



Política Corporativa de Seguridad de la Información y Ciberseguridad

Aprobó: Gerente Representante Legal	Revisó: Asesora de Sistema	Elaboró: Colaborador de Infraestructura	Fecha 13/10/2022
			Pág. de 1 a la 6

Contenido

1. Objetivo
2. Alcance y Ámbito de Aplicación
3. Definiciones
4. Declaración
5. Objetivo de Seguridad de la Información
6. Políticas Seguridad de la Información
7. Referencias

1. Objetivo

En cumplimiento de la Ley 1581 de 2012. Artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015. Sociedad **CIFEL**, como entidad responsable. Establece una política corporativa de seguridad de la información que refleje los objetivos de negocio.

2. Alcance y Ámbito de Aplicación

La Política de Seguridad y Privacidad de la Información y Seguridad Digital y sus lineamientos, aplican a toda la empresa cuando se recolecte, procese, almacene, recupere, intercambie, consulte información y demás, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

3. Declaración

Con el fin de prevenir incidentes tanto accidentales como intencionados e implementar controles y medidas asociadas con las personas, los procesos y la tecnología, se establece una política corporativa de seguridad de la información que refleja los objetivos del negocio cumpliendo con los de requisitos legales, regulatorios y/o contractuales que deben cumplirse.

4. Objetivo de Seguridad de la Información

Con el fin de dar cumplimiento al marco normativo y regulatorio, se describen los objetivos del sistema de gestión corporativo de seguridad de la información:

- Gestionar los riesgos de seguridad y privacidad de la información y seguridad digital.
- Mitigar los Incidentes de seguridad y privacidad de la información y seguridad digital.
- Fomentar una Cultura de seguridad y privacidad de la información y seguridad digital, para que todos los Colaboradores tomen conciencia de sus deberes y responsabilidades frente al SGSI.

- Establecer las directrices y lineamientos requeridos para proteger la información y los sistemas de información ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de esta.
- La Información es uno de los activos más importantes y por tanto será utilizada conforme con los procesos del negocio, condiciones y regulaciones.
- La confidencialidad de la Información será mantenida, sin importar su medio, forma, sea física o digital o su estado, almacenada o en tránsito.
- Cumplir con los requisitos de seguridad de la información y ciberseguridad definidos por CIFEL y/o establecidos por la legislación y regulación vigente.
- La privacidad de la Información de CIFEL, de sus usuarios, proveedores y colaboradores será preservada.

5. Política de Seguridad de la Información

CIFEL establece la política general de Seguridad y Privacidad de la Información y seguridad digital mediante lineamientos que permiten cumplir con una cultura de seguridad de la Información, con el objetivo de prevenir incidentes a través de la Gestión de Riesgos, frente a las amenazas internas o externas, deliberadas o accidentales, que garanticen y preserven la confidencialidad, integridad y disponibilidad de la información, de todos los funcionarios, usuarios y grupos de interés de CIFEL, con el fin de prestar servicios con calidad y recurso humano comprometido con toda su población objetivo.

CIFEL, en desarrollo de sus actividades y en cumplimiento del marco normativo y regulatorio,

- Desarrolla e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad, que esté alineado con la estrategia corporativa y los objetivos del negocio.
- Diseña, implementa, gestiona y controla lo relacionado con el inventario, uso razonable, clasificación y manejo de soportes para activos de información que hacen parte del sistema de gestión de seguridad de la información.
- Define los lineamientos para garantizar la seguridad de las operaciones, protección contra código malicioso, copias de respaldo, sistemas operativos, y vulnerabilidades técnicas de sistemas de información.
- Establece protocolos para prevenir, gestionar y dar respuesta de incidentes de Seguridad de la Información y Ciberseguridad de forma oportuna.

6. Glosario

- Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.
- Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.
- Seguridad de la Información: es el conjunto de medidas que tienen como fin proteger y mantener los principios de confidencialidad, integridad y disponibilidad de los Activos de Información.
- Confidencialidad: Asegura que sólo quienes estén autorizados puedan acceder a la Información.
- Integridad: Asegura que la Información y sus métodos de proceso sean exactos y completos.
- Disponibilidad: asegura que los usuarios autorizados tengan acceso a la Información cuando lo requieran.
- Control de accesos: Proceso mediante el cual se permite o no el acceso de un usuario a aplicaciones, servidores, equipos tecnológicos entre otros, según los perfiles asignados.

7. Referencias

Diccionario Definiciones de Oxford Languages. Ministerio de Salud.

Instituto Nacional de Salud.

Políticas Seguridad de la Información www.finagro.com.co

Políticas Seguridad de la Información www.epssanitas.com

CONTROL DE CAMBIOS				
No.	Descripción del cambio	Fecha de cambio	Quien aprueba el cambio	Versión anterior
1	Creación	2022		N/A
2				