1. OBJETIVO.

Establecer la protección adecuada de la información con respecto a la integridad, disponibilidad y confidencialidad de esta, sin importar el medio por el cual sea distribuida o almacenada.

1. CONTENIDO

1.1 Alcance de la política de la seguridad de la Información para Comfenalco Tolima.

PROCESO	ALCANCE
Todos	Aplica para todos los trabajadores de la Caja de Compensación Familiar de Fenalco del Tolima "Comfenalco" en las diferentes sedes de trabajo independientemente de su contratación o vinculación incluyendo, consultores, contratistas, subcontratistas y demás partes interesadas.

2.2 Política

La CAJA DE COMPENSACION FAMILIAR DE FENALCO DEL TOLIMA COMFENALCO, en el ejercicio de la buena práctica enmarcada en la norma de seguridad de la Información ISO 27001 27002, a fin de proteger y mantener la disponibilidad, integridad y confiabilidad de la información, es responsable de mejorar continuamente los procesos tecnológicos, ejecutando acciones que disminuyan el impacto del riesgo de pérdida, adulteración y captura por accesos indebidos de la información.

2.3 Objetivos de la Seguridad de la Información

En concordancia con lo anterior, la política de seguridad de la información de COMFENALCO TOLIMA contempla los siguientes objetivos:

- Establecer las políticas y lineamientos de la seguridad de la información que garanticen protección de esta tanto a nivel interno como externo.
- Regular la gestión de la información y proteger los activos informáticos de la Caja
- Promover la implementación de las políticas de seguridad de la información acorde con el plan Estratégico de la Caja.
- Establecer de acuerdo con el Plan Estratégico de TI (PETIC) un marco de gobierno, mediante el cual se implementen los modelos de decisión necesarios para gestionar, controlar y monitorear las tecnologías de información en la organización.
- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos específicos de la Caja para asegurar su permanencia, liderazgo y eficacia.

Este documento hace parte de las políticas de gestión de la empresa, por lo tanto será revisada anualmente y comunicada a todos los trabajadores y entra a regir a partir de la fecha de su aprobación.

POLITICAS GENERALES DE LA SEGURIDAD DE LA INFORMACION.

De acuerdo con el nivel jerárquico establecido los líderes de los procesos, están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información que estén bajo su responsabilidad estén lo suficientemente protegidos y tengan el adecuado manejo.

En este sentido es necesario estandarizar e implantar acciones preventivas y correctivas, que se conozcan y apliquen, en los diferentes eventos y situaciones, tendientes a la protección de la información, reduciendo así los diferentes riesgos a los que está expuesta.

Acorde con lo anterior, se ha constituido un Comité Tecnológico, que tiene como función, con cierta regularidad o en casos excepcionales, efectuar un análisis de riesgos y revisar las políticas de seguridad, aplicables a la Caja, del cual se desprende un informe para la Dirección y el Consejo Directivo, en el cual se refleja el estado actual de la Corporación en cuanto a Seguridad de la información.

Se deben llevar a cabo los procedimientos de escalamiento y reporte cuando se observe el incumplimiento, riesgo, o se genere una excepción de la política de seguridad de la Entidad.

Se deben revisar regularmente los procesos y procedimientos dentro de las áreas para asegurar que las responsabilidades y deberes referidos a la seguridad de la información y activos informáticos, se realizan apropiadamente. Los resultados de esta revisión y las acciones correctivas deben ser documentados.

La persona que se delegue por parte de la Dirección Administrativa debe revisar el cumplimiento con las buenas prácticas de seguridad de la información. Las situaciones que dan como resultado los incumplimientos de estas prácticas deben ser reportadas a la Unidad Especializada de TI y esta a su vez a la Dirección Administrativa. Las actividades de revisión deben incluir el monitoreo operacional del cumplimiento, análisis individual del sistema, revisiones de terceros, pruebas de conformidad internas, y revisiones de los procedimientos.

Todos los colaboradores de la Caja de Compensación deberán acatar y respectar las políticas de seguridad aquí establecidas a fin de no generar riesgos en la información y los activos tecnológicos de COMFENALCO TOLIMA.

La violación deliberada de las políticas de seguridad de la información o del incumplimiento de regulaciones por algún colaborador de la Caja de Compensación, será sancionada mediante un proceso disciplinario que determine COMFENALCO TOLIMA o a través de contratos o procesos jurídicos en caso de terceros.

POLITICAS DE REPORTE DE INCIDENTES DE SEGURIDAD

- El talento humano de Comfenalco Tolima deberá reportar de manera oportuna cualquier incidente o evento de seguridad de la información que se pueda detectar o presentar en la Caja, inclusive con los activos de la información, lo cual debe registrarse en la mesa de servicios Aranda.

- El único medio de reporte de incidentes de seguridad será a través de la mesa de servicios establecido por la Caja (Aranda) a fin de llevar un control efectivo y asignarlo al especialista que corresponda y pueda ser solucionado en el menor tiempo posible, tomando medidas necesarias que impidan su reincidencia así como también contar con la trazabilidad de los reportes y la base de datos de conocimiento de las acciones que se realizan para mitigar los incidentes que se reportan.

- Todos los incidentes de seguridad que se presenten en la Caja deben ser documentados a fin de tener una Base de conocimientos describiendo toda la gestión realizada al incidente tratado, de tal forma que en caso de repetición sea más rápida su solución.

- En el evento de experimentar un número significativo en incidentes de seguridad, se debe analizar las circunstancias y causas particulares y exponer ante el Comité Tecnológico con el propósito de tomar acciones que permitan su solución definitiva.

- Se debe establecer roles y responsabilidades al interior de la Caja para evaluar los riesgos tecnológicos que permitan garantizar la operación, la continuidad y la disponibilidad de los servicios.

- Gestionar campañas de concientización a todos los usuarios de la Caja de cómo prevenir los incidentes de seguridad que afecten la operación tecnológica y como reportarlos oportunamente a la Unidad Especializada de TI para su tratamiento.

POLITICA ESTABLECIMIENTO ACUERDOS DE CONFIDENCIALIDAD

- Todos los colaboradores de la Caja, sin importar el tipo de contrato, ya sea a término fijo o indefinido, deben firmar un acuerdo de confidencialidad conforme a la política de protección de datos y a la de seguridad de la información en el momento en que se establezca vínculo con COMFENALCO TOLIMA; donde se comprometan a dar buen uso de la información que interactúe en el desarrollo de su actividad.

- Se debe asegurar que todo el personal que sea vinculado a la Caja como contratista, trabajador en misión, contrato de aprendizaje, practicante, etc. se le debe incluir una cláusula de confidencialidad dentro del contrato que se firme antes que inicien sus labores en **COMFENALCO TOLIMA.**

- Garantizar el cumplimiento de los acuerdos y/o cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información establecidas por la Caja.

POLITICA DE CONTROL DE ACCESO FISICO.

- Se deberá identificar a todos los colaboradores de COMFENALCO **TOLIMA** para lo cual deben portar en un lugar visible el carné que lo acredite como funcionario de la Caja.

- Todos los visitantes, empleados temporales, contratistas y practicantes deben ser autorizados para la entrada física a las instalaciones la **COMFENALCO TOLIMA**, sobre todo cuando se dirigen a áreas administrativas o de acceso restringido.

- El ingreso de dispositivos de grabación de audio, fotos y video a las áreas de acceso restringido (Tesorería, Auditoría Interna, Centros de Computo y/o Cableado, archivos físicos, Jurídica, Dirección Administrativa, etc.) debe controlarse de tal manera que no sea extraída información confidencial o de uso exclusivo de **COMFENALCO TOLIMA**.

- **COMFENALCO TOLIMA** debe asegurar que los derechos de acceso a todas las instalaciones son revisados anualmente. El acceso a lugares considerados como áreas restringidas, debe ser revisado regularmente.

- Las áreas de procesamiento de información y demás infraestructura que soporte la operación de los servicios informáticos de **COMFENALCO TOLIMA** son considerados de acceso restringido por lo tanto deben de contar con medidas de control en su acceso de tal manera que puedan ser auditadas a fin de evitar al máximo el daño accidental o intencional.

- Se deberá realizar la devolución del carné institucional tan pronto el personal termine su vinculación a COMFENALCO TOLIMA.

POLITICA DE CLASIFICACION DE LA INFORMACIÓN.

Los lideres de la Caja son responsables para clasificar su información de acuerdo con los criterios de confidencialidad, sensibilidad, riesgo de pérdida, requisitos legales, criticidad, susceptibilidad y genera la guía para la clasificación de los activos de información con el fin de que los propietarios de esta las apliquen y ejecuten los controles requeridos para su debida protección.

Por lo tanto la política establece los siguientes niveles de clasificación de la información:

- Información de uso público o informativa:
  Su divulgación no requiere de autorización especial dentro y fuera de la Caja y su función es de comunicación del personal en general.

Puede darse a conocer al público en general a través de carteleras, Intranet, página web institucional, correos electrónicos, memorandos. No se requiere brindar las garantías para que no existan problemas de disponibilidad o de denegación en su consulta.

Su modificación debe ser realizada exclusivamente por los autores y el personal asignado para esas tareas.

- Información de uso interno o privada:
  Su divulgación no autorizada, principalmente fuera de la Caja sería inadecuada o inconveniente, debe ser de conocimiento únicamente por parte de los funcionarios de la Caja y del área que la procesa.

  Puede ser compartida entre áreas dada su necesidad para la operación diaria y no consolida resultados finales de gestión.

- Información de uso confidencial:
  Sustenta estrategias del negocio, información financiera consolidada, informes de gestión para el Consejo Directivo, la Dirección Administrativa, Divisiones, registros para toma de decisiones, información de Afiliados, información de personal y cualquier otra que pueda comprometer la seguridad de Caja o de las personas.

  Su divulgación no está autorizada, incluso dentro de la organización, por el impacto de daño que puede causar a la Caja. Debe ser usada únicamente por ciertos funcionarios de la Caja quienes son responsables de su manejo.

  La Caja determina que la información de los afiliados y clientes es clasificada como confidencial, por lo tanto, su manejo debe ser exclusivo para personas debidamente autorizadas y está limitado a actividades propias de las áreas, está totalmente prohibida su divulgación a personas no autorizadas.

- Información de uso Restringido:

Información que solo se encuentra disponible para un proceso especifico de la Caja, por lo que de ser accedida por un tercero que no cuente con la debida autorización, puede tener impactos negativos.
Por lo tanto el uso de esta información es de conocimiento únicamente a nivel directivo, jefes y empleados claves de la Caja.

De acuerdo con lo descrito anteriormente la información desclasificarse o disminuir su nivel de clasificación sin llevar a cabo un análisis de los riesgos que esto implica, y una aprobación por el responsable de la información. Este determinará si su información puede moverse a una clasificación más baja o alta basado en las definiciones de clasificación desarrolladas por **COMFENALCO TOLIMA** y descritas anteriormente.

POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO.

Seguridad de las Redes de Datos

- Se debe adoptar por parte de la Unidad Especializada de TI lo necesario para garantizar la disponibilidad de los recursos y servicios en todas las sedes de la Caja.
- Debe haber un monitoreo periódico sobre las redes de cableado estructurado de datos y los racks de cableado, para detectar, eliminar o prevenir el uso de dispositivos no autorizados conectados a los cables.
- Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red para la Caja , acogiendo buenas prácticas de configuración segura.
- Se debe asegurar que todas las conexiones de red que existan en un lugar y que no estén siendo utilizado de manera permanente sean deshabilitadas.
- Los ductos o la canalización de cableado de red deben ser protegidos contra interferencia o interrupción. Esto incluye evitar cableado en áreas públicas, segregación de cableado de energía para eliminar interferencia y el rotulado claro para la identificación de los equipos.
- Las áreas asignadas para los Racks de cableado estructurado deben contar con acceso físico restringido y no se debe almacenar ningún tipo de material que ponga en riesgo su operación.

Mantenimiento de Equipos

- El mantenimiento preventivo y/o correctivo de software o hardware debe ser realizado por colaboradores de la Unidad Especializada de TI de la Caja o por terceros debidamente autorizados e identificados. Ningún funcionario de **COMFENALCO TOLIMA** debe permitir la manipulación de equipos y/o software por personal que no esté plenamente identificado y autorizado por la Unidad Especializada de TI.
- En caso de que el equipo de cómputo deba ser retirado de algunas de las sedes de la Caja , para realizar labres de mantenimiento correctivo y/o preventivo se debe garantizar por parte de la Unidad Especializada de TI la confidencialidad e integridad de la información que registre este equipo.
- Todos los recursos de TI (hardware y software) que soportan la operación de los procesos de la Caja y que por alguna razón no puede ser atendido por el personal técnico de la Unidad Especializada de TI, deben contar con un contrato de mantenimiento preventivo y/o correctivo por parte del fabricante o proveedor ante la eventualidad que se presente.

Protección y Ubicación de Equipos

- Generar y aplicar estándares de configuración segura para los equipos de cómputo de los colaboradores de la Caja.
- Para prevenir el acceso, la duplicación y la transmisión no autorizada de información de la Caja se debe hacer uso de contraseñas seguras en los equipos de cómputo.
- Todos los equipos tecnológicos de **COMFENALCO TOLIMA** deben ser ubicados o localizados de tal forma que se reduzca al mínimo los riesgos o amenazas. Esto incluye hurto, exposición al agua o humedad, caídas o golpes, sustancias químicas, pérdida de servicios de soporte como energía, comunicación, agua o cualquier otra amenaza física.
- Se prohíbe el consumo de alimentos o bebidas cerca a los equipos de cómputo o en las instalaciones de procesamiento de información.
- Los espacios adyacentes a las instalaciones de procesamiento de información no se deben utilizar para propósitos que pueden implicar los altos riesgos (Ej. espacio de almacenaje, cuarto de servicio, cafeterías y demás). Fumar, beber y comer en instalaciones de procesamiento de información.

Seguridad de Equipos de Cómputo Portátiles.

- Los equipos de cómputo portables que se asignen a los colaborades en cada área de la Caja se deben entregar con acta escrita y se deberá reportar una copia a la Unidad Especializada de TI para el control respectivo e inclusión en el inventario de la herramienta Aranda.
- Todo equipo de propiedad de **COMFENALCO TOLIMA** que esté fuera de las instalaciones de la Caja no debe ser desatendido por su responsable en lugares donde se presente la posibilidad de extracción no autorizada de la información o perdida/hurto de este.
- COMFENALCO TOLIMA debe asegurar a través de pólizas de seguro las computadoras portátiles a fin de poder reclamar ante una eventualidad.
- El líder de área donde pertenezca el funcionario a quien le sea asignado un portátil y que tenga exposición a riesgos como caídas, robo; debe solicitar la compra e instalación de guayas de protección para los portátiles.

Retiro de equipos de Cómputo y/o periféricos de las Instalaciones de la Caja.

- En caso de retiro de un equipo de las instalaciones de **COMFENALCO TOLIMA**, se debe solicitar permiso (utilizando el formato establecido) a la Jefatura de la Unidad Especializada de TI y debe quedar el registro en la bitácora del guarda de seguridad el nombre de la persona, el cargo, el área donde pertenece el equipo, la fecha y hora de salida.

- Todo equipo que por necesidad del servicio se traslade de área, se debe realizar correspondiente informando a la Unidad Especializada de TI y a la Unidad de Contabilidad a fin de mantener el control de inventarios respectivos.

Suministro de Equipos de Soporte Energético

- El líder de cada servicio debe asegurar que las fuentes de electricidad (UPS) son utilizadas únicamente de los equipos de cómputo que apoyan las operaciones de negocio de la Caja, para lo cual la Unidad Especializada de TI garantiza la diferenciación de color de estas.

- Las UPS deben ser revisadas periódicamente por el líder de mantenimiento e infraestructura, para asegurar que tienen la capacidad adecuada y aprobada, de acuerdo con las recomendaciones del fabricante.

Devolución de Activos (Baja o Reasignación)

- Cualquier equipo de procesamiento de datos que haya contenido información privada o confidencial y que vaya a ser reasignado en otra área de la Caja o por cambio de usuario dentro de la misma área, la Unidad Especializada de TI debe garantizar el proceso de limpieza lógica antes de ser utilizado nuevamente. Este proceso debe consistir en la destrucción de la información que reside en el equipo y la validación del proceso, para asegurar que ningún dato se deja en el equipo o pueda ser recuperado.

- Cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y que vaya a ser dado de baja, sus unidades de almacenamiento de información se les debe realizarse la limpieza lógica (Formatear) o en su defecto deben ser destruidos físicamente antes de su disposición final.

- En los periodos de vacaciones, licencias e incapacidad de los colaboradores de la Caja y en el evento de que el equipo se reasigne a la persona quien realiza su remplazo, debe existir un procedimiento formal para crear y/o trasladar el usuario a este equipo a utilizar.

POLITICA DE RESPONSABILIDAD DE CREACION Y ACCESO A CUENTAS DE USUARIOS

- A los usuarios a quien se les asigne cuentas de usuario y contraseñas en los distintos aplicativos o de acceso, serán responsables de las acciones realizadas de acuerdo con los privilegios otorgados.

- Está totalmente prohibido que las áreas utilicen las cuentas de usuarios de sus colaboradores que se encuentren ausentes de la Caja. En caso de que se requiera el acceso a un aplicativo, es necesario hacer la solicitud formal mediante el procedimiento establecido.

a) Los usuarios a quienes se les asigne usuarios para el ingreso a las diferentes aplicaciones y/o recursos informáticos de **COMFENALCO TOLIMA;** en ninguna circunstancia pueden compartir su usuario / contraseña o cualquier mecanismo otorgado para su identificación y autenticación, excepto que por necesidad de algunas áreas de la Caja se creen usuarios y contraseñas de uso general.

- La eliminación de accesos y servicios asociados a una cuenta de usuario debe ser realizada inmediatamente el usuario ha finalizado su vinculación laboral, contractual o comercial con **COMFENALCO TOLIMA** o ha cambiado de rol dentro de la Caja y no se requiere que acceda a estos recursos informáticos.

- La Unidad de Gestión Humana es responsable en reportar a la Unidad Especializada de TI las novedades presentadas con los funcionarios sin importar el tipo de vinculación laboral con la Caja (temporales, de planta, practicantes SENA, etc.). Los Líderes de las áreas son responsables por reportar a la Unidad Especializada de TI las novedades de personal a su cargo que haya realizado, traslados, vacaciones o licencias, usuarios pertenecientes a consultores, asesores, auditores externos y otros terceros que tengan acceso a los sistemas de información.

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

- La Unidad Especializada de TI debe de definir los perfiles de usuario para asesar los sistemas de información de la Caja.

- Se debe monitorear de manera permanente los perfiles definidos en los sistemas de información bajo responsabilidad y privilegios asignados a cada usuario que accede a las aplicaciones dispuestas en la Caja.

- Es completamente prohibido almacenar contraseñas en lugares que puedan ser accedidos por terceras personas o almacenarlas en navegadores o archivos no contralados que coloque en riesgo la seguridad de la información de COMFENALCO TOLIMA.

- Establecer ambientes separados a nivel lógico para pruebas y producción a fin de establecer acciones que puedan evitar el riesgo la integridad de la información de producción.

POLITICA DE USO ADECUADO DE LOS EQUIPOS DE COMPUTO

- Los recursos de tecnología (hardware) son para uso exclusivo de COMFENALCO TOLIMA; El uso inadecuado de cualquier recurso de tecnología de la entidad o la utilización para otros propósitos diferentes a los definidos por la Caja está prohibido. Cualquier actividad no autorizada debe ser reportada a la Unidad Especializada de TI quien tomara los correctivos que sean necesarios.

- Los usuarios deben de abstenerse realizar prácticas o usos que puedan comprometer los recursos tecnológicos o que afecten la privacidad y la seguridad de la información de la Caja.

- Se prohíbe descargar y/o ejecutar programas ejecutables desde cualquier medio (unidades extraíbles de almacenamiento, paginas, etc.) que pueden contener software o código malicioso.

- Se prohíbe totalmente alterar la configuración de los dispositivos asignados, incluyendo sus periféricos.

- La Unidad Especializada de TI debe realizar periódicamente el control y verificación del cumplimiento legal sobre e licenciamiento de software y aplicaciones instaladas en los equipos de cómputo de la Caja.

- Reportar a través de la mesa de servicios Aranda dispuesta por la Unidad Especializada de TI en caso de que algún equipo de cómputo presente mal funcionamiento.

POLITICA ESCRITORIO Y PANTALLA LIMPIA

- Está totalmente prohibido el uso unidades de almacenamiento externo (USB, CD, DVD, etc.) en las estaciones de trabajo asignadas para el cumplimiento de las funciones en donde se maneje información sensible y confidencial de la Caja; en caso de requerirse debe informarse a la Unidad Especializada de TI.

- La información clasificada confidencial que no esté siendo utilizada por personal autorizado, debe permanecer siempre restringida y en custodia, no debe ser desatendida en ninguna ubicación no controlada.

- Todos los colaboradores de la Caja que tengan bajo su responsabilidad información confidencial deben garantizar su almacenamiento en lugares que estén protegidos con llave o algún otro medio que impidan la extracción no autorizada.

- Todos los colaboradores son responsables de bloquear la sesión de su computador en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos debidamente apagados.

POLITICA TRANSFERENCIA DE INFORMACION ENTRE AREAS Y/O TERCEROS

Todas las áreas de COMFENALCO TOLIMA son responsables del manejo adecuado y tramite de su información, por lo tanto, se establece lo siguiente:

- Extraer la información solo desde los reportes y medios establecidos en cada aplicación a fin de garantizar la veracidad de esta.

- No está permitido la transmisión o transferencia de información de la Caja, por medios de divulgación masiva (cadenas de correos, WhatsApp, Facebook, etc.); excepto las áreas que por su naturaleza deban de realizarlo o que aquellas que cuenten con la autorización de la Dirección Administrativa, por lo tanto a estas áreas o colaboradores se les permitirá el acceso a estas plataformas.

- Si se requiere información de otra área y que no sea posible extraer de los reportes oficiales de las aplicaciones (SEVEN, KACTUS, ATHENEA, BI), es necesario que se solicite a ella directamente pues será la información válida para cualquier proceso.

- La información que requiera cualquier entidad externa (Entes de Control, Empresas, y demás.), debe ser generada únicamente por el área la Caja que la administra.

- En caso de que el área no cuente con el reporte, con las variables de información requeridas o no pueda extraerla por sus propios medios justificables, puede solicitar la interacción a la Unidad Especializada de TI.

- En todo caso el líder del área es responsable de la revisión de los datos de manera que no se transmita información con defectos de consolidación o que no corresponda con la veracidad requerida.

- Cuando se requiera la validación y él envió de información ante portales en Internet de Entes de Control o a otras entidades, la estructura y el contenido de la información solo puede ser modificada por el área que tiene la responsabilidad de generarla.

- Cuando se transmita información a entes de control u otras entidades es necesario contar con la autorización del líder del área que maneja la información, toda vez que asume la responsabilidad de lo que se entrega.

POLITICA DISPOSITIVOS MOVILES

- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de COMFENALCO TOLIMA; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos.

- La sincronización de dispositivos móviles, tales como tabletas, u otros dispositivos electrónicos que no sean propiedad de la Caja y sobre los que por necesidad se requiera realizar intercambios de información con cualquier recurso de Comfenalco Tolima, debe estar autorizado de forma explícita por la Dirección Administrativa.

- La utilización de VPN para los funcionarios que realizan su labor fuera de la sede principal de COMFENALCO TOLIMA solo será instalada una vez se cuente con la autorización de la Dirección Administrativa y solo podrá tener acceso a las aplicaciones en las que se haya creado a su usuario.

En todo caso y en ninguna circunstancia en la utilización de los medios tecnológicos descritos en esta política, no está permitido la extracción de información no autorizada, así mismo la divulgación o transferencia sin la autorización del líder y/o de la Dirección Administrativa.

POLITICA SOBRE RESTRINCCIONES DE INSTALACIONES Y USO DEL SOFTWARE

- La instalación de software o el uso de información externa en los equipos de Cómputo de **COMFENALCO TOLIMA** debe ser previamente autorizada y debe cumplir con los requerimientos legales que faculten su utilización.

- El software que reside en los computadores de **COMFENALCO TOLIMA** sólo podrá ser el autorizado. Es prohibido instalar en los computadores de la Caja, software que no esté registrado y autorizado.

- Solo el personal Idóneo que tenga privilegios de Administrador o usuarios delegados podrá realizar instalación del software debidamente legalizado (Nuevo Software, Actualizaciones, Parches de Seguridad al Software Existente).

POLITICA DE COPIAS DE RESPALDO.

- La información que se genere de los diferentes sistemas de Información contenidas en la plataforma tecnológica administradas por COMFENALCO TOLIMA como servidores, dispositivos de red, archivos de configuración de dispositivos de red y seguridad; debe ser protegidas mediante copias de seguridad que garanticen la integridad, disponibilidad y autenticidad.

- Se deberá establecer un plan de restauración de copias de seguridad y probados periódicamente con intervalos regulares, con el fin de asegurar su efectividad en caso de que sea necesaria su restauración y retenidas por un periodo de tiempo determinado.

- Se deberá establecer conjuntamente un procedimiento de resguardo de las copias de seguridad para los servicios de Hosting Externo que cumpla con las condiciones de almacenamiento y de seguridad para garantizar garanticen la integridad, disponibilidad y autenticidad de la información, además es indispensable que sea monitoreado periódicamente a fin de que se cumpla integralmente. (medios de conservación, responsables de ejecución, intervalos de realización, tiempos de retención y que esté plenamente probado, etc.)

- Se debe establecer acuerdos con el proveedor de Hosting Externo para se ejecute periódicamente el plan de restauración de copias a fin de que se garantice la integridad de la información y que se permita atender cualquier evento que ponga en riesgo la operación y la continuidad de la Caja.

POLITICA PROTECCION CONTRA CODIGO O SOFTWARE MALICIOSO

- Se establece que COMFENALCO TOLIMA debe proteger todos los recursos informáticos con herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra intrusión de código malicioso y prevención a la red de datos de COMFENALCO TOLIMA, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso.

- Se deben instalar herramientas debidamente licenciadas permitiendo su continua actualización; además el software de seguridad no deberá ser modificado en su configuración o deshabilitado en las maquinas en ninguna circunstancia; por lo tanto, los usuarios deben abstenerse de:

- La desactivación o desinstalación de software y herramientas de seguridad.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo que pueda generar la intrusión de código malicioso que pueda poner en riesgo la operación de la Caja.

- Ante sospechas o detección de alguna infección por software malicioso deben notificar inmediatamente a la Unidad Especializada a través de la mesa de servicios Aranda a fin de tomar las medidas de control necesarias.

- Se debe evitar abrir correos de fuentes desconocidas, y publicidad engañosa que pueda causar daño o intrusiones no autorizadas a las plataformas tecnológicas de COMFENALCO TOLIMA y que pongan en riesgo la seguridad de la información.

POLITICA GESTION DE VULNERABILIADES TECNICAS

- Se deben identificar los riesgos y vulnerabilidades del área de Tecnología a fin de crear planes de contingencia que permitan mitigar su impacto.

- Se debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas que puedan ser detectadas en la plataforma tecnológica de la Caja.

- Se deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación (Hacking Ético, etc.)

- Se deberá revisar habitualmente la aparición de nuevas vulnerabilidades técnicas a fin de que los proveedores de los sistemas de información puedan dar prevención la exposición al riesgo.

POLITICA CONTROLES CRIPTOGRAFICOS

- Se deberá propender que todos sistemas de información con que cuenta la Caja y que requiera realizar transmisión de información reservada o restringida, cuente a futuro con mecanismos de cifrado de datos.

- Se debe desarrollar y establecer estándares para la aplicación de controles criptográficos dentro de la Información que genere la Caja y que se considere reservada o restringida.

- Verificar que los controles criptográficos se ejecuten y apliquen adecuadamente con revisiones periódicas.

POLITICA SEGURIDAD DE LAS COMUNICACIONES.

Acceso a Redes Inalámbricas (Wifi)

- Asegurar que las redes inalámbricas de COMFENALCO TOLIMA cuenten con métodos de autenticación y cifrado que eviten accesos no autorizados.

- Todas las redes inalámbricas de acceso wifi son únicamente al servicio del personal administrativo de la Caja y visitantes de la sede principal de Comfenalco Tolima.

- 2. En ninguna circunstancia está permitido facilitar el acceso a las redes inalámbricas de COMFFENALCO TOLIMA en cualquiera de sus sedes a personas, entidades, etc. Que no estén

debidamente autorizadas, se exceptúa las redes wifi para usuarios visitantes en los centros recreacionales.

- El uso de la redes wifi-administrativas son de uso laboral, por lo tanto es responsabilidad de del usuario propender por el uso adecuado y licito.

- Para los usuarios y/o lideres que conozcan las contraseñas de conexión wifi, se prohíbe su divulgación en personas o entidades ajenas a Comfenalco Tolima, a menos que por necesidad del servicio de requiera.

- Las contraseñas deben ser cambiadas periódicamente, además contar con una longitud mínima y combinando caracteres (letras, números, carácter especial, etc.)

Se establecen las siguientes redes wifi:

- CAIKE_VISITANTES - COMFE_GIMNASIO - COMFENALCO TOLIMA – COMFENALCOTOLIMA. Esta red segura requiere aprobación de usabilidad que realiza el usuario interno y externo en el portal cautivo con inicio de sesión por redes sociales e implementado desde el XG SOPHOS principal para su uso.

- COMFENALCO SALA SISTEMAS 1- COMFENALCO SALA SISTEMAS 2- COMFENALCO SALA SISTEMAS 3 – COMFENALCO BIBLIOTECA – COMFENALCO COLEGIO ADMON, estas redes seguras ubicadas en el colegio Augusto E medina Ibagué requieren IP estática el cual se maneja desde un archivo compartido en OneDrive OFFICE 365 y es administrada por cada uno de los AP SOPHOS para su uso.

- COMFENALCO PREESCOLAR – COMFENALCO DOCENTES - CAIKE_FUNCIONARIOS - CAIKE_EVALB - CAIKE_TIROLINA - COMFENALCO_ADMIN - CAIKE_DATAFONOS, Estas redes seguras ubicada en el colegio Augusto E medina Ibagué, Sede CAIKE, SEDE 37, INSTITUTO, entregan un direccionamiento dinámico y es administrada por cada XG SOPHOS para su uso.

- COMFENALCO_EVENTOS - INSTITUTO COMFENALCO, Estas redes seguras ubicada en la sede 37, Instituto entregan un direccionamiento dinámico y se realiza una entrega de claves diarias a los correos registrados y es administrada por cada XG SOPHOS para su uso.

- COMFENALCO RECTORIA, Estas redes seguras ubicada en la sede colegio AEM Ibagué entregan un direccionamiento dinámico y se un filtrado por MAC registradas y es administrada por cada XG SOPHOS para su uso.

- CAIKE_DATAFONOS aparte de los ajustes mencionados anteriormente, se tiene la red oculta protegiendo los equipos de conexiones no autorizadas y así garantizar las transacciones por la red.

6. La Unidad Especializada de TI, mantendrá actualizada la información de estas redes wifi realizando constantemente filtrando la navegación a paginas no autorizadas y filtrando la navegación con reglas específicas a fin de establecer sitios seguros que garanticen la seguridad de la información.

o Uso del Correo electrónico

El único correo autorizado al interior de COMFENALCO TOLIMA es el de la plataforma tecnológica Office 365, por lo tanto, los funcionarios a quienes se les asigno correo deberán acogerse a los siguientes lineamientos:

- El servicio de correo electrónico es para uso exclusivo de las actividades relacionadas con el trabajo de cada funcionario.

- Desde la cuenta de correo asignado por COMFENALCO TOLMA debe de abstenerse en difundir de puntos de vista personales referentes a temas políticos, raciales y religiosos, al igual que la inclusión de mensajes sobre creencias, convocatorias políticas entre otros, al igual que usar el email para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

- La cuenta de correo asignada no debe utilizarse como medio de envío de cadenas de mensajes, recepción o envío de mensajes con archivos adjuntos de video, música, gráficos, juegos, ejecutables, y demás.

- Este servicio no debe usarse para enviar SPAM o mensajes no solicitados ni tampoco para enviar material obsceno e ilegal o relacionado a pornografía infantil o cualquier clase de pornografía.

- En la cuenta de correo no debe configurarse reglas en los buzones de correo electrónico que reenvíen los mensajes a servidores públicos de Internet como Hotmail, Gmail, entre otros.

- No se puede utilizar el correo electrónico, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de la Caja.

- Los niveles de almacenamiento de los buzones no pueden exceder el estándar de la herramienta tecnológica office 365, por lo tanto, el usuario debe eliminar periódicamente los mensajes leídos de modo tal que no exceda el espacio de acuerdo con el plan de office 365 que tiene cada usuario.

- La firma predeterminada solo puede contener nombre y apellidos, cargo, dirección, teléfonos y nombre de la Caja, su logo, tamaño de letra, formato de letra son los que establece la Dirección Administrativa. Se prohíbe una configuración diferente.

- En caso de recibir un mensaje bajo sospecha de virus, (de personas desconocidas con asuntos desconocidos o sospechosos) debe abstenerse de abrirlo y en su defecto marcarlo como no deseado y caso de ser necesario reportarlo como un evento de seguridad ante la Unidad Especializada de TI para que se atendido por él administrador de la plataforma de office 365. no se debe abrir y se debe reportar de inmediato a la Unidad Especializada de TI.

- No está permitido el uso de cuentas de correo personales o de servicios de correo externo como Hotmail, Gmail, y demás., para transmitir o intercambiar información referente o perteneciente a COMFENALCO TOLIMA.

Acceso a Internet

El internet es una herramienta fundamental para el desarrollo del trabajo, ya que permite el ingreso a diversos sitios que se relacionan o no con las actividades propias de la Caja; por lo tanto, el uso adecuado de este recurso se debe controlar, restringir, verificar, monitorear y su uso puede darse excepto en los siguientes casos:

- Ingresar a cualquier página que contenga pornografía, alusión a la drogadicción, alcoholismo, material ofensivo, discriminatorio o que se considere prohibido según el reglamento interno de COMFENALCO TOLIMA y a las leyes colombianas.
- Descargar música, videos, fotos, fondos de pantalla, programas, juegos etc. los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor.

- Ingresar a páginas que ofrezcan servicios de radio, televisión o juegos en línea.

- Utilizar los servicios de Internet para enviar archivos que sean confidenciales y de propiedad exclusiva de COMFENALCO TOLIMA.

- Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocios particulares.

- El acceso no autorizado a cualquier intento de prueba, verificación o rastreo (scan) de vulnerabilidades de un sistema o red, violando las medidas de seguridad o de autenticación sin la expresa autorización del propietario del sistema o la red.

- El acceso a páginas relacionadas con Web Proxys, hacking y cualquier otra página que ponga en riesgo la seguridad de la plataforma tecnológica de COMFENALCO TOLIMA.

POLITICA PARA EL ASEGURAMIENTO DE LA INFORMACION EN DATA CENTER EXTERNO O NUBE PRIVADA.

COMFENALCO TOLIMA, pensando en que la información de la Caja este en un sitio seguro y que cumpla con la reglamentación colombiana, ley de protección de datos (Ley 1581 de 2012) establece las siguientes políticas y restricciones:

- Los servicios de nube que se contrate bajo cualquier modelo de despliegue (nube privada, pública o hibrida) y bajo el modelo de servicios que la Caja decida (IaaS, SaaS, PaaS) se debe garantizar que el alojamiento de la información se preste en el estado colombiano.

- Se debe inspeccionar el Data Center que se contrate a fin de verificar las condiciones de operación y validar el cumplimiento de sus certificaciones.

- Se debe garantizar que al terminar el contrato de nube con el proveedor y si se decide migrar hacia otra nube, luego de migrada la información se elimine completamente de los servidores del contratista inicial.

- Se debe revisar la política de seguridad del oferente y/o proveedor de nube, para comprar que este cumple con todos los criterios, que aseguren la información de Comfenalco Tolima.

- Se debe establecer quien gestiona y quien los accede, para lo cual se debe tener claro los roles de cada una de las personas que intervienen.

- Se debe asegurar la constitución de un acuerdo de confidencialidad con el proveedor de servicios de nube.

- se debe asegura que el proveedor presente el plan de contingencia para preservar la información almacenada en servicios de nube.

POLITICA DE SEGURIDAD DE LA INFORMACION EN RELACION CON LOS PROVEEDORES.

Con el propósito de salvaguardar los activos de información de la Caja, se deberán cumplir y acoger por parte de los proveedores las siguientes políticas:

- Con todos los proveedores con que la Caja tiene relación y donde de alguna manera exista relación de acceso a la información confidencial o privilegiada de la Caja, se deberán generar acuerdos de confidencialidad, acuerdos de niveles de servicio y acuerdos de intercambio de información cuando estos apliquen.

- Los acuerdos que se establezcan deberán definir responsabilidades tanto a nivel penal como civil para la tercera parte contratada.

- La Caja establecerá a través de su Unidad Especializada de TI, los medios y condiciones para monitorear las condiciones de comunicación seguras y cifradas para la transmisión de información desde y hacia los proveedores que se conecten de manera remota a los servicios tecnológicos de la Caja.

- Se deberá identificar, mitigar y monitorear los riesgos relacionados con los proveedores de servicios, incluidos en la cadena de suministro de los servicios de tecnología y/o de comunicaciones.

- La Unidad Especializada de TI deberá evaluar y aprobar de manera formal los accesos a la información de la Caja requeridos por proveedores y/o terceras partes.

- Los proveedores con quien se tiene relación y dependiendo de su clasificación deberán reportar los incidentes de seguridad de la información que se detecten al jefe de la Unidad Especializada de TI.

- Los proveedores que traten información confidencial y/o sensible de la Caja que haya sido suministrada o que tenga acceso a través de conexiones a los servicios informáticos, una vez finalizada la relación contractual deberá ejecutar un procedimiento de borrado seguro y/o inactivación de las credenciales de acceso, para lo cual se deberá certificar por parte del proveedor la ejecución de estas acciones.

- Se deberá propender por la divulgación de las políticas de seguridad de la información de la Caja a los proveedores, así velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento por parte de los terceros; se realice de acuerdo con las políticas de seguridad de la información establecidas por la Caja.

POLITICAS DE CIBERSEGURIDAD

La Caja mediante su Unidad Especializada de TI debe asegurar que la información, las aplicaciones que están dispuestas en nube y que son esenciales para la operación de COMFENALCO TOLIMA, por lo tanto se debe mitigar y/o disminuir potencialmente las amenazas o ataques cibernéticos, implementando controles tecnológicos, procedimientos y políticas de seguridad, por lo tanto se establece lo siguiente:

- La Unidad Especializada implementara controles adecuados para garantizar la gestión de la ciberseguridad tanto a nivel de la infraestructura interna como con su proveedor de hosting externo, a través de un análisis de riegos que se identifique en los activos de información.
- La gestión de la ciberseguridad debe será alineada con la gestión de la Unidad de TI y con todas las actividades que se desarrollen en las diferentes áreas de la Caja.
- La gestión de la ciberseguridad de contribuir a mantener la continuidad de las operaciones críticas de la Caja y mantener la disponibilidad de la información ante el evento o una interrupción significativa.
- La Caja debe establecer un responsable que gestione los riesgos de seguridad de la información y de la ciberseguridad.
- Se deben establecer procedimientos de recuperación ante posibles incidentes de seguridad alineados con el plan de continuidad que se establezca para la Caja
- Establecer un programa de capacitación o sensibilización en materia de ciberseguridad y seguridad de la información a nivel de los colaboradores de la Caja y a los terceros que se consideren relevantes.
- Se debe mantener actualizados las herramientas y/o servicios que puedan alertar tempranamente incidentes de seguridad.
- Actualizar de manera permanente el sistema de gestión del riesgo y de seguridad de la información como consecuencia de los incidentes que se presenten y que sea necesario adoptar nuevos controles.

POLITICAS DE CONTINUIDAD DEL NEGOCIO

Se debe identificar y gestionar proactivamente potencialmente los riesgos y los impactos que estos podrían tener sobre las operaciones críticas en los diferentes servicios o áreas de la Caja a fin de actuar

diligentemente frente a una posible situación de emergencia o crisis, recuperando los servicios ofrecidos a nuestros afiliados en el menor tiempo posible, por lo tanto se establece lo siguiente:

- Se debe generar planes para minimizar los efectos adversos que pueda tener la ocurrencia de un evento catastrófico sobre la normalidad de las operaciones de los procesos en la Caja.

- La Caja debe realizar evaluaciones, de conformidad con los requisitos de la política, para identificar los riesgos de continuidad del negocio y las necesidades asociadas.

- Se debe definir estrategias que permitan recuperar la operación de áreas y/o servicios críticos de la Caja y proveer un plan de recuperación ante desastres tanto para Data Center contratado externamente como para los servicios y/o infraestructura administrada internamente.

- Definir y establecer procedimientos de generación de copias de seguridad y recuperación de acuerdo con las necesidades y las definiciones establecidas por los líderes de cada proceso de la Caja.

- Capacitar y difundir los planes de contingencia y de continuidad del negocio a todos los colaboradores de la Caja, según su necesidad de conocer de acuerdo con sus responsabilidades.

- Se debe considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.

- Realizar las pruebas periódicas del Plan de Continuidad de los recursos tecnológicos y documentar los resultados de dichas pruebas. La Caja debe mantener informados al personal y terceras partes de la situación y las expectativas de recuperación de la operación normal, utilizando los conductos regulares de comunicación establecidos.

Las presentes políticas son aprobadas por el Consejo Directivo, en sesión del 22 de Junio de 2023, tal como consta en Acta No 819 de la misma fecha.

Jaime Cortés Suárez

Presidente Consejo Directivo

Comfenalco Tolima.