	<p align="center">MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR</p>	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 1 DE 62

**MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
SGSI**

CAJA DE COMPENSACIÓ FAMILIAR DE ARAUCA COMFIAR

Tu Puedes COMFIAR En Mi Calidad






	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 2 DE 62

Tabla de Contenido

INTRODUCCIÓN	6
1. OBJETIVO GENERAL	7
1.1. Objetivos del Sistema de Seguridad de la Información.....	7
2. TÉRMINOS Y DEFINICIONES	9
3. CONTACTO CON LAS AUTORIDADES	11
4. ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?	12
5. ENFOQUE BASADO EN PROCESOS	13
6. METODOLOGÍA DE VALORACIÓN DEL RIESGO	18
6.1. Análisis de calificación y valoración del riesgo.....	22
6.2. Calificación y Zona del Riesgo.....	24
6.3. Matriz De Riesgo	26
7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	27
8. ALCANCE/APLICABILIDAD	28
9. REVISIÓN DE LA POLÍTICA	28
10. PRINCIPIOS QUE SOPORTAN LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACIÓN DE COMFIAR.....	29
11. CLASIFICACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACIÓN DE COMFIAR.....	30
11.1. Seguridad de los Recursos Humanos.....	30
11.1.1. Antes de la Contratación Laboral.....	30
11.1.2. Roles y responsables.....	31
11.2. Durante la Vigencia del Contrato Laboral	31
11.3. Terminación o Cambio de la Contratación Laboral	32
11.4. Devolución de los Activos	32
11.5. Retiro de los derechos de acceso.....	32
11.6. Gestión de Activos.....	33
11.6.1. Instalaciones de equipos de cómputos y comunicaciones.....	33
11.6.2. Dispositivos móviles, teletrabajo o trabajo remoto.....	34
11.6.3. Reglas para el uso del correo electrónico y de Internet.....	35
11.7. Responsables de los activos.....	37
11.8. Control de acceso a equipos de cómputo, de comunicaciones y plataformas	38
11.8.1. Control de acceso con usuario y contraseña	38
11.8.2. Gestión de Contraseñas	39
11.8.3. Control de acceso remoto.....	40
11.8.4. Control de acceso a la Web.....	40
11.9. Seguridad Física y del Entorno	41
11.9.1. Áreas seguras.....	41

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 3 DE 62

11.9.2.	Perímetro de Seguridad Física	41
11.9.3.	Controles de acceso físico.....	42
11.9.4.	Seguridad de oficinas, recintos e instalaciones	42
11.9.5.	Acceso a áreas críticas.....	43
11.9.6.	Protección Contra Amenazas Externas y Ambientales.....	43
11.9.7.	Áreas de carga, despacho y acceso público.....	44
11.9.8.	Seguridad de los equipos	44
11.9.9.	Ubicación y protección de los equipos.....	46
11.9.9.1.	Mantenimientos de equipos de cómputo.	47
11.9.10.	Seguridad de cableado	48
11.10.	Gestión de Software	50
11.10.1.	Adquisición de Software.....	50
11.10.2.	Instalación del Software	51
11.10.3.	Actualización de Software	51
11.10.4.	Auditoria de Software instalado.....	52
11.10.5.	Software e información propiedad de COMFIAR	52
11.10.6.	Supervisión y evaluación.....	53
11.11.	Gestión de Comunicaciones y Operaciones.....	53
11.11.1.	Respaldo.....	53
11.11.2.	Respaldo de la Información.....	53
11.12.	Gestión de la seguridad de las redes	54
11.12.1.	Controles de las redes	55
11.13.	Control De Acceso.	55
11.13.1.	Requisitos de la Corporación para el control de acceso	55
11.13.2.	Control de acceso	56
11.13.3.	Control de acceso al sistema operativo.....	57
11.13.4.	Procedimientos de ingreso seguros	57
11.13.5.	Identificación y autenticación de usuarios	58
12.	COMPROMISO DE LA DIRECCIÓN.....	58
13.	SANCIONES PREVISTAS POR EL INCUMPLIMIENTO	59
14.	RECOMENDACIONES	59
15.	ANEXOS	60

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 4 DE 62

Lista de Tablas

Tabla 1. Alineamiento del SGSI y el proceso de Gestión del Riesgo en la seguridad de la información.....	21
Tabla 2. Pasos de la metodología.	22
Tabla 3. Calificación de la Frecuencia.	22
Tabla 4. Calificación del Impacto.	23
Tabla 5. Calificación del Alcance.	23
Tabla 6. Calificación de la Zona de Riesgo.....	24
Tabla 7. Valoración del Control.	25
Tabla 8. Valoración del Riesgo.	25



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 5 DE 62

Tabla de Figuras

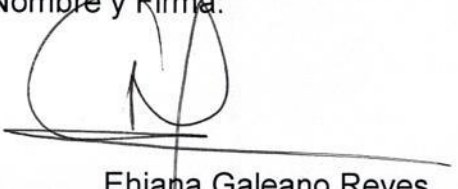
Figura 1. Ciclo PHVA del Modelo de Seguridad y Privacidad de la Información	14
Figura 2. Relación entre la ciberseguridad y otros ámbitos de la seguridad	15
Figura 3. Modelo PHVA aplicados a los procesos de SGSI.	16
Figura 4. Mapa de Procesos Comfiar.	17
Figura 5. Proceso de gestión del riesgo en la seguridad de la información.....	20

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 6 DE 62


INTRODUCCIÓN

El Sistema de Seguridad de la información de *la Caja de Compensación Familiar de Arauca COMFIAR*, tiene por objeto describir el sistema de gestión de la seguridad de la información que la Corporación ha establecido de acuerdo a la Norma Técnica Colombiana ISO 27001, para lograr la satisfacción de los usuarios y/o afiliados clientes y comunidad en general respecto al manejo de su información, garantizar el cumplimiento de los requisitos legales, los reglamentarios aplicables y la orientación misional de la corporación donde además se identifican la política y objetivos de la seguridad de la información, el alcance, la descripción e interacción de los procesos.

Es compromiso de todos los trabajadores de La Caja de Compensación Familiar de Arauca COMFIAR, aplicar este SGSI como principal documento para la consolidación y mejora continua, que le permita a la Corporación años tras año ser más competitiva. La implementación del SGSI refleja la convicción de que el Sistema de Gestión de la Información contribuya a salvaguardar la información como bien primordial para la toma de decisiones.

REVISO:	APROBO:
Nombre y Firma:	Nombre y Firma:
 Uriel Fernando de Avila Castro	 Ehiana Galeano Reyes
Fecha: 14 de junio de 2022	Fecha: 14 de junio de 2022



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 7 DE 62


1. OBJETIVO GENERAL.

Establecer lineamientos para la adecuada gestión de la seguridad y privacidad de la información de la Caja de Compensación Familiar de Arauca COMFIAR, basado en la identificación y valoración de los riesgos de la información utilizada por la corporación, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio, donde se garantice el cumplimiento de la normatividad vigente en toda la organización.


1.1. Objetivos del Sistema de Seguridad de la Información

Comfiar ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en los lineamientos definidos de acuerdo a las necesidades de la Corporación, y a los requerimientos regulatorios de acuerdo como lo determina la Superintendencia del Subsidio familiar basados en la ISO/IEC 27001.

- Brindar disponibilidad, integridad, seguridad y confidencialidad de la información de los Clientes externos (usuarios y/o afiliados de la Caja de Compensación Familiar de Arauca Comfiar) y clientes internos (procesos de la Corporación), cumpliendo con los requisitos legales.
- Proteger la información generada, procesada o resguardada por los procesos de la Corporación y activos de información que hacen parte de los mismos.
- Proteger la información creada, procesada, transmitida o resguardada por los procesos de la Corporación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o custodia.
- Garantizar la satisfacción de los clientes internos y externos en materia de seguridad de la información.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 8 DE 62

- Proteger la información de las amenazas originadas por parte del personal o colaboradores.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soportan los procesos críticos.
- Controlar la operación de los procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizar a través de una adecuada gestión de los elementos de seguridad y las debilidades asociadas con los sistemas de información una mejora continua y efectiva del modelo de seguridad.
- Garantizar la disponibilidad de los procesos de negocio y la continuidad de la operación basado en el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales que están establecidas y vigentes.
- Asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso que ésta sufra daños o pérdida producto de accidentes, atentados o desastres.


	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 9 DE 62

2. TÉRMINOS Y DEFINICIONES.


A efectos de este documento se aplican los siguientes términos y definiciones:

- **Comfiar:** Caja de Compensación Familiar de Arauca.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de gestión de la seguridad de la información:** parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y totalidad de la información y sus métodos de procesamiento.
- **Disponibilidad:** acceso autorizado de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **No repudio:** se refiere a evitar que una entidad o individuo que haya enviado o recibido información alegue ante terceros que no la envió o recibió
- **Activo:** Bien o elemento tangible o intangible que tiene valor para la organización.
- **Amenaza:** causa potencial de un incidente que puede producir daño a un sistema u organización
- **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar la magnitud del riesgo
- **Confiabilidad:** propiedad de tener comportamiento y resultados previstos consistentes
- **Control:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 10 DE 62

- que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **Directrices:** descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- **Impacto:** resultado de un incidente de seguridad de la información.
- **Política:** Toda intención de directriz expresada formalmente por la dirección.
- **Proceso:** es cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas.
- **Riesgo:** potencial de una amenaza determinada aproveche las vulnerabilidades de un activo o un grupo de activos y produzca daño a la organización. Se mide en términos de la combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo residual:** riesgo que permanece después del tratamiento del riesgo.
- **Evaluación del Riesgo:** se entiende por evaluación de riesgo a la evolución de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad que ocurran y su potencial impacto en Comfiar.
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
- **Vulnerabilidad:** debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.
- **Open-Source:** también llamado “Código Abierto” es un término que se utiliza para denominar a cierto tipo de software que se distribuye mediante una licencia que le permite al usuario final, si tiene los conocimientos necesarios, utilizar el código fuente del programa para estudiarlo, modificarlo y realizar mejoras en el mismo, pudiendo incluso hasta redistribuirlo.
- **GLPI:** (acrónimo: en francés, Gestionnaire Libre de Parc Informatique), es un software que permite gestionar el área tecnológica de una organización.
- **ERP** (Planificación de Recursos Empresariales): es un conjunto de aplicaciones de software integradas, que nos permiten automatizar la

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 11 DE 62

mayoría de las prácticas de Comfiar relacionadas con los aspectos operativos o productivos de nuestra empresa, facilitando y centralizando la información de todas las áreas que la componen: compras, producción, logística, finanzas, recursos humanos, marketing, servicios, proyectos y atención al cliente.

3. CONTACTO CON LAS AUTORIDADES.

Contactos con las autoridades pertinentes:

Para efectos de robos, incendio, accidentes laborales y otros:


ÍTEM	NOMBRE	DIRECCIÓN	TELEFONOS
1	POLICIA NACIONAL	Cra 20 con 19 Esquina	(607)8853300
2	BOMBEROS	Calle 23 # 16 -	119
3	DEFENSA CIVIL	Cra 21 # 19 -	(607)8852292
4	HOSPITAL	Calle 15 con 16 esquina	(607)8852024
5	CRUZ ROJA	KR 18 # 30-25	(607)8857010

Para efectos contactos de proveedores de servicios:

Ítem	Proveedor de Servicios	Correo Electrónico	Teléfono
1	Sistemas y Soluciones Integradas E.U	sysintegradas@gmail.com	(601) 833 4545

Tu Puedes COMFIAR En Mi Cali



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 12 DE 62

2	Telefónica Telecom	sandra.parra@telefonica.com	018000 940099
3	Servicios Profesionales Wicom S.A.S	soporte@wicomsas.co	(607) 885 0389

4. ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?


La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en el entorno de negocio cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transferir por correo o por medio electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio.

La seguridad de la información se logra implementado un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplen con los objetivos específicos de seguridad y del negocio de la organización.



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 13 DE 62

5. ENFOQUE BASADO EN PROCESOS

Basado en el enfoque de procesos adoptado por la Comfiar, la Sección de Sistemas hace parte del Proceso de Gestión Administrativa, será la responsable de velar por el cumplimiento de la política y directrices en el manejo de seguridad de la información.

De igual manera todos los procesos son responsables del cumplimiento de esta SGSI que se detallan a continuación:

- **Planificar:** Se establece la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de Comfiar.
- **Hacer:** Se implementa y aplica la política, los controles, procesos y procedimientos del SGSI
- **Verificar:** Realizar evaluación, y en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección para su revisión.
- **Actuar:** Ejecutar acciones correctivas y preventivas con base a los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.


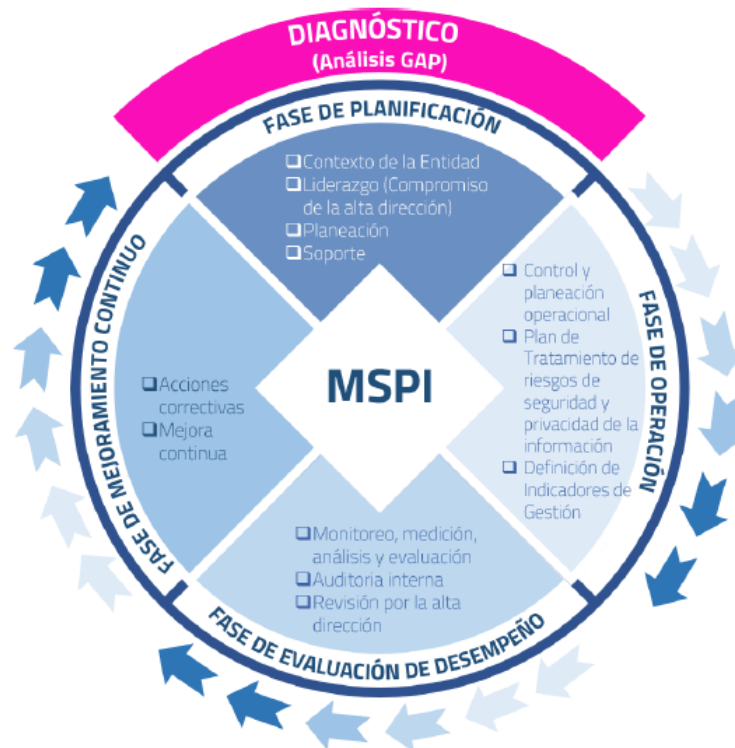
	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 14 DE 62

Figura 1. Ciclo PHVA del Modelo de Seguridad y Privacidad de la Información



Fuente: ISO/IEC 27032


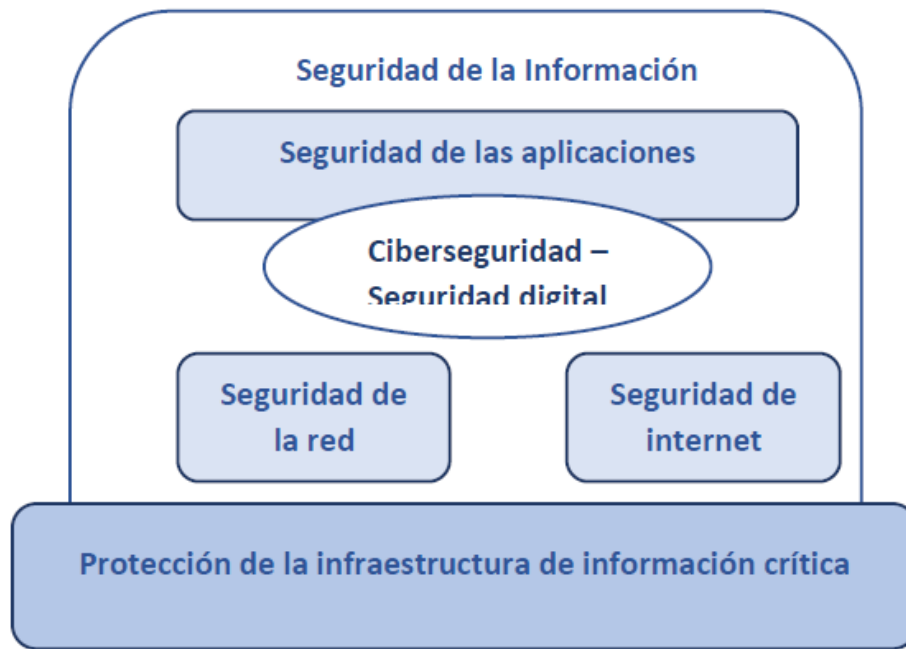
	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 15 DE 62

Figura 2. Relación entre la ciberseguridad y otros ámbitos de la seguridad



Fuente: ISO/IEC 27032

Ver Anexo 1 – **Análisis Gap**


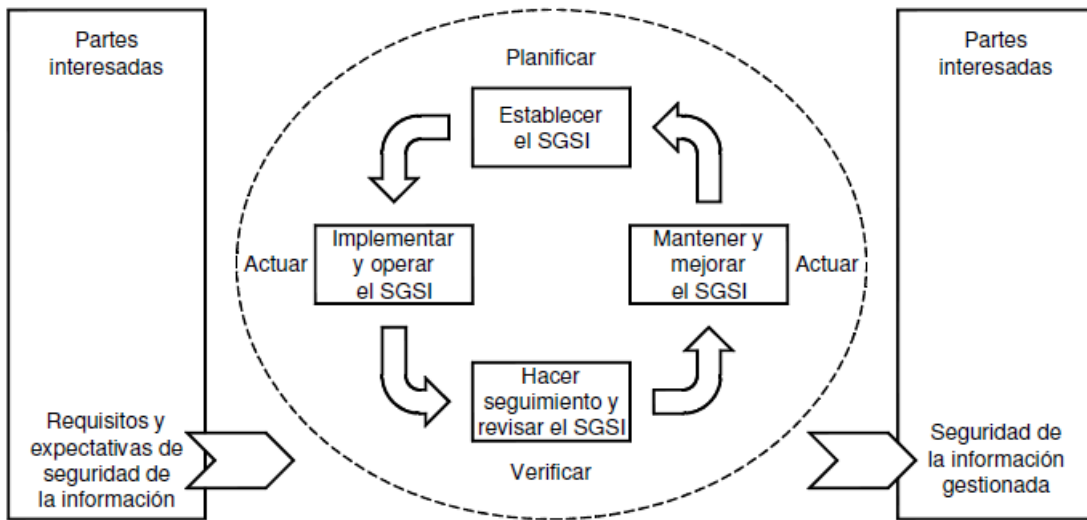
	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 16 DE 62

Figura 3. Modelo PHVA aplicados a los procesos de SGSI.



Fuente: NTC-ISO-/IEC 27001



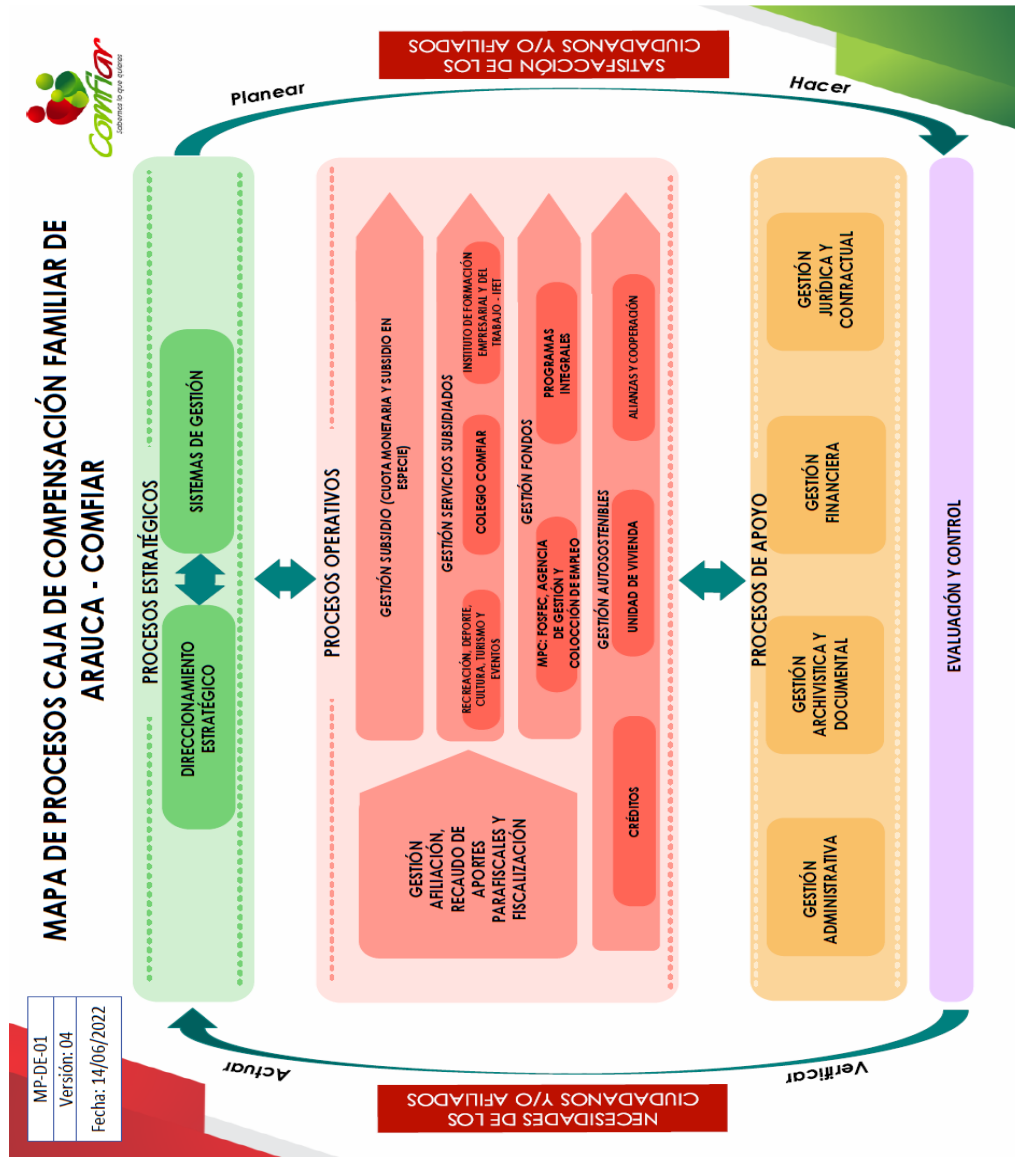
	<p>MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR</p>	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 17 DE 62

Figura 4. Mapa de Procesos Comfiar.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR		CODIGO: ML-GA-01
			VERSION: 03
			FECHA: 14 de junio de 2022
			PÁGINA 18 DE 62




Fuente: El Autor

6. METODOLOGÍA DE VALORACIÓN DEL RIESGO

Tu Puedes COMFIAR En Mi Cali



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 19 DE 62

El proceso de gestión del riesgo se basa de acuerdo a la estructura ISO/IEC 27005:2009 la cual suministra directrices para la gestión del riesgo en la seguridad de la información.

Esta metodología contribuye a:

- Identificación de los riesgos
- Valoración de los riesgos en términos de las consecuencias para Comfiar y la probabilidad de ocurrencia.
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos para Comfiar.
- Establecer el orden por prioridad para el tratamiento de los riesgos.
- La priorización de las acciones para reducir la ocurrencia de los riesgos.
- La participación de los interesados para la toma de decisiones sobre la gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo.
- La eficacia del monitoreo del tratamiento del riesgo.
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos.
- La captura de información para mejorar el enfoque de la gestión del riesgo.
- La educación de la Dirección, gerentes, jefes de sección, líderes de procesos y demás colaboradores acerca de los riesgos y las acciones que se toman para mitigarlos.

El proceso de Gestión del riesgo en la seguridad de la información consta de:

- Establecimiento del contexto.
- Evaluación del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.
- Monitoreo y revisión del riesgo.


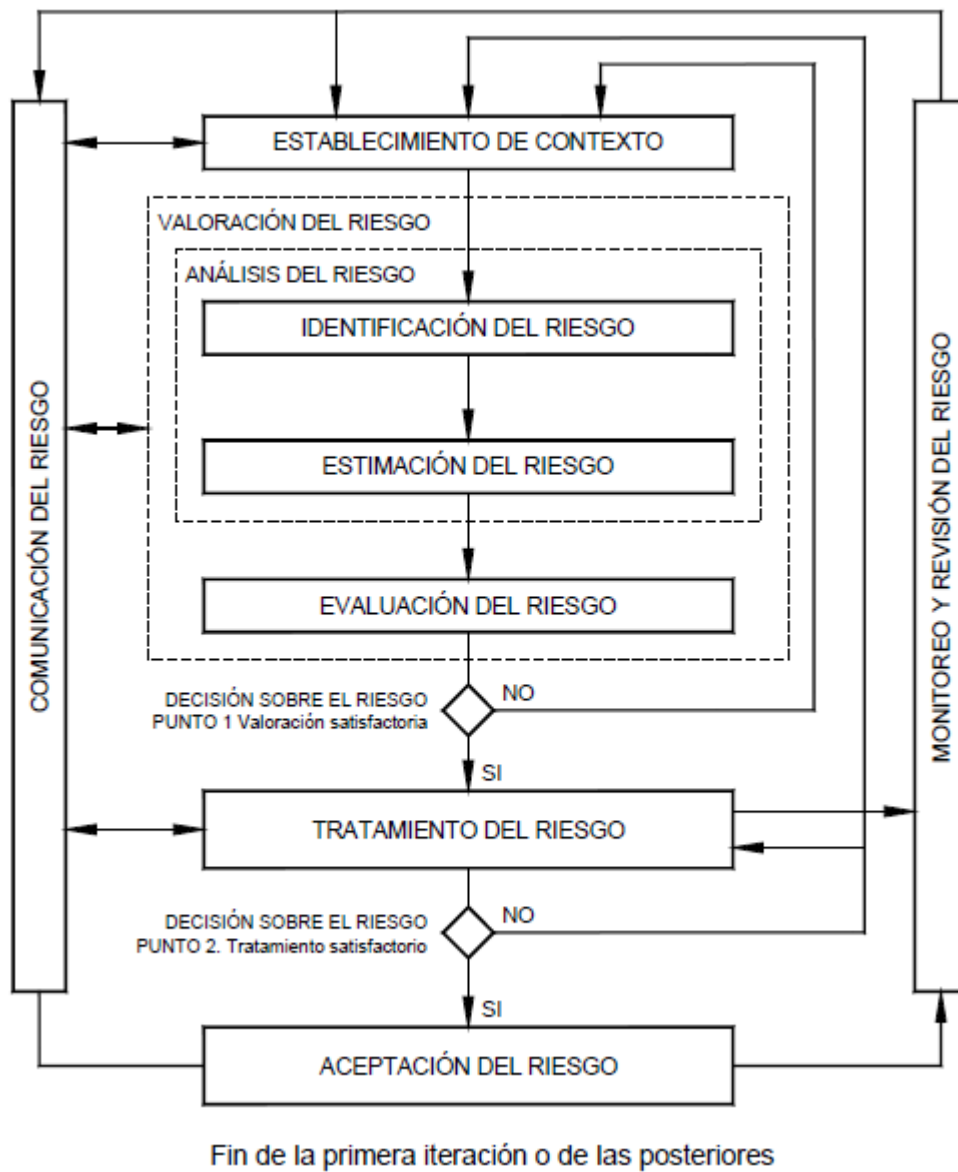

 <p>COMFIAR Caja de compensación familiar de Arauca</p>	<p>MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR</p>	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 20 DE 62

Figura 5. Proceso de gestión del riesgo en la seguridad de la información.



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 21 DE 62

Fuente: El Autor.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del SGSI alineadas al modelo PHVA.

Tabla 1. Alineamiento del SGSI y el proceso de Gestión del Riesgo en la seguridad de la información.

PLANEAR	Definición del plan del riesgo	
	Establecer el contexto de la organización	
	Valoración del riesgo (identificación de activos, amenazas, vulnerabilidades y controles)	Identification del riesgo
		Estimación del riesgo
		Evaluación del riesgo
	Desarrollo del plan para el tratamiento de riesgos	
Aceptación del riesgo		
HACER	Implementar el plan de tratamiento de riesgos	
	Implementar el plan de comunicación de riesgos	
VERIFICAR	Monitoreo y revisión del riesgo	
ACTUAR	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información	

Fuente: El Autor.


	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 22 DE 62


Tabla 2. Pasos de la metodología.

1 - Escenarios de Riesgos (sobre las propiedades de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad)	Información electrónica/digital
	Hardware
	Software/aplicaciones
	Sitios Web
	Servicios
	Infraestructura (Locaciones)
	Servidores IT
	Dispositivos (comunicaciones y seguridad)
	Base de datos
Personal	
2 - Establecimientos del contexto	
3 - establecimiento del plan de comunicación interno y externo	
4 - Valoración de riesgos por escenarios	
5 - Tratamiento de riesgos pos escenarios	
6 - Monitoreo y mejora continua del proceso de gestión	

Fuente: El Autor.

6.1. Análisis de calificación y valoración del riesgo

Tabla 3. Calificación de la Frecuencia.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 23 DE 62

FRECUENCIA (20%)			365 días o menos
No.	Rango	Formula	
3	Alta	Entre > 0,5	# de Veces que ocurre la actividad/# días trabajados al año
2	Media	Entre <= 0,5 y >0,2	
1	Bajo	Entre <=0,2	


Fuente: El autor.

Tabla 4. Calificación del Impacto.

IMPACTO (50%)		
No.	Rango	Criterio
3	Severo	Supera o incumple el rango permitido por los requisitos establecidos (Normatividad Legal - Acuerdos - Disposiciones establecidas por la entidad o partes interesadas)
2	Moderado	Se encuentra dentro de los rangos o parametros establecidos (Normatividad Legal - Acuerdos - Disposiciones establecidas por la entidad o partes interesadas)
1	Leve	Supera las expectativas de los rangos o parametros establecidos (Normatividad Legal - Acuerdos - Disposiciones establecidas por la entidad)

Fuente: El autor.

Tabla 5. Calificación del Alcance.


	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 24 DE 62

ALCANCE (30%)		
No.	Rango	Criterio
3	Global	Eventos que Superan los limites del área donde se ejecutan las actividades propias de la entidad
2	Local	Eventos que están dentro de los límites donde se ejecutan las actividades propias de la entidad
1	Puntual	Eventos que suceden puntualmente y que se pueden tratar dentro de los límites donde se ejecutan las actividades propias de la entidad

Fuente: El autor.

6.2. Calificación y Zona del Riesgo

Tabla 6. Calificación de la Zona de Riesgo.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 25 DE 62

ZONA DEL RIESGO		
No.	Rango	Descripción
> = 2,5	ALTO	La zona de riesgo supera los límites establecidos en cuanto a impacto y alcance afectando las actividades que realiza la entidad para lo cual se deben implementar o establecer controles adicionales
> 2,0 a < 2,5	MEDIO	La zona de riesgo se encuentra en los límites permisibles en cuanto a impacto y alcance, para lo cual se debe evitar que el riesgo se materialice implementando los controles adecuados
< = 2,0	BAJO	La zona de riesgo se encuentra dentro de los rangos establecidos por la entidad en cuanto alcance e impacto permitiendo asumir el control del riesgo.

Fuente: El autor.

Tabla 7. Valoración del Control.


VALORACION DEL CONTROL		
No.	Rango	Formula
3	INEFECTIVO	El control no existe, o existe pero no se aplica, o existe y se aplica pero el mismo no es efectivo.
2	EN PRUEBA	El Control existe y está en implementación pero aún no se evidencia su efectividad.
1	EFECTIVO	El control existe y se aplica de manera efectiva, asegurando la no materialización del riesgo

Fuente: El autor.

Tabla 8. Valoración del Riesgo.

Tu Puedes COMFIAR En Mi Cali




	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 26 DE 62

VALORACION DEL RIESGO		
No.	Rango	Descripción
> = 6	INACEPTABLE	El control con el que actualmente se cuenta para la mitigación del riesgo no asegura que la materialización del mismo no se presente, por lo cual la entidad debe adelantar las acciones inmediatas con el fin de asegurar la efectividad del control (establecer el control, reevaluarlo, establecer unos nuevos, entre otros).
>3 y <6	MODERADO	El Control existente debe evaluarse mediante auditorias o seguimiento permanente con el fin de garantizar el resultado satisfactorio del proceso mediante la mitigación del riesgo.
<=3	ACEPTABLE	Ya la entidad evaluó el control y se está asegurando el resultado del proceso, el riesgo no se ha materializado y mediante la aplicación de estos controles se puede asegurar que el riesgo es aceptable y se controlará a través de seguimiento de auditorias de gestión y externas por parte de los entes de control.

Fuente: El autor.

6.3. Matriz De Riesgo

Ver Anexo 2 - Matriz de Riesgo

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 27 DE 62


7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección Administrativa de la CAJA DE COMPENSACIÓN FAMILIAR DE ARAUCA COMFIAR, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión, visión y la planeación estratégica de la entidad. Para COMFIAR, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

COMFIAR orienta sus esfuerzos con el fin de proteger, asegurar, preservar, conservar y administrar la confidencialidad, integridad, autenticidad, disponibilidad y no repudio de la información, así como el buen uso de esta en medio magnético y/o físicos de los afiliados, beneficiarios, proveedores, comunidad en general y partes interesadas, teniendo en cuenta el cumplimiento de los requisitos legales aplicables.

De acuerdo con lo anterior, esta aplica a la Entidad según como se defina en el alcance, sus trabajadores, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo de las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios estratégicos y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 28 DE 62

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de COMFIAR.
- Garantizar la continuidad de la corporación frente a incidentes.
- COMFIAR ha decidido definir, implementar, operar y mejorar de forma continua de un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros de acuerdo a las necesidades de la Caja, y a los requerimientos regulatorios.

8. ALCANCE/APLICABILIDAD


La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la Seguridad de la Información, los sistemas de comunicación e informáticos y el ambiente tecnológico de Comfiar.

Los lineamientos contenidos en la presente política se aplican a la información circulante en el Mapa de Proceso (Tablas de Retención Documental) documentos y demás información que administre, proteja y preserve la Caja de Compensación Familiar de Arauca COMFIAR y cualquier entidad que ejerza en su nombre o a través de convenios, recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con el personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

Todas las personas cubiertas por el alcance deberán ser comunicadas y cumplir con un 100% de la política.

9. REVISIÓN DE LA POLÍTICA

La Política de Seguridad y Privacidad de la Información se deberá revisar cada 12 meses desde su aprobación y/o actualización o cambios significativos para garantizar que sigue siendo adecuada, suficiente y eficaz.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 29 DE 62


El responsable de la Seguridad de la Información es el jefe de la Sección de Sistemas de Confiar, el cual cumple con la función de supervisar el cumplimiento de La política de seguridad y privacidad de la información y de asesorar en materia de seguridad de la información a los colaboradores de la Corporación que así lo requieran.

Se debe tener en cuenta los resultados de la revisión por parte del responsable. Debe existir procedimientos definidos para la revisión por la Dirección Administrativa, incluyendo una programación o periodo de revisión. las entradas para la revisión por la Dirección Administrativa incluyen información sobre:

- retroalimentación de las partes interesadas.
- resultados de las revisiones independientes.
- Estado de las acciones preventivas y correctivas.
- Resultado de las revisiones previas por parte de la dirección.
- Desempeño del proceso y cumplimiento de la política de seguridad y privacidad de la información.
- Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.
- Tendencias relacionadas con las amenazas y vulnerabilidades.
- Incidentes de seguridad de la información reportados.
- Recomendaciones de las autoridades pertinentes.

10. PRINCIPIOS QUE SOPORTAN LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE COMFIAR

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los líderes de los procesos, y serán compartidas por cualquier medio a los trabajadores, proveedores, socios de negocio o terceros.


	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 30 DE 62

- Proteger la información generada, procesada o resguardada por los procesos de Comfiar, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- Salvaguardar la información creada, procesada, transmitida o resguardada por sus procesos de la corporación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Aplicar las herramientas al alcance para proteger la información de las amenazas originadas por parte del personal.
- Proteger las instalaciones físicas de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de los procesos de la corporación garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar control de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Asegurar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Garantizar la disponibilidad de los procesos de Comfiar y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Cumplir con las obligaciones legales, regulatorias y contractuales establecidas.

11. CLASIFICACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE COMFIAR.

11.1. Seguridad de los Recursos Humanos

11.1.1. Antes de la Contratación Laboral

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 31 DE 62

Se debe cumplir con el procedimiento PR-GA-01 “Procedimiento: Reclutamiento, Selección y Contratación de Personal”; además asegurar que los contratistas y usuarios externos, entiendan sus responsabilidades y que estos sean apropiados y se ajusten a los roles para los que se les considera, esto para reducir el riesgo de robo, fraude o uso de las instalaciones. Para los empleados de esta Corporación lo anterior se realizará una vez se haya suscrito el vínculo contractual.


11.1.2. Roles y responsables

Es responsabilidad de los empleados de Comfiar:

- Proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizada.
- Implementar y actuar de acuerdo con las políticas de seguridad de la información de la Corporación.
- Garantizar que se asigne la responsabilidad a la persona que tome las acciones.
- Informar los eventos de seguridad, los eventos potenciales u otros riesgos de seguridad.
- Cumplir con los acuerdos de confidencialidad.

11.2. Durante la Vigencia del Contrato Laboral

- Asegurar que todos los empleados, contratistas y usuarios visitantes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el error humano mediante concientización, educación y formación en los procedimientos de seguridad y el uso correcto de los servicios y de la información para minimizar los posibles riesgos de seguridad.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 32 DE 62

11.3. Terminación o Cambio de la Contratación Laboral

- Asegurar que los empleados, los contratistas y los usuarios visitantes salgan de la organización o cambien su contrato laboral de forma ordenada.
- En el momento que un empleado, contratista o usuario termine su contrato con esta entidad, se debe asegurar la completa devolución de todos los activos el equipo y la cancelación de todos los derechos de acceso a estos, a la red, correos institucionales, a toda la información y a los aplicativos de la corporación.
- Para la devolución de los equipos cargados al empleado, se debe diligenciar el formato de reintegro a almacén y corroborar con la que allí está cargada a esta persona, para que cruce esta información y recibir el visto bueno.


11.4. Devolución de los Activos

Todos los empleados, contratistas o usuarios externos deben devolver todos los activos pertenecientes a la organización que estén cargados a su nombre a la oficina de almacén, al finalizar su vinculación o acuerdo.

Es necesario que los empleados, contratistas o usuarios externos, tengan conocimiento de la importancia de una información para la continuidad de los procesos o de las operaciones, esta información será entregada a su jefe directo manifestándole la importancia y en qué estado se encuentra el proceso.

11.5. Retiro de los derechos de acceso

A todos los empleados, contratistas o usuarios de terceras partes, una vez finalizada su vinculación con esta entidad o se encuentren en periodo de vacaciones previa notificación de la oficina de Talento Humano, se le cancelarán las contraseñas de las sesiones de ingreso al sistemas operativo, redes inalámbricas, usuario y contraseñas de los diferentes plataformas de la Corporación y demás accesos o permisos que llegare a tener, generándole un

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 33 DE 62


nuevo usuario, contraseña y permisos al funcionario entrante, la cual es solicitada por el jefe de sección o de división al cual corresponda o en su defecto la sección de Talento Humano.

11.6. Gestión de Activos.

Todos los empleados, contratistas, visitantes y usuarios deben dar cumplimiento a la política de seguridad de la información, para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información incluyendo:

11.6.1. Instalaciones de equipos de cómputos y comunicaciones.


- Todo equipo de cómputo y de comunicaciones (computadoras, servidores, estaciones de trabajo, equipos de acceso y de distribución) que sean propiedad de Comfiar, debe sujetarse a las normas y procedimientos de instalación que emite la Sección de Sistemas.
- La Sección de Almacén y Compras elaborara cronograma de toma de inventarios anual, para la verificación y actualización de estos de acuerdo con el procedimiento PR-GA-22 “Procedimiento Inventario de Activos Fijos”.
- La Sección de Almacén y Compras es la responsable de mantener actualizados los inventarios y registros de activos tecnológicos (equipos de computación y de comunicaciones) en el módulo de Activos pertenecientes a Comfiar, los cuales están cedulados (inventariados) de tal manera que puedan ser ubicados, identificados y registrada su trazabilidad desde de su compra y deberá registrar toda actividad de este (trazabilidad y/o repotenciación).
- El custodio del activo responderá por su protección física, así como la información que allí almacene en caso de que sea un equipo de cómputo, dispositivo móvil o de almacenamiento resaltando que es obligación hacer buen uso de este.
- Los movimientos (traslado de activos) en caso de que existan, el responsable del activo deberá notificar a la Oficina de Almacén y Compras mediante el diligenciamiento del respectivo formato de reintegro a Almacén.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 34 DE 62

- Mediante el diligenciamiento del formato FT-GA-28 “Reintegro a Almacén” los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo, contrato que se tenga con la entidad o un traslado interno a otra dependencia.
- Se ejecuta el proceso mediante el cual se realiza de forma segura y correcta la eliminación, retiro, traslado o re-uso cuando ya no se requieran los activos.
- Mediante el procedimiento de copias de seguridad el cual determina la toma de backup de los activos evitando así el acceso o borrado no autorizado de la información, este procedimiento contiene las correspondientes autorizaciones y aplica tanto para medios removibles (todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores) como activos de procesamiento y/o almacenamiento de información.

11.6.2. Dispositivos móviles, teletrabajo o trabajo remoto.


- Todos los trabajadores, contratistas o terceros que tengan acceso a las redes inalámbricas deben cumplir con los lineamientos de control de acceso a la red contemplados en él; y que tengan acceso de la información propiedad de COMFIAR, tienen la obligación y responsabilidad de dar buen uso a la información cumpliendo con los controles de seguridad que protegen el buen uso de la tecnología y de la información así como como las revisiones de seguridad que la corporación utilice para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.
- Los dispositivos (hardware) que se quieran conectar a la red de Comfiar deberán ser autorizados por la Sección de Sistemas mediante el registro en la lista ARP tanto para redes físicas e inalámbricas
- Los usuarios logueados a las diferentes redes inalámbricas deberán permitir el acceso a su equipo para verificación de dirección física de la tarjeta de red "MAC", y se le asignará usuario y contraseña válida para única conexión y exclusiva para el equipo registrado cumpliendo los parámetros de gestión de contraseñas.
- Si el equipo de cómputo portátil se conectará por cable está sujeto a la misma revisión anteriormente descrita.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 35 DE 62

- Los computadores portátiles y/o dispositivos móviles de propiedad de los trabajadores no se incluirán en el dominio ccfcomfiar.local o cualquiera que funcione dentro de las instalaciones de COMFIAR sin antes cumplir con los lineamientos referentes a seguridad de la información.
- Para la modalidad teletrabajo en caso de que se llegue a dar, la Sección de Sistemas suministrará las herramientas tecnológicas (VPN, usuarios a plataformas, etc.) para acceder a la información, estableciendo las condiciones de seguridad y privacidad de la información, de acuerdo con la Resolución 2133 de 2018 y las enmarcadas en el Libro Blanco del Teletrabajo o cualquiera que la adicione, modifique o complemente.
- Para la modalidad de trabajo en casa o trabajo remoto la cual es improvisada por la circunstancia, se debe solicitar mediante la plataforma de mesa de ayuda GLPI, el acceso a las diferentes plataformas y conexiones remotas a la información, especificando las fechas en que se va a realizar las actividades de manera remota.
- La Sección de Sistemas debe realizar monitoreo sobre las conexiones y los servicios tecnológicos a las que el teletrabajador tiene acceso

11.6.3. Reglas para el uso del correo electrónico y de Internet


- Toda información, documentación o trámite electrónicamente que tiene como remitente u origen el nombre de la Caja de Compensación Familiar de Arauca Comfiar, se debe realizar por la cuenta de correo institucional que se le ha sido asignado a cada usuario, si este no tiene cuenta de correo institucional, es necesario diligenciar la solicitud a los administradores de las cuentas de correos, en este caso a la Sección de Sistemas, a través de su jefe inmediato por medio de la plataforma GLPI ya que la información es de interés único de la corporación, y toda información electrónica debe quedar como registro dentro del dominio [@comfiar.com.co](mailto:comfiar.com.co); así mismo el Colegio Comfiar con el dominio [@colegiocomfiar.edu.co](mailto:colegiocomfiar.edu.co) y el Instituto de Formación Empresarial y del Trabajo con el dominio [@ifet.edu.co](mailto:ifet.edu.co).
- El correo electrónico institucional es únicamente para el uso de trámites, contactos y demás diligencias a fines que cumplan con el objetivo principal que

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 36 DE 62

es el envío y recepción de información que involucre los procesos al cual hace parte el personal que esté laborado en la corporación. No se permite el uso para el envío o recepción de información personal, ni para la administración de cuentas de páginas de redes sociales diferentes a la de corporación y de otras características.

- Todo correo electrónico debe tener configurado una firma donde especifique el nombre del usuario quien se le asignó la cuenta de correo corporativo, el cargo, el número telefónico de la corporación con la extensión, número móvil en caso de tener, el número de la línea gratuita de atención al ciudadano, la dirección web de la corporación www.comfiar.com.co y el siguiente mensaje: *“La información contenida en este mensaje y sus anexos tiene carácter confidencial, y está dirigida únicamente al destinatario de la misma y sólo podrá ser usada por éste. Si el lector de este mensaje no es el destinatario del mismo, se le notifica que cualquier copia o distribución de éste se encuentra totalmente prohibida. Si usted ha recibido este mensaje por error, por favor notifique inmediatamente al remitente por este mismo medio y borre el mensaje de su sistema. Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinión oficial de la Caja de Compensación Familiar de Arauca COMFIAR.”*
- No está permitido usar plataformas de video conferencias (cuando el organizador crea una reunión en representación de la Corporación) por plataformas no licenciadas y que no está autorizadas por la Sección de Sistemas.
- Los contratistas y visitantes a la Corporación, deberán solicitar autorización a la Sección de Sistemas para poder tener acceso a los dispositivos o puntos de red o redes inalámbricas que prestan el servicio de internet, datos y demás sistemas de información el cual lo habilitará y restringirá su uso dependiendo del periodo que este vaya a durar en la entidad.

De acuerdo a las reglas anteriores los empleadores, contratistas y usuarios de tercera parte serán consientes de los límites que existen para el uso de la información, así como de los recursos, por esto son responsables del uso que

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 37 DE 62

hagan de los recursos de procesamiento de información y de cualquier uso efectivo bajo su responsabilidad.

11.7. Responsables de los activos


- Toda la información y los activos asociados con los servicios de procesamiento de información deberán ser del responsable al cual se le ha sido asignado.
- Este se le hará entrega mediante formato acta individual de recibido a satisfacción de computadores (FT-GD-10) y este se cargará en el inventario de activos en la Sección de Almacén y Compras.
- Los activos se asignan como herramienta de trabajo para el óptimo funcionamiento y desempeño de sus actividades laborales y/o procesos al cual pertenece y demás funciones que se encuentran en el manual de funciones.

El propietario del activo será responsable de:

- Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifiquen adecuadamente.
- Respetar continuamente las restricciones y clasificaciones del acceso.

Los activos se pueden delegar por ejemplo a un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del propietario.

- Si un funcionario de la Corporación necesita hacer uso de un activo fuera de las instalaciones donde está ubicado o asignado, es necesario solicitar a la Oficina de Almacén, dicha autorización la cual se realizará mediante el diligenciamiento del formato comprobante de Préstamo Interno o Externo de Bienes Inmuebles. Si este activo no es previamente autorizado por la Oficina de Almacén se puede clasificar como hurto, y estará expuesto a sanciones disciplinarias administrativas, civiles, penales y de ley.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 38 DE 62


Cuando el activo y/o información esté autorizado con el proceso anteriormente nombrado, se debe adoptar las medidas de seguridad apropiadas para la protección contra:

- Hurto por terceros
- El acceso por contraseña: esta debe únicamente ser conocida por el propietario del activo en la sesión habilitada para ese usuario

11.8. Control de acceso a equipos de cómputo, de comunicaciones y plataformas

11.8.1. Control de acceso con usuario y contraseña


- La Sección de Talento Humano, notifica a la Sección de Sistemas el ingreso de los colaboradores para que le sean creadas las credenciales de acceso a las plataformas GLPI y ORFEO; así mismo, cuando haya traslado para que le sea cambiado el perfil y/o dependencia; también cuando suspensión, vacaciones o terminación del contrato para que le sea suspendidos todas las credenciales de accesos a las plataformas que conforma la ERP y a la red y/o dominio.
- Los jefes inmediatos de los colaboradores contratados solicitan mediante la plataforma de mesa de ayuda GLPI, creación de las credenciales de registro a las diferentes plataformas que podrán acceder; así como a qué equipo de cómputo para acceder a la información y desarrollar sus funciones.
- Los usuarios y contraseñas son de uso personal e intransferibles; no se debe prestar ni compartir.
- Cada equipo de cómputo tiene dos inicios de sesión el cual uno pertenece a la sesión de Sistemas o de algún colaborador de la Sección de Sistemas que tienen todos los permisos de administrador el cual permita la instalación o desinstalación de hardware de ser necesario, y el otro usuario

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 39 DE 62

- pertenece al responsable del activo que tiene permisos de invitado, lo cual lo limita a realizar cualquier tipo de instalación y/o modificación de software.
- Cada usuario al que se le haya asignado credenciales de acceso (usuario y contraseña) para ingresar a un equipo de cómputo tiene carpeta acceso a una compartida en el servidor de datos que se encuentran en el dominio ccfcomfiar. local.
 - Si algún equipo de cómputo está afectando el óptimo rendimiento de la red, la Sección de Sistemas está en la facultad de desconectarlo y verificar en presencia del custodio del activo el problema o hecho presentado, con el fin de solucionar el inconveniente.
 - La Sección de Sistemas es la responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
 - La Sección de Sistemas es la responsable de difundir el reglamento para el buen uso de la red y procurar su cumplimiento.
 - Todo equipo de cómputo que esté o sea conectado a la red y que no sean propiedad de COMFIAR, debe tener licencia de sistema operativo y antivirus en caso de ser necesario (Sistema operativo Windows) y debe sujetarse a los procedimientos de acceso, restricciones y demás políticas de seguridad que emita le Sección de sistemas.
 - El acceso lógico a equipos especializados de cómputos (servidores, enrutadores, bases de daos, etc.) conectado a la red es administrado por la Sección de Sistemas.

11.8.2. Gestión de Contraseñas.

- El parámetro de contraseña debe contener como longitud mínima 8 caracteres, mínimo un número, una minúscula, una mayúscula, un símbolo.
- Para acceso a aplicaciones se adiciona un Captcha de seguridad.
- La contraseña de acceso a la sesión se configura para que tenga un ciclo de vida de 30 días; esto garantiza la protección del acceso de usuarios o terceros no autorizados.
- Se asigna una contraseña temporal al usuario para cuando realice su primer acceso, el sistema le solicite el cambio inmediato de la contraseña temporal cumpliendo con los parámetros de seguridad de contraseñas. Aplica para

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 40 DE 62


acceso al equipo de cómputo y para acceso a aplicaciones de ERP (Planificación de Recursos Empresariales) corporativo.

- Los manuales de configuración, contraseñas y documentación técnica los equipos de cómputo y servidores se manejará como documentos confidenciales, con acceso únicamente del personal autorizado para manipular esta información.

11.8.3. Control de acceso remoto.

- La Sección de Sistemas es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
- Los puertos de acceso remotos a los servidores y sistemas de información tanto por la Web (externos) como por la red interna de la Corporación, se encuentran bloqueados; únicamente se podrá acceder de manera presencial a estos servidores.
- Si se establece algún tipo de soporte o mantenimiento remoto con algún tipo de proveedor, se debe reprogramar el acceso remoto a los puertos de acceso, fecha, duración del soporte.
- La empresa encargada del soporte deberá sujetarse a las políticas de seguridad y en concordancia con los lineamientos generales de uso de la Internet.
- Para las conexiones remotas por medio del protocolo VPN se autoriza únicamente por medio de listas blancas de acceso (Ip's públicas y MAC negando el servicio a las que no se encuentren en ella, generando conexiones criptográficas cifradas para garantizar la disponibilidad, integridad y confidencialidad de la información.

11.8.4. Control de acceso a la Web

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 41 DE 62

- La Sección de Sistemas emite y socializa las políticas de privacidad y condiciones de navegación web, uso de la Internet, páginas institucionales y demás permitidas para el acceso seguro.
- Los accesos a las páginas web a través de los navegadores se sujetan a las normas que previamente se establecieron en la Sección de Sistemas la cuales están aprobadas por la alta dirección
- Se realizan seguimientos a las restricciones de navegación las cuales permiten el óptimo funcionamiento establecidas para cada funcionario.
- Toda página de navegación que no está permitida se niega el acceso.
- Toda información que se envíe vía Web y que tenga fines corporativos referentes a Comfiar, debe llevar como firma digital el nombre del propietario o administrador de la cuenta de correo, cargo, dirección, teléfono incluyendo la extensión, y el enunciado de confidencialidad de la Corporación.
- Toda aplicación Web corporativa cuenta con certificado SSL el cual permite la transferencia de datos cifrados entre un navegador y un servidor web.

11.9. Seguridad Física y del Entorno


11.9.1. Áreas seguras

Tiene como objetivo principal evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la Corporación.

Los servidores que prestan los diferentes servicios en la corporación están ubicados en la primera planta de la Sede Administrativa ubicada en la Calle 22 # 16-51.

Están aislados de todo contacto del personal no autorizado, daño e interferencia con cualquier otra señal que afecte el perfecto funcionamiento de los sistemas de información en el Data Center.

11.9.2. Perímetro de Seguridad Física

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 42 DE 62

- Se utiliza un perímetro de seguridad (paredes, puertas con llaves) que protegen el área que contiene los servidores (Data Center) con la información de la corporación.
- El Data Center cuenta con puerta contra incendios, termómetro para control de temperatura, iluminación de emergencia, cámara de seguridad, alarmas visuales y de ruido según con el código local de incendios.

11.9.3. Controles de acceso físico


- En las áreas tales como cuarto de servidores y planta eléctrica sólo se permite el acceso al personal autorizado.
- El personal autorizado debe contar con conocimientos e instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia.
- El cuarto de servidores tiene acceso controlado, únicamente tiene acceso el personal de la Sección de Sistemas,

Al personal del servicio de soporte de terceras partes se les da acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario; este acceso debe ser autorizado y monitoreado por la Sección de Sistemas

11.9.4. Seguridad de oficinas, recintos e instalaciones

- Se presenta como objetivo el diseño e implementación de seguridad física para oficinas, recintos e instalaciones, teniendo como base los reglamentos y las normas pertinentes a la seguridad y la salud.
- Las oficinas que no atienden al público (directamente), se les notifica por parte del personal de seguridad la solicitud de requerimiento para que éste




	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 43 DE 62

autorice el acceso a las instalaciones, teniendo en cuenta la utilización de alguna forma de identificación visible.

11.9.5. Acceso a áreas críticas.

- Se debe proteger la ubicación física de todo activo tecnológico y de información que permite brindar el óptimo rendimiento y funcionamiento de los sistemas de información.
- Los equipos de la corporación que sean de propósito específico y sirvan como herramienta para el desarrollo de las funciones, requiere estar ubicado en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales, alimentación eléctrica (protección con estabilizador o ups), y su acceso.
- El personal de la Sección de Sistemas y de la Sección de Almacén y Compras son los únicos facultados para adecuaciones físicas, reubicaciones y todo aquello que implique movimientos de equipos de cómputo.
- Las áreas donde se tienen equipos de cómputo como los equipos de las auxiliares de subsidio, auxiliar de aportes y atención al cliente, están sujetas a fácil vigilancia del personal de seguridad privada de COMFIAR y circuito cerrado de televisión CCTV.
- El acceso a servidores y al Data Center, es exclusivo del personal de la Sección de Sistemas. Si es necesario la instalación de algún equipo nuevo, mantenimiento, revisión, soporte técnico etc., éste se realiza bajo la supervisión y acompañamiento de cualquier colaborador de la Sección de Sistemas. Si es personal externo, se debe diligenciar el formato FT-GA-26 Registro Control De Acceso A Personal Externo Para Soporte Técnico.
- Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las directivas de la corporación

11.9.6. Protección Contra Amenazas Externas y Ambientales.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 44 DE 62


- Se tienen en cuenta todas las amenazas para la seguridad que presenta las instalaciones circundantes tales como: incendios, fuga de agua, atentados terroristas, explosiones, etc.
- Los materiales combustibles o peligrosos se almacenan a una distancia prudente del área de seguridad.
- Se cuenta con el suministro de equipo apropiado contra incendios (Extintores de los siguientes tipos: polvo químico seco ABC, dióxido de carbono, Solcaflan y de agua) y están ubicados adecuadamente según estudio.

11.9.7. Áreas de carga, despacho y acceso público


- Los puntos de acceso tales como las áreas de carga y despacho, y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se controlan y están aisladas externamente a las áreas de procesamiento de información, evitando así el acceso no autorizado.
- El personal de vigilancia privada contratado para la protección de todos los bienes de la Corporación, a manera de colaboración se encargan de guiar, asesorar a los visitantes a esta entidad, y los encargados de abrir y cerrar las puertas de acceso para la carga o descarga de los diferentes productos o activos que se utilizan en Comfiar.

11.9.8. Seguridad de los equipos

- Se evita pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de Comfiar
- Todos los equipos de cómputo (computadores de escritorio, portátiles, equipos de comunicaciones, servidores) de todas las sedes de la corporación, están protegidos contra amenazas físicas y ambientales. (Seguro Multi riesgo Empresarial)

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 45 DE 62


- Está prohibido ingerir alimentos, bebidas o fumar cerca de los equipos informáticos que se encuentran en operación que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterioro del mismo, en estos casos se informará a la oficina de la División Administrativa o Dirección Administrativa para que ésta determine las acciones a seguir o el remplazo del equipo. Se cuenta con avisos de advertencia ubicados en *cada área* específica.
- No está permitida la manipulación maliciosa de los recursos informáticos que puedan originar daños en los servidores, equipos pc, periféricos, equipos de comunicaciones, la estructura de red, las aplicaciones desarrolladas, la base de datos, el servicio de internet, el servicio de aula virtual, el servicio de correo electrónico y los servicios y/o recursos informáticos asociados.
- No está permitido imprimir trabajos personales sin autorización del jefe de la División Administrativa, empleando los recursos del área (papel, tóner, tinta, cinta) como lo contempla el Reglamento de Trabajo.
- No se deberá usar los recursos informáticos para acceso, descarga, transmisión, distribución almacenamiento de material: obsceno, ilegal, nocivo o que contenga derecho de autor, para fines ilegales.
- No está permitido el uso de los recursos informáticos para generar ganancias económicas personales o desarrollar actividades o labores de terceros. En el caso de los ambientes de aulas y auditorio queda bajo la responsabilidad del personal encargado velar por el cumplimiento de esta política.
- En las oficinas los equipos de cómputo, el software y aplicaciones instalados en ellos, son usados únicamente por el usuario asignado o por las personas designadas como responsables de dichos equipos (activos). En las aulas y auditorios tanto docentes como alumnos pueden hacer uso de los equipos y sistemas, pero bajo responsabilidad del propietario y respetando las políticas implementadas en este documento.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 46 DE 62

- No está permitido usar los equipos informáticos incluidas las impresoras de la corporación para fines que no sean académicos o propias de la labor del usuario.
- El uso de la sala de juntas como toda la parte tecnológica que allí se encuentra, es responsabilidad del usuario, contratistas, usuarios terceros que lo soliciten a la división Administrativa por medio de la plataforma de calendario de Sala de Juntas el cual se puede acceder por el portal de la intranet institucional. Dicha oficina es la encargada de realizar préstamo del sitio, y responsable de los activos correspondientes a esta sala.
- No está permitido el uso de los equipos informáticos, servicios y red de datos para propagar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva; esto deberá ser reportado por la Sección Sistemas al jefe de la División Administrativa para que inicie las acciones pertinentes.


11.9.9. Ubicación y protección de los equipos

- Los equipos están ubicados o protegidos en recintos cerrados para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado, exceptuando los equipos de afiliación en subsidio, atención aportes, y servicio al cliente, los cuales se encuentran a la vista del personal de vigilancia privada y las cámaras del circuito cerrado de televisión CCTV.
- Los equipos que requieren protección especial tales como servidores de datos, servidor CCTV, Firewall, Racks de datos, etc., están ubicados de forma tal que se minimice el riesgo de visualización de la información por personas no autorizadas durante su uso, y los sitios de almacenamiento se encuentran seguros evitando el acceso no autorizado.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 47 DE 62

11.9.9.1. Mantenimientos de equipos de cómputo.

- A la Sección de Sistemas corresponde la realización del mantenimiento preventivo y correctivo de los equipos de cómputo, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar.
- Todo mantenimiento de dispositivos de comunicación por parte de algún proveedor, personal externo o terceros, se debe verificar con la existencia de un contrato de soporte de mantenimiento, una solicitud, orden de servicio u autorización realizada a dicha entidad o actividad programada; se debe validar y tomar nota de los datos del personal técnico antes que se lleve a cabo la actividad, si éstos deben tener acceso al data center de la Sede Administrativa, se debe diligenciar el formato FT-GA-26 (Registro Control De Acceso A Personal Externo Para Soporte Técnico).
- Los equipos deben recibir mantenimiento adecuado para asegurar su continua funcionalidad, disponibilidad e integridad.
- El mantenimiento preventivo de los equipos de cómputo se realiza según lo programado mediante el diligenciamiento del formato FT-GA-08 (CRONOGRAMA MANTENIMIENTO PREVENTIVO EQUIPOS DE CÓMPUTO Y/O PERIFÉRICOS).
 - Sólo el personal de la Sección de Sistemas está autorizado para realizar los mantenimientos de los equipos de cómputo; cuando un equipo de cómputo se encuentra en garantía el mantenimiento es realizado por el respectivo proveedor.
 - Se debe realizar una apertura de ticket para soporte técnico mediante la plataforma de mesa de ayuda GLPI como lo indica el procedimiento PR-GA-03 ASISTENCIA TÉCNICA Y OPERATIVA A EQUIPOS DE CÓMPUTO, APLICATIVOS Y/O PERIFÉRICOS Y MANTENIMIENTO A LOCATIVOS
 - No es permitido al personal de la Sección de Sistemas realizar cualquier tipo de mantenimiento, manipulación de equipos de cómputo o de


	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 48 DE 62

telecomunicaciones que no sea propiedad de Comfiar; excepto aquellos que estén autorizados mediante un convenio o contrato.

11.9.10. Seguridad de cableado

- El tendido de cableado de datos cumple con las normas de cableado estructurado según los organismos ANSI/TIA/EIA/IEEE, el cual nos permite interconectar equipos activos, de diferente o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc, cumpliendo el objetivo fundamental que es brindar los diferentes servicios y cubrir las necesidades de los usuarios durante la vida útil de las instalaciones sin necesidad de realizar más tendido de cables.
- El cableado de red está protegido contra interceptaciones no autorizadas o daño, por medio de conductos evitando rutas a través de áreas públicas.
- Los cables de datos están debidamente etiquetados según norma ANSI/TIA/EIA-606A
- Antes de entrar al etiquetado es necesario saber los componentes de comunicaciones.

Componentes de Comunicaciones		
Componente	Símbolo	Ubicación
Gabinete 1	GAB1	Primer Piso
Gabinete 2	GAB2	Primer Piso
Gabinete 3	GAB3	Segundo Piso
Switch 1	SW1	Primer Piso
Switch 2	SW2	Primer Piso


	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 49 DE 62

Switch 3	SW3	Segundo Piso
Switch 4	SW4	Segundo Piso
Patch Panel 1	PP1	Primer Piso
Patch Panel 2	PP2	Primer Piso
Patch Panel 3	PP3	Segundo Piso
Patch Panel 4	PP4	Segundo Piso
Datos	Dxx	Todos los Pisos
Voz	Vxx	Todos los Pisos
Video	VCxx	Todos los Pisos
Face Plate	FP	Todos los Pisos

- PP3-D01-OFA: Este cable indicaría que está tendido desde la OFICINA A y que ese cable es de DATOS con número consecutivo 01 y el otro extremo está en el PATCH PANEL 3 y detrás del Patch Panel va marcado de la siguiente manera: OFA-D01-PP3
 - OFx = Letra que representa a una oficina
 - Dx, Vx, VCx = Tipo de servicio Datos, Voz o Video y el número de la conexión (x)
 - PP3: El tipo de elemento al cual está conectado

Los cables de energía están separados de los cables de comunicaciones para evitar interferencias.



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 50 DE 62

- Las líneas de energía cumplen con el Reglamento Técnico de Instalaciones Eléctricas (RETIE) que fija las condiciones técnicas que garantizan la seguridad en los procesos de Generación, Trasmisión, Transformación, Distribución y Utilización de energía eléctrica en Colombia y asegura la calidad de las instalaciones y productos que las empresas utilizan para la correcta prestación de los servicios eléctricos.


Cumple con los requerimientos para la instalaciones de sistemas puesta a tierra (SPT) de telecomunicaciones ANSI/TIA/EIA-607, la cual es especifica cómo se debe hacer la conexión del sistema de tierras confiable

- Los gabinetes y los protectores de voltaje son conectados a una barra de cobre (busbar) con “agujeros”. Estas barras se conectan al sistema de tierras (grounding backbone) mediante un cable de cobre cubierto con material aislante (mínimo número 6 AWG, de color verde. Este backbone estará conectado a la barra principal del sistema de telecomunicaciones en la acometida del sistema de telecomunicaciones.

11.10. Gestión de Software

11.10.1. Adquisición de Software

- La Sección de Sistemas es la encargada de presupuestar anualmente la renovación y adquisición de programas como sistemas operativos, antivirus, etc. con sus respectivas licencias, en caso de que los programas no sean Open-Source.
- La Sección de Sistemas es la encargada de instalar y en caso de que sea necesario distribuir los instaladores y licencias de los diferentes programas adquiridos para la Corporación.
- La Sección de Sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
- La Sección de Sistemas es la encargada de realizar mantenimiento preventivo y/o correctivo al software instalado en los equipos de cómputo de la Corporación.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 51 DE 62


- Cuando se adquiere nuevos sistemas de información se tiene en cuenta lo recibido cumpla con lo ofertado; cada proceso y/o reporte y en caso de tener la aprobación de otra área, ésta se incluye para determinar si cumple con el objeto de la compra.

11.10.2. Instalación del Software

- Corresponde únicamente a la Sección de Sistemas instalar software de cualquier aplicación, sistema operativo, o programas en cualquier equipo de la Corporación.
- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado, adquirido por compra y/o OpenSource.
- El personal de la Sección de Sistemas son los únicos autorizados para la instalación, desinstalación de cualquier software, firmware o actualización en los equipos de cómputo y de comunicaciones lo cuales deben ser licenciados o con licenciamiento libre (OpenSource).
- La Sección de Sistemas es la responsable de brindar asesoría y supervisión para la instalación de software informático.
- La instalación de software que desde el punto de vista pueda poner en riesgo los recursos informáticos o activos de corporación no está permitida.
- La protección lógica de los sistemas corresponde a quienes en un principio se les fue asignado y les compete notificar cualquier anomalía a la Sección de Sistemas.

11.10.3. Actualización de Software

- La adquisición y actualización de software para cada equipo de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con las fechas de vencimientos de licencias o renovaciones de software.
- Corresponde a la Dirección Administrativa autorizar cualquier adquisición y actualización del software, con el visto bueno de la Sección de Sistemas, de lo

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 52 DE 62

contrario esta Sección no se hará responsable de adquisiciones en cuanto a su calidad y buen funcionamiento.


11.10.4. Auditoria de Software instalado

- La Sección de Sistemas es el responsable de realizar revisiones periódicas para asegurarse que sólo software con licencia paga por Comfiar esté instalada en los equipos de cómputo.
- En caso de que haya algún tipo de violación por contraseña y se encuentre instalado algún tipo de software no autorizado, se debe generar un reporte a la Dirección Administrativa para que tome acciones al respecto.

11.10.5. Software e información propiedad de COMFIAR

- Todo software, licencias, bases de datos y lo referente a programación adquirida por la Corporación sea por compra, donación o cesión es propiedad de COMFIAR, y mantendrá los derechos que la ley de propiedad y privacidad los permita.
- Las bases de datos propias de COMFIAR, no son de uso comercial, cualquier difusión de estas no autorizada, tendrá sanciones disciplinarias y legales de acuerdo con lo permitido por la ley para la protección de la información y de los datos, ya que, va en contra del patrimonio de la Corporación y la Ley Estatutaria 1581 de 2012, Ley de Habeas Data.
- Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces, aplicativo SYS) desarrollados o adquiridos con o a través de los recursos de la Corporación, se mantendrán como propiedad de COMFIAR respetando la propiedad intelectual del mismo.
- Cada funcionario tiene la responsabilidad de mantener asegurado y respaldada la información interna de la Corporación, para ello debe realizar copia a la unidad D.
- Los datos, bases de datos, y la información generada por el personal y los recursos informáticos de la Corporación están asegurados con copias de seguridad almacenados en un servidor local y otro en la nube.



	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 53 DE 62

- Corresponde a la Sección de Sistemas difundir y promover los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos, como el periodo que se deben realizar.

11.10.6. Supervisión y evaluación.

- Cada equipo de cómputo que esté en riesgo la seguridad u operatividad, los usuarios custodios de estos activos deberán comunicar en el menor tiempo posible a la Sección de Sistemas para que actúen y tomen acciones preventivas o correctivas para el bien de estos activos y la información.
- Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física, es coordinada con la Sección de Sistemas para que no afecte la operación ni la seguridad de la empresa.
- Para efectos de seguridad de la red, se realiza monitoreo constante sobre todos y cada uno de los servicios que disponga en ese momento Comfiar.
- Los sistemas considerados críticos, están bajo monitoreo permanente.

11.11. Gestión de Comunicaciones y Operaciones.


Asegurar la operación correcta y segura de los servicios de procesamiento de información.

11.11.1. Respaldo

Se mantiene la integridad y disponibilidad de la información y los servicios de procesamiento de información.

11.11.2. Respaldo de la Información.

Se realizan diariamente copias de respaldo de la información y de software.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 54 DE 62

- Se tiene servidor de copias de seguridad (Backup) local, donde se guarda toda la información que es generada por los trabajadores (ofimáticos y otros) y las fuentes y datos de las diferentes plataformas que tiene Comfiar en propiedad y o terceros.
- Se tiene servicio en la Nube donde se envían en manera inmediata las copias generadas en el servidor local de Copias de Seguridad.

Las copias de seguridad tendrán como consideración los siguientes lineamientos:


- El respaldo de los datos del aplicativo interno de la Caja, se realiza diariamente de la base datos y cada viernes de las fuentes del software.
- Se Clasificó y definió los niveles necesarios para la información de respaldo. Con excepción a los funcionarios de recreación y deportes, publicidad y mercadeo, eventos y programas especiales, ningún otro funcionario tendrá derecho a realizar el respaldo de imágenes, música y videos (contenido multimedia), el restante de funcionarios solamente se les salvaguardará archivos tales como documentos con extensiones (doc, docx, docm, txt, pdf, ppt, pptx, ppsx, sldx, xls, xlsx, csv).
- No se debe guardar respaldo de archivos personales (información concerniente a personas físicas identificadas o identificables).

Se usará el siguiente método de copias de seguridad:

- Se crea una carpeta individual de cada usuario dentro otra carpeta de la Gerencia o Sección al cual haga parte el usuario; así mismo, se crea una carpeta compartida en el grupo de trabajo al cual pertenece dicho trabajador. A estas carpetas se realiza copia de seguridad en la nube de manera inmediata en el momento en que haya una modificación.

11.12. Gestión de la seguridad de las redes

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 55 DE 62

11.12.1. Controles de las redes


- Las redes se mantienen y controlan adecuadamente para protección de las amenazas, manteniendo la seguridad de los sistemas y aplicaciones que se utilizan en esta red.
- Para el soporte remoto que se brinda a los usuarios de otras sedes, este se hace con previo aviso para que los usuarios a los cuales se esté brindado dicho soporte, autoricen la conexión remota y tenga conocimiento del soporte que se está realizando.
- Para los soportes remotos hechos hacia la corporación, también es necesaria la autorización, la cual se define el tipo de soporte y el tiempo en que se llevará a cabo.
- Las redes físicas se deben cambiar en un periodo de uso de 10 años, ya que es la vida útil de dicho material para el óptimo rendimiento de la red, y se debe realizar mantenimiento cada vez que se requiera o se detecte alguna falla de conexión o si en su defecto se requiera cambio físico de la misma

11.13. Control De Acceso.

11.13.1. Requisitos de la Corporación para el control de acceso

El acceso a la información, a los servicios de procesamiento de información se debe controlar con base en los requisitos de seguridad y de la empresa.

Las reglas para el control del acceso tienen en cuenta las políticas de distribución y autorización de la información.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 56 DE 62


11.13.2. Control de acceso

Las políticas de navegación web tienen como objetivo salvaguardar la información y todo sistema de información que pueda atentar con el óptimo funcionamiento del mismo el mal uso de los recursos informáticos y servicios.

La sección de sistemas controla el acceso a Internet mediante el uso "listas negras" y "listas blancas" para bloquear o permitir el acceso a sitios determinados; aplicando una serie de reglas (Calidad de Servicio - QoS) dando prioridades a diferentes tipos de contenidos que hagan del este servicio, un servicio óptimo e ideal para el buen funcionamiento de las funciones de cada uno de los usuarios y que garanticen la seguridad y fomentan uso responsable por parte de los empleados.

Los perfiles son determinados de acuerdo el nivel jerárquico de los funcionarios de la Comfiar, clasificándose de la siguiente manera:

- **Jefes de División y asesores:** Se adoptan para este grupo la regla general de bloqueo y el contenido streaming exceptuando el acceso a YouTube, permitiendo la consulta o navegación de cualquier otro contenido y aplicaciones internas de la corporación, también se incluye a este grupo el perfil del contador.
- **Jefes de Sección y auxiliares:** Se adopta para este grupo la regla general de bloqueo y contenido streaming los cuales no tienen acceso a los sitios de redes sociales (chat, facebook, msn, entre otros), vídeo, sitios online. permitiendo la consulta o navegación de cualquier otro contenido y aplicaciones internas de la corporación
- **Administradores de redes sociales:** Es el caso de la sección de comunicaciones, y áreas como instituto de formación empresarial, que administran perfiles de redes sociales se activara el acceso a dichas redes en horarios específicos para poder alimentar y tener actualizadas estas cuentas.

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 57 DE 62

- **Especiales:** A este grupo pertenece la sección de comunicaciones, recreación y deportes ya que por sus funciones necesitan de estos contenidos online tales como YouTube, emisoras radiales, según requerimiento directo a la sección de sistemas.

11.13.3. Control de acceso al sistema operativo


Objetivo: evitar el acceso no autorizado a los sistemas operativos para asegurar que no se realicen cambios que interfieran en el buen funcionamiento de estos.

En las estaciones de trabajo de los funcionarios de la Corporación (PC's) están habilitados dos usuarios de sesión. La primera sesión es sistemas, la cual tiene permisos de administrador y sólo tiene ingreso los funcionarios de la Sección de Sistemas, en esta sesión se es permitido realizar cualquier tipo de instalaciones de programas o software no licenciado o corrupto.

El otro usuario con permisos de invitado "**USUARIO STANDAR**" es donde los funcionarios de la entidad tienen su información y a la vez es la sesión de trabajo la cual debe tener protección por contraseña para salvaguardar sus datos.

11.13.4. Procedimientos de ingreso seguros

- El acceso a los sistemas operativos se controla mediante un procedimiento de registro de usuarios y contraseñas de inicio seguro asignadas individualmente a los funcionarios a los cuales pertenece la estación de trabajo.
- Este procedimiento de registro en el sistema operativo está diseñado para minimizar la oportunidad de acceso no autorizado.
- El procedimiento de registro de inicio cumple con los siguientes aspectos:

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 58 DE 62

- No se suministra mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.
- Si se presenta una condición de error al ingresar la contraseña de un usuario, el sistema no indica que parte de los datos es correcta o no.
- No se muestra la contraseña que se introduce, los caracteres se cifran mediante puntos.


11.13.5. Identificación y autenticación de usuarios

Todos los usuarios tienen un identificador único (ID del usuario) para su uso personal, ya sea para el ingreso al módulo interno de la corporación, sistema de gestión documental, plataforma mesa de ayuda GLPI, internet, entre otros.

12. COMPROMISO DE LA DIRECCIÓN.

- La Dirección Administrativa acepta la Política de Seguridad y Privacidad de la información; así como la implementación, operación, seguimiento, revisión, mantenimiento y mejora.
- Establecer funciones y responsabilidades de la Seguridad de la Información.
- Hacer cumplir con los planes de capacitación y/o divulgación de la Política de Seguridad y Privacidad de la Información.
- Brindar los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisión, mantener y mejorar la Política de Seguridad y Privacidad de la Información.




	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 59 DE 62

- Asegurar la realización de auditorías internas a la Política de Seguridad y Privacidad de la Información.
- Revisar la eficacia de la implementación de la Política de Seguridad y Privacidad de la Información.

13. SANCIONES PREVISTAS POR EL INCUMPLIMIENTO

- Cualquier violación o incumplimiento a la Política de Seguridad de la Información, traerá consigo, sanciones legales de acuerdo con el reglamento interno de COMFIAR y el código penal en los artículos que refiere a la protección de la información y de los datos.
- Las sanciones pueden ser desde una llamada de atención al empleado hasta la suspensión del servicio dependiendo de la gravedad de la falta que esta manifiesta.
- Cualquier acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso o no autorizado, violación de datos personales y corporativos, suplantación de sitio web para capturar datos personales, violación a las políticas de seguridad de la información, políticas de privacidad y condicione de navegación web, hurto por medios informáticos semejantes, transferencia no consentida de activos y demás delitos informáticos, puede ser sancionado de acuerdo al reglamento interno y código penal

14. RECOMENDACIONES

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 60 DE 62

El Sistema de Gestión de Seguridad de la Información SGSI deberá seguir un proceso de actualización periódica, sujeta a los cambios organizacionales relevantes; crecimiento de la planta de personal, cambio de infraestructura computacional, implementación de nuevas tecnologías y servicios, etc.

Este documento debe ser difundido a todo el personal de COMFIAR.

15. ANEXOS

➤ Anexo 1 – Análisis Gap




AnalisisGap.xlsx

➤ Anexo 2 – Matriz de riesgos



MatrizDeRiesgos20
21.xls

VERSIÓN	FECHA APROBACIÓN	PAGINA(S)	NUMERAL(ES)	CAMBIO
Versión 02	07 Diciembre de 2017	16	4.1.2	En las áreas tales como cuarto de servidores y planta eléctrica sólo se permite el

	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI DE COMFIAR	CODIGO: ML-GA-01
		VERSION: 03
		FECHA: 14 de junio de 2022
		PÁGINA 62 DE 62

		19	4.2.1	se actualiza la palabra ventanilla de la sección de subsidio y equipo de atención al cliente
		22	4.2.2	Se incluyó nombre del formato y nombramiento del procedimiento pr-ga-03
		23	4.2.5	Se actualiza debido que algunos formatos de Almacén fueron eliminados.
		24	4.2.7	Se elimina párrafo debido a la eliminación de formato Alm-01 y Alm-02.
		24	5.1.1	Se actualiza la manera de realizar las copias de seguridad.