

## 1. OBJETO

Establecer los lineamientos principales de gestión de la seguridad de la información para el COMFAMILIAR Cartagena y Bolívar.

## 2. ALCANCE

El manual contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en COMFAMILIAR Cartagena y Bolívar, los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o transmitan información de la Corporación o sus afiliados.

## 3. RESPONSABILIDADES

**Comité de Seguridad de la Información:** El comité de seguridad de la información tiene como objetivo principal la aprobación de lineamientos estratégicos en cuanto a seguridad de la información, garantiza los recursos y la toma de decisiones orientadas al cumplimiento de la estrategia por ellos definida.

Supervisa la aplicación de los requisitos definidos por gobierno en línea en lo relacionado con la seguridad de la información.

**Oficial de Seguridad Información (CISO):** Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.

Tienen la responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.

**Líderes de los Procesos:** Tienen la responsabilidad de dar la cobertura de los lineamientos de seguridad a cada uno de sus procesos operacionales.

**Jefe de Tecnología:** Responsable del seguimiento global de la seguridad de la información.

Debe administrar las iniciativas de seguridad definidas en el comité.

Responsable de aplicar los controles y las iniciativas de seguridad de tipo tecnológico definidas en el comité. Debe tener una comprensión de los riesgos empresariales/operativos, costos y beneficios, y los requisitos específicos de seguridad de la información aplicables a COMFAMILIAR Cartagena y Bolívar.

**Jefe de Planeación:** Responsable de la asignación presupuestal para las iniciativas de seguridad definidas por el comité.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

**Subdirector Financiero:** Captura, procesamiento y distribución de la información financiera.

#### 4. DEFINICIONES Y TERMINOS

**4.1. ACTIVOS DE INFORMACIÓN:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada corporación, órgano u organismo.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para COMFAMILIAR Cartagena y Bolívar

**4.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI):** Instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos.

**4.3. CONFIDENCIALIDAD:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, corporaciones o procesos no autorizados.

**4.4. CONTROL:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

**4.5. DISPONIBILIDAD:** Propiedad de que la información sea accesible y utilizable por solicitud de una corporación autorizada.

**4.6. EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

**4.7. INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información de COMFAMILIAR Cartagena y Bolívar y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

**4.8. INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

**4.9. PROPIETARIO/RESPONSABLE DE ACTIVO DE INFORMACIÓN:** Individuo, corporación o centro de operación que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

**4.10. SERVICIO:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

**4.11. USUARIO:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

## **5. CONDICIONES GENERALES**

### **Normatividad**

Para la construcción de este manual se tiene como base, la norma ISO – IEC 27001:2005 Sistema de Gestión de la Seguridad de la Información, el modelo de gestión de la seguridad de la información y la política de información del COMFAMILIAR Cartagena y Bolívar.

La Caja de Compensación Familiar COMFAMILIAR Cartagena y Bolívar reconoce la información como un activo importante para la gestión de sus afiliados en el desarrollo de sus procesos internos, por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para la Información.

El manual de seguridad es un documento que contiene lineamientos que apoyan la gestión y administración de los planes y procedimientos de seguridad de la información dando claridad sobre las prácticas de seguridad aplicadas a la corporación.

## **6. DESCRICION DEL PROCESO**

### **6.1. COMPROMISO DE LA DIRECCIÓN**

El Consejo directivo o quien haga sus veces y la Alta Dirección del COMFAMILIAR Cartagena y Bolívar muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información a través de la asignación de recursos, la definición de la política de información, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a continuación.

### **6.2. GOBIERNO DE SEGURIDAD**

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

La definición de un modelo de gobierno de seguridad adecuado representado en una estructura organizacional definida y aprobada por la Corporación, permite la correcta toma de decisiones y ofrece una alineación y rumbo adecuado en las actividades para proteger los activos de información.

Una estructura organizacional es un organismo viviente dentro de la organización que puede cambiar según la estructura y las necesidades de la Corporación, pero que en todo momento debe ser clarificada con el fin de que se conozca la cadena de toma de decisión de cada uno de los temas necesarios para la gestión de la seguridad de la información.

Cada rol dentro del Gobierno debe tener unas responsabilidades asociadas para realizar su tarea, estas responsabilidades se asignan haciendo uso de una matriz RACI donde cada tipo de responsabilidad se asigna a los roles definidos. Los tipos de responsabilidades usados son los siguientes:

TIPO DE RESPONSABILIDAD		DESCRIPCIÓN	
<b>R</b>	<b>Responsable</b>	<b>Responsable</b>	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea.
<b>A</b>	<b>Accountable</b>	<b>Quien rinde cuentas</b>	Este rol se responsabiliza de que la tarea se realice y es quien debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su responsable (R).
<b>C</b>	<b>Consulted</b>	<b>Consultado</b>	Este rol posee alguna información o capacidad necesaria para realizar la tarea. Se le informa y se le consulta información (comunicación bidireccional).
<b>I</b>	<b>Informed</b>	<b>Informado</b>	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

A continuación, se presenta la estructura de roles para el gobierno de seguridad de la información el COMFAMILIAR Cartagena y Bolívar.

### 6.3. Estructura de roles

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

### 6.3.1. Comité de Seguridad de la información.

<b>Objetivo</b>	Garantizar a través del monitoreo y la revisión, la aplicación de las buenas prácticas en seguridad de la información y la toma de decisiones orientadas al cumplimiento de la estrategia. Aprobar los lineamientos estratégicos en cuanto a seguridad de la información y garantizar los recursos para su cumplimiento.
<b>Principios de Operación</b>	El comité se debe reunir trimestralmente o cuando una eventualidad lo requiera. La participación de los designados en el Comité es obligatoria, en caso de no poder asistir se debe enviar un sustituto que contará con el mismo poder de decisión. El número de miembros del comité se limita a un grupo relativamente pequeño de líderes de procesos para asegurar la comunicación y toma de decisiones apropiado. Las actas de todas las reuniones deben ser aprobadas y almacenadas en el Sistema de información respectivo. El jefe del área de Tecnología preside las reuniones del comité.
<b>Responsabilidades</b>	El comité es el responsable de que las decisiones de seguridad de la información estén orientadas al apoyo de las decisiones estratégicas.

<b>ROL</b>	<b>DESCRIPCIÓN</b>
<b>Jefe de Tecnología</b>	Responsable del seguimiento global de la seguridad de la información. Debe administrar las iniciativas de seguridad definidas en el comité. Responsable de aplicar los controles y las iniciativas de seguridad de tipo tecnológico definidas en el comité. Debe tener una comprensión de los riesgos empresariales/operativos, costos y beneficios, y los requisitos específicos de seguridad de la información aplicables a COMFAMILIAR Cartagena y Bolívar.
<b>Jefe de Planeación</b>	Responsable de la asignación presupuestal para las iniciativas de seguridad definidas por el comité.
<b>Subdirector Financiero</b>	Captura, procesamiento y distribución de la información financiera.
<b>Coordinador de Riesgos</b>	Debe tener una comprensión de los riesgos de las áreas de apoyo administrativo en cuanto al manejo de la información y sobre los requisitos específicos de seguridad de la información aplicables al Comfamiliar.
<b>Jefe de Talento Humano</b>	Responsable de aplicar las iniciativas de seguridad concernientes a la vinculación, mantenimiento y retiro o cambio de personal.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

--	--

### 6.3.2. Competencias de rol

#### Habilidades

- Establecer y mantener un marco de gobierno de la seguridad de la información y procesos de apoyo para asegurar que la estrategia de seguridad de la información está alineada con las metas y objetivos de la organización.
- Definir e implementar los objetivos de seguridad de la información alineados con la planeación estratégica de la corporación.

#### Experiencia

Varios años de gestión empresarial, incluyendo experiencia en:

- Definición y seguimiento de lineamientos de seguridad de la información.
- Alinear la estrategia de seguridad de la información con el gobierno corporativo.
- Creación de políticas de seguridad de la información que se alineen con las necesidades de la corporación y los métodos para medir su elaboración.
- Comunicación con liderazgo ejecutivo.
- Experiencia en la creación e implementación de estrategias y principios de seguridad de información.

### 6.3.3. Oficial de seguridad CISO

<b>Objetivo</b>	Tiene la responsabilidad general del programa de seguridad de la información empresarial.
<b>Principios de operación</b>	El CISO debe ser el enlace entre el consejo directivo o quien haga sus veces y el área de tecnología y sistemas de información. El CISO debe coordinar las relaciones con los

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

actores clave de la corporación para hacer frente a las necesidades de protección de la información.  
El CISO debe tener una comprensión exacta de la planeación estratégica de la corporación.  
El CISO debe ser un comunicador eficaz.  
El CISO debe ser hábil en la construcción de relaciones efectivas con los líderes de procesos.

#### 6.3.4. RACI de prácticas de Oficial de seguridad CISO

PRACTICA	NIVEL DE PARTICIPANTE
Identificar y comunicar las amenazas de seguridad de información, las conductas deseables y los cambios necesarios para hacer frente a estos puntos.	Accountable
Tomar decisiones sobre la protección contra malware.	Accountable
Administrar la red y la seguridad de la conectividad.	Accountable
Administrar la seguridad del punto final.	Accountable
Gestione la incorporación del usuario y de acceso lógico.	Accountable
Administrar el acceso físico a los activos de TI.	Accountable
Monitorear la infraestructura para eventos relacionados con la seguridad.	Accountable

PRACTICA	NIVEL DE PARTICIPACIÓN (RACI)
Proporcionar formas de mejorar la eficiencia y eficacia de la función de seguridad de la información (por ejemplo, mediante la capacitación del personal de seguridad de la información; documentación de los procesos, la tecnología y las aplicaciones, y la estandarización y la automatización de procesos).	Accountable
Desarrollar un plan de seguridad de la información que identifique las actividades a ser implementadas por el equipo de seguridad para proteger los activos de la organización de seguridad de información.	Responsable

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*



<b>Supervisar la gestión de riesgos de TI.</b>	Responsable
<b>Definir y comunicar una estrategia de seguridad de la información que esté en línea con la estrategia de la corporación.</b>	Responsable
<b>Investigar, definir y documentar los requisitos de seguridad de la información.</b>	Responsable
<b>Validar los requisitos de seguridad de la información con las partes interesadas y personal de implementación técnica.</b>	Responsable
<b>Desarrollar políticas y procedimientos de seguridad de la información.</b>	Responsable
<b>Definir e implementar estrategias de evaluación de riesgos y cooperar con la coordinación de riesgos para gestionar el riesgo de la información.</b>	Responsable
<b>Asegurar que el impacto potencial de los cambios frente a la seguridad de la información sea evaluado.</b>	Responsable
<b>Recopilar y analizar los datos de rendimiento y de cumplimiento relacionados con la seguridad de la información y la gestión de riesgos de la información.</b>	Responsable

### 6.3.5. Competencias de rol Habilidades

- Gestionar adecuadamente los riesgos de la información.
- Administrar los recursos del programa de seguridad de manera responsable.
- Crear un modelo de medición del desempeño basado en los indicadores de gobernabilidad de seguridad de la información para asegurar que se logran los objetivos organizacionales.
- Líder probado con excelentes habilidades de comunicación y capacidad de interactuar con todos los niveles de la empresa.
- Método de trabajo con orientación de procesos.
- Comprensión sobre como las funciones de seguridad de la información se relacionan con la organización.

Varios años de experiencia en seguridad de la información, incluyendo experiencia en:

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*



- Cumplimiento de la seguridad de la información con las regulaciones externas.
- Alinear la estrategia de seguridad de la información con el gobierno corporativo.
- Creación de políticas de seguridad de la información que se alinean con las necesidades del corporación y eficacia de las políticas.
- Comunicación y liderazgo ejecutivo.

### **Conocimiento**

- Los requisitos legales y reglamentarios que afectan a la seguridad de información.
- Roles y responsabilidades necesarias para la seguridad de la información en toda la empresa.
- El buen entendimiento de las prácticas de seguridad de la información que se aplican a la Corporación.
- Métodos para poner en práctica las políticas de gobierno de seguridad de información.
- Los conceptos fundamentales de la gobernabilidad y cómo se relacionan con la seguridad de información.
- Normas, marcos y mejores prácticas relacionadas con el gobierno de la seguridad de información internacionalmente reconocidos y desarrollo de estrategias.
- El buen entendimiento del protocolo de red, bases de datos, aplicaciones y sistemas operativos, y la forma en que son aplicables a los procesos de negocio.
- Amplio conocimiento de gestión de accesos, gestión de amenazas y vulnerabilidad, arquitectura de seguridad de la información y protección de datos en cada plataforma.
- Estándares de la industria de seguridad de la Información / mejores prácticas (por ejemplo, la norma ISO / IEC 27000).
- Legislación relacionada con la seguridad de información.
- Nuevas tecnologías de seguridad de la información y metodologías de desarrollo.
- Detectar, investigar, responder y recuperarse de incidentes de seguridad de la información para reducir al mínimo impacto en el negocio.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

- Realizar tareas de aprovisionamiento de usuario para sistemas empresariales y entornos de aplicaciones.
- Asistir en la definición de roles y modelos de acceso para diferentes aplicaciones y entornos de plataforma.
- Plataformas de vigilancia y mantenimiento de tecnología.

### 6.3.6. Líderes de proceso

Los líderes de proceso actúan como enlace entre las funciones empresariales y de seguridad de la información. Pueden estar asociados con tipos de información, aplicaciones específicas, o centros de operación de la organización.

La persona en este rol debe poseer un buen conocimiento de la corporación y del tipo de información que requiere protección del proceso que representa.

Los custodios sirven como asesores y agentes de supervisión con respecto a la información dentro de la empresa.

Este papel debe equilibrar el impacto de los riesgos de la corporación y la información para que las decisiones de seguridad estén alienadas con las de la corporación.

### 6.3.7. RACI de prácticas de Custodios de información

<b>PRACTICA</b>	<b>NIVEL DE PARTICIPACIÓN (RAI)</b>
<b>Comunicar, coordinar y asesorar sobre los esfuerzos de gestión de riesgos de la información con los gerentes de línea.</b>	Responsable
<b>Informar sobre los cambios en los procesos y/o estrategias (por ejemplo, nuevos productos o servicios) a la ISSC.</b>	Responsable

### Habilidades

Gestionar adecuadamente los riesgos de la información.

Líder probado con excelentes habilidades de comunicación y capacidad de interactuar con todos los niveles de la empresa.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

Método de trabajo con orientación de procesos.

Comprensión sobre como las funciones de seguridad de la información se relacionan con el negocio.

### **Experiencia**

Cumplimiento de la seguridad de la información con las regulaciones externas.

Comunicación y liderazgo ejecutivo.

### **Conocimiento**

Los requisitos legales y reglamentarios que afectan a la seguridad de información en su área de desempeño.

Métodos para poner en práctica las políticas de gobierno de seguridad de información. El buen entendimiento de las prácticas de seguridad de la información que se aplican a la Corporación.

#### **6.4. Objetivos de seguridad**

El gobierno de seguridad tiene unos objetivos de seguridad primordiales los cuales rigen sus decisiones. Todos los lineamientos de seguridad establecidos para COMFAMILIAR Cartagena y Bolívar están orientados a cumplir con los siguientes objetivos:

- Alinear las iniciativas de seguridad de la información con la estrategia de la corporación y dar cumplimiento con las regulaciones internas y externas aplicables.
- Mitigar los riesgos de la corporación relacionados con problemas en la seguridad de la información.
- Asegurar en una medida razonable la confidencialidad, integridad y disponibilidad de la información relevante para la toma de decisiones de COMFAMILIAR Cartagena

#### **6.5. COMUNICACIÓN CON EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI)**

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

	<b>MANUAL DE SEGURIDAD DE LA INFORMACION</b>	<b>CÓDIGO:</b> SIS-MA-001	
		<b>Versión:</b> 002	<b>Fecha de Versión:</b> 24/01/2022
		Página <b>12</b> de <b>31</b>	

Para que el comité de seguridad pueda cumplir con sus actividades y tomar las decisiones pertinentes según los acontecimientos en la Corporación, se debe llevar la información necesaria. Dentro de la agenda de reunión el comité debe recibir la siguiente información como mínimo:

El estado de las acciones de las revisiones previas:

- Seguimiento de las decisiones o actividades asignadas por el comité.
- Solicitudes al comité para lograr el cumplimiento de las actividades designadas.

Resultados de las acciones finalmente implementadas.

Cambios externos e internos que son relevantes para el Sistema de Gestión de Seguridad de la información:

- Cambios en regulaciones.
- Cambios en ambiente físico y social.
- Cambios de herramientas o infraestructura que soporta los procesos.

Retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:

Estado de los hallazgos de auditoría, las no conformidades y acciones correctivas.

- Seguimiento y medición de las actividades de seguridad desarrolladas
- Estado de los hallazgos de auditoría, las no conformidades y acciones correctivas.
- Seguimiento y medición de las actividades de seguridad desarrolladas.

Retroalimentación de las partes interesadas:

- Resultados de encuestas de satisfacción de los cambios implementados.
- Resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos.
- Las oportunidades o propuesta de mejora en temas relacionados con la seguridad de la información.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

Las decisiones tomadas por el comité quedarán documentadas en la correspondiente acta de reunión, dentro de la cual para cada una de las decisiones tomadas se establecerá el responsable.

Las actas de comité deben incluir las decisiones relacionadas con las oportunidades de mejora continua y de cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.

## **6.6. LINEAMIENTOS DE SEGURIDAD**

### **6.6.1. Gestión de activos**

Las diferentes áreas con el fin de garantizar la administración y control sobre los activos de la corporación, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada proceso, el cual debe estar alineado con el inventario general de activos de información. En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

### **6.7. Política de Uso Aceptable de los Activos**

La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de COMFAMILIAR Cartagena y Bolívar, son activos de la Corporación y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos de la corporación.

COMFAMILIAR Cartagena y Bolívar podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en esta manual y en cualquier proceso legal que se requiera.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y terceros determinadas.

La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas de COMFAMILIAR Cartagena y Bolívar se permitirá en días y horas laborales, con la presencia del funcionario responsable.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

Para la consulta de documentos cargados se establecerán privilegios de acceso a los funcionarios, terceros y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Jefe del área, quien comunicará al grupo encargado de la administración del software el listado con los funcionarios y sus privilegios.

El Jefe del área, será quien determine el carácter de reserva o restricción de los documentos físicos. Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "Acuerdo de Confidencialidad de la Información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en la Política de Información del COMFAMILIAR Cartagena y Bolívar y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

### **6.7.1. Acceso a Internet:**

No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del Comfamiliar.
- El Intercambio no autorizado de información de propiedad de Comfamiliar, de sus clientes, usuarios y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Líder respectivo y la Líder de los estándares de Dirección de la Información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

COMFAMILIAR Cartagena y Bolívar debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente.

Cada usuario es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

Los funcionarios, contratistas y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de COMFAMILIAR Cartagena y Bolívar, posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos similares.

El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de COMFAMILIAR Cartagena y Bolívar.

#### **6.7.2. Correo electrónico:**

El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de COMFAMILIAR Cartagena y Bolívar.

Los mensajes y la información contenida en los buzones de correo son propiedad de COMFAMILIAR Cartagena y Bolívar y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de los buzones de correo es determinado por el área de Tecnología y Sistemas de Información de la corporación de acuerdo con las necesidades de cada usuario y previa autorización del Jefe del área correspondiente.

El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por el área de Tecnología y Sistemas de Información de COMFAMILIAR Cartagena y Bolívar

El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que COMFAMILIAR Cartagena y Bolívar, proporciona.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*



El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del área de Comunicaciones y la autorización del área de Tecnología y Sistemas de Información de Comfamiliar. Si una dependencia debe por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de la cuenta [comunicaciones@comfamiliar.org.co](mailto:comunicaciones@comfamiliar.org.co) y/o servicio habilitado para tal fin y no a través de cuenta de correo electrónico asignadas a un funcionario o cargo particular.

Toda información de COMFAMILIAR Cartagena y Bolívar generada con los diferentes programas computacionales que requiera ser enviada fuera de la corporación, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de Tecnología y Sistemas de Información. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por COMFAMILIAR Cartagena y Bolívar y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correos.

El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto, COMFAMILIAR Cartagena y Bolívar no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.

Las únicas áreas de la Corporación autorizadas para enviar mensajes a través de la lista de correo denominada personal en la cual se incluyen todas las direcciones de correo del Comfamiliar son: La Dirección, Comunicaciones, Sistemas y Talento Humano.

El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en COMFAMILIAR Cartagena y Bolívar.

Se aplicarán además los siguientes parámetros para la utilización del correo electrónico de COMFAMILIAR Cartagena y Bolívar.

No está permitido:

Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Corporación, mensajes mal intencionados que puedan afectar los sistemas

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

Utilizar la dirección de correo electrónico de COMFAMILIAR Cartagena y Bolívar como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el jefe de área respectivo y el área de Tecnología y Sistemas de Información de COMFAMILIAR Cartagena y Bolívar.

### **6.7.3. Recursos tecnológicos:**

La instalación de cualquier tipo de software o hardware en los equipos de cómputo de COMFAMILIAR Cartagena y Bolívar es responsabilidad del área de Tecnología y Sistemas de Información, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por COMFAMILIAR Cartagena y Bolívar a través de esta área.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como: conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por el área de Tecnología y Sistemas de Información.

El área de Tecnología y Sistemas de Información de COMFAMILIAR Cartagena y Bolívar definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por el Comfamiliar.

Los funcionarios serán conectados a la red de COMFAMILIAR Cartagena y Bolívar con previa solicitud escrita y autorizada por el jefe del área. Los terceros y/o contratistas se conectarán a la red de COMFAMILIAR, bajo los lineamientos del área de Tecnología y Sistemas de Información, asegurando la legalidad del equipo a través de certificados emitidos por la empresa contratista, de acuerdo con lo definido por el área de Tecnología y Sistemas de Información.

Los usuarios que requieren acceder a la infraestructura tecnológica de COMFAMILIAR Cartagena y Bolívar desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Tecnología y Sistemas de Información. Además, deberán informar previamente a la misma área para autorizar el

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

acceso y brindar los permisos respectivos para la protección de la información, de acuerdo con lo definido por el área de Tecnología y Sistemas de Información.

La sincronización de dispositivos móviles, tales como tablets, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe ser autorizado de forma explícita por el jefe del área respectiva, con el apoyo del área de Tecnología y Sistemas de Información de COMFAMILIAR Cartagena y Bolívar

COMFAMILIAR Cartagena y Bolívar brindará el servicio de Internet a los usuarios que accedan a alguno de los servicios de la corporación.

Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas, entre otras, jugar o grabar música.

Ningún funcionario, contratista o tercero podrá copiar para uso personal archivos o programas de propiedad de la COMFAMILIAR Cartagena y Bolívar.

#### **6.8. Acuerdos sobre confidencialidad.**

Todos los funcionarios, colaboradores y/o terceros que presten sus servicios a COMFAMILIAR Cartagena y Bolívar deberán aceptar los acuerdos de confidencialidad definidos por la corporación, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de COMFAMILIAR Cartagena y Bolívar a personas o corporaciones externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

#### **6.9. Partes externas**

COMFAMILIAR Cartagena y Bolívar identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

## **6.10. Clasificación de la información**

COMFAMILIAR Cartagena y Bolívar con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios,

contratistas, proveedores o clientes, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

Toda la información de COMFAMILIAR Cartagena y Bolívar debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por el Comité de Seguridad de la información.

Los niveles de clasificación de la información definidos en COMFAMILIAR Cartagena y Bolívar son:

- Externa
- Categoría pública
- Pública uso interno
- Pública clasificada
- Pública reservada

Los criterios, niveles de clasificación y aplicación se encuentran detallados en los lineamientos de inventario del documento y estos son revisados y aprobados de manera periódica por el Comité de Seguridad de la Información de Comfamiliar.

Los propietarios de los activos de información son los responsables de identificar y asociar el nivel de clasificación a cada activo, teniendo en cuenta los criterios de clasificación, y su protección se establece de acuerdo con lo definido en el inventario de activos de información COMFAMILIAR Cartagena y Bolívar.

## **6.11. Seguridad de los recursos humanos**

Todos los funcionarios de COMFAMILIAR Cartagena y Bolívar, contratistas y terceros que tengan la posibilidad de acceder a la información de la organización y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información de

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

COMFAMILIAR Cartagena y Bolívar, de igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

Todos los funcionarios de COMFAMILIAR Cartagena y Bolívar, deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la organización.

#### **6.11.1. Roles y responsabilidades**

El área de Talento Humano es la encargada de diseñar, documentar y actualizar el Manual de funciones de COMFAMILIAR Cartagena y Bolívar, donde se detallan los roles, las responsabilidades y funciones a ser ejecutadas durante el desarrollo de las actividades en la Corporación. Para los contratistas y terceros se describirán las responsabilidades en los contratos respectivos que intervienen con el COMFAMILIAR Cartagena y Bolívar.

#### **6.11.2. Selección de personal**

Toda vinculación laboral realizada por COMFAMILIAR Cartagena y Bolívar se rige por las leyes de la República de Colombia y por lo dispuesto en el Código Sustantivo del Trabajo.

Todo funcionario contratado por COMFAMILIAR Cartagena y Bolívar es seleccionado adecuadamente, de acuerdo con los requerimientos de cada cargo y siguiendo las tareas descritas en el Procedimiento selección y contratación. En caso que el proceso de selección o la contratación se realice por intermedio de terceros, COMFAMILIAR Cartagena y Bolívar debe asegurar la definición clara de las responsabilidades y los mecanismos para manejar el incumplimiento de los requisitos. Sin importar el método de contratación, todo funcionario recibe y acepta las políticas de seguridad de la Corporación.

COMFAMILIAR Cartagena y Bolívar verifica la información brindada durante el proceso de vinculación de los funcionarios; conforme con lo dispuesto en el Procedimiento Selección y contratación de la Corporación.

#### **6.11.3. Términos y condiciones laborales**

Todos los funcionarios y aquellos terceros definidos por COMFAMILIAR Cartagena y Bolívar están obligados a cumplir los acuerdos de confidencialidad por todo el período de vigencia del contrato de trabajo y un lapso posterior de carácter indefinido, acorde a las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos de información que le son entregados y que éstos son extensibles aún fuera de la Corporación.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

	<b>MANUAL DE SEGURIDAD DE LA INFORMACION</b>	<b>CÓDIGO:</b> SIS-MA-001	
		<b>Versión:</b> 002	<b>Fecha de Versión:</b> 24/01/2022
		Página <b>21</b> de <b>31</b>	

Adicionalmente, con funcionarios y terceros deben quedar establecidos en aspectos como propiedad intelectual, protección de la información y leyes aplicables.

#### **6.11.4. Educación, formación y concientización sobre la Seguridad de la Información**

El área de Talento Humano de COMFAMILIAR Cartagena y Bolívar debe asegurar que todos los funcionarios que tengan definidas responsabilidades de Seguridad de la Información son competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para ello.

De igual forma, todos los funcionarios y, cuando sea relevante, los terceros tendrán un proceso formal de concientización, mediante el cual se capacitará sobre las políticas de seguridad de la Corporación y los riesgos conocidos a los que se puede ver expuesta, en caso que estas no se cumplan.

Los programas de concientización, educación y entrenamiento se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

#### **6.11.5. Proceso disciplinario**

En el caso de identificarse un incidente de seguridad se hará la investigación respectiva para determinar las causas y responsables, posteriormente, COMFAMILIAR Cartagena y Bolívar tomará las acciones pertinentes para el funcionario y/o tercero vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la organización dicho incidente.

#### **6.11.6. Terminación o cambio de la contratación laboral**

La Subdirección Administrativa, será la encargada de informar a las áreas implicadas en los procesos de vinculación y desvinculación, los movimientos del personal según los lineamientos establecidos en COMFAMILIAR Cartagena y Bolívar.

#### **6.11.7. Responsabilidades en la terminación o cambio de funciones.**

El Jefe de Talento Humano, en conjunto con el jefe directo del funcionario y/o responsable del tercero y un funcionario designado del área de Tecnología y Sistemas de Información, son los encargados del proceso de terminación de labores y asegurar que todos los activos propios de la organización sean devueltos, los accesos físicos y lógicos sean eliminados, y la

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

información pertinente sea transferida, de acuerdo con los procedimientos establecidos por la corporación y deben quedar consignadas en el acta de entrega de cargo.

En caso que un funcionario y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su rol y aplicando el formato de acta de entrega de cargo.

#### **6.11.8. Devolución de Activos.**

Todo funcionario al momento de su retiro o cambio de funciones en la Corporación debe hacer entrega del equipo que se le había asignado a El Jefe de Talento Humano, en conjunto con el jefe directo del funcionario y/o responsable del tercero y un funcionario designado del área de Tecnología y Sistemas de Información su jefe inmediato, con toda la información contenida en él y una relación de la misma.

### **6.12. Seguridad física y del entorno**

COMFAMILIAR Cartagena y Bolívar será el responsable de definir el perímetro de la seguridad física de acuerdo a la clasificación de los activos de la información, controlando el acceso a la información a través de controles (Ejemplo: acceso a áreas restringidas, registro de entrada de equipos, autenticación biométrica), los cuales disminuyen la posibilidad de riesgo de divulgación o pérdida de información.

#### **6.12.1. Controles de Acceso Físico**

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.).

#### **6.12.2. Protección y ubicación de los equipos**

Los equipos que hacen parte de la Infraestructura tecnológica de COMFAMILIAR Cartagena

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*



y Bolívar tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de COMFAMILIAR Cartagena y Bolívar no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

Cualquier traslado de equipos informáticos se realizará con la coordinación del área de Tecnología y Sistemas de Información previa verificación de las condiciones técnicas y de seguridad.

Toda persona que note algún problema de funcionamiento en una estación de trabajo informático está obligada a reportarlo de inmediato al personal de soporte técnico del área de Tecnología y Sistemas de Información mediante el uso de los canales de comunicación dispuestos para tal fin.

COMFAMILIAR Cartagena y Bolívar debe proveer suministros y equipamiento de soporte como electricidad, aire acondicionado, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

De igual manera, COMFAMILIAR Cartagena y Bolívar debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a la infraestructura tecnológica.

Ningún empleado, contratista o tercero podrá desarmar o destapar equipos sin la autorización previa del Tecnología y Sistemas de Información.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

	<b>MANUAL DE SEGURIDAD DE LA INFORMACION</b>	<b>CÓDIGO:</b> SIS-MA-001	
		<b>Versión:</b> 002	<b>Fecha de Versión:</b> 24/01/2022
		Página <b>24</b> de <b>31</b>	

### **6.12.3. Seguridad de los equipos y medios de información fuera de las instalaciones**

Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos de COMFAMILIAR Cartagena y Bolívar que se encuentren fuera de las instalaciones de la organización.

Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

Los equipos de infraestructura de Comfamiliar Cartagena y Bolívar deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.

Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

En caso de pérdida, daño o robo de un equipo de COMFAMILIAR Cartagena y Bolívar, el funcionario deberá informar inmediatamente al Jefe de área respectiva y al jefe de tecnología; así como responder reemplazando el equipo o en su defecto cancelar el valor del equipo de acuerdo al avalúo comercial al momento del incidente, además debe colocar la denuncia respectiva ante la autoridad competente.

El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad de COMFAMILIAR Cartagena y Bolívar, fuera de las instalaciones de la organización debe seguir los procedimientos establecidos.

### **6.12.4. Eliminación o reutilización segura de equipos y medios**

COMFAMILIAR Cartagena y Bolívar debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

Cuando un equipo sea reasignado o dado de baja, se deberá realizar el proceso de acuerdo con el procedimiento establecido.

## **6.13. Gestión de comunicaciones y operaciones**

### **6.13.1. Documentación de procedimientos operativos**

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

Se debe contar con procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica de COMFAMILIAR Cartagena y Bolívar. Cada procedimiento debe tener un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

### **6.13.2. Control de Cambios**

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos asociados que pueden afectar la operación de la corporación de acuerdo con los lineamientos establecidos en la matriz de riesgos del área de Tecnología y Sistemas de Información.

Los cambios estructurales que se planteen realizar sobre las plataformas críticas deben ser revisados por el Comité de Seguridad de la Información, el cual debe establecer los requerimientos de seguridad necesarios conforme a las políticas establecidas por COMFAMILIAR Cartagena y Bolívar, que tengan como fin evitar un impacto adverso en las operaciones del negocio.

La Gestión de Cambios debe contener como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, responsabilidades definidas, un plan alternativo para abortar cambios no satisfactorios (Rollback), eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio, todo ello deberá estar registrado.

### **6.13.3. Segregación de funciones**

Toda tarea en la cual sus funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

Todos los sistemas de disponibilidad crítica o media de la Corporación, en lo posible, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

### **6.13.4. Separación de los ambientes de desarrollo, prueba y producción**

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

COMFAMILIAR Cartagena y Bolívar ha definido diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.

Dado lo anterior, los ambientes establecidos por COMFAMILIAR Cartagena y Bolívar se definen así:

- **Ambiente de Desarrollo:** Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.
- **Ambiente de Pruebas:** Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos para realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción de COMFAMILIAR Cartagena y Bolívar.
- **Ambiente de Producción:** Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de COMFAMILIAR Cartagena y Bolívar. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, base de datos, programas ejecutables o compilados.

A través de las políticas de control de acceso físico y lógico definidas por la Corporación, se controla el acceso a cada uno de los ambientes. Adicionalmente, ambientes de desarrollo, pruebas y producción están totalmente separados, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros dos ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

El área de Tecnología y Sistemas de Información debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados.

Igualmente debe asegurar, mediante los controles adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, así mismo que cada menú de opciones muestren los mensajes de identificación apropiados para reducir los riesgos de error.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

### **6.13.5. Gestión de la capacidad**

COMFAMILIAR Cartagena y Bolívar mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

Periódicamente, se realizarán mediciones de las variables críticas de operación de la infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos. De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.

Los resultados de dichas mediciones serán analizados y presentados al Comité de Seguridad de la Información y en caso de ser necesario la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos con autorización de la alta dirección.

### **6.13.6. Aceptación de sistemas**

El área de Tecnología y Sistemas de Información debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software estén claras y adecuadamente definidos, documentados y aprobados acordes a las necesidades de COMFAMILIAR Cartagena y Bolívar. Estos nuevos requerimientos, actualizaciones y/o nuevas versiones de tecnología, sólo deben ser migrados al ambiente de producción después de haber sido formalmente aceptados de acuerdo a las necesidades técnicas y funcionales establecidas.

Todo sistema que se implemente o instale en COMFAMILIAR Cartagena y Bolívar, en cualquier modalidad de adquisición, debe tener la capacidad de integrarse al sistema ERP corporativo y será evaluado por el área de Tecnología y Sistemas de Información para verificar su buen funcionamiento y los procedimientos de mantenimiento y soporte de la solución.

### **6.13.7. Protección contra software malicioso**

COMFAMILIAR Cartagena y Bolívar establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del área de Tecnología y Sistemas de Información autorizar el uso de

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia por el funcionario, así como de su actualización permanente.

Así mismo, COMFAMILIAR Cartagena y Bolívar define que no está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por COMFAMILIAR Cartagena y Bolívar.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo. Si estos medios son requeridos por la organización, deben ser provisto por ella con previa autorización del área de Tecnología y Sistemas de Información.
- El uso de código móvil, solo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por el área de Tecnología y Sistemas de Información.

#### **6.13.8. Copias de Respaldo**

COMFAMILIAR Cartagena y Bolívar debe asegurar que la información con cierto nivel de clasificación, definida en conjunto con el área de Tecnología y Sistemas de Información y las áreas responsables de la misma, contenida en la plataforma tecnológica de la Corporación, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El área de Tecnología y Sistemas de Información establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Además, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medida de protección y seguridad física apropiados.

Es responsabilidad del funcionario realizar copia de seguridad en la nube corporativa asociada a su cuenta, de los archivos de trabajo diario y periódico que no se almacenan en ninguna base de datos o Sistema de Información.

#### **6.13.9. Gestión de medios removibles**

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, IPod, celulares, cintas) sobre la infraestructura para el procesamiento de la información de COMFAMILIAR Cartagena y Bolívar, estará autorizado para aquellos funcionarios cuyo perfil de cargo y funciones lo requiera.

El área de Tecnología y Sistemas de Información es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de COMFAMILIAR Cartagena y Bolívar sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de COMFAMILIAR Cartagena y Bolívar.

#### **6.13.10. Intercambio de información**

COMFAMILIAR Cartagena y Bolívar firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Corporación. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deber firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario de COMFAMILIAR Cartagena y Bolívar es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los medios transportados fuera de las instalaciones de COMFAMILIAR Cartagena y Bolívar deberán cumplir con los controles establecidos.

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*



#### **6.14. Política de prestación de servicios por Proveedores**

Todos los proveedores que por actividades internas tengan un contrato con COMFAMILIAR Cartagena y Bolívar, deberán acogerse a los siguientes lineamientos:

- Todo proveedor deberá cumplir con los lineamientos de seguridad de la información establecidos en COMFAMILIAR Cartagena y Bolívar, así mismo como con la normatividad definida en sus procesos internos.
- Los proveedores deberán reportar las debilidades de seguridad que puedan encontrar durante la ejecución del contrato con COMFAMILIAR Cartagena y Bolívar.
- Se deberá informar sobre todas las actualizaciones existentes de cada plataforma que mejoren el desempeño de los procesos y subprocesos de COMFAMILIAR Cartagena y Bolívar.
- Todo proveedor adquiere el compromiso de reportar los impactos de los cambios aplicados a los procesos y subprocesos de COMFAMILIAR Cartagena y Bolívar.
- Los proveedores deberán reportar los eventos que afecten el desarrollo de los cambios que se aplicarán, desde la realización de las pruebas hasta la salida a producción del requerimiento.
- Todos los proveedores deberán adherirse al flujo de requerimientos e incidentes establecido como proceso interno de COMFAMILIAR Cartagena y Bolívar.
- Los proveedores deberán realizar transferencia de conocimiento y /o acompañamiento a los funcionarios del proceso a través de capacitaciones y manuales descriptivos de la operación contratada por COMFAMILIAR Cartagena y Bolívar.
- Los proveedores tienen el compromiso de aportar y realizar sugerencias para el mejoramiento de los procesos y óptimo aprovechamiento del servicio que se esté prestando.
- COMFAMILIAR Cartagena y Bolívar en general será el único dueño de los derechos de autor de los desarrollos que se realicen internamente, los proveedores deberán respetar su confidencialidad conforme a lo establecido en el contrato.

#### **7. FORMATOS/ANEXO**

[Ver Listado Maestro de Documentos de la Corporación](#)

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*

	<b>MANUAL DE SEGURIDAD DE LA INFORMACION</b>	<b>CÓDIGO:</b> SIS-MA-001	
		<b>Versión:</b> 002	<b>Fecha de Versión:</b> 24/01/2022
		Página <b>31</b> de <b>31</b>	

## 8. DOCUMENTOS EXTERNOS

[Ver Normagrama.](#)

## 9. RIESGOS

[Ver Matriz Modulo Riesgos en KAWAK](#)

## 10. CONTROL DE CAMBIOS

Fecha Cambio	Versión	Descripción del Cambio	Responsable	Fecha verificación en listado maestro de documentos
05/04/2018	001	CREACION	Jefe de Tecnología	05/04/2018
24/01/2022	002	Actualización de acuerdo a la Norma 27001:2005 Actualización CSI y responsables y roles del comité	Jefe de Tecnología	24/01/2022

*Este documento es propiedad de Comfamiliar Cartagena y Bolívar, prohibida su reproducción. Cualquier modificación debe solicitar permiso al encargado del Sistema Integrado de Gestión (SIG)*