POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

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 encuentra apoyada por información documentada que da directrices sobre el manejo de la información y activos de la Caja De Compensación Del Oriente Colombiano.

Fecha de Aprobación: 27 de marzo de 2023. Mediante Acta No. 1164 de reunión ordinaria celebrada por el Consejo Directivo.

1. 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 contenida 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 de 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

2. 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, desastres naturales tales como terremotos, inundaciones, incendios y otros que a criterio de la gerencia de la Corporación ameriten que se realicen las actividades laborales desde casa.
- 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

3. 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.

3.1. 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 garantizara 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.

3.2. Gestión de Accesos al Usuario.

Lineamientos:

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

3.3. Control de Acceso a Sistemas y Aplicativos.

Lineamientos:

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

4. 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 solo 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: ¡,$, %, &)

4.1. 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

5. 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

6. 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 de dominio y no debe ser superior a 5 minutos

Excepciones a la política: N/A

7. 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 abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen 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

8. 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 tener deshabilitada la opción de instalación de software.
- Toda instalación o actualización de software se debe hacer con permisos de administrador previo entendimiento de los acuerdos de licencia de usuario final (EULA).
- Cada computador tendrá usuario de administrador y solo este contará con permisos para instalación de software.
- 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

9. 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 procedimeinto; **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 **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 medios diferentes y uno de ellos se encuentra en un lugar externo a las instalaciones principales 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

10. Política de 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.

11. 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 los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.
- Se deben mitigar los riesgos relacionados con terceras partes que tengan acceso a los 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

12. 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 debe incluir la definición o aplicación de requisitos de seguridad según los riesgos identificados.
- En el caso que el proveedor no especifique requisitos de seguridad en el software, la Corporación deberá establecer un estándar mínimo de requisitos de seguridad y aplicarlos basados en las buenas prácticas actuales para el SSDLC (Ciclo de Vida de Desarrollo Seguro de Sistemas).

12.1. 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

13. 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

14. 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

15. 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

16. 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

VERSION	DESCRIPCIÓN DEL CAMBIO	FECHA
03	Se realiza actualización	Mar/27/2023