POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las políticas y normas de seguridad de la información en la Caja de Compensación Familiar del Oriente Colombiano, en adelante COMFAORIENTE, con el fin de reforzar lineamientos y buenas prácticas establecidas para el Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El presente documento desarrolla en COMFAORIENTE de manera sistémica, estratégica, metodológica y estructurada las políticas específicas de seguridad de la información en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

3. DEFINICIONES

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Integridad: La información se mantiene íntegra, exacta y completa desde su emisión hasta su recepción, entre las partes autorizadas.

SGSI (Sistema de Gestión de Seguridad de Información): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque normativo. (ISO/IEC 27000).

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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

Todo el personal interno y externo que tenga acceso a la información de COMFAORIENTE deben adoptar las definiciones en el marco del Sistema de Gestión de Seguridad de la Información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. La Política Global del Sistema de Gestión de Seguridad de la Información se encuentra apoyada por información documentada que dará directrices sobre el manejo de la información y activos de la Caja de Compensación. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales consideran elementos del anexo A de la norma internacional ISO 27001:2013

5. SANCIONES

Las políticas de seguridad de la información pretenden instituir y afianzar la cultura de seguridad de la información entre el personal interno, externo y terceros; por lo cual, es necesario que como producto de violaciones a las políticas seguridad de la información sean tomadas medidas correctivas conforme a la clase de contravención. Las medidas correctivas pueden considerar desde acciones administrativas, disciplinarias o penal.

6. POLÍTICAS DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

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.

6.1.1. Normas para uso de dispositivos móviles

- Se debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la caja.
- 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.

- Se deben actualizar los dispositivos cada vez que el sistema notifique de una actualización disponible.
- Se deben evitar hacer uso de redes inalámbricas de uso público.

6.2. POLÍTICA PARA USO DE CONEXIONES REMOTAS

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.

6.2.1. Normas para uso de conexiones remotas

- Se deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la caja.
- Se debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica.
- 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 en computadores previamente identificados.

7. POLÍTICAS DE SEGURIDAD DEL PERSONAL

7.1. POLÍTICA ANTES DE LA VINCULACIÓN DEL PERSONAL

COMFAORIENTE, asegurará la verificación del historial laboral y académico, así como de los antecedentes de las personas que aspiran ingresar a la caja, antes de su contratación.

7.1.1. Normas antes de la vinculación del personal

- Se debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en Tu Compra, antes de su vinculación definitiva.
- Se debe velar porque el personal firme un acuerdo o cláusula de Confidencialidad; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- Se debe velar porque periódicamente se logre conseguir la aceptación de políticas de seguridad de la información por parte del personal, dicha aceptación se puede obtener de manera física o electrónica.

7.2. POLÍTICA DURANTE LA VINCULACIÓN DEL PERSONAL

COMFAORIENTE, en su interés por proteger su información y los recursos de procesamiento de esta demostrará el compromiso de la Alta Dirección en este esfuerzo, promoviendo que el personal

cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de Seguridad de la Información de la caja.

7.2.1. Normas durante la vinculación del personal

- Se debe diseñar y ejecutar de manera permanente un programa de capacitación y concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
- Se debe capacitar y entrenar al personal de acuerdo con el programa, en busca de evitar posibles riesgos de seguridad de la información.
- Todo personal interno o externo debe dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

7.3. POLÍTICA DE DESVINCULACIÓN O CAMBIO DE LABORES DEL PERSONAL

COMFAORIENTE, asegurará que el personal interno o externo será desvinculado o reasignado para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

7.3.1. Normas de desvinculación o cambio de labores del personal

- Se debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores del personal llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
- Se debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
- En el momento de desvinculación o cambio de labores, el personal debe realizar la entrega de su puesto de trabajo al jefe inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

8. POLÍTICAS DE GESTIÓN DE ACTIVOS

8.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

COMFAORIENTE, como propietario de la información física y electrónica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen su uso; toda la información, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que se dicten. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

8.1.1. Normas de responsabilidad por los activos

- Se deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
- Se deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Se debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos o áreas definidas por la caja.
- Se debe asegurar la apropiada operación y administración de los activos de información correspondientes a la plataforma tecnológica.
- Se debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos
- Se debe autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica.
- Se deben preparar las estaciones de trabajo fijas o portátiles del personal y de hacer entrega de estas.
- Se deben recibir los equipos de trabajo fijos y/o portátiles para su reasignación o disposición final, y generar copias de seguridad de la información del personal que se retira o cambian de labores, cuando les es formalmente solicitado.
- Los recursos tecnológicos asignados al personal interno o externo son proporcionados con el único fin de llevar a cabo las labores de la caja; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- En el momento de desvinculación o cambio de labores, el personal realizará la entrega de su puesto de trabajo al jefe inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

8.2. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

COMFAORIENTE, definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad y criticidad; y generará una guía de clasificación de la información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección; toda la información será identificada, clasificada y documentada de acuerdo con los lineamientos definidos y se promoverá el uso adecuado por parte del personal interno o externo que la requiera para la ejecución de sus actividades.

8.2.1. Normas de clasificación y manejo de la información

- Se deben definir los lineamientos y criterios para la clasificación de la información de la caja.
- Se deben socializar y divulgar los lineamientos y criterios de clasificación de la Información al personal de la caja.
- Se debe adoptar los mecanismos para la eliminación segura de la información contenida o almacenada en los activos, ya sea cuando son dados de baja o cambian de usuario.

- Se debe aplicar los controles tecnológicos que apalanquen el cumplimiento de los lineamientos de clasificación.
- Los propietarios de los activos de información deben clasificar su información de acuerdo con los lineamientos y criterios de clasificación de la Información definidos.
- Se debe monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación
- El personal interno o externo de la caja debe acatar los lineamientos establecidos para la clasificación y el manejo de los activos de Información
- El personal interno o externo de la caja debe tener en cuenta estas consideraciones de manejo de los activos de información sin importar su medio (físico o electrónico).

8.3. POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

COMFAORIENTE, establecerá los lineamientos específicos de la gestión, la disposición y transferencia de medios de almacenamiento en la plataforma tecnológica, con el objetivo de evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información.

8.3.1. Normas de uso de periféricos y medios de almacenamiento

- Se deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica, considerando situaciones como cuando son dados de baja o reasignados a un nuevo usuario.
- Se debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la caja, de acuerdo con los lineamientos y condiciones establecidas.
- Se deben aplicar los lineamientos para la disposición segura de los medios de almacenamiento de la caja
- El personal interno o externo deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos en la caja.
- El personal interno o externo no deben modificar la configuración de periféricos y medios de almacenamiento establecidos.
- El personal interno o externo son responsables por la custodia de los medios de almacenamiento asignados.

9. POLÍTICAS DE CONTROL DE ACCESOS

9.1. POLÍTICA DE ACCESOS A REDES Y RECURSOS DE RED

COMFAORIENTE, garantizará el desarrollo de actividades con base en las mejores prácticas de seguridad y protección mediante la adopción e implantación de mecanismos y controles aplicables con el fin de garantizar la gestión segura del acceso lógico para que los usuarios internos y externos encuentren un ambiente seguro que aporte al desempeño y al cumplimiento de las funciones a su cargo.

9.1.1. Normas de accesos a redes y recursos de red

- Se debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la caja.
- Se debe asegurar que las redes inalámbricas de la caja cuenten con métodos de autenticación que evite accesos no autorizados.
- Se debe verificar periódicamente los controles de acceso para los usuarios internos o externos, 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 o externo deben contar con el registro de creación de cuentas debidamente autorizado acorde a los procedimientos establecidos.
- El personal interno o externo 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.

9.2. POLÍTICA DE GESTIÓN DEL ACCESOS AL USUARIO

COMFAORIENTE, establecerá 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

9.2.1. Normas de gestión del acceso al usuario

- Se debe establecer 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.
- Se debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- Se debe definir 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 debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo al personal designado para dichas funciones.
- Se debe establecer cuentas personalizadas para la administración de los recursos tecnológicos, servicios de red y sistemas de información.
- Se debe limitar las conexiones remotas en los recursos de la plataforma tecnológica únicamente a personal autorizado, de acuerdo con las labores desempeñadas.
- Se debe asegurar 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.
- El personal interno o externo deben evitar compartir sus cuentas de usuario y contraseñas con personal interno o externo.
- El personal interno o externo deben acoger los lineamientos definidos para la configuración de contraseñas.

9.3. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

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.

9.3.1. Normas de control de acceso a sistemas y aplicativos

- Se debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la caja.
- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
- 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.

10. POLÍTICAS DE CRIPTOGRAFÍA

10.1. POLÍTICA DE CONTROLES CRIPOGRÁFICOS

COMFAORIENTE, velará porque la implementación de controles criptográficos en la información que por su nivel de clasificación o requisito de negocio lo requiera, aplicando algoritmos considerados como seguros en la industria y realizando una gestión controlada de llaves, con el fin de proteger la información en el momento de almacenarse o transmitirse por cualquier medio.

10.1.1. Normas de controles criptográficos

- Se debe asegurar la implementación de controles criptográficos para el almacenamiento o transmisión de la información que así lo requiera.
- Se debe velar porque todo sistema de información o aplicativo públicamente accesible realice transmisión segura de información haciendo uso de estándares considerados como seguros en la industria.
- Se debe establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- Se debe implementar estándares para la aplicación de controles criptográficos.

- Se debe certificar que los controles criptográficos implementados usan algoritmos considerados seguros en la industria

11. POLÍTICAS DE SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

11.1. POLÍTICA DE ÁREAS SEGURAS

COMFAORIENTE, proveerá los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones y mantengan las condiciones medioambientales adecuadas, a través de la gestión administrativa y de las instalaciones para evitar situaciones riesgo que expongan los activos físicos como aquellos que soporten la operación de los sistemas de información y comunicaciones, los cuales podrían ser considerados de acceso restringido.

11.1.1. Normas de áreas seguras

- Se deben proporcionar los recursos y mecanismos para la protección física de los activos de información ya sean físicos o electrónicos.
- Se deben establecer controles de acceso físico para evitar que personas no autorizadas puedan obtener acceso a las instalaciones de la caja.
- Se deben utilizar mecanismos de monitoreo, a fin de supervisar el acceso físico de personas a áreas restringidas de la caja; estos mecanismos de monitoreo deben ser ubicadas en lugares que sean inalcanzables y que, detecten acciones de alteración.
- Se debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas; no obstante, los visitantes siempre deberán estar acompañados de personal interno durante su visita.
- Se debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos.
- Se deben desarrollar procedimientos que permitan: identificar visitantes autorizados, de modo que se puedan distinguir fácilmente del personal interno en aras de evitar accesos no autorizados
- Se debe portar el carné que los identifica en un lugar visible mientras se encuentren en las instalaciones de la caja; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Se deben revocar o inhabilitar todos los mecanismos de acceso físico del personal cesante a la mayor brevedad, para evitar que el funcionario acceda físicamente a la información cuando ya no trabaje más en la caja.

- El personal interno o externo debe asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

11.2. **POLÍTICA DE SEGURIDAD DE LOS EQUIPOS**

COMFAORIENTE, para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que propendan por la seguridad de dicha plataforma tecnológica a través de la instauración de controles físicos, tecnológicos y procedimentales.

11.2.1. **Normas de seguridad de los equipos**

- Se debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la caja.
- Se debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica , equipos de cómputos y dispositivos móviles que pertenecen a la caja.
- Se debe generar y aplicar estándares de configuración segura para los equipos de cómputo.
- Se deben generar y aplicar lineamientos para la disposición segura de los equipos de cómputo del personal de la caja, ya sea cuando son dados de baja o cambian de usuario.
- Se debe aislar los equipos de áreas sensibles, en busca de proteger su acceso de personal no autorizado.
- Se debe garantizar la inclusión dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo.
- Se debe verificar los resultados de hallazgos de las auditorías y proponer acciones correctivas.
- Personal interno o externo debe evitar movimientos o reasignaciones no autorizadas sobre los recursos tecnológicos.
- Personal interno o externo debe acoger las instrucciones técnicas establecidas para el uso de los recursos tecnológicos.
- Todos los usuarios deben evitar la instalación, reparación o retiro de cualquier componente de hardware o software de los recursos tecnológicos, dado que solo puede ser realizado por personal previamente autorizado.
- Todos los usuarios deben bloquear las estaciones de trabajo en el momento de abandonar el puesto de trabajo.
- Todos los usuarios deben evitar dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Todos los usuarios deben informar de forma inmediata a su jefe la pérdida o robo de un equipo de cómputo en caso de que esto ocurra, para que se inicie el trámite interno correspondiente.

12. **POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES**

12.1. POLÍTICA DE RESPONSABILIDADES OPERATIVAS

COMFAORIENTE, asignará funciones específicas para efectuar la operación y administración de los recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades, con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada, asegurando así que los cambios efectuados serán adecuadamente controlados y debidamente autorizados.

12.1.1. Normas de responsabilidades operativas

- Se debe efectuar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la caja.
- Se debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos tecnológicos, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.
- Se debe garantizar el uso de manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica.

12.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

COMFAORIENTE, proporcionará los mecanismos que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles antimalware o similares para evitar la divulgación, modificación o daño permanente ocasionados por software malicioso.

12.2.1. Normas de protección frente a software malicioso

- Se debe 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 encargada.

12.3. **POLÍTICA DE RESPALDO DE INFORMACIÓN**

COMFAORIENTE, certificará la generación de copias de respaldo y almacenamiento de su información, proporcionando los recursos necesarios, estableciendo los procedimientos y mecanismos para la realización de estas actividades junto a la definición de la estrategia de retención para el respaldo y almacenamiento de la información, en busca de garantizar la disponibilidad de la información.

12.3.1. **Normas de respaldo de información**

- Se debe efectuar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la caja.
- Se debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- Se deben llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- Se debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo.

12.4. **POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO**

COMFAORIENTE, realizará monitoreo del uso que da el personal interno y externo a los recursos de la plataforma tecnológica y los sistemas de información; se implementarán pistas de auditoria en las cuales se registren los accesos a los componentes del sistema.

12.4.1. **Normas de registro de eventos y monitoreo**

- Se deben determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
- Se debe 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 debe definir los roles y responsabilidades respecto al monitoreo de eventos, así como, la periodicidad de revisión de estos.
- Se debe 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.

- 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 la identidad o nombre de los datos, componentes del sistema o recursos afectados.

12.5. **POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO**

COMFAORIENTE, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de software, para asegurar la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica ante actualizaciones o cambios.

12.5.1. **Normas de responsabilidades operativas**

- Se debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios definido.
- Se deben cambiar todos los valores predeterminados proporcionados por los proveedores de tecnología inalámbrica al momento de la instalación.
- Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- Se debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo.

12.6. **POLÍTICA DE GESTIÓN DE VULNERABILIDADES**

COMFAORIENTE, velará por el establecimiento de mecanismos para realizar de análisis internos y externos de vulnerabilidades de la red y los sistemas de la caja.

12.6.1. **Normas de responsabilidades operativas**

- Se debe garantizar la objetividad del desarrollo pruebas de vulnerabilidades mediante la destinación de los recursos necesarios para la realización de pruebas de vulnerabilidades y hacking ético, por un ente independiente al área objeto de las pruebas o los colaboradores administradores de plataforma tecnológica.
- Se debe canalizar el reporte de nuevas vulnerabilidades a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información.
- Se debe garantizar la adopción e implementación de los lineamientos y recomendaciones generados a partir de los hallazgos de las pruebas de vulnerabilidades y hacking ético.

13. **POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES**

13.1. **POLÍTICA DE GESTIÓN DE LA SEGURIDAD DE LAS REDES DE DATOS**

COMFAORIENTE, establecerá los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. Todo ello, mediante la adopción de procesos continuos y formales para el diseño, implementación y evaluación de la arquitectura tecnológica.

13.1.1. Normas de gestión de la seguridad de las redes de datos

- Se debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red.
- Se debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de la caja.
- Se debe mantener las redes segmentadas de acuerdo con las definiciones de la caja.
- Se debe identificar los acuerdos de nivel de servicio que deben ser considerados con proveedores.
- Se debe establecer estándares de configuración de los dispositivos de la plataforma tecnológica, acogiendo prácticas de configuración segura.
- Se debe instalar protección entre las redes internas y cualquier red externa.

13.2. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

COMFAORIENTE, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y 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.

13.2.1. Normas de intercambio de información

- Se debe establecer los controles físicos y tecnológicos de intercambio de información, considerando medios de transmisión confiables, con el fin de proteger la confidencialidad e integridad de la información
- Se debe apoyar la definición de modelos de acuerdos de confidencialidad o de intercambio de información.
- Se debe velar porque el intercambio de información con entidades externas se realice en cumplimiento de las políticas de seguridad y los acuerdos de intercambio de información
- Se debe verificar la destrucción de la información suministrada a terceros, una vez esta ha cumplido el cometido por el cual fue enviada.

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

14.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

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.

14.1.1. Normas para el establecimiento de requisitos de seguridad

- 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.
-

14.2. POLÍTICA DE DESARROLLO SEGURO, PRUEBAS Y SOPORTE DE LOS SISTEMAS

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.

14.2.1. Normas para el establecimiento de requisitos de seguridad

- Se deben implementar controles para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- Se debe establecer el procedimiento de gestión de cambios incluyendo el manejo de los cambios en el software aplicativo y los sistemas de información.
- Se debe asegurar que los sistemas de información cuenten con licenciamiento, condiciones de uso del software y los derechos de propiedad intelectual.
- Se debe velar por que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- Se debe considerar las prácticas y lineamientos de desarrollo seguro durante el ciclo de vida del software, pasando desde el diseño hasta la puesta en marcha.
- Se debe proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software.
- Se debe construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Se debe asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Se debe suministrar opciones de desconexión o cierre de sesión de los aplicativos en todos los sitios protegidos por autenticación.
- Se debe garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios.
- Se debe remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Se debe prevenir la revelación de la estructura de directorios de los sistemas de información desarrollados.
- Se debe evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Se debe proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado, ni modificado por personal no autorizado.
- Se debe asegurar que no se permita que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

15. POLÍTICAS QUE RIGEN A LA RELACIÓN CON TERCERAS PARTES

15.1. POLÍTICA DE INCLUSIÓN DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

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.

15.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes

- Se debe generar un modelo base para los requisitos de seguridad de la información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas.
- Se debe elaborar un modelo de acuerdos de confidencialidad y acuerdos de intercambio de información con terceras partes.
- Se debe establecer las condiciones de conexión para los equipos de cómputo y dispositivos de los terceros en la red interna.
- Se debe 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 debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica.

- Se debe manejar de manera adecuada la información recibida, en cumplimiento de las políticas de seguridad, procedimientos y las condiciones contractuales establecidas.
- Se debe destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

15.2. POLÍTICA DE GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE TERCERAS PARTES

COMFAORIENTE, velará por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos. Asi mismo, velará por la adecuada gestión de cambios, propendiendo siempre por la disponibilidad de los servicios.

15.2.1. Normas de gestión de la prestación de servicios de terceras parte

- Se debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos de los terceros en la red.
- Se debe verificar las condiciones de comunicación segura y transmisión de información desde y hacia los terceros proveedores de servicios.
- Se debe monitorear periódicamente, el cumplimiento de los requisitos de seguridad de la información de parte de los terceros proveedores de servicios

16. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

16.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

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.

16.1.1. Normas para el reporte y tratamiento de incidentes de seguridad

- 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.

17. POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

COMFAORIENTE, proporcionará los recursos en términos de personal y procesos para suministrar 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.

17.1.1. Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información.

- Se deben establecer las consideraciones de seguridad de la información para la implementación de un plan de continuidad de negocio o acciones de recuperación ante desastres.
- Se debe participar activamente en las pruebas de recuperación ante desastres y notificar los resultados a las áreas pertinentes.

17.2. POLÍTICA DE REDUNDANCIA

COMFAORIENTE, buscará contar con una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad y seguridad de la caja, a través de estrategias o recursos de hardware y software.

17.2.1. Normas de redundancia

- Se debe establecer los requerimientos de redundancia para los sistemas críticos.
- Se debe probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos establecidos.
- Se debe realizar pruebas periódicas sobre las soluciones de redundancia tecnológica establecidas.

18. POLÍTICAS DE CUMPLIMIENTO

18.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

COMFAORIENTE, velará por la identificación y documentación de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual buscará que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables, en busca de asegurar su cumplimiento.

18.1.1. **Normas de cumplimiento con requisitos legales y contractuales**

- Se debe realizar la identificación, documentación y mantenimiento actualizado de los requisitos legales, reglamentarios o contractuales aplicables, entre ellos los relacionados con seguridad de la información.
- Se debe certificar que todo el software que se ejecute esté protegido por derechos de autor y requiera licencia de uso.
- Se debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo para el desarrollo de las actividades laborales.
- Se debe verificar periódicamente que el software instalado en las estaciones de trabajo corresponda con lo permitido.