CAFASUR

Amigo afiliado:
¡Usted es nuestra razón de ser!

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"
EL ESPINAL - TOLIMA
DICIEMBRE DE 2024

Tabla de contenido

1 Objetivo

Establecer los lineamientos para garantizar la integridad, confidencialidad, y disponibilidad de la información manejada por Cafasur, como datos sensibles, confidenciales y críticos de los afiliados, empleados y demás partes interesadas de la organización, sin importar el medio por el cual sea distribuida o almacenada; así como dar cumplimiento normativo, garantizando un ambiente controlado de los riesgos de información de la Corporación.

2 Alcance

Esta política y todas las políticas específicas y procedimientos que se deriven del Sistema de Gestión de Seguridad de la Información son de obligatorio cumplimiento para:

a) Todos los funcionarios de la Caja de Compensación Familiar del Sur del Tolima "**CAFASUR"**, incluyendo estudiantes en práctica, estudiantes del SENA, y otras figuras de contratación que se adopten.

b) Partes interesadas como clientes, socios de negocios, proveedores, acreedores, compañías de outsourcing, auditores externos, consultores externos, entidades públicas, entes de control y en general cualquier tipo de usuario de los sistemas de información de la Corporación.

La política de seguridad de la información es aplicable a todos los activos de información tecnológicos, dentro de los cuales están los sistemas de información, las bases de datos, los dispositivos de telecomunicación, equipos de cómputo, dispositivos móviles, documentación digital, sean propios o gestionados por terceros.

3 Definiciones

- **ACTIVOS DE INFORMACIÓN TECNOLÓGICOS**: Recursos del sistema de información o relacionados con éste, necesarios para que la Entidad funcione correctamente y alcance los objetivos propuestos por la Dirección.

- **BASE DE DATOS:** Colección organizada de información estructurada o datos, normalmente almacenados electrónicamente en un sistema informático.

- **CIFRADO**: Es el proceso que se aplica a unos datos para hacerlos incomprensibles. Este proceso o transformación precisa de una clave de cifrado, que es una cadena

aleatoria de bits, de una medida determinada (como, se denomina, de una determinada longitud de clave). Sólo aplicando el proceso contrario, denominado descifrado, a los datos cifrados será posible regenerar los datos originales y por tanto, hacerlas otra vez comprensibles.

- **CLASIFICACIÓN DE LA INFORMACIÓN**: Es la decisión para asignar un nivel de sensibilidad a los datos cuando se están creando, corrigiendo, almacenando o transmitiendo. Un esquema de clasificación debe usarse para definir un conjunto apropiado de niveles de protección y comunicar las medidas especiales de tratamiento.

- **CONTROLES**: Medidas para garantizar que los riesgos sean reducidos a un nivel aceptable.

- **DUEÑO DE LA INFORMACIÓN**: Es responsable de la información que le sea asignada, así como de la clasificación, control y monitoreo del uso y gestión de la misma. Son Dueños de Información todas aquellas personas de la Caja de Compensación Familiar del Sur del Tolima "**CAFASUR",** que tienen bajo su responsabilidad parte o la totalidad de la información. Los Responsables de la información son encargados de preservar los principios de seguridad de la información (integridad, disponibilidad y confidencialidad) y deben coordinar la implementación de políticas con otros dueños de información y con custodios de la información. Los Dueños deben especificar cómo se debe utilizar la información y cómo se debe proteger, además de definir cómo se administrarán los procedimientos de seguridad de la información y cómo se aplicarán los niveles apropiados de protección para cada una de las clases de información (pública, privada y confidencial).

- **IMPACTO:** Daño producido a la entidad por un posible incidente, evento, cambio no autorizado en los estados de seguridad y operación o resultado de la agresión sobre un activo.

- **INCIDENTE:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos, inesperados o no deseados, de seguridad de la información que tienen una probabilidad significativa de poner en peligro las operaciones y procesos del negocio y amenazar la seguridad de la información. Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, sistemas de información, procesos del negocio o recursos tecnológicos de la Caja de Compensación Familiar del Sur del Tolima "**CAFASUR".**

- **INFORMACIÓN:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

- **INFRAESTRUCTURA TECNOLÓGICA:** Todos los componentes tecnológicos que están al servicio de la entidad.

- **INFRAESTRUCTURA:** La tecnología, el recurso humano y las instalaciones que permiten el procesamiento de las aplicaciones.

- **ISO 27001:** Código de práctica para la administración de la seguridad de la información de la Organización Internacional para la Estandarización (ISO).

- **MONITOREO:** Es aquella actividad que pretende hacer seguimiento periódico y revisión de ciertas tareas realizadas en los sistemas de información.

- **NORMA:** Guía general de Seguridad de la Información sobre un tema específico, pero independiente de la plataforma tecnológica. La norma está sustentada en una política y regula parte o la totalidad del objetivo de la misma.

- **PROCESO:** Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

- **RIESGO:** Es la probabilidad de que una amenaza se concrete sobre uno o más activos causando daños o perjuicios a la Organización por medio de una vulnerabilidad o punto débil.

- **ROL/PERFIL:** Conjunto de funciones, normas, comportamientos y derechos definidos en un sistema de información que se espera que un usuario cumpla o ejerza de acuerdo a su nivel adquirido o atribuido en la Caja de Compensación Familiar del Sur del Tolima "**CAFASUR"**

- **SEGURIDAD DE LA INFORMACIÓN**: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; otras características también pueden estar involucradas, tales como la autenticidad, responsabilidad, aceptabilidad y confiabilidad.
- **SISTEMA DE INFORMACIÓN:** Conjunto de programas o aplicaciones desarrollados en diferentes lenguajes de programación, que facilitan el manejo de la información generada por los diferentes procesos de la Entidad.

- **TI:** Tecnología de información.

- **PRACTICANTE:** Personal que desempeña labores en la empresa bajo contrato de aprendizaje SENA, pasante o practicante universitario y estudiantes de colegio realizando su servicio social obligatorio.

4 Responsables

Los siguientes son responsables, en distintos grados, de la seguridad en la Compañía:

a. La Dirección Administrativa de la Caja de Compensación Familiar del Sur del Tolima "CAFASUR" debe apoyar activamente la seguridad de la información dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

- Crear el Comité de Seguridad Informática, conformado por un grupo interdisciplinario incluyendo el Departamento de Sistemas.
- Asignar un responsable de la seguridad de la información (Coordinador de Sistemas).
- Aprobar las políticas de seguridad de la información y Velar por el cumplimiento de las mismas
- Asignar las responsabilidades asociadas al tema de la seguridad de la información.
- Es responsable que los funcionarios de la Caja, conozcan y apliquen las políticas de seguridad de la información.

b. El Comité de Seguridad Informática está compuesto por el Director Administrativo, El Coordinador de Sistemas, el Jefe de la División Financiera, El Jefe de la División de Auditoría, el Revisor Fiscal, el Jefe de la División Jurídica y la representación con voto de las diferentes áreas a las que le competa los temas a tratar y sean invitados al comité.

- Debe periódicamente revisar el estado general de la seguridad de la información.
- Revisar y monitorear los incidentes de seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información.
- Aprobar las modificaciones o nuevas políticas de seguridad de la información.
- Realizar otras actividades de alto nivel relacionadas con la seguridad de la Información.

c. El Departamento de Sistemas es responsable de implantar, revisar, actualizar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de la estrategia de la seguridad a lo largo de toda la organización, evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances, todo esto en coordinación con la Dirección.

d. El **Coordinador de Sistemas** es responsable de otorgar los controles de acceso para cada usuario, con base a los lineamientos de los roles o perfiles de usuario, creados por el Comité de Seguridad Informática y solicitados por jefe Inmediato. Supervisar y controlar el uso de los recursos informáticos, revisar las bitácoras de acceso, llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto, actualización de antivirus y control del licenciamiento del software operativo de la organización, Backup, tramite de requerimientos de usuarios, contratos y soportes.

e. **Los usuarios** son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

a. Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
b. No divulgar información confidencial de la Compañía a personas no autorizadas.
c. No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.
d. No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.
e. Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
f. Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
g. Reportar inmediatamente a su jefe inmediato cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
h. Proteger la integridad física de los sistemas de cómputo a cargo. (Computador de Escritorio, Portátil, impresoras, ups, estabilizador, etc).
i. No dejar sesiones abiertas de los aplicativos o el Windows si no está presente.

j. No intentar hacer ingresos no permitidos ni efectuar impresiones, toma de fotos a las pantallas de los aplicativos, impresiones o demás actividades que no sean propias de la operación de los usuarios.

5 POLÍTICAS O NORMAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Corporación. Sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón la Dirección y el Consejo Directivo tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales, garantizar la no obsolescencia de la Tecnología (software, hardware y redes).

La Dirección Administrativa está en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de la información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el Comité de Seguridad Informática llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará al final de cada año un informe para la Dirección y el Consejo Directivo que muestre el estado actual de la Compañía en cuanto a Tecnología (Software, hardware, seguridad informática y redes).

A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.

5.1.1 Políticas Específicas del Sistema de Gestión de Seguridad de la Información

a) El Sistema de Gestión de Seguridad de la Información de la Caja de Compensación Familiar del Sur del Tolima **"CAFASUR"** se implementa dentro del marco de la norma NTC ISO/IEC 27001:2005 o sus versiones posteriores y la Circular Externa 023 del 2010, emitida por la Superintendencia el Subsidio Familiar.

b) El presente documento así como todas las políticas y procedimientos de seguridad de la información que se deriven del SGSI deben ser comunicadas a todos los funcionarios de la Organización.

5.1.2 Revisión de la Política de Seguridad

a) El Coordinador de Sistemas es responsable por la actualización permanente del Documento de Políticas de Seguridad de la Información de la Caja de Compensación Familiar del Sur del Tolima **"CAFASUR"**, los principios rectores, políticas específicas, procedimientos, estándares y guías de uso. La actualización debe ser realizada en la medida en que ocurra alguno de los siguientes eventos:

   a. Cambios en el ambiente de negocios o estrategia empresarial (ejemplo: nuevas estrategias de mercado, nuevos productos, cambios de prioridades, fusiones o cesiones, cambios en la estructura organizacional, nueva Dirección, etc.)

   b. Cambios en la infraestructura de riesgos de seguridad de información de la compañía. Estos cambios pueden ser como consecuencia de un análisis de riesgos y vulnerabilidades o por aparición de nuevas vulnerabilidades y/o amenazas que cambien el perfil de riesgo de la infraestructura técnica de la Organización.

   c. Nuevas obligaciones legales y/o reglamentarias o cambio de las existentes que afecten el procesamiento de la información, intercambio de información con terceros, etc.

   d. Avances en las mejores prácticas de seguridad de la Información registradas en el código de prácticas ISO/IEC 27002:2005 o cambios en la norma ISO/IEC 27001:2005, o las que en su momento apliquen y que previamente evaluadas sean necesarias para la organización.

   e. Aplicación de nuevos controles identificados como resultado de los análisis de los incidentes de seguridad de la información o el resultado de auditorías de TI.

f. Es responsabilidad del Coordinador de sistemas informar a la Compañía y terceros la actualización y publicación de nuevas versiones de este documento.

5.1.3 Organización de Seguridad

a) La Dirección de la Caja de Compensación Familiar del Sur del Tolima **"CAFASUR"**, se encargará de dar una Dirección estratégica al sistema de Gestión de Seguridad de la Información acorde con los lineamientos de la Organización y aprobará los principios rectores, políticas específicas y procedimientos que hacen parte de este documento, pero delega las responsabilidades operativas de la Seguridad de la Información al Comité de Seguridad Informática, el cual estará conformado por los siguientes integrantes:

- Director Administrativo
- El Coordinador de Sistemas
- Jefe de la División Financiera
- Jefe de la División de Auditoria
- Revisoría Fiscal
- Jefe de la División Jurídica
- Representación con voto de las diferentes áreas a las que le competa los temas a tratar y sean invitados al comité.

b) La Dirección revisará periódicamente las actas e informes del Comité de Seguridad Informática.

c) El Comité de Seguridad Informática coordinará las actividades relacionadas con la Administración y operación del Sistema de Gestión de Seguridad de la Información.

d) Otras responsabilidades del Comité de Seguridad Informática son:

a. Revisar y aprobar la Política de Seguridad de la Información de La Caja de Compensación Familiar del Sur del Tolima "CAFASUR", los principios rectores, políticas específicas, procedimientos, estándares y guías de uso de los temas relacionados a seguridad informática.

b. Evaluar, revisar, aprobar e implementar los controles de seguridad de la información.

c. Identificar las tendencias y los cambios importantes de los riesgos de seguridad informática de la Organización y proponer los cambios de políticas y procedimientos adecuados con el fin de controlar las vulnerabilidades identificadas.

d. Asegurar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios.

e. Establecer mecanismos de control que permitan medir el cumplimiento de las Políticas y Procedimientos de Seguridad de la Información.

f. Recomendar, hacer seguimiento y realizar acciones correctivas a los incidentes de seguridad reportados.

g. Establecer mecanismos de control de la información confidencial de la Empresa

h. Establecer y gestionar las sanciones aplicables por incumplimiento a las Políticas de Seguridad de la Información, principios rectores, políticas específicas, procedimientos, estándares y guías de uso de los temas relacionados a seguridad informática.

i. Coordinar revisiones periódicas al Sistema de Gestión de Seguridad de Información, realizadas por consultores externos ó internos, cuando el nivel de experiencia y capacitación lo permita.

j. Realizar reportes periódicos a la Dirección indicando el nivel de seguridad obtenido mediante la ejecución de los controles del Sistema de Gestión de Seguridad de la Información.

k. Desarrollar programas de concientización y capacitación a todos los funcionarios que enfatice la importancia del cumplimiento del Sistema de Gestión de Seguridad de la información y su contribución al logro de los objetivos del negocio.

l. El Comité de Seguridad Informática realizará sus reuniones en el evento en que ocurra uno (o varios) de los siguientes eventos:

    1. Hayan pasado máximo 6 meses después del último Comité de Seguridad Informática.

2. Ocurrencia de un incidente de seguridad que requiera una sesión especial del comité.

3. Ocurrencia de un evento por el cual sea necesaria la declaración de contingencia técnica y/o operativa.

5.2 GESTIÓN Y ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

5.2.1 Responsabilidad de los Activos de Información

a) Los propietarios o responsables de los activos de información deben ser claramente designados por la Dirección de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** o los jefes respectivos de cada división. Los propietarios serán los responsables de la protección de los activos de información contra incidentes de seguridad.

b) Los propietarios de los activos de información, son responsables por la clasificación de sus activos y la definición y auditoria constante de las restricciones de acceso y otros controles de seguridad de la información

5.2.2 Inventario de los Activos de Información

a) Los responsables de los activos de información deben realizar un inventario de los datos (información) almacenados en las estaciones de trabajo y bases de datos de los servidores, así como de los documentos en medio físico necesarios para el desarrollo de las actividades.

b) Los datos mínimos que debe contener el inventario de los datos (físicos y magnéticos) son:

   a. Nombre del archivo o documento
   b. Ubicación (carpeta física o lógica)
   c. Responsable
   d. Custodio
   e. Clasificación de la información de acuerdo a los criterios de esta política.

c) El inventario de los datos y documentos físicos (activos de información) debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:

a. Cambios en el ambiente de negocios o estrategia empresarial.
b. Nuevas obligaciones legales o reglamentarias.
c. Pasado un año después de la última actualización del inventario.

d) El Coordinador de Sistemas debe realizar el inventario de los aplicativos y programas bajo licencia con que cuenta la organización. Los datos que debe incluir el inventario son:

a. Nombre del aplicativo o software
b. Versión
c. Número de licencias adquiridas por la Organización
d. Número de licencias instaladas

e) El Coordinador de sistemas debe realizar el inventario de los activos de información tangibles (computadores, impresoras, equipos de comunicaciones, etc.). Los datos mínimos que debe contener el inventario de activos son:

a. Nombre del equipo
b. Marca
c. Modelo
d. No. De serie
e. No. De activo
f. Ubicación

f) El inventario de los activos de información tangibles debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:

a. Cambios en el ambiente de negocios o estrategia empresarial
b. Renovación o actualización tecnológica.
c. Desarrollo o compra de un sistema de información (aplicativo)
d. Pasado un año de la última actualización del inventario.

1.1.1. Clasificación de la Información

a) Los responsables de la información en medio físico y magnético deben realizar la clasificación de acuerdo a los criterios de confidencialidad, sensibilidad, riesgo

de pérdida o compromiso, aspectos legales, requerimientos de retención y facilidad de recuperación que deben ser empleados.

b) Los requerimientos legales, estatutarios y regulatorios deben ser considerados al momento de evaluar la clasificación de la información.

c) La clasificación de la información debe ser realizada simultáneamente con el inventario.

d) Los criterios para clasificar la información son:

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

Puede darse a conocer al público en general a través de carteleras, Intranet, memorandos, etc. 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.

b. Información de uso interno o privada. Su divulgación no autorizada, principalmente fuera de la organización sería inadecuada o inconveniente, debe ser de conocimiento únicamente por parte de los funcionarios de la organización. Puede ser compartida entre áreas dada su necesidad para la operación diaria y no consolida resultados finales de gestión.

c. Información de uso confidencial. Sustenta estrategias del negocio, información financiera consolidada, informes de gestión para junta y Dirección, registros para toma de decisiones, información de Clientes y competencia, información de personal y cualquier otra que pueda comprometer la seguridad de la empresa o de las personas.

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

e) La Organización determina que la información de los Clientes es clasificada como confidencial, por lo tanto, su manejo debe ser exclusivo para personas debidamente autorizadas y está limitado a actividades propias del Negocio, está totalmente prohibida su divulgación a personas no autorizadas.

f) La información no puede 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 más alta basado en las definiciones de clasificación desarrolladas por **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**

5.2.3 Rotulación y tratamiento de la Información

a) La información impresa debe ser rotulada en cada página con la clasificación de la información definida para dicho documento. Los documentos electrónicos deben tener la etiqueta de clasificación en el encabezado o en el pie de cada página.

b) Todos los documentos que contienen información altamente sensible deben tener una portada o etiqueta donde se identifique su clasificación.

5.2.4 Controles para la Información Clasificada como Confidencial

a) El envío a un tercero (incluyendo los Clientes) de información clasificada como confidencial debe ser autorizado por el responsable de la información, por medio del formato de solicitud de requerimientos.

b) La información clasificada como confidencial que sea necesario enviar a un tercero (incluyendo los Clientes), debe ser transmitida utilizando mecanismos de criptografía.

c) El acceso a la información confidencial almacenada en las bases de datos y archivos digitales debe ser estrictamente controlado. Si la información se encuentra almacenada en estaciones de trabajo o en dispositivos de almacenamiento portables (discos duros, memorias USB, cintas magnéticas, medios ópticos, etc), se debe utilizar un mecanismo de cifrado fuerte que garantice su confidencialidad e integridad.

d) La información confidencial en medio físico debe ser almacenada en áreas con acceso físico controlado, de tal forma que se garantice que solamente el personal autorizado tiene acceso a ella.

e) Se debe llevar un log que permita realizar una trazabilidad de los cambios realizados a la información confidencial almacenada en medios magnéticos. El log debe identificar el responsable, fecha y hora del cambio.

f) Cualquier información electrónica eliminada de sistemas informáticos y documentos impresos deben ser destruidos de tal forma que se proteja la confidencialidad de la información.

5.3 SEGURIDAD DEL PERSONAL

1.1.2. Cumplimiento del Sistema de Gestión de Seguridad de la Información

a) Es obligación de los usuarios, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir las políticas de seguridad de la información de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR".**

b) La responsabilidad de seguridad es parte de los términos y condiciones del empleo. La violación o no cumplimiento de cualquiera de las directrices documentadas en las políticas de seguridad de la información establecidas por **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**, serán argumentos para la aplicación de acciones disciplinarias, incluyendo la terminación del contrato.

1.1.3. Acuerdos de Confidencialidad

a) Todos los empleados, sin importar el tipo de contrato, ya sea a término fijo o indefinido, deben firmar un acuerdo de confidencialidad en el momento en que ingresan a **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR".**

b) Todo el personal vinculado como contratista, trabajador en misión, contrato de aprendizaje, practicante, etc., debe firmar un acuerdo de confidencialidad en el momento del inicio de sus labores en **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR".**

1.1.4. Procesos Disciplinarios

a) Todo el personal que cometa un fallo de seguridad, por ejemplo la violación deliberada de estas políticas de seguridad de la información, debe ser sancionado mediante un proceso disciplinario ejecutado por el Director Administrativo, para el caso de funcionarios de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** o a través de contratos o procesos jurídicos en caso de terceros.

b) Los procesos disciplinarios pueden incluir una serie de acciones en función de la gravedad de la violación, iniciando por memorandos con copia a la hoja de vida del infractor hasta la cancelación del contrato laboral y acciones legales para recuperar las perdidas y los daños consecuentes.

c) Para el caso de funcionarios de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**, los procesos disciplinarios a los que se someterán los empleados que no cumplan las políticas de seguridad son:

   a. Llamado de atención por parte del Comité de Seguridad Informática de la Información, en donde se detalle el incumplimiento y las causas que puede generar.

   b. En caso de reincidencia, se enviara un llamado de atención con copia a la Hoja de vida y al jefe inmediato.

   c. En caso de reincidencia, el empleado se suspenderá de sus actividades por un lapso de 3 a 5 días dependiente de la gravedad del incidente.

   d. En caso de reincidencia continua, se cancelará su contrato laboral.

d) Si el incidente afecta económicamente o la reputación de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**, se realizarán las acciones civiles correspondientes de acuerdo a la legislación Colombiana.

1.1.5. Conocimiento, educación y Entrenamiento de seguridad de la información

a) **El JEFE DE LA DIVSIÓN CORPORATIVA Y GESTION HUMANA** es responsable del desarrollo de planes de capacitación, educación y sensibilización en seguridad de la información y uso adecuado de los recursos tecnológicos para todos los funcionarios.

b) Todo el personal debe participar en las sesiones de concientización frente a temas de seguridad de la información. Un resumen impreso de las medidas de seguridad básicas de la información se debe proporcionar a cada empleado, temporal, contratista o practicante y guardar una copia firmada en archivo.

c) **El JEFE DE LA DIVSIÓN CORPORATIVA Y GESTION HUMANA** con asesoría del **Departamento de Sistemas,** deben desarrollar estrategias de sensibilización, entrenamiento y educación en seguridad de la información, para promover conocimiento constante a todos los empleados, temporales, contratistas y practicantes. La estrategia de sensibilización de seguridad debe consistir en entrenamiento y resúmenes impresos constantes.

1.1.6. Terminación o Cambio de Empleo de los Funcionarios

a) El personal que se retira de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe recibir por parte del Jefe de la División correspondiente un recordatorio acerca de los compromisos legales y éticos adquiridos con respecto a mantener la confidencialidad de la información a la cual tuvo acceso durante el transcurso de su desempeño.

b) Consideraciones similares deben ser aplicadas cuando un funcionario de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** cambie de funciones en una misma área o en áreas diferentes. En este caso, los Jefe de la División involucrados en la transferencia del personal, deben tramitar que el acceso a la información confidencial de las áreas involucradas es protegida de accesos o modificaciones no autorizadas.

c) Todo el personal sin importar el tipo de vinculación laboral, que se retire de LA **CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**, debe entregar al Jefe de la División y/o Coordinador de Sistemas los activos informáticos asignados para su cargo (incluyendo documentos, archivos digitalizados, computadores, información de Clientes almacenada en teléfonos móviles o computadores de mano, dispositivos de almacenamiento USB, y los password de los diferentes usuarios en los sistemas de información).

d) **El JEFE INMEDIATO** debe informar las novedades de (ingresos, retiros, reemplazos, traslados, etc.) del personal a cargo, al Coordinador de Sistemas solicitando la asignación, modificación o desactivación de los respectivos permisos y perfiles de cada usuario a los sistemas de información, según sea el caso, a través del formato de solicitud de requerimientos.

e) El acceso a la información, computadores, redes de datos e instalaciones físicas, deben ser revocadas de inmediato cuando un funcionario o un tercero se retira de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**.

1.1.7. Investigación de Empleados

a) **EL JEFE DE LA DIVISIÓN CORPORATIVA Y GESTIÓN HUMANA** debe realizar una investigación a todo candidato potencial que pueda llegar a ser empleado de la Entidad. Esto puede incluir pruebas psicológicas, referencias personales y laborales, verificación de la educación, entre otros. Si el empleado se está buscando a través de terceros o una agencia apropiada, debe seguirse los mismos análisis definidos para la investigación en ambos casos.

b) Los empleados contratados para cargos en los cuales deban tener acceso a información Confidencial de la Entidad debe tener investigación adicional de acuerdo con las necesidades definidas en las leyes o regulaciones.

5.4 SEGURIDAD FÍSICA Y DEL ENTORNO

5.4.1 Áreas de Acceso Restringido

a) Se define como aquellas áreas que necesitan autorización previa para permitir el ingreso de personas ajenas al área, por la naturaleza de la información confidencial que se maneja o los procesos que allí se realizan. Dentro de la Organización fueron identificadas las siguientes:

a. Oficina de Sistemas
b. Tesorería
c. Archivo (histórico, subsidios, Administración).

5.4.2 Control de Acceso Físico a las dependencias de LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"

a) El ingreso de dispositivos de grabación de audio, fotos y video a las áreas de acceso restringido o áreas seguras está totalmente prohibido.

b) **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe asegurar que los derechos de acceso a todas las instalaciones son revisados anualmente. El acceso a lugares considerados áreas seguras, debe ser revisado regularmente.

c) Todos los visitantes, empleados, temporales, contratistas y practicantes deben ser autorizados para la entrada física a las instalaciones de acceso restringido de la **CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**

d) Los funcionarios de la **CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** deben portar en un lugar visible el carnet de identificación como funcionarios.

e) La autorización del acceso de visitantes a las áreas seguras está en cabeza de la Dirección o el delegado de ésta de acuerdo al procedimiento establecido según corresponda.

f) Una vez autorizado el ingreso del visitante, el funcionario visitado deberá recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área segura.

g) Todos los visitantes a las áreas seguras deben firmar una lista de control de acceso antes de ingresar al área. En esta bitácora se debe registrar entre otros los siguientes datos: nombre del visitante, la fecha, la hora de entrada y de salida y la persona que es visitada. Esta bitácora debe estar disponible para efectos de auditoría por un periodo no inferior a un año.

5.4.3 Protección de Centros de Cómputo

a) Las sala de sistemas de las sedes de Colegios de **LA CAJA DE COMPENSACIÓN FAMILIAR DE EL SUR DE EL TOLIMA "CAFASUR",** deben

incorporar medidas de protección para reducir al mínimo la posibilidad y las repercusiones de incidentes como incendios, inundaciones, terremotos, explosiones, disturbios civiles, etc.

b) El sistema eléctrico del centro de cómputo debe contar con un sistema de UPS, así como de condiciones eléctricas acordes a las normas internacionales.

c) Las instalaciones del centro de cómputo se deben supervisar 24 horas al día. Esta supervisión puede ser realizada por medio de las cámaras de video, puertas de emergencia y ventanas, personas de vigilancia en los centros, o una combinación de lo antes nombrado.

d) Los operadores, administradores y visitantes frecuentes al centro de cómputo, deben ser capacitados en los procedimientos que deben seguir cuando se presente un evento de origen físico que afecte la continuidad en la operación normal del centro de cómputo.

e) Los equipos y dispositivos que son utilizados para soportar las funciones del negocio, deben estar en un área de acceso restringido y separadas del ambiente de las oficinas y puntos de atención.

f) Está totalmente prohibido fumar y consumir alimentos en el centro de cómputo.

g) Cuartos que contienen el cableado o el equipo de comunicaciones (armarios de cableado, cuartos de PBX, etc.) debe estar siempre con acceso restringido y solamente a personal autorizado.

5.4.4 Seguridad del Cableado

a) Debe haber un monitoreo periódico sobre las redes de cableado estructurado de voz y datos y los gabinetes de cableado, para detectar, eliminar o prevenir el uso de dispositivos no autorizados conectados a los cables.

b) El Coordinador de Sistemas debe asegurar que todas las conexiones de red que existan en un lugar que no está siendo utilizado de manera permanente están deshabilitadas.

c) Los conductos 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.

d) Los cuartos asignados para los gabinetes de cableado estructurado deben contar con acceso físico restringido y no se debe almacenar ningún tipo de material inflamable.

5.4.5 Mantenimiento de Equipos

a) El Coordinador de Sistemas **con el apoyo de la Dirección,** debe garantizar que el acceso al mantenimiento preventivo y/o correctivo de software o hardware es realizado por funcionarios debidamente autorizados e identificados. Ningún funcionario de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe permitir la manipulación de equipos y/o software por personal que no esté identificado y autorizado. Si el equipo debe ser sacado de las instalaciones para realizar las reparaciones, la confidencialidad e integridad de cualquier información debe ser garantizada.

b) Todos los recursos de TI (hardware y software) que soportan la operación de los procesos de la organización, así como la atención de los Clientes en los diferentes canales de servicio, deben contar con un mantenimiento preventivo y correctivo por parte del Departamento de Sistemas, el fabricante o proveedor.

c) En caso de presentarse un daño sobre algún elemento de trabajo por causas como: golpes, derrame de bebidas, elementos extraños, etc., la reparación o reposición debe estar a cargo de la persona a cargo del activo tecnológico.

5.4.6 Protección y Ubicación de Equipos

a) Para prevenir el acceso, la duplicación y la transmisión no autorizada de información confidencial, todas las impresoras, copiadoras, y máquinas de fax se deben situar en áreas seguras.

b) Todos los equipos tecnológicos de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** deben ser ubicados o localizados de tal forma que se reduzca al mínimo los riesgos o amenazas. Esto incluye amenazas como hurto o vandalismo, fuego, explosión, humo, agentes químicos, pérdida de servicios de soporte como energía, comunicación, agua o cualquier otra amenaza física.

c) Los cuartos 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, etc)

d) Fumar, beber y comer en instalaciones de procesamiento de información está terminantemente prohibido.

e) **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe asegurar que cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y que vaya a ser reutilizado, experimente un proceso de limpieza lógica antes de ser utilizado nuevamente. El proceso de limpieza lógica 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.

f) **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe asegurar que para cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y vaya a ser dado de baja, sus dispositivos de almacenamiento de información (disco duro, memoria RAM, memoria FLASH, etc.) sean destruidos físicamente antes de su disposición final.

5.4.7 Seguridad de Equipos Móviles

a) Todo equipo de propiedad de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** que esté fuera de las instalaciones de la Organización, no debe ser desatendido por su responsable en lugares públicos.

b) El Departamento de Sistemas debe asegurar físicamente los equipos portátiles y contar con pólizas de seguro para los computadores y equipos tecnológicos.

c) El Departamento de Sistemas debe velar porque los estándares de seguridad documentados dentro de la política se apliquen a todos los equipos y la información que en ellos se almacena, sin importar la localización de los mismos.

5.4.8 Retiro de equipos de las Instalaciones

a) En caso de retiro de un equipo de las instalaciones de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**, se debe solicitar permiso a la Dirección y debe quedar el registro en el formato de Orden

de Salida con la fecha y hora de salida, también debe registrarse el nombre del responsable a cargo del equipo.

5.4.9 Suministros de Equipos de Soporte Energético

a) El Departamento de Sistemas debe asegurarse que las fuentes de alimentación continuas (UPS) son utilizadas en los equipos que apoyan las operaciones de negocio críticas para facilitar la disponibilidad de los sistemas y su correcto apagado. Las UPS deben ser revisadas periódicamente para asegurar que tienen la capacidad adecuada y aprobada, de acuerdo con las recomendaciones del fabricante.

b) El Departamento de Sistemas, con el apoyo del Director Administrativo deben realizar o contratar un estudio de las cargas en los circuitos, para que en un eventual apagón, la planta eléctrica envíe los voltajes adecuados, para sostener el sistema de corriente ininterrumpido en la corporación.

5.4.10 Política de Escritorio Limpio

a) Realizar un escaneo con el antivirus en las unidades de almacenamiento externo (USB, CDROM, DVD, CAMARAS, TELEFONOS CELULARES etc.) antes de ser utilizados en las estaciones de trabajo asignadas para el cumplimiento de las funciones.

b) El uso del correo electrónico institucional es obligatorio para el intercambio de archivos en vez de unidades de almacenamiento externo.

c) La información clasificada confidencial que no esté siendo utilizada por personal autorizado, debe permanecer siempre bajo llave y no debe ser desatendida en ninguna ubicación no controlada.

d) Todos los funcionarios que tengan bajo su responsabilidad información confidencial, deben contar con un archivador con llave para guardar todo el material sensible (material impreso, en medios magnéticos, etc.) y una copia de la llave debe ser entregada a la Dirección Administrativa.

5.4.11 Política de Equipos Desatendidos

a) Cuando un funcionario se retire temporalmente de su puesto de trabajo, debe salir de la sesión del aplicativo.

b) La opción de protector de pantalla de Windows debe configurarse con los siguientes parámetros:

   a. Activar el protector de pantalla después de 5 minutos de inactividad del computador.

   b. El desbloqueo requiere contraseña

c) Durante cualquier reubicación del espacio de trabajo de un empleado, el empleado debe asegurar que todos los activos de información están protegidos durante el proceso de reubicación.

d) Durante cualquier reubicación del espacio de trabajo del empleado, la información altamente sensible debe ser trasladada por el dueño de la información.

5.5 CONTROL DE ACCESO

5.5.1 Política de Control de Acceso Lógico

a) Todos los recursos informáticos y/o aplicativos de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** deben usar controles de acceso lógico, con el fin de prevenir el acceso no autorizado a la información confidencial de la Organización.

b) El acceso lógico a los recursos informáticos de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe ser controlado en función de los requerimientos de la Organización.

c) El control de acceso a la información debe ser definido, aprobado y documentado por el Comité de Seguridad Informática con el apoyo de los responsables de la información y deben estar basados en requerimientos específicos del negocio.

d) Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes (cargos); estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios (política de menor privilegio). Los permisos de acceso a los aplicativos deben ser garantizados por cargos y no por Funcionarios.

e) Los permisos de acceso a las redes, servicios y sistemas de información de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**, serán otorgados de acuerdo a los lineamientos otorgados por el Comité de Seguridad Informática mediante un proceso de aprobación que asegure el acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

f) Se deben deshabilitar o actualizar los privilegios de acceso a los recursos informáticos inmediatamente se presente la novedad correspondiente o cuando se genere un cambio de privilegios en un rol o perfil.

g) Cuando un empleado o un usuario externo deja la Institución o cambia de cargo, **EL JEFE DE LA DIVISIÓN CORPORATIVA Y GESTIÓN HUMANA**, debe informar al Coordinador de Sistemas para realizar la Inactivación, eliminación o reasignación de los privilegios de acceso a los recursos informáticos de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**

h) El Coordinador de Sistemas debe realizar una comparación periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan y verificar que los usuarios que efectivamente acceden a la información corresponden a los autorizados previamente por él.

i) Los aplicativos deben ser el único vehículo para acceder a los datos de producción de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**.

j) Está totalmente prohibido el uso de usuarios compartidos en los sistemas de información.

k) El Coordinador de Sistemas debe garantizar que todos los usuarios que tienen acceso a cuentas privilegiadas tienen sus propias cuentas personales para el

uso diario. El uso de estas cuentas debe ser rastreado y monitoreado periódicamente.

5.5.2 Registro de Usuarios

a) A cada usuario interno y/o externo de la Organización que requiera acceso a los sistemas de información, se le asignará un único código de usuario, el cual es de carácter personal e intransferible.

b) Los usuarios de los recursos informáticos de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** no deben compartir su código de usuario / contraseña o cualquier mecanismo otorgado para su identificación y autenticación. La responsabilidad que un usuario de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** adquiere al recibir su código de usuario / contraseña o cualquier mecanismo de identificación y autenticación se extiende a todo tipo de interacción que ese identificador tenga con el sistema.

c) La creación, modificación y eliminación de cuentas de usuarios debe ser realizada mediante un procedimiento formal y debe ser autorizado por el responsable de los datos.

d) Debe existir un procedimiento formal para deshabilitar los códigos de usuario que no requieren el acceso a los sistemas de información por un periodo de tiempo determinado. Ejemplo funcionarios que salen de vacaciones, licencias, etc. Está totalmente prohibido que las áreas utilicen los códigos de usuarios de funcionarios que se encuentren ausentes de La Empresa. En caso de que se requiere el acceso a un aplicativo, es necesario hacer la solicitud formal para otro funcionario mediante el procedimiento establecido.

e) La eliminación de accesos y servicios de red asociados a un código de usuario debe ser realizada inmediatamente el usuario ha finalizado su vinculación laboral, contractual o comercial con **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** o ha cambiado de rol dentro de la Organización y no se requiere que acceda a éstos recursos informáticos.

f) El Coordinador de Sistemas debe conservar un registro de la solicitud, entrega y eliminación de los usuarios.

g) El Coordinador de Sistemas debe garantizar que los usuarios internos y externos firmen una declaración en la que certifican que reciben el usuario y la contraseña y se comprometen a cumplir las políticas de seguridad y garantizar su confidencialidad.

5.5.3 Política de Administración de Contraseñas

a) Las contraseñas deben cumplir con el siguiente estándar:

   a. Longitud mínima de 8 caracteres
   b. Alfanumérica
   c. Debe contener mayúsculas y minúsculas.

b) La contraseña expira cada 30 días y debe ser cambiada por los usuarios. El sistema avisará antes de iniciar sesión que se debe cambiar la contraseña

c) No se permite repetir ninguna de las ultimas 3 contraseñas

d) El sistema debe solicitar el cambio de la contraseña de manera obligatoria la primera vez que se ingrese al sistema.

e) Los sistemas de información deben permitir que los usuarios puedan crear y modificar sus propias contraseñas.

f) Los sistemas de información deben exigir que los usuarios confirmen su contraseña.

g) Los sistemas deben almacenar y transmitir las contraseñas de modo seguro.

h) El Coordinador de Sistemas debe asegurar que las computadoras, las bases de datos y aplicaciones que almacenan la cuenta de usuario y la contraseña, restringen el acceso sólo al personal autorizado. Este acceso debe ser revisado trimestralmente y debe coincidir con la revisión técnica del servidor y los usuarios utilizados.

i) Los usuarios internos y externos que presenten 3 intentos fallidos en el momento de digitar la contraseña, la cuenta debe ser bloqueada y no pueden tener acceso al sistema de información al cual está intentando acceder. Estas cuentas deben ser desbloqueadas manualmente por El Departamento de Sistemas. La identidad de los usuarios que soliciten restablecer la contraseña debe ser verificada antes de restablecer la contraseña.

j) Los usuarios deben asegurar que las contraseñas no están escritas o almacenadas en los sistemas de información en archivos no protegidos. Los usuarios no deben copiar nombres de usuarios y/o contraseñas en los scripts o archivos de texto claro, trabajos por lotes o la documentación de procesos.

k) El Coordinador de Sistemas debe garantizar que las cuentas de usuario que no hayan sido utilizadas por 90 días se deshabilitan automáticamente.

5.5.4 Inicio de sesión seguro

a) El Coordinador de Sistemas debe garantizar que en el momento de ingresar a los sistemas de información, se le informa al usuario que:

   a. El sistema debe ser utilizado únicamente por usuarios autorizados
   b. Mediante el uso del sistema, el usuario acepta que él o ella es un usuario autorizado
   c. Es consciente que está siendo monitoreado al utilizar este sistema.

b) El Departamento de Sistemas debe garantizar que los sistemas de información no ofrecen a los usuarios toda la información sin antes haber iniciado sesión. El proceso de acceso no debe ofrecer ninguna 'Ayuda' o revelar que característica de la secuencia de inicio de sesión (ID de usuario o contraseña) es incorrecta.

5.5.5 Restricciones en el período de uso de las sesiones

a) El Coordinador de Sistemas debe asegurar que los dispositivos que tengan la capacidad de ejecutar con un protector de pantalla protegido por contraseña sean configurados de esta manera, con el fin de proteger la información allí almacenada. El protector de pantalla debe exigir a la entrada de contraseña después de que el dispositivo ha quedado inactivo durante 5 minutos.

5.5.6 Política de Uso del Correo Electrónico

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

b) El envío de información clasificada como confidencial, debe ser aprobado por la Dirección, Administrador o el Dueño de la Información. Para el envío de esta información, es recomendable utilizar algún mecanismo de cifrado o protección mediante password.

c) Se prohíbe la difusión no solicitada de puntos de vista personales referentes a temas políticos, raciales y religiosos, la inclusión de mensajes sobre creencias, frases célebres, 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.

d) Se prohíbe fomentar el envío de cadenas de mensajes, recepción o envío de mensajes con archivos adjuntos con extensiones .exe, .avi, .mp3, .vbs, .mpg, .Jpg los cuales corresponden a archivos de video, música, gráficos, juegos, ejecutables, etc.

e) Este servicio no debe usarse para enviar SPAM o mensajes no solicitados ni tampoco para enviar material obsceno e ilegal o relacionado a pornografía.

f) Está prohibido configurar reglas en los buzones de correo electrónico que reenvíen los mensajes a servidores públicos de Internet como Hotmail, yahoo, etc.

g) 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 Empresa.

h) No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye sin limitación alguna, todo material protegido por derechos de autor (copyright), Marcas registradas, secretos comerciales u otros de propiedad intelectual.

i) El tamaño de los archivos adjuntos no debe exceder de 20 MB, este tamaño puede ser chequeado por medio de las propiedades de cada archivo. Si el archivo adjunto excede este tamaño, es necesario comprimir el archivo.

j) Los buzones tienen una cuota máxima de hasta 2000 MB de almacenamiento por usuario, por lo tanto, el usuario debe eliminar periódicamente los mensajes leídos de modo tal que no exceda esa cuota. En caso de que el usuario requiera ampliación de esta capacidad, debe ser autorizada por el Coordinador de Sistemas

k) La firma predeterminada solo puede contener nombre y apellidos, cargo, extensión y nombre de la compañía.

l) En caso de recibir un mensaje bajo sospecha de virus, (de personas desconocidas con asuntos desconocidos o sospechosos) no se debe abrir y se debe reportar de inmediato al Departamento de sistemas.

m) No está permitido el uso de cuentas de correo personales o de servicios de correo externo como Hotmail, Yahoo, Gmail, etc., para transmitir o intercambiar información referente o perteneciente a **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**

5.5.7 Políticas de Uso de Internet

a) El acceso a internet debe ser aprobado por el Director de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**.

b) El acceso a internet está restringido únicamente a páginas de información financiera, técnica, comercial, cultural, etc., a las cuales por desarrollo de las actividades propias de cada cargo sea necesario ingresar para consultar información que faciliten las labores relacionadas al cargo. En el caso de Tener excepción deben ser autorizado por el Director Administrativo.

c) El acceso a internet NO puede ser utilizado para los siguientes propósitos:

a. Actividades relacionadas a juegos online por internet.

b. Ingreso a cualquier material considerado como pornográfico, ofensivo, discriminatorio o ilegal según las normas internas de La Empresa y la legislación.

c. Ingreso a páginas de pornografía infantil.

d. Ingreso a Redes sociales como Facebook, Twitter, Linkedin, etc.

e. 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.

f. Utilizar los servicios de RADIO y TV por demanda.

g. Utilizar los servicios de Internet para enviar archivos que sean confidenciales y de propiedad exclusiva de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"**.

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

i. Utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegido por las leyes vigentes. Esto incluye todos los archivos protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.

j. 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.

k. No se podrán utilizar los servicios de internet corporativo para establecer comunicaciones vía chat sin el VoBo de la Dirección.

5.6 CUMPLIMIENTO DE LOS REQUISITOS LEGALES

5.6.1 Identificación de la legislación aplicable

a) Todos los requisitos legales, contractuales, o regulatorios que sean aplicables a la Organización deben ser documentados y definidos por la Oficina Jurídica. Los requisitos y las responsabilidades específicas de controles u otras actividades relacionadas, con estas regulaciones legales, deben ser delegadas a la división apropiada.

5.6.2 Derechos de Propiedad Intelectual

a) Todo el software instalado en las estaciones de trabajo y servidores de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe ser licenciado y los usuarios deben cumplir con las leyes y las restricciones de derecho de autor definidos por el fabricante. Adicionalmente, todo el software instalado en los recursos informáticos de la Entidad debe ser aprobado por el Coordinado de Sistemas. Cualquier software debe ser analizado y aprobado por esta área.

b) La instalación de software o el uso de información externa en los recursos informáticos de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** debe ser previamente autorizada por la Dirección y debe cumplir con los requerimientos legales que faculten su utilización.

c) El software que reside en los computadores de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** sólo podrá ser autorizado por la Dirección. No se podrá instalar en los computadores de la Empresa software que no esté registrado y autorizado.

d) El Departamento de Sistemas de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** realizará revisiones periódicas al software instalado en las estaciones de trabajo y eliminará sin previo aviso todos los aplicativos y archivos que no estén autorizados previamente. Los responsables de la instalación, descarga y/o uso de software que viole los acuerdos de licenciamiento serán sujetos a las acciones disciplinarias definidas por parte de la Dirección.

e) El Coordinador de Sistemas debe aprobar todo el shareware y freeware para ser usados en los recursos de cómputo de la Entidad con el fin de asegurar que en

el software no esté presente código malicioso y/o que no cumpla con las necesidades de la Entidad o de seguridad.

f) Las violaciones de los derechos o políticas de propiedad intelectual de la Entidad están sujetas a acciones disciplinarias.

g) La compra o uso de software de terceros debe cumplir con los acuerdos de licenciamiento definidos por el fabricante. Estos acuerdos pueden detallar restricciones específicas del usuario (ej.: el número de las copias instaladas permitidas, número de máquinas donde es posible instalar el software o número de usuarios concurrentes que pueden conectarse al software). Los niveles de soporte a **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** (en sitio o por teléfono) se pueden también especificar dentro del acuerdo. El uso o copia del software comprado en un equipo adicional se prohíbe terminantemente.

5.6.3 Propiedad Intelectual

a) Todos los desarrollos de productos realizados por funcionarios de la Organización, contratados o producidos bajo acuerdos que le asignen la propiedad intelectual del trabajo a **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR"** son de propiedad de **LA CAJA DE COMPENSACIÓN FAMILIAR DEL SUR DEL TOLIMA "CAFASUR".**

5.6.4 Prevención del mal uso de las instalaciones de procesamiento de información

a) El monitoreo de los sistemas de información y/o estaciones de trabajo se realizara exclusivamente por los organismos de control interno de la Organización y se debe llevar a cabo de acuerdo a las leyes y regulaciones locales.

b) Los recursos de tecnología (hardware y software) son para uso exclusivo del negocio. El uso no adecuado de cualquier recurso de tecnología de la Entidad o para otros propósitos diferentes a los definidos por el negocio está prohibido. Cualquier actividad no autorizada debe ser reportada a la Dirección.

c) Los usuarios deben ser notificados, mediante mensajes escritos o a través de mensajes de alerta al obtener acceso a sistemas, que la actividad está siendo monitoreada.

5.6.5 Protección de registros de la Entidad

a) Los estándares para la recolección, custodia, manejo y destrucción de registros deben ser desarrollados para cualquier información cubierta por estatutos legales o regulatorios. El cronograma de retención para este tipo de información debe ser definido y divulgado. Dicho cronograma debe contener, sin limitar:

- Tipo de información.
- Estatutos reguladores relacionados.
- Inventario de fuentes de este tipo de información.
- Período de retención de registro.
- Requerimientos apropiados de almacenaje y manejo.
- Métodos apropiados de destrucción.
- Cualquier requisito especial implementado que no esté definido en la política de seguridad de la Entidad.

b) Es responsabilidad del dueño de la información definir el cronograma de retención de cada registro documental.

5.6.6 Regulación de controles criptográficos

a) La seguridad criptográfica, incluyendo el uso de hardware o software, implementados en los sistemas corporativos deben cumplir con cualquier legislación local o internacional.

5.6.7 Cumplimiento de las políticas de seguridad

a) Los Administradores de Unidades y Coordinadores deben llevar a cabo los procedimientos de escalamiento y reporte cuando se observa el incumplimiento o se genera una excepción de la política de seguridad de la Entidad.

b) Los Administradores de Unidades y Coordinadores deben revisar regularmente los procesos y procedimientos dentro de su área para asegurar que las responsabilidades y deberes de seguridad se realizan apropiadamente. Los resultados de esta revisión y las acciones correctivas deben ser documentados.

c) El Comité de Seguridad Informática debe asignar las actividades de revisión para mantener el cumplimiento con las prácticas de seguridad de la Entidad. Las

situaciones que dan como resultado el incumplimiento de las prácticas deben ser reportadas a Dirección. Las actividades de revisión deben incluir el monitoreo operacional del cumplimiento, análisis individual del sistema, revisiones de terceros, pruebas de conformidad internas, y/o revisiones de los procedimientos.

d) La violación deliberada de las políticas de seguridad de la información y/o del incumplimiento de regulaciones, será sancionada mediante un proceso disciplinario ejecutado por el Director Administrativo para el caso de funcionarios de La Empresa o a través de contratos o procesos jurídicos en caso de terceros

6 Control de cambios

Control de cambios		
Fecha	**Descripción**	**Versión**
10/02/2022	Política de resarcimiento y/o reconexión con el afiliado	1.0.0
/12/2024	Actualización de la política según PDM de la SSF	2.0.0

7 Registro de aprobación

	Nombre	Cargo	Fecha
Actualizó	Sergio Alejandro Gómez Franco	Coordinador de Sistemas	16/12/2024
Revisó	Jenny Milena Gutiérrez	Jefe de División de Planeación	16/12/2024
Revisó	Jhonatan Steven Arias M.	Jefe de División Corporativa y Gestión Humana	18/12/2024
Revisó	Diana María Barrios Murillo	Jefe de División Jurídica	18/12/2024
Revisó	Julio Cesar Murillo Prada	Jefe División de Auditoría	18/12/2024
Aprobó	Carlos Alfonso Melo P.	Director Administrativo	19/12/2024
Observaciones			