibles.
- El personal interno o externo deben acoger los lineamientos definidos para la configuración de contraseñas seguras.

7.4.3. Control de Acceso a Sistemas y Aplicativos.

Lineamientos:

- COMFAORIENTE, velará por la asignación, modificación y revocación de privilegios accesos a sus sistemas o aplicativos de manera controlada, velando porque estos se

debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

- Se establece el procedimiento para la asignación de accesos a los sistemas y aplicativos de la caja. **Procedimiento de Control de Acceso a los Sistemas de Información P-TEC-05** el cual debe ser seguido para la asignación y control de acceso a los sistemas de información de la corporación.
- Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.
- Se debe asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

Excepciones a la política: N/A

7.5. Políticas de Creación y Uso de Contraseñas.

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.

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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.

Lineamientos:

- Ningún usuario deberá acceder a la red o a los servicios de COMFAORIENTE, utilizando una cuenta de usuario o clave de otro usuario, estas son para uso personal e intransferibles.
- Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó la clave.
- COMFAORIENTE suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible, según lo indicado en el **Procedimiento de Control de Acceso a los Sistemas de Información P-TEC-05**
- El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta, en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato comunicándose con la División de Tecnología.
- Las contraseñas de los sistemas de información tienen una vigencia de máximo 120 días.
- Las claves o contraseñas deben:
    - Tener mínimo ocho (10) caracteres alfanuméricos y cumplir con los siguientes requisitos:
        - Caracteres en mayúsculas
        - Caracteres en minúsculas
        - Base de 10 dígitos (0 a 9)
        - Caracteres no alfabéticos (Ejemplo: ¡,$, %, &)

7.5.1. Gestión de contraseñas para administradores de tecnología.

Lineamientos:

- Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
- El personal de la División de Tecnología **NO** debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Jefe de la División de Tecnología.
- Los usuarios y claves de los administradores de sistemas y del personal de la División de Tecnología son de uso personal e intransferible y deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y/o utilizar los servicios de autenticación fuerte de acuerdo al rol asignado.

Excepciones a la política: N/A

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

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.

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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.

Lineamientos:

- COMFAORIENTE para todos sus sitios web bajo el dominio comfaoriente.com utiliza los certificados SSL emitido por una autoridad certificadora reconocida con el fin de para garantizar la autenticidad del sitio, proteger los datos y cifrar la comunicación entre el cliente y el servidor web.
- Para el caso del acceso remoto a la infraestructura de TIC y sistemas e información, el acceso se debe realizar a través de VPN site to client utilizando protocolos seguros (SSL, IPSec) para establecer la conexión.
- Los equipos de cómputo y unidades de almacenamiento 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.
- La gestión de las llaves de cifrado está a cargo de la División Tecnología.
- Las copias de seguridad de los archivos y sistemas de información críticos de la corporación deberán incorporar protocolos seguros de cifrado.

Excepciones a la política: N/A

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

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.

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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.

Lineamientos:

- En los equipos de cómputo, 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.
- En cuanto a archivos digitales y enlaces, si bien se pueden mantener (de forma temporal) algunos ejemplares en el escritorio, la carpeta de descargas y de documentos, éstos deben ser eliminados o archivados donde corresponde cuando finalice su procesamiento o sea necesario que la persona a cargo se retire de la estación de trabajo, así sea solo momentáneamente.
- 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.
- Cada usuario debe asegurar que el acceso al equipo de cómputo quede bloqueado y protegido contra acceso no autorizado cuando el equipo este desatendido.
- Se debe configurar el bloqueo por inactividad en los equipos de cómputo de COMFAORIENTE. Este tiempo está establecido por política en el Controlador dominio y no debe ser superior a 5 minutos.

Excepciones a la política: N/A

7.8. Política de Protección Contra Código Malicioso y Antimalware.

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.

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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 equipos de cómputo y sistemas informáticos de la Corporación.

Lineamientos:

- COMFAORIENTE administra el antivirus con funciones de antimalware, antispam, antispyware, entre otras, como herramienta para reducir el riesgo de infección de software malicioso y el Backup respalda la seguridad de la información contenida y administrada en la plataforma tecnológica de información y los servicios que se ejecutan en la misma.
- Se deben proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la caja y los servicios que se ejecutan en la misma.
- Se debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- Se debe configurar la solución de antivirus de manera que genere registros de auditoría y asegure que esos registros se administren conforme se establezca; los registros de auditoría proporcionan la capacidad de supervisar actividad de virus y reacciones antimalware.
- Se debe asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abier o ejecutados por primera vez, especialmente los que se encuentran en medios almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónic descargados de internet o copiados de cualquier medio de almacenamiento, provien

de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área de soporte de la División Tecnología. A través de los canales de atención disponibles.

Excepciones a la política: N/A

7.9. Política de Instalación de Software.

Objetivo de la política:

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

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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

Lineamientos:

- COMFAORIENTE proporciona al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de COMFAORIENTE, la copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Caja de Compensación no están autorizados.
- Periódicamente, la División de Tecnología podrá realizar la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos, software no licenciado o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de COMFAORIENTE.
- 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 critico 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 ter deshabilitada la opción de instalación de software.
- Toda instalación o actualización de software se debe hacer con permisos 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.
- Los recursos informáticos de COMFAORIENTE NO podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas y software malicioso (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la División de Tecnología:
    - Instalar software en cualquier equipo de COMFAORIENTE.
    - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la Caja.
    - Modificar, revisar, transformar o adaptar cualquier software propiedad del COMFAORIENTE.
    - Descompilar o realizar ingeniería inversa en cualquier software de propiedad de COMFAORIENTE.
    - Copiar o distribuir cualquier software de propiedad de COMFAORIENTE.
    - Cambiar la configuración de hardware de propiedad de COMFOAORIENTE.
- El usuario deberá informar a División de Tecnología de COMFAORIENTE a través del Software de Solicitudes Informáticas o a través del correo electrónico sistemas@comfaoriente.com, y al Jefe Inmediato, sobre cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de COMFAORIENTE que tenga conocimiento.
- Los usuarios NO están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la Corporación (modem USB, router, wifi público, etc), esto compromete la seguridad de los recursos informáticos de COMFAORIENTE.
- Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, es revisado por el antivirus institucional para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura de COMFAORIENTE.

Excepciones a la política: N/A

-

7.10. Política de Copia de Respaldo

Objetivo de la política:

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

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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.

Lineamientos:

- COMFAORIENTE, proporciona los recursos en términos de personal y procesos para diariamente generar el respaldo o copia de seguridad de los archivos y sistemas de información críticos para los procesos de la Corporación, siguiendo lo establecido en el procedimiento; **REALIZACION DE COPIAS DE SEGURIDAD DE BASE DE DATOS Y ARCHIVOS DE USUARIOS P-TEC-04**.
- De la misma manera COMFAORIENTE suministra una respuesta efectiva en caso de contingencia o eventos que afecten la continuidad de la operación, con el fin de reestablecer las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos, según el **Manual de Continuidad del Negocio COMFAORIENTE M-TEC-16**
- Es responsabilidad de cada funcionario de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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 Google Drive, el correo electrónico corporativo.
- El período mínimo para la ejecución de copias de seguridad es diario.
- 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 med diferentes y uno de ellos se encuentra en un lugar externo a las instalaciones principal de procesamiento de información de COMFAORIENTE.

- Se conservarán históricos de los Backus realizados diariamente de las bases de datos de la siguiente manera: se mantendrá la copia diaria de los últimos dos meses; excluyendo estos dos meses, una semanal del último año, excluyendo los dos meses y el año anterior una copia por mes durante de los últimos dos años.

Excepciones a la política: N/A

-

7.11. Política de Seguridad para la Transferencia de Información.

Objetivo de la política:

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

Aplicabilidad de la política:

La presente política aplica para todas las partes interesadas, en todos los niveles de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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.

Lineamientos:

- COMFAORIENTE, asegurará la protección de la información en el momento de ser transferida o intercambiada con terceros y partes interesadas, por lo tanto, establecerá los procedimientos, controles y acuerdos de confidencialidad o de intercambio de información necesarios, con el fin de mitigar los riesgos asociados a dichos intercambios.
- No está permitido que ningún funcionario y/o terceros de La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE 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 Entidad 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 Oriente Colombiano. COMFAORIENTE 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, 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)
- Se deben establecer acuerdos de transferencia de información entre la Corporación y partes externas las cuales deben incluidas contractualmente y estar soportadas como mínimo por la 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 Oriente Colombiano. COMFAORIENTE y partes externas, de acuerdo al contexto y dando cumplimiento a la normatividad vigente aplicable.
- La transferencia de información de carácter reservado y confidencial no está permitida por medio de correo electrónico corporativo, la demás información de la Corporación transferida por este medio debe estar acompañada por el aviso de confidencialidad y tratamiento de datos personales.
- Todos los equipos de cómputo de escritorio deberán tener deshabilitados los puertos USB, y la unidad óptica solo cumplirá la función de lectura.

Excepciones a la política: El lineamiento que trata acerca de que “Todos los equipos de cómputo de escritorio deberán tener deshabilitados los puertos USB, y la unidad óptica solo cumplirá la función de lectura” se aplica únicamente al grupo de usuarios que hacer parte del grupo “Bloqueo_USB” y este control está configurado por medio de una política en el controlador de dominio.

.

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

Objetivo de la política:

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

Aplicabilidad de la política:

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

Lineamientos:

- COMFAORIENTE, establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, den cumplimiento con las políticas, normas y procedimientos de seguridad de la información.
- 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 de la información y establecer controles para garantizar la confidencialidad, integridad y disponibilidad de la información que gestiona.
- Todo acuerdo, contrato o similar, propuesta comercial que requiera de manera previa la transferencia información sensible o de negocio, 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, con proveedores críticos de tecnología deberá incorporar requisitos de control y audibilidad según el riesgo, con el fin de evaluar la aplicación de los lineamientos y controles de seguridad de la información acordados para la prestación del servicio contratado.
- Se deben identificar y monitorear los riesgos relacionados con terceras partes o servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suminis de los servicios de tecnología o comunicaciones provistos.
- Se deben mitigar los riesgos relacionados con terceras partes que tengan acceso a sistemas de información y la plataforma tecnológica.

- Se deben gestionar de manera adecuada la información recibida, en cumplimiento de las políticas de seguridad, procedimientos y las condiciones contractuales establecidas.
- Ante la terminación de la relación contractual, el proveedor debe garantizar la destrucción y/o borrado seguro de la información suministrada, evidenciando la realización de estas actividades según las mejores prácticas dadas por NIST SP 800-88.

Excepciones a la política: N/A

7.13. Política de desarrollo Seguro.

Objetivo de la política:

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

Aplicabilidad de la política:

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

Lineamientos:

- COMFAORIENTE asegurará que el software adquirido y desarrollado cumplirá con los requisitos de seguridad y calidad establecidos a través de la definición de requisitos formales que aseguren su cumplimiento, con el fin de mitigar vulnerabilidades inherentes al desarrollo o mantenimiento de software.
- Se deben establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- Se deben establecer las especificaciones de seguridad en la adquisición o desarrollo de sistemas de información.
- Se deben realizar las pruebas para asegurar que los sistemas cumplen con los requerimientos de seguridad establecidos antes de su paso a producción.
- Se debe asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- Todo desarrollo, mantenimiento, prueba, implementación o cambio de software de incluir la definición o aplicación de requisitos de seguridad según los riesg identificados.
- En el caso que el proveedor no especifique requisitos de seguridad en el software, Corporación deberá establecer un estándar mínimo de requisitos de seguridad

aplicarlos basados en las buenas prácticas actuales para el SSDLC (Ciclo de Vida de Desarrollo Seguro de Sistemas).

7.13.1. Desarrollo Seguro, Pruebas y Soporte de los Sistemas.

Lineamientos:

- COMFAORIENTE, velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados y con las buenas prácticas para desarrollo seguro dentro del ciclo de vida de desarrollo de software, según el **Manual para la Implementación del Ciclo de Vida del Desarrollo Seguro de Software y el Procedimiento de Desarrollo de Software P-TEC-01.**

Excepciones a la política: N/A

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

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.

Aplicabilidad de la política:

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

Lineamientos:

- 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.

Excepciones a la política: N/A

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

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.

Aplicabilidad de la política:

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

Lineamientos:

- De acuerdo al ciclo de vida de la información, COMFAORIENTE 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 o reutilizados por otro usuario.
- 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 seguirán el procedimiento estipulado para tal fin de acuerdo a la tecnología y clasificación de la información a eliminar.

Excepciones a la política: N/A

7.16. Política de Registro De Eventos Y Monitoreo.

Objetivo de la política:

Asegurar que las fuentes de registro de eventos de los sistemas de información, sistemas operativos, aplicaciones y redes sean protegidas y se almacenen de forma segura con el fin estar disponibles para su revisión, correlación y verificación de las actividades de los usuarios.

Aplicabilidad de la política:

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

Lineamientos:

- Se deben determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
- Se deben implementar pistas de auditoría para registrar los accesos a los componentes del sistema; estas pistas de auditoría deben registrar los accesos a componentes del sistema para cada uno de los usuarios.
- Se deben definir los roles y responsabilidades respecto al monitoreo de eventos, así como, la periodicidad de revisión de estos.
- Se deben velar por la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la caja. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
- La infraestructura de TI, red y los sistemas de información deben tener sincronizados los relojes con una única fuente de referencia de tiempo.
- En los eventos registrados deben contener la identificación de usuarios, el tipo de evento, la fecha y hora, la indicación de éxito o fallo, el origen del evento y el nombre de los datos, componentes del sistema o recursos afectados.

Excepciones a la política: N/A

7.17. Política de Gestión de Incidentes de Seguridad de la Información.

Objetivo de la política:

Establecer los lineamientos para una gestión de intendentes de seguridad de la información eficaz que permita responder ante las amenazas y la materialización de riesgos relacionados con la seguridad de la información en COMFAORIENTE.

Aplicabilidad de la política:

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

Lineamientos:

- COMFAORIENTE, promoverá entre el personal interno y provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas, según **Procedimiento para Gestión de Incidentes. P-TEC-07.**
- Se debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Se deben evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar aquellos en los que se considere pertinente.
- Se debe crear una base de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
- Se debe mantener al tanto al Comité de Seguridad de la Información de los incidentes de seguridad de la información recibidos.
- Es responsabilidad del personal interno y provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

Excepciones a la política: N/A

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN.

La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, ha determinado un procedimiento formal para la gestión de activos, el cual busca asegurar la gestión eficaz de los 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 A.8.2.1 de ISO/IEC 27001:2013 y los lineamientos normativos aplicables, y considerará la guía 5 del MSPI en términos de requisitos[1], valor[2],

[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.

criticidad[3] y sensibilidad[4] a su divulgación (confidencialidad) o modificación no autorizados, considerando la siguiente tabla:

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

[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:

- 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 excepciones del título III "Excepciones acceso a la información", asegurando la disponibilidad de la información se 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 dentr 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)

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		

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:

a. Manejo de activos [control A.8.2.3 de la norma ISO/IEC 27001:2013]: Según el tipo de activos, se tiene el siguiente enfoque:

I. 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 el decreto 2609/2012 posteriormente compilado en el decreto 1080/2015 sobre la convergencia de los archivos soporte físico o digital) y su tratamiento unificado, así como lo referente a documentos y mensajes de da electrónicos (Ley 527/1999) en especial el Título II "Patrimonio archivístico" Cap. V "Gestión de documentos" y Cap. "La Gestión de Documentos Electrónicos de Archivo".

- La gestión de activos incluirá al programa 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 programa de gestión documental[10]
- Los activos de información estarán sujetos a la clasificación de activos de información definida en así como con el cuadro de clasificación documental que haya definido y aprobado la Corporación, 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.
- El etiquetado de información [control A.8.2.2 de la norma ISO/IEC 27001:2013] seguirá los esquemas de clasificación de la información adoptados por la Corporación, es decir:
  (a) En 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;
  (b) En archivo en 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 organización 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

[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 Gest 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 2002 y decreto 1080/2015 Art. 2.8.2.2.2. “Elaboración y aprobación de las tablas de retención documental y las tab de valoración documental”.

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 en su posesión al terminar su empleo, contrato o acuerdo [control A.8.1.4 de la norma ISO/IEC 27001:2013] como requisito para la liquidación y finalización del contrato, y de ello será evidencia de cumplimiento el inventario documental (de información).

II. 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 (a) desarrollo, adquisición y mantenimiento de sistemas; (b) de comunicaciones; (c) operacional; (d) áreas físicas.

b. El uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de información [control A.8.1.3 de la norma técnica ISO/IEC 27001:2013] estará basado en las siguientes reglas:

- Todo uso de activos, de información como aquellos relacionados con ella, será permitido siempre y cuando esté orientado a la consecución de los objetivos de negocio y de seguridad de la información 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 carácter o con fines 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

[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. … “Transferencias Secundarias”, Capítulo X “Transferencia de documentos de las demás ramas del poder público y de 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. … “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

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.

a. El inventario de activos [control A.8.1.1 de ISO/IEC 27001:2013] 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]

b. 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.
- 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)

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

- Hardware e infraestructura: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos. Aquí es importante considerar la configuración como activo de información.

- Clasificaciones 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.

c. Cada uno de los activos indicados en el inventario de activos debe indicar el propietario de los activos [Control A.8.1.2 de la norma ISO/IEC 27001:2013] 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.

a. Gestión de medios removibles [Control A.8.3.1 de la norma ISO/IEC 27001:2013]

- Los medios removibles serán permitidos, en cada caso, según la política de medios y la clasificación de activos de información.
- Está prohibido el uso de medios removibles salvo autorización expresa por parte de 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.
- 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 no vaya a ser más utilizado (por capacidad, daño o cualquier otra razón) deberá ser entregado a la persona formalmente autorizada, quien procederá a su eliminación [Control A.8.3.2 de la norma ISO/IEC 27001:2013] de forma segura.
- No está permitido la reutilización de medios removibles o su obsequio a otras partes interesadas.
- Los medios que contengan información deben ser protegidos contra acceso no autorizado, mal uso o daño, durante su transporte (Transferencia física de medios [Control A.8.3.3 de la norma técnica ISO/IEC 27001:2013]).
- 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 para tal fin haya definido la Corporación.

b. 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 A.18.1.3 de la norma ISO/IEC 27001:2013].

8.5. Gestión y remoción de equipos.

a. 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;

b. 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; remoción de tales equipos será realizado de forma exclusiva por las personas delegac para tal fin quienes deberán realizar el desensamble seguro de sus piezas y borrado segu de aquellos elementos que pudiesen contener información, en especial discos duros; U

vez finalizada esta etapa, se deberá proceder a su reciclado con un proveedor especializado que cuente con la licencia ambiental pertinente.

9. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE gestiona los riesgos de seguridad de la información de todos los procesos que se desarrollan dentro de las unidades de negocio a través del programa de gestión de riesgo empresarial el cual está basado en la norma ISO: 31000:2018.

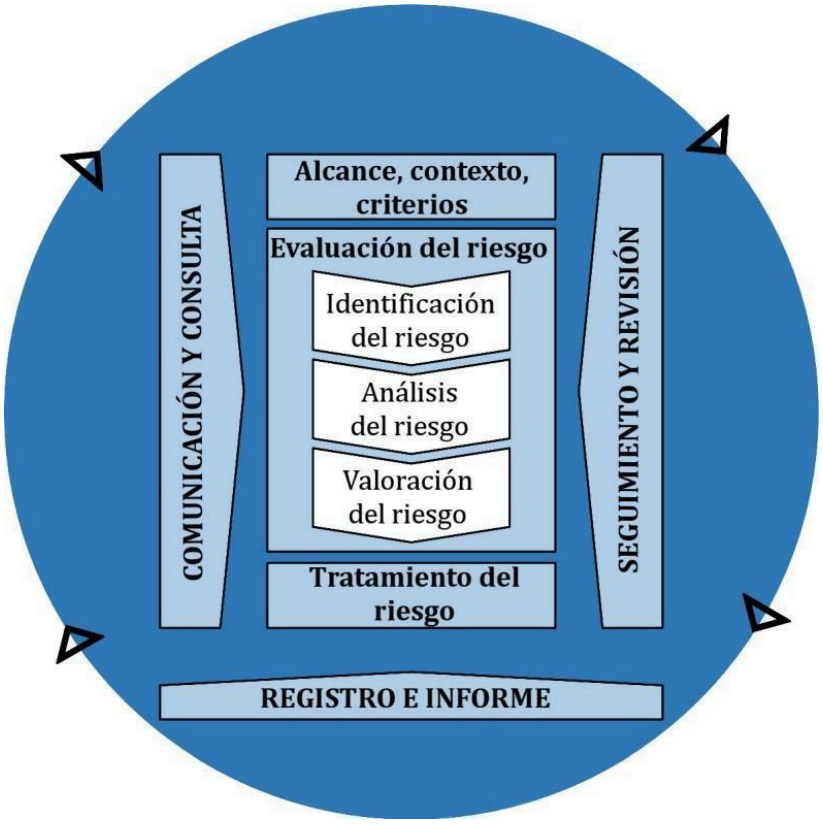

Ilustración 1. Procesos de la metodología de gestión de riesgos.

La metodología de gestión de riesgos y los procedimientos que están implementados en la Corporación están establecidos en el **Instructivo de Gestión del Riesgo I-AUD-02**, en el cual se abordan los riesgos de tecnología con el fin de mantener la capacidad de la Corporación para que la tecnología disponible satisfaga las necesidades actuales y futuras COMFAORIENTE y soporte el cumplimiento de la misión.

Causas (factores internos o externos): son los medios, las circunstancias y agent generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos

objetos que tienen la capacidad de originar un riesgo; se pueden clasificar en cinco categorías: personas, materiales, Comités, instalaciones y entorno.

Efectos (consecuencias): constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Impacto: la escala de valoración de impacto es Leve (5), Moderado (10) y Catastrófico (20).

Frecuencia: la escala de valoración de frecuencia es Baja (1), Media (2), y Alta (3).

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Determinar las causas (factores internos o externos) de las situaciones identificadas como riesgos para la entidad.
- Describir los riesgos identificados con sus características.
- Precisar los efectos que los riesgos puedan ocasionar a la entidad.

9.1. Análisis del riesgo.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la información obtenida en el formato de identificación de riesgos y la disponibilidad de datos históricos y aportes de los servidores de la entidad.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, *Probabilidad e Impacto.* Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de *Frecuencia*, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de *Factibilidad* teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por *Impacto* se entiende las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos:

- La *Valoración del Riesgo:* se logra a través de la estimación de la probabilidad de ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa número de veces que el riesgo se ha presentado en un determinado tiempo o pue

presentarse, y la segunda se refiere a la magnitud de sus efectos. Para efectos de la matriz se puede entender como ***Impacto X Frecuencia (ver tabla 1).***

Se debe calificar cada uno de los Riesgos según la matriz de acuerdo con las siguientes especificaciones*: Frecuencia Alta* se califica con 3, *Frecuencia Media* con 2 y *Frecuencia Baja* con 1, de acuerdo con el número de veces que se presenta o puede presentarse el riesgo. Y el *Impacto* si es *Leve* con 5, si es *Moderado* con 10 y si es *Catastrófico* con 20.

- La *Evaluación del Riesgo:* permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para realizar la Evaluación del Riesgo se debe tener en cuenta la posición del riesgo en la Matriz, según la celda que ocupa, aplicando los siguientes criterios:

Si el riesgo se ubica en la Zona de Riesgo Aceptable (calificación 5), significa que su *Frecuencia* es baja y su *Impacto* es leve, lo cual permite a la Entidad asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Si el riesgo se ubica en la Zona de Riesgo Inaceptable (calificación 60), su *Frecuencia* es alta y su *Impacto* catastrófico, por tanto, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la *Frecuencia* del riesgo, de Protección para disminuir el *Impacto* o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. Las medidas dependen de la celda en la cual se ubica el riesgo, así: los Riesgos de *Impacto* leve y *Frecuencia* alta se previenen; los Riesgos con *Impacto* moderado y *Frecuencia* leve, se reduce o se comparte el riesgo, si es posible; también es viable combinar estas medidas con evitar el riesgo cuando éste presente una *Frecuencia* alta y media, y el *Impacto* sea moderado o catastrófico.

Siempre que el riesgo sea calificado con Impacto catastrófico la Entidad debe diseñar planes contingencia, para protegerse en caso de su ocurrencia.

●*Nivel del Riesgo*: se sombrea de color de acuerdo con la siguiente tabla de Valoración y Evaluación del riesgo.

	IMPACTO		
FRECUENCIA	**Leve (5)**	**Moderado (10)**	**Catastrófico (20**
Alta (3)	15-Moderado	30-Importante	60-Inaceptable
Media (2)	10-Tolerable	20-Moderado	40-Importante
Baja (1)	5-Aceptable	10-Tolerable	20-Moderado

Tabla 1. Tabla de valoración y evaluación del riesgo.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Establecer la probabilidad de ocurrencia de los riesgos, que pueden disminuir la capacidad institucional de la entidad, para cumplir su propósito.

- Medir el impacto las consecuencias del riesgo sobre las personas, los recursos o la coordinación de las acciones necesarias para llevar el logro de los objetivos institucionales o el desarrollo de los procesos.
- Establecer criterios de calificación y evaluación de los riesgos que permiten tomar decisiones pertinentes sobre su tratamiento.

9.2. Establecimiento y análisis de controles.

Para determinar los controles existentes es necesario recordar que éstos se clasifican según su naturaleza en:

- *Preventivo*: aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización, es decir, evitan que un evento suceda. Ej.: login y password en un sistema de información previene (teóricamente) que personas no autorizadas puedan ingresar al mismo.

- *Detectivo:* permiten registrar un evento después de que ha sucedido, Ej.: registro de las entradas de todas las actividades llevadas a cabo en el sistema de información, traza de registros realizados, de las personas que ingresaron, entre otros.

- *Correctivo:* No prevén que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Ej.: pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, que permiten volver a recuperar las operaciones.

Se debe determinar si los controles están documentados lo que permite conocer cómo se lleva a cabo el control y las evidencias que respaldarán la ejecución del mismo.

También se establece si el control es Automático (utilización de herramientas tecnológicas como sistemas de información o sistemas de grabación, etc.) o Manual (políticas de operación aplicables, autorizaciones con firmas, listas de chequeo, etc.).

Una vez se finaliza la fase de análisis, donde se identificaron los riesgos y controles del proceso, se define la matriz de riesgos donde se documenta: actividad, riesgo, controles, impacto, entre otros.

10. SEGURIDAD DE RECURSOS HUMANOS.

La Caja de Compensación Familiar del Oriente Colombiano. COMFAORIENTE para controlar que sus empleados y contratistas entiendan sus responsabilidades y sean idóneos para los roles para los cuales son considerados realiza el proceso de selección de sus funcionarios de acuerdo Procedimiento de Selección y Contratación establecido por la Corporación.

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 COMFAORIENTE asegura que los empleados y contratistas son conscientes y cumplen sus responsabilidades en relación a la seguridad de la información y a la protección de datos personales.

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 Oriente Colombiano COMFAORIENTE.

Se han definido dentro de las instalaciones de COMFAORIENTE 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:

- Centro de cómputo, de comunicaciones,
- Cuartos de centro de cableado.
- Áreas de gestión documental, radicación y archivo.
- Área de almacenamiento de archivo Físico.
- Cuartos y plantas eléctricas
- Cuartos de UPS y banco de baterías
- Despachos de la Dirección Administrativa y Subdirecciones.

11.2. Perímetro de Seguridad Física.

Las instalaciones de la COMFAORIENTE 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 las 24 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, en caso de ser un visitante; se permite el acceso con autorización de un funcionario de la Corporación portando el carnet de visitante entregado por el guarda de seguridad.

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

El cuarto principal de comunicaciones y servidores, centros de cableado cuentan con un cont de acceso con cerradura electrónica que abre con validación de huella digital y solo el perso de Infraestructura y Comunicaciones del área de TI están autorizados a ingresar. En caso ser necesario el ingreso de un proveedor de servicio se debe registrar la actividad y el tiem de permanencia dentro de esta área.

11.3. Seguridad en Equipos de Cómputo.

Los equipos de Cómputo sean de escritorio y/o portátil que son asignados a cada funcionario de COMFAORIENTE en el primer ingreso se establece una contraseña para la cuenta de usuario del Sistema Operativo y una credencial de administrador del Sistema Operativo preinstalada por el operador externo de soporte.

La contraseña de ingreso al Sistema Operativo permite contar con la seguridad del funcionario que personal no autorizado ingrese al equipo a consultar o modificar información.

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.

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 área de soporte técnico de Gestión Tecnológica.

Está prohibida la instalación de software No Licenciado y la instalación de Software libre debe presentar autorización previa del área de sistemas a 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, COMFAORIENTE 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.
- COMFAORIENTE 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.
- COMFAORIENTE tiene una política de instalación de software enunciada en este documento en el numeral 7.9.
- La red de COMFAORIENTE es monitoreada por el operador soporte externo las 24 horas.

12.1. Procedimientos y Responsabilidades de operación.

Para asegurar las comunicaciones, COMFAORIENTE 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.
- Las redes lógicamente están segregadas por VLAN.
- COMFAORIENTE tiene una política de seguridad para la trasferencia de información, la cual esta enunciada en este documento en el numeral 7.11. de este documento.
- COMFAORIENTE en toda cotización, propuesta comercial y contrato requiere una cláusula de confidencialidad y no divulgación para proteger la información de la organización.
- La trasferencia de cualquier tipo de información de COMFAORIENTE debe realizarse a través de las herramientas colaborativas licenciadas para tal fin.

12.2. Monitoreo.

La Corporación cuenta con sistemas de identificación del riesgo que permiten monitorear tiempo real la supervisión de seguridad de la información y de la red que permiten la detecci 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 Oriente Colombiano COMFAORIENTE, por parte de funcionarios y visitantes se debe hacer cumpliendo lo siguiente:

- Para ingresar a las sedes de COMFAORIENTE 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.
- En caso de los visitantes, deben informar al guarda de seguridad el motivo de su visita y a la oficina que se dirigen para entregar el carnet de visitante con la tarjeta de control de acceso al piso.
- El ingreso de computadores que no sean propiedad de la COMFAORIENTE deben 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 Oriente Colombiano– COMFAORIENTE para mitigar el riesgo de pérdida de información de sus instalaciones adopta las siguientes medidas.

- El personal de vigilancia de la Corporación, así como el personal de vigilancia del edificio, deben revisar todo bolso o paquetes del personal al ingresar o salir de las instalaciones.
- Todo ingreso de contratistas o visitantes para los fines de semana deberá ser solicitado previamente, indicando el motivo del requerimiento, en caso de ser autorizado se informará vía correo electrónico a la vigilancia del edificio el ingreso del personal.
- El ingreso del personal en los días no hábiles, deberá ser autorizado por el jefe de División de talento humano y recursos físicos con solicitud escrita firmada por el jefe

proceso, en caso de requerirse la entrada de personal contratista su ingreso es permitido con el acompañamiento de personal de planta de la corporación.

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 a la mano contraseñas de ingreso a los sistemas operativos y de información de la Corporación.

Es responsabilidad de los funcionarios el reporte de cualquier daño, falla, riego o amenaza detectada por terceros en los sistemas de información o componentes físicos al personal técnico calificado de soporte y al área administrativa.

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 Oriente Colombiano COMFAORIENTE, están contratados con terceros los cuales deben cumplir las políticas de seguridad en relación con proveedores, política desarrollo de seguro y la política de seguridad para la gestión de proyectos enunciadas en los numerales 7.12, 7.13 y 7.14. del presente documento.

Adicional la Corporación estableció el **Manual para la Implementación del Ciclo de Vida del Desarrollo Seguro de Software y el Procedimiento de Desarrollo de Software P-TEC-01,** con el fin gestionar los riesgos de seguridad de la información en cada una de las fases de los procesos de adquisición, desarrollo y mantenimiento de los sistemas de información.

Para cada proyecto nuevo, mejora sustancial o cambio a los sistemas de información de COMFAORIENTE 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 es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye 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 requisitos para 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 den 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 y 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 Oriente Colombiano COMFAORIENTE, gestiona los incidentes y eventos de seguridad de la información mediante el reporte oportuno de los funcionarios, terceros, aprendices, practicantes y proveedores 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 los lineamientos de la política de gestión de incidentes de seguridad de la información y el **Procedimiento para Gestión de Incidentes. P-TEC-07** establecido en la Corporación.

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 e información.

Cada evento será evaluado por el comité de seguridad de la información, para decidir si se clasifica como incidente.

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

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

La evidencia recolectada por cada incidente será salvaguardada por el área de sistemas y seguridad de la información 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 y 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 Seguridad Informática Colombia	https://cc-csirt.policia.gov.co/
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
Cuadrante de la Policía CAI	CAI del cuadrante.	xxx

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 Oriente Colombiano COMFAORIENTE, 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, 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 área de control interno y auditoria ejecuta de manera periódica auditorías internas a los procesos de seguridad de la información con el fin establecer el estado actual de cumplimiento de los planes de acción y del estado de gestión de los riesgos de seguridad de la información dentro de la Corporación.

El comité de seguridad de la información de COMFAORIENTE está encargado de supervisar el cumplimento de todas las políticas de seguridad de la información dentro 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 de La Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE, 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.

VERSION	DESCRIPCIÓN DEL CAMBIO	FECHA
00	Emisión inicial	11/Nov/2021
01	Se realiza actualización de acuerdo con lo dispuesto por el MinTIC y aborda los objetivos de control de la ISO 27001. (Para dar cumplimiento a los lineamientos de la Circular externa 2023-00002 de la Superintendencia de Subsidio Familiar	27/Mar/2023

	específicamente en la Tabla S2: ESTÁNDAR DE SEGURIDAD, Código 2.	