POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 2

VIGENCIA, JUNIO DE 2018

M-A-05-01

Comfamiliar-Más Felicidad

TABLA DE CONTENIDO

1. OBJETIVO

Comunicar a los colaboradores de la Caja, contratistas, outsourcing, proveedores y Clientes las políticas y normas establecidos por la Dirección de la Caja para garantizar altos niveles de seguridad de la información de la Caja y nuestros Clientes.

1.1. Objetivos específicos:

a) *Garantizar altos niveles de seguridad a la información de* ***COMFAMILIAR*** *y sus Clientes*

b) *Proteger la información en la forma en que se encuentre (física o digital) de las amenazas que afecten su confidencialidad, integridad y disponibilidad.*

c) *Optimizar los controles de seguridad en el manejo de recursos de TI*

2. ALCANCE

Este documento establece la política de seguridad de la información y las normas relacionadas con la seguridad y es de obligatorio cumplimiento para todos los colaboradores, contratistas, outsourcing y proveedores de ***COMFAMILIAR****.*

La consulta permanente de este documento está reservada a los colaboradores y los contratistas que por sus funciones tienen acceso a los sistemas de información de la Caja.

Este documento tiene la clasificación de confidencial

La estructura de este documento este enmarcado bajo la norma ISO/IEC 27001:2005 y documenta las normas de seguridad para los siguientes dominios:

a. *Política de Seguridad de* ***COMFAMILIAR***
b. *Seguridad física y del entorno*
c. *Gestión de comunicaciones y operaciones*
d. *Control de acceso lógico*

3. DEFINICIONES

- ***ACTIVOS DE INFORMACIÓN:*** *Recursos del sistema de información o relacionados con éste, necesarios para que la Caja funcione correctamente y alcance los objetivos propuestos por su dirección. Se pueden estructurar en cinco categorías: La gente (empleados, contratistas, temporales, practicantes, afiliados y entidades), la información en cualquiera que sea su medio (oral, escrita, magnética, óptica, digital), los procesos de* ***COMFAMILIAR****, el hardware (equipos de cómputo centrales y locales, redes de comunicación y redes eléctricas) y el software (programas aplicativos en general, BD y sistemas operacionales).*

- ***CONFIDENCIALIDAD:*** *Criterio de seguridad de la información que hace referencia a la protección y acceso a la información por parte únicamente de quienes estén autorizados*

- ***DISPONIBILIDAD****: Criterio de seguridad de la información que hace referencia al acceso a la información y a los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.*

- ***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.*

- ***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.*

- ***INTEGRIDAD****: Criterio de seguridad de la información que hace referencia al mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.*

- ***INTERNET****: es un sistema mundial de redes interconectadas entre si, accesible desde cualquier parte del mundo mediante un dispositivo electrónico diseñado para navegar en la red, extrayendo y/o adicionando información que el usuario considere pertinente en su momento.*

- ***INTRANET****: el servicio que utiliza tecnología de internet aplicada a una red interna o de área local, con la diferencia que el contenido solo esta disponible dentro de la misma red.*

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

- ***RECURSOS INFORMATICOS****: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con ordenadores y periféricos, tanto a nivel individual como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.*

- ***RESPONSABLE 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. 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.*

- ***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.*

- ***CORREO ELECTRÓNICO:*** *Es el intercambio de mensajes escritos digitalmente entre usuarios con el mismo servicio en donde se pueden adjuntar archivos de cualquier tipo, y se realiza por medio de una conexión a Internet o Intranet.*

4. ABREVIATURAS

La letra A indica a que proceso funcional de la organización va dirigida cada política. Las letras U G ó T las puntualizan y su significado es el siguiente:

***(U)** Dirigida a los usuarios finales*

***(G)** Dirigida a la Gerencia y/o Coordinaciones.*

***(T)** Dirigida a la División de Tecnología Informática*

5. RESPONSABILIDADES

Coordinador de TI

Es responsable de:

- ✓ *Elaborar y actualizar el Manual de Políticas de Seguridad de la Información*
- ✓ *Publicar, difundir, capacitar y concienciar a todos los colaboradores y externos de* ***COMFAMILIAR*** *acerca de las políticas de seguridad de la información y su cumplimiento.*

6. DOCUMENTOS DE REFERENCIA

- *Norma ISO/IEC 27001:2005*
- *Norma ISO/IEC 27002:2005*

7. NORMAS PARA LA SEGURIDAD DE LA INFORMACIÓN DE COMFAMILIAR HUILA

7.1. Política de seguridad de la información de Comfamiliar Huila

*La Dirección de **COMFAMILIAR** teniendo en cuenta que la información y los sistemas implicados en su procesamiento, almacenamiento y comunicación son recursos críticos para el normal desarrollo de los procesos de la Caja y soporte primordial para la consecución de los objetivos estratégicos, establece el Manual de Políticas de Seguridad de la Información en el cual se definen las normas necesarias para preservar su confidencialidad, integridad y disponibilidad e invita a todos los Colaboradores y contratistas de la Caja a acatarlas y velar por el uso adecuado y seguro de la información de **COMFAMILIAR** y sus Clientes.*

7.2. Responsabilidades del personal de Comfamiliar

***Coordinador de TI:** Es responsable de:*

- ✓ *Elaborar y actualizar el Manual de Políticas de Seguridad de la Información*
- ✓ *Publicar, difundir, capacitar y concienciar a todos los funcionarios y externos de **COMFAMILIAR** acerca de las políticas de seguridad de la información y su cumplimiento.*

- ***Responsabilidad del personal:** Todos los colaboradores y terceros que presten servicios para Comfamiliar, serán responsables del cumplimiento de las políticas, normas, procedimientos y estándares establecidos que buscan garantizar la seguridad de la plataforma tecnológica.*

- ***Responsabilidad en manejo de la información:** Es responsabilidad de todos los colaboradores de Comfamiliar, velar por la veracidad, integridad, seguridad, confidencialidad y disponibilidad de los datos y porque la información sea elaborada, generada, operada, modificada, almacenada, conservada, transportada, accedida, divulgada o destruida, de acuerdo con las normas establecidas.*

La información confidencial y la jerarquía de los colaboradores han de emplearse de manera acorde con su naturaleza y carácter, y ningún empleado podrá aprovecharse de ellas para obtener ventajas o beneficios para sí o para terceros, ni ejercer tráfico de influencias con ellas.

La circulación de "rumores o comunicaciones informales" es un comportamiento contrario a la cultura de la Organización y a la dignidad de las personas que afecta. El

adecuado manejo de la información y de la comunicación obliga a brindar, un trato digno, respetuoso y cordial.

Los contratistas que tengan acceso a la información de Comfamiliar tendrán iguales responsabilidades y ésta exigencia deberá hacerse constar en los contratos por ellos suscritos. (Acuerdo de Cofidencialidad).

7.3. Propiedad de la Información

Toda la información generada, adquirida o administrada por las personas que laboran para la Caja es propiedad de Comfamiliar, y como tal no debe ser empleada para usos diferentes al cumplimiento de sus funciones. Asimismo, toda la información generada, adquirida o administrada por terceros, en virtud de la ejecución de procesos institucionales y de la prestación de servicios, también se considera propiedad de la Organización y en consecuencia no deberá ser empleada para usos diferentes a los que se acuerden contractualmente.

7.4. Privacidad de la Información

La información institucional será clasificada y requerida por cada Coordinador de Proceso según el grado de privacidad y confidencialidad. Los usuarios de la información tendrán restricciones para el acceso a la misma, de acuerdo con las clasificaciones establecidas, en el presente manual.

Las normas y procedimientos restrictivos para el acceso a la información no aplicarán cuando se trate de suministrarla a los entes de control y a las instancias que legalmente tengan derecho, siempre y cuando busquen acceder a ella a través de los conductos regulares.

La información oficial de la Caja, dirigida a públicos externos deberá siempre contar con la revisión y la aprobación de la Dirección y/o Secretario General, quien la suscribirá

De acuerdo a la privacidad de la información Comfamiliar cuenta con el siguiente esquema de clasificación:

CLASIFICACIÓN	***EJEMPLOS***	***DESCRIPCIÓN***
Pública	*Información de página Web*	*Información compartida con los usuarios externos a COMFAMILIAR. Normas, reglamentos, resultados, servicios ofrecidos, etc.*

Interna	*Información de beneficios de los colaboradores, reglamento interno de trabajo.*	*Información que solo le compete a los colaboradores de COMFAMILIAR, que puede ser conocida por todos estos pero que no debe ser conocida por terceros o personal externo.*
Confidencial	*Facturación, Nómina, Presupuesto, Cartera, Jurídica, Calidad, Estrategias de Mercadeo y Operación. Usuario y contraseña.*	*Información de COMFAMILIAR que soporta los procesos de negocio de información. Procedimientos, políticas, datos de identificación del cliente interno (Colaboradores) y externo (proveedores, afiliados, usuarios),etc.*

7.5. Procedimiento para la elaboración y clasificación de la Información

- ✓ *El dueño de la información es responsable por la definición de la clasificación de la misma.*

- ✓ *Toda actualización realizada en la información clasificada, debe estar soportada por un cambio previamente aprobado por el Coordinador del proceso sobre los componentes que afectan la información y dicho cambio ha de realizarse a través de los procedimientos establecidos para tal efecto.*

- ✓ *Debe ser posible, en todo momento, determinar el estado de la información con respecto a posibles cambios relacionados que lo afecte. (Incluir en gestión reporte de novedades la autorización para la elaboración, actualización y anulación de los registros).*

- ✓ *Toda inconsistencia entre la información de las bases de datos y la infraestructura real del sistema, deberá ser reportada a través del aplicativo Soltic al Coordinador de TI.*

✓ *Toda inconsistencia entre la información de las bases de datos y la infraestructura real del sistema deberá ser investigada y rastreada para determinar los responsables.*

✓ *La información debe seguir los estándares de clasificación definidos.*

✓ *La Matriz de información debe documentarse en un formato consolidado por proceso que contenga la clasificación según establecida por COMFAMILIAR.*

✓ *La Matriz de información se debe actualizar anualmente, con el fin de mantenerla identificada.*

✓ *La información no puede desclasificarse o disminuir su nivel de clasificación sin llevar a cabo un análisis, el cual debe ser aprobado por el dueño de la información, quien determinará si su información puede moverse a una clasificación más baja basado en las definiciones de clasificación desarrolladas por COMFAMILIAR. Alternativamente, el dueño de la información determinará si se incrementa el nivel de clasificación de un activo de información basado en dichas definiciones. Es responsabilidad del dueño de la información supervisar sus activos de información y de validar continuamente su clasificación de la información.*

Normas de uso de la información física

a. *Cada responsable adaptará el archivo de gestión con las condiciones de seguridad necesarias para archivar y salvaguardar la información confidencial.*

b. *Los colaboradores de Comfamiliar no podrán emplear la información entregada para obtener un beneficio propio, ni podrá compartirla con terceros para que ellos obtengan algún beneficio.*

c. *Los documentos o archivos que contienen información confidencial no deben exhibirse en lugares públicos, no pueden dejarse abandonados en salas de reuniones, escritorios o mesas de trabajo en donde puedan ser vistos por personas ajenas a Comfamiliar o por personal no autorizado de ésta. De igual forma, los computadores personales o terminales que permitan accesar información confidencial deben quedar apagados y bloqueados a personas ajenas a Comfamiliar o de personal no autorizado.*

8. SEGURIDAD FÍSICA Y DEL ENTORNO

8.1. Áreas de Acceso Restringido

Se definen como aquellas áreas que por la naturaleza y nivel de confidencialidad de la información que se maneja el acceso físico se encuentra restringido y exclusivo para los funcionarios pertenecientes al área. Los invitados sean funcionarios de la Caja o no necesitan autorización previa para el ingreso. Las áreas de acceso restringido en ***COMFAMILIAR*** *son:*

a) *Centro de cómputo Principal*
b) *Centro de cómputo alterno o de contingencia*
c) *Centros de cableado estructurado y/o comunicaciones en los pisos*
d) *Área de TI*
e) *Cajas de Tesorería*
f) *Archivo Central e Histórico*
g) *CDI (Centro de Documentación e Información)*
h) *Áreas de Cajas Fuertes*
i) *Archivo Hojas de Vida*
j) *Área Análisis de Credito*
k) *Archivo Proceso Jurídica*
l) *Circuito Cerrado de Televisión*
m) *Archivo de Historias Clínicas*
n) *Oficina Servicio al Cliente PQR*

8.2. Normas de seguridad para el Acceso Físico a las áreas restringidas

a) *La autorización de ingreso de visitantes a las áreas restringidas esta en cabeza de los Jefes de las áreas y se debe otorgar exclusivamente por razones del negocio.*

b) *Una vez autorizado el ingreso del visitante, el colaborador visitado debe recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área restringida.*

c) *Todos los visitantes deben registrar su ingreso en la Bitácora de visitas. Entre otros datos se debe registrar el nombre del visitante, fecha y hora de entrada y salida, persona visitada y la razón de la visita.*

d) *Se deben conservar los registros de las bitácoras de acceso a las áreas restringidas de la Caja por un periodo de 2 años, con el objeto de contar con información acerca*

de las personas que entran y salen de las instalaciones con información sensible, la cual deberá ser proporcionada en caso de revisiones de auditoría.

e) *El ingreso de cualquier dispositivo de grabación de audio, fotos y video a las áreas de acceso restringido está totalmente prohibido.*

8.2.1 Protección y Ubicación de Equipos y redes

a) *Todos los equipos principales que soportan los aplicativos, bases de datos, sistemas de comunicación y sistemas de seguridad se deben alojar en áreas restringidas protegidas por un perímetro de seguridad y con controles de acceso físico.*

b) *Los Jefes de las áreas de la Caja deben establecer controles de seguridad física contra la pérdida de computadores, impresoras, equipos de oficina o sus partes.*

c) *Está totalmente prohibido retirar computadores o algunos de sus accesorios fuera de las instalaciones de la Caja sin la debida autorización y diligenciamiento del formato correspondiente.*

d) *El retiro de las instalaciones de la Caja de cualquier equipo de cómputo, debe ser autorizado por el Coordinador del proceso y Coordinador de Servicios Generales. La autorización en las Sucursales será firmada por el Coordinador de la Agencia.*

e) *El Coordinador de TI debe establecer un plan de mantenimientos preventivos y correctivos para todos los computadores de la Caja.*

f) *Está prohibido manipular las redes de cableado estructurado de voz, datos o eléctrico así como instalar cables, extensiones eléctricas, desprender marcaciones de tomas de cableado o dañar los tubos o canaletas de cableado.*

g) *Está totalmente prohibido fumar, beber y comer cerca de los equipos de cómputo o en áreas de alojamiento de equipos críticos como los centros de cómputo o centros de distribución de cableado estructurado.*

h) *Esta totalmente prohibido utilizar equipos de cómputo que han sido dados de baja, mediante concepto técnico, ya sea porque cumplieron su vida útil o su sistema operativo es obsoleto, por lo anterior a estos equipos no se les realizará mantenimiento preventivo ni correctivo.*

8.2.2 Seguridad de Equipos Móviles

a) *El suministro de equipos móviles de la Caja debe ser autorizado por el Coordinador de TI y el Coordinador del proceso y se entregará por razones estrictas del negocio.*

b) *No se debe almacenar ningún tipo de información confidencial en los dispositivos móviles que permanezca parte o todo el tiempo fuera de las instalaciones de* ***COMFAMILIAR****.*

c) *Si por razones estrictas del negocio se requiere almacenar información confidencial en equipos móviles, esta información debe estar, en lo posible, cifrada o en su defecto autorizada por el coordinador de proceso respectivo y Coordinador de TI.*

d) *La seguridad física de los equipos móviles de propiedad de* ***COMFAMILIAR*** *esta bajo responsabilidad del custodio, por lo tanto dichos equipos no deben ser desatendidos en sitios públicos. En caso de pérdida o daño del dispositivo, el valor de la reparación o reposición estará a cargo del custodio.*

8.2.3 Suministros de Equipos de Soporte Energético

a) *La Dirección Administrativa debe asegurarse que todos los equipos de cómputo de la Caja cuentan con un sistema de alimentación continua (UPS) y que dichos equipos son revisados periódicamente para asegurar su funcionamiento y que tienen la capacidad adecuada para soportar la carga.*

8.3 Gestión de Comunicaciones y Operaciones

8.3.1 Protección contra código malicioso.

a) *El Coordinador de TI debe garantizar que todos los computadores conectados a la red de* ***COMFAMILIAR*** *tengan instalado el software antivirus.*

b) *El software antivirus debe configurar para que realice un escaneo de todas las unidades de almacenamiento de manera automática.*

c) *El software antivirus debe contar con los mecanismos de actualización automática.*

d) *Se debe implementar un procedimiento para actualizar el antivirus instalado en computadores que no se conectan de manera permanente a la red.*

e) *Los archivos adjuntos a los correos electrónicos deben ser escaneados por el antivirus antes de su entrega en el buzón.*

f) *Todos los archivos enviados a terceros (Clientes, proveedores, entidades de regulación, etc.), sin importar el medio por el cual sean enviados (correo electrónico, CD, DVD, etc.), deben ser escaneados por el antivirus antes de su envío.*

g) *Si los usuarios detectan un comportamiento anormal del computador y sospechen la presencia de virus o código malicioso, deben reportar de inmediato el incidente a la coordinación de TI para que se tomen las acciones correspondientes y prevenir la propagación del mismo.*

8.3.2 Gestión de copias de respaldo

a) *El coordinador de TI es responsable de disponer del sistema de almacenamiento centralizado para custodiar las copias de seguridad a la información, sin embargo es responsabilidad de los dueños de la información garantizar que toda la información sensible y crítica para la Caja cuente con un mecanismo de backup o copia de seguridad.*

b) *El dueño de la información de cada área, debe garantizar que la información a su cargo almacenada en los equipos de cómputo está incluida en los procedimientos de backup.*

c) *Los respaldos de información sensible y crítica deben almacenarse en un sitio protegido contra amenazas físicas y ambientales. Así mismo, debe existir un sitio de almacenamiento externo para dichos respaldos. El sitio de almacenamiento externo debe contar con sistemas de protección física y ambiental.*

d) *El Coordinador de TI debe documentar e implementar un sistema de rotación y retención de medios de backup para la información sensible y crítica. La rotación y custodia de medios debe considerar las exigencias de los organismos de control y la legislación aplicable a la Caja.*

e) *Los usuarios de **COMFAMILIAR** que requieran respaldo de la información sensible y crítica para el negocio almacenado en sus estaciones de trabajo, dentro de los sistemas de backup centralizado, deben hacer un requerimiento a la coordinación de TI mediante el aplicativo SOLTIC.*

f) *El Coordinador de TI garantizará que se realice una prueba de restauración de una cinta de backup con el fin de verificar su funcionalidad y que la información almacenada corresponda a la que se debe hacer backup.*

g) *El Coordinador de TI y los coordinadores de cada proceso deben garantizar que toda información de la Caja que ya no sea utilizada por la operación y no se requiera por requerimientos legales, será destruida de manera segura evitando su recuperación por un tercero.*

8.3.4 Gestión de seguridad de redes

a) *La Coordinación de TI debe garantizar que se instalen sistemas de protección perimetral que filtren el tráfico de información desde las redes externas a la red interna de* ***COMFAMILIAR****.*

b) *Todas las conexiones hacia redes externas con terceros deben ser autorizadas por el Coordinador del proceso a través del aplicativo Soltic, previa verificación por la Coordinación de TI de que se requiere por razones estrictas del negocio y que los riesgos de la información son conocidos y controlados.*

c) *Sin excepción todas las conexiones a redes externas, mediante servicios de acceso Internet, se debe realizar utilizando VPN (redes virtuales privadas) y/o estrategias DMZ(Zonas Desmilitarizadas) que garanticen altos niveles de seguridad a la información en tránsito.*

d) *La información relacionada con la configuración de la red y direccionamiento de la misma es considerada confidencial y su acceso físico y lógico debe estar restringido a personal autorizado por el Coordinador de TI.*

e) *La conexión de equipos personales o de terceros a la red interna de* ***COMFAMILIAR*** *debe ser previamente solicitada a la Coordinación de TI mediante el aplicativo SOLTIC.*

f) *El Coordinador de TI verificará que la conexión de equipos personales o de terceros a la red interna se hace por razones estrictas del negocio y que los equipos cuentan con un antivirus actualizado y las licencias de software de los equipos están debidamente legalizadas. El Coordinador de TI se reserva el derecho de solicitar copia de las licencias de sistemas operativos y aplicativos de los equipos personales o de terceros conectados a la red de* ***COMFAMILIAR****. Si los equipos no cuentan con las licencias debidamente legalizadas, no se autorizará su conexión a la red o se retirarán de inmediato.*

g) *El acceso remoto de colaboradores, contratistas, proveedores o terceros en general a las redes de COMFAMILIAR debe ser autorizado por el Coordinador de TI previa*

verificación de que se hace por razones estrictas del negocio y en todos los casos se realizará utilizando sistemas seguros como VPN (redes virtuales privadas).

h) *Programas o procesos que consumen excesivos recursos de Red, los usuarios no deben ejecutar programas o procesos automáticos que consuman demasiados recursos de máquina y que puedan afectar el normal desempeño de la red; en estos casos debe existir una tarea planeada con Tecnología Informática para ejecutarse en horas que no afecte el trabajo de los demás usuarios.*

A	UGT

8.3.5 Intercambio de información confidencial

a) *El envío de archivos a terceros que contengan información confidencial de* ***COMFAMILIAR*** *y/o sus Clientes debe ser autorizado por el dueño de la información a través del Soltic y se debe hacerse por razones estrictas del negocio.*

b) *El envío de archivos a terceros con información confidencial de* ***COMFAMILIAR*** *y/o sus Clientes se debe hacer en forma cifrada. Para tal efecto se debe solicitar a la coordinación de TI el soporte necesario vía SOLTIC.*

c) *Previo al envío de información confidencial a terceros, se debe firmar un acuerdo de confidencialidad entre las partes.*

8.3.6 Monitoreo

a) *El Coordinador de TI implementará los mecanismos necesarios para generar, almacenar y custodiar los registros de auditoria que permitan la trazabilidad de las transacciones realizadas en los aplicativos críticos (si su tecnología e infraestructura lo permita) para la operación de la Caja.*

b) *El Coordinador de TI velará para que los nuevos aplicativos adquiridos o desarrollados por la Caja, deben contar con la funcionalidad de auditoria y trazabilidad de las transacciones en las cuales se maneje información confidencial.*

c) *El Coordinador de TI debe implementar los mecanismos para generar, almacenar y custodiar los registros de auditoria que permita hacer seguimiento a la confidencialidad, integridad y disponibilidad de los sistemas operativos de servidores críticos, equipos de comunicaciones, equipos de protección perimetral,*

bases de datos, consolas de antivirus y en general todos los recursos de TI críticos para soportar la operación de la Caja.

d) *El Coordinador de TI implementará un procedimiento automático que permita la visualización y análisis de los registros de auditoria de manera preventiva.*

e) *Los registros de auditoria se deben conservar por un lapso de tiempo de 2 años y el acceso a los mismos debe estar restringido y exclusivo a personal autorizado por el Coordinador de TI.*

f) *Todas las actividades realizadas por los usuarios, con privilegios de administración sobre los sistemas de información (si su tecnología e infraestructura lo permita), deben ser registradas en un log que debe ser revisado periódicamente por el colaborador asignado por la Coordinación de TI.*

g) *Los registros de auditoria que reporten las fallas de aplicativos, servidores, sistemas operativos, bases de datos, sistemas de protección perimetral y sistemas de control ambiental (si su tecnología e infraestructura lo permita), deben ser revisadas periódicamente por el Administrador del Sistema y de manera preventiva y tomar las medidas adecuadas para detectar y prevenir posibles incidentes que afecten la continuidad de los procesos de la Caja.*

h) *El Coordinador de TI debe garantizar que la fecha y hora de todos los recursos informativos estén sincronizados, para asegurar que los registros reflejan el tiempo exacto de ocurrencia.*

8.4 Control de Acceso

8.4.1 Política de control de acceso de COMFAMILIAR

Todos los aplicativos de ***COMFAMILIAR*** *deben usar controles de acceso lógico que mitiguen los riesgos relacionados con el acceso no autorizado a la información confidencial de la Caja y sus Clientes.*

1. *En caso de ser necesario la creación o modificación de un rol del aplicativo JD Edwards, se debe gestionar esta aprobación a través de un comité de tecnología informática, con la participación de los procesos involucrados.*
2. *La solicitudes realizadas por los usuarios, para modificaciones a los roles ya existentes, de acuerdo a la matriz de perfiles del aplicativo JD Edwards, afectará a todos los usuarios que tenga asignados este rol.*
3. *En caso que los usuarios del aplicativo JD Edwards requieran tener varios roles, podrán ser asignados siempre y cuando no exista conflicto entre los mismos.*
4. *Las solicitudes de permisos individuales o específicos en el aplicativo JD Edwards, no serán permitidos, estos deberán estar asignados a un rol.*

8.4.2 Gestión de acceso de usuarios

a) *La creación de usuarios se realizará mediante el aplicativo SOLTIC previa aprobación del Coordinador del proceso o área, que garantice el acceso únicamente a los recursos e información que requiera para desempeñar sus funciones de acuerdo a los perfiles establecidos por Tecnología.*

b) *El control de acceso a los diferentes sistemas de información deben ser aprobados por los dueños de la información.*

c) *Los usuarios de los sistemas de información de* ***COMFAMILIAR*** *son de carácter personal e intransferible. El colaborador y/o externo a cargo debe velar por la confidencialidad del usuario y será responsable de todas las actividades que se realicen con el.*

d) *Cuando un colaborador o externo se retira o se traslada del proceso, el usuario se debe bloquear en todos los sistemas de información. Es responsabilidad del proceso de Gestión Humana reportar a la Coordinación de TI todos los retiros o traslados de personal para el bloqueo correspondiente. De igual forma, los Coordinadores de los diferentes procesos deben reportar a la Coordinación de TI el retiro de los externos para proceder con el bloqueo del usuario.*

e) *El periodo de caducidad del usuario no debe ser superior a 12 meses, en el caso de prorrogar o ser indefinido el contrato, se deberá realizar nuevamente la solicitud de activación de usuarios a través del aplicativo Soltic.*

f) *Cuando un usuario es trasladado a otra dependencia y se crea un nuevo cargo, se requiere la solicitud formal del coordinador del proceso de donde se retira el colaborador y/o de recursos humanos para proceder a inactivar el usuario actual. El Coordinador del proceso quien recibe el traslado del colaborador debe solicitar la creación del nuevo usuario mediante el aplicativo Soltic.*

g) *Está totalmente prohibido el uso de usuarios compartidos o genéricos en los sistemas de información de* ***COMFAMILIAR.***

h) *El proceso de Gestión Humana reportará a la Coordinación de TI los usuarios que no requieren el acceso a los sistemas de información por un periodo de tiempo determinado (ejemplo: colaboradores en vacaciones, licencias, etc) con el fin de que TI bloquee el acceso de los mismos. Está totalmente prohibido utilizar usuarios de colaboradores que se encuentren fuera de la Caja.*

i) *En el contrato laboral de cada colaborador se establecerá el compromiso para cumplir con las políticas de seguridad y el uso adecuado y seguro del usuario asignado.*

j) *Gestión inapropiada y revocación de privilegios de acceso, la administración de la entidad se reserva el derecho de revocar los privilegios de cualquier usuario en cualquier momento. No se permitirá la gestión que interfiera con el funcionamiento normal y apropiado de los sistemas de información o la red corporativa de Comfamiliar, que adversamente afecte la capacidad de otros en el uso de los recursos informáticos o que sea nocivo u ofensivo.*

A	UGT

Definición nombre de usuarios aplicativos

Política: Para la definición del nombre de usuario se establece un límite entre 5 y 6 caracteres compuestos así:

Usuarios de la Sede principal Neiva:

1. *Los primeros dos (2) o tres (3) caracteres corresponden a las dos (2) o tres (3) primeras letras del área.*

Si los dos (2) o tres(3) primeros caracteres se repiten con los de otra área, se tomará el carácter siguiente al tercero, hasta que se cumpla la política.

2. *Los tres (3) últimos corresponden a las iníciales del nombre de la persona (cuando el nombre es compuesto irán las iníciales de dos primeros nombres y el primer apellido), si los caracteres se repiten con los de otra persona de la misma área y por consiguiente el Login queda repetido, se tomará la inicial del apellido siguiente hasta que se cumpla la política.*

Usuarios de las sedes y los municipios:

1. *Los primeros tres (3) caracteres corresponden a las tres (3) primeras letras del municipio, ciudad o sede.*

2. *Los tres (3) últimos corresponden a las iníciales del nombre de la persona (cuando el nombre es compuesto irán las iníciales de dos primeros nombres y el primer apellido), si los caracteres se repiten con los de otra persona de la misma área y por consiguiente el Login queda repetido, se tomara la inicial del apellido siguiente hasta que se cumpla la política.*

A	UGT

Casos especiales:

La Dirección de COMFAMILIAR estará compuesta así:

2. dir_dir => Director de la caja de Compensación Familiar del Huila.
3. dir_sec =>Secretaria del director de la caja de Compensación Familiar del Huila.

Con el fin de dejar evidencia de donde ingresan los funcionarios de TI con sus usuarios, estos se crearan de la siguiente forma:

4. Las siglas del área (TI) continuada por las siglas del nombre del funcionario (si es nombre compuesto puede usar la primera letra de cada nombre y primera letra del primer apellido, si es nombre no compuesto usar la primera letra del nombre y primeras letras de los dos apellidos, si el nombre del usuario se repite, se tomara la letra del apellido siguiente. Y se seguirá conjugando hasta que se cumpla la política de tener login de usuarios sin repetir.

5. En la creación de usuarios para los prestadores en el área de salud, se utilizará el código de habilitación generado por el Ministerio de Salud asignado

Al prestador, que será único y el cual permitirá la identificación correspondiente en el registro de usuarios (este código será el login del user del prestador para ingresar al aplicativo de salud solicitado).

6. Se creará un usuario Tides en donde se registraran las solicitudes que requieren desarrollos.

7. Para los usuarios que se registran a través del aplicativo ciudad educativa, quien en este caso son los acudientes o líderes, estos se registrarán utilizando el número de cédula. No aplica la política de usuarios utilizado en el proceso de Tecnología informática.

Definición nombre de usuarios acceso a la red corporativa (Dominio)

A: *Todos los computadores, portátiles que tienen acceso a la red corporativa tendrán que identificarse en el dominio de Comfamiliar con un login compuesto así:*

1. *El primer nombre (.) apellido, si al confirmar el login este se repite con el de otro funcionario, se agregara la primer letra del segundo apellido; si después de esto el login no fuese único se seguirán agregando las siguientes letras del segundo apellido hasta que se cumpla la política.*

Ejemplo: José armando sierra trujillo

Jose.sierra

8.4.3 Definición nombre del equipo

***A:** Todos los computadores, portátiles se denomina el nombre del equipo así:*

***1**. El primer nombre (.) Apellido, si al confirmar el login este se repite con el de otro funcionario, se agregara la primer letra del segundo apellido; si después de esto el login no fuese único se seguirán agregando las siguientes letras del segundo apellido hasta que se cumpla la política.*

Ejemplo: josé armando sierra trujillo

Jose.Sierra

8.4.4 Definición Identificación del equipo

***A**: Todos los computadores, portátiles se identificaran por la placa de inventario y/o serial de la siguiente manera:*

***1**. Pl_08838383 cuando sea placa*

***2**. SN_993xdfs cuando no tenga placa y se identifique con serial*.

***3.** Para la identificación de los servidores dentro de la red de Comfamiliar, estos tendrán una denominación diferente a la de los equipos de cómputo, sin embargo sus especificaciones técnicas y su uso permiten diferenciarlos el uno del otro dentro del rango de servidores.*

***4.** para la identificación de los equipos de cómputo que serán configurados para el uso de los usuarios del aplicativo JD Edwards estos tendrán una denominación dentro de la red de Comfamiliar con las iniciales de la placa pl seguido del número que identifica cada equipo.*

9. GESTIÓN DE PRIVILEGIOS

a) *Los perfiles de seguridad de los diferentes sistemas de información deben ser definidos y controlados por los dueños de la información y Tecnología Informática.*

b) *Los dueños de la información y Tecnología Informática deben verificar periódicamente (cada dos años) que los usuarios con determinados perfiles son los que deben estar de acuerdo a sus cargos y responsabilidades.*

c) *La asignación de los perfiles de seguridad para los sistemas de información debe ser aprobada por los dueños de la información mediante el aplicativo Soltic y asociado a la creación de usuarios.*

d) *El Coordinador de TI debe garantizar que los colaboradores que tienen permisos de administración sobre los aplicativos y sistemas de información, cuentan con un usuario personalizado para realizar sus tareas. Las contraseñas de los usuarios administradores que vienen por defecto en los diferentes sistemas de información deben permanecer en custodia y su uso es exclusivo para eventos de contingencia.*

9.1.1. Manejo de contraseñas.

a) *El Coordinador de TI debe configurar los sistemas de autenticación de usuarios para que las contraseñas cumplan con las siguientes características:*

- ***a.*** *Longitud mínima de 8 caracteres*
- ***b.*** *Debe contener Números y letras*
- ***c.*** *Debe contener mayúsculas y minúsculas*

En el caso de aquellos aplicativos que no solicitan el cambio obligatorio de contraseña en el primer inicio de sesión, es responsabilidad del usuario realizar el cambio.

b) *Todos los sistemas de información críticos deben solicitar el cambio obligatorio de contraseña en el primer inicio de sesión (si su tecnología e infraestructura lo permite).*

En el caso de aquellos aplicativos que no solicitan el cambio obligatorio de contraseña en el primer inicio de sesión, es responsabilidad del usuario realizar el cambio.

c) *La contraseña debe expirar cada 30 días y el sistema de información crítico debe pedir cambio obligatorio.*

En el caso de aquellos aplicativos que no solicitan el cambio obligatorio de contraseña, es responsabilidad del usuario realizar el cambio.

El sistema de información crítico debe guardar un historial de las ultimas 10 contraseñas y ninguna de ellas se puede reutilizar. En el caso de aquellos aplicativos que no cuentan con este control de manera automática, responsabilidad del usuario cumplir la norma tratando de no utilizar ninguna de las ultimas 10 contraseñas.

d) *Cuando y cómo los password pueden ser cambiados por el administrador de Seguridad; El administrador de seguridad solamente puede eliminar un passwords si el usuario en cuestión ha olvidado su clave de acceso, la solicitud para eliminación de password se debe hacer personalmente o proporcionando evidencia definitiva de identidad.*

A	*UT*

9.1.2. Responsabilidades de los usuarios

a) *Los colaboradores y/o externos deben hacer uso adecuado de los usuarios asignados. Entre otros los cuidados que debe tener son:*

- ***a.*** *Bajo ninguna circunstancia se debe prestar el usuario y la contraseña.*
- ***b.*** *Nunca suministrar el usuario y contraseña vía telefónica.*
- ***c.*** *Si por razones de soporte, se requiere que los colaboradores de TI conozcan o ingresen al sistema con la contraseña de un colaborador, el equipo no se debe dejar desatendido y se debe cambiar la contraseña una vez termine el soporte de TI.*
- ***d.*** *La contraseña se debe memorizar, nunca la escriba en ninguna parte.*
- ***e.*** *Se debe cambiar la contraseña cuando se tiene sospecha que ha sido descubierta por terceros.*

b) *Cuando un colaborador se retire temporalmente de su puesto de trabajo, debe hacer un logout de la sesión del aplicativo y activar el bloqueo del escritorio de trabajo del computador mediante la opción de protector de pantalla.*

c) *El Coordinador de TI debe garantizar que el protector de pantalla de todos los equipos de la Caja sean configurados con los siguientes parámetros:*

- ***a.*** *Activar el protector de pantalla después de 5 minutos de inactividad del computador.*
- ***b.*** *El desbloqueo requiere contraseña de red*

d) *El fondo de escritorio debe contener información comercial de la Caja.*

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

9.1.3. Controles de seguridad en los servicios de red

b) *Normas de uso de equipos de cómputo*

- ***a.*** *Los recursos de TI se deben usar única y exclusivamente para cumplir con las responsabilidades asignadas por la Caja.*
- ***b.*** *Tecnología Informática hará entrega formal del equipo en correcto funcionamiento y con el software estándar instalado de acuerdo al cargo y perfil del colaborador.*
- ***c.*** *Solo el personal de TI o a quien designe el Coordinador de TI está autorizado para llevar a cabo tareas de mantenimiento de software, hardware y del acceso a la red.*
- ***d.*** *Está prohibido descargar y almacenar archivos o documentos personales, tales como 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, en caso de evidenciar alguna de las situaciones anteriormente expuestas se notificará al usuario y de ser reincidente será acreedor de sanciones administrativas.*

- ***e.*** *Prohibición para explorar vulnerabilidades de los sistemas de seguridad, Los usuarios no deben explorar vulnerabilidades o deficiencias en la seguridad de los SI para dañar sistemas o datos, para obtener privilegios mayores a los que han sido autorizados, para tomar recursos de otros usuarios, o para tener acceso a otros sistemas a los cuales no se les ha otorgado autorización apropiada, a no ser que se haga con la intención de ayudar a mejorar la seguridad, en este caso las vulnerabilidades y deficiencias deben ser reportadas inmediatamente al administrador del sistema y seguridad y al coordinador de Tecnología Informática.*

A	UGT

c) *Normas de uso de correo electrónico*

Administrativos, Coordinadores y Demás Colaboradores:

1. *Los espacios en disco para el buzón de correo electrónico externo para el director, usuarios miembros del comité estratégico, coordinadores de proceso, coordinadores de área y colaboradores que lo soliciten a través de requerimiento SOLTIC, será de 50 gigabytes.*

2. *Servicio de correo electrónico durante 7 días a la semana, 24 horas del día, a excepción de los casos de mantenimiento y procesos externos del proveedor de Internet ó por daños que interfieran el normal funcionamiento del centro de cómputo.*

3. *El usuario es el encargado de administrar el espacio de su correo electrónico y en caso de exceder el límite asignado en disco con mensajes recibidos, enviados y/o borrados, recibirá un mensaje informándole el espacio en Disco disponible, con el fin de que libere espacio en el buzón y pueda recibir nuevamente mensajes.*

4. *Soporte técnico para la solución de problemas relacionados con el correo electrónico.*

5. *Acceso a Internet en los computadores de las áreas que así lo soliciten mediante requerimiento solicitado a través del aplicativo SOLTIC*

6. *Acceso a la Intranet o red corporativa de COMFAMILIAR HUILA.*

7. *Para la creación de usuarios con respecto a los correos internos y externos, el usuario será creado así:*

El primer nombre (.) Seguido del primer apellido, si el nombre y/o apellido se repite con los de otra persona y por consiguiente queda repetido, se tomará la inicial del segundo nombre y/o del segundo apellido hasta que se cumpla la política.

Ejemplo: josé armando sierra trujillo

Jose. Sierra @_____

Si se repite con otra cuenta

Josea.sierra@_____

Si se repite con otra cuenta

Jose.sierrat@_____

Nota: 1. Los contratistas o terceros que mediante contrato por prestación de servicios necesiten de acceso a la Intranet y/o Internet deberán solicitarlo por medio del aplicativo SOLTIC realizado y autorizado por el interventor del contrato especificando las restricciones del permiso, la conexión a Internet será cargada al área al cual el contratista realiza el trabajo y no se le asignara un correo Corporativo, la maquina del contratista autorizada para disfrutar de estos servicios debe estar debidamente configurada para que cumpla con las políticas de seguridad TI.

1. *Para el caso de las cuentas de correo que ya existen esas no serán objeto de modificación, solo en caso que sean eliminadas y que requieren la creación nuevamente de la cuenta de correo.*

a. *El servicio de correo electrónico es para uso exclusivo de las actividades relacionadas con el trabajo de cada colaborador.*
b. *Está prohibido utilizar el correo electrónico para atentar contra la integridad de* ***COMFAMILIAR*** *o cualquiera de sus colaboradores.*
c. *Todos los correos recibidos deben ser escaneados por el antivirus.*
d. *El envío de información confidencial debe ser aprobada por el dueño de la información y se debe realizar utilizando algún sistema de cifrado de información.*
e. *Se prohíbe difundir información que incite a la discriminación, la violencia o con contenido ilícito o que atente contra la dignidad humana: aquellas que hacen apología del terrorismo, racismo, pornografía, juegos, música, videos o cualquier tipo de contenido que no esté relacionado con el desempeño laboral.*
f. *Se prohíbe enviar mensajes con fines publicitarios y comerciales de bienes y servicios en beneficio propio, de familiares o terceros.*
g. *Se prohíbe enviar correo Spam es decir correo basura relacionado con falsos virus, publicidad de empresas, cadenas de mensajes, etc.*
h. *Se prohíbe falsificar mensajes de correo electrónico.*
i. *Se prohíbe leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas sin su autorización.*
j. *Se prohíbe enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a terceros.*
k. *Está prohibido suscribir el correo electrónico corporativo a servicios de noticias no relacionadas con la actividad profesional.*
l. *No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye todo material protegido por*

derechos de autor (copyright), Marcas registradas, secretos comerciales u otros de propiedad intelectual.

m. *La firma predeterminada solo puede contener nombre y apellidos, cargo, extensión y nombre de la compañía. No se pueden adjuntar firmas escaneadas.*

n. *Para el manejo de envío y recibo de información corporativa, se debe utilizar única y exclusivamente correos corporativos*

d) *Normas de uso de internet*

a. *El acceso a internet debe ser autorizado por el coordinador de proceso*

b. *No está permitido acceder a internet con fines diferentes a los propios de las actividades de* ***COMFAMILIAR***

c. *No está permitido acceder a páginas web con contenido ilícito que atenten contra la dignidad humana como aquellas que hagan apología del terrorismo, páginas con contenido xenófobo, racista, antisemita, violento, pornográfico, juegos, descargas de música, videos, o cualquier tipo de contenido que no esté relacionado con la actividad laboral.*

d. *Está prohibido el Ingreso a páginas de pornografía infantil.*

e. *Está prohibido 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. *Está prohibido 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.*

e) *Normas de uso de la Intranet*

a) *Respetar la privacidad de otros usuarios. No está permitido obtener copias intencionales de archivos, códigos, contraseñas o información ajena; ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento del titular de la cuenta.*

b) *Respetar la protección legal otorgada a programas, textos, artículos y bases de datos según legislación internacional sobre propiedad intelectual y las normas pertinentes de nuestro país.*

c) *Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la Caja de Compensación Familiar del Huila COMFAMILIAR, a través de medio físico o electrónico alguno.*

d) *No obtener ni suministrar información sin la debida autorización, no dar a conocer códigos de seguridad tales como contraseñas a otras personas, o entorpecer por ningún medio el funcionamiento de los sistemas de información y telecomunicaciones.*

e) *La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser adelantada por personal autorizado por la Coordinación del área de TI.*

f) *El uso indebido de los recursos de la Intranet recaerá directamente sobre el usuario que se registra en el sistema y sobre el recaerá toda la responsabilidad de los actos realizados*

"*Excepción: en caso que el proceso requiera que las cuentas de correo tengan un nombre especifico y no aplique el nombre del usuario, esta observación se deberá realizar a través del requerimiento documentado en el aplicativo Soltic y se deberá crear la cuenta como lo solicite el proceso*"

LUIS MIGUEL LOSADA POLANCO
Director Administrativo

SONIA CRISTINA RAMIREZ
Coordinadora Tecnología Informática

CASO	ESTADO DOCUMENTO	COD.DOC	NOMB.DOC	TIPO.DOC	RESPONSABLE	AREA	TIPO NOV.	FECHA.NOV.(MM/DD/AAAA)	ARCHIVO
9955	ACTIVO	M-A-05-01	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	MANUALES	LILIANA PERDOMO CASTRO	PLANEACION	A	02/26/2018	

NOVEDAD:Se Genera Cambio en el codigo por Acta Se realiza recodificaciÃ³n del documento segun cambio de estructura organizacionl aprobada por Consejo Directivo Acta NÂ° 880 del 19 de diciembre de 2017. de consejo directivo, donde se modifica la estructura organizacional

APROBADO: SI	OBSERVACION:		FECHA: 02/26/2018	APRUEBA: LILIANA PERDOMO CASTRO

SEGUIMIENTO

DESCRIPCION	FECHA	USUARIO

FECHA SOLUC.(MM/DD/AAAA):		02/26/2018	USU.CIERRE	LILIANA PERDOMO CASTRO	ESTADO SOLICITUD:	SOLUCIONADO

CASO	ESTADO DOCUMENTO	COD.DOC	NOMB.DOC	TIPO.DOC	RESPONSABLE	AREA	TIPO NOV.	FECHA.NOV.(MM/DD/AAAA)	ARCHIVO
12448	ACTIVO	M-A-05-01	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	MANUALES	EDNA YANITH GORDO BARREIRO	TECNOLOGIA INFORMATICA	A	05/21/2018	

NOVEDAD:AGREGAR EN EL PUNTO C: NORMAS DE USO DE CORREO ELECTRONICO UN PUNTO N: PARA EL MANEJO DE ENVÍO Y RECIBO DE INFORMACIÓN CORPORATIVA SE DEBE UTILIZAR ÚNICA Y EXCLUSIVAMENTE CORREOS CORPORATIVOS

APROBADO: SI	OBSERVACION:		FECHA: 06/18/2018	APRUEBA: Sonia Cristina Ramirez Perez

SEGUIMIENTO

DESCRIPCION	FECHA	USUARIO
Se incluye lo solicitado	28-6-2018 0:00	plalpc

FECHA SOLUC.(MM/DD/AAAA):		06/28/2018	USU.CIERRE	LILIANA PERDOMO CASTRO	ESTADO SOLICITUD:	SOLUCIONADO