POLÍTICA DE SEGURIDAD INFORMÁTICA

CONTROL DOCUMENTAL		
Realizado por:	**Cargo**	**Fecha**
Andrés Gutiérrez	Ingeniero en Analítica de datos	20-09-2024
Aprobado por:	**Cargo**	**Fecha**
David Correa	Gerente General	

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**CAMBIO**	**REALIZADO POR**
1.0	20-09-2024	Creación de documento	Andrés Gutiérrez

CONTENIDO

1. Objetivo

El objetivo de esta política es garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por COMFICA Colombia, protegiéndola de amenazas internas y externas. Esta política también asegura el cumplimiento de las políticas y procedimientos relacionados con la seguridad de la información, como se describe en los documentos referenciados.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas y terceros que tengan acceso a los sistemas de información y datos de COMFICA Colombia. Se deben cumplir todas las políticas relacionadas con el uso de recursos tecnológicos, tales como la **Política de uso aceptable y dispositivos móviles (SGSI-PR-06).**

3. Principios de seguridad de la información

Las auditorías internas se realizarán al menos una vez al año, o cuando se considere necesario, en función de cambios importantes en el sistema o incidentes relacionados con la seguridad de la información.

3.1 Confidencialidad:

Hay que asegurar que la información sea accesible solo a quienes están autorizados, en línea con la **Política de gestión y acceso a la información (SGSI-PR-05).**

3.2 Integridad:

Mantener la exactitud y completitud de la información y de los métodos de procesamiento, cumpliendo con las medidas establecidas en los procedimientos de Gestión de Cambios.

3.3 Disponibilidad:

Asegurar que los usuarios autorizados tengan acceso a la información y a los activos cuando lo requieran, conforme al **Plan de continuidad de negocio (SGSI-PR-14).**

4. Gestión de riesgos

- Se llevará a cabo una evaluación periódica de riesgos, conforme al **Procedimiento de Análisis de Riesgos TIC (SGSI-PR-14),** para identificar y mitigar posibles amenazas que puedan comprometer la seguridad de la información.
- Las medidas de seguridad se ajustarán según el nivel de riesgo y la criticidad de los activos.
- Se implementarán controles de seguridad basados en los resultados de la evaluación de riesgos, en las políticas y procedimientos pertinentes.

5. Control de acceso

- El acceso a los sistemas y datos estará basado en el principio de mínimo privilegio, donde cada colaborador solo tendrá acceso a la información necesaria para el desempeño de su trabajo, conforme a la **Política de gestión y acceso a la información (SGSI-PR-05).**
- El acceso a los sistemas críticos deberá seguir los lineamientos del **Procedimiento de uso, creación y gestión de accesos (SGSI-PR-10).**
- Los usuarios deben autenticarse mediante credenciales seguras, y se revisarán periódicamente conforme a las políticas establecidas.

6. Protección de los activos de información

- Se mantendrá un inventario de activos, que incluya hardware, software y datos críticos.
- Los sistemas deberán ser protegidos contra accesos no autorizados mediante firewalls, antivirus y otros sistemas de seguridad definidos en la Política de uso aceptable y dispositivos móviles.
- Las copias de seguridad (backups) deben realizarse periódicamente y almacenarse en lugares seguros, tanto locales como en la nube, conforme al **Procedimiento de respuesta ante incidentes (SGSI-PR-10).**

7. Gestión de incidentes de seguridad

- Se implementa un Procedimiento de Respuesta a Incidentes, que incluirá la detección, notificación, análisis, contención y recuperación de incidentes de seguridad, alineado con el Procedimiento de Auditorías Internas.
- Todos los incidentes deben ser reportados inmediatamente al área de TI.

8. Cumplimiento legal y normativo

- COMFICA Colombia se compromete a cumplir con las normativas locales e internacionales relacionadas con la seguridad de la información y la protección de datos personales.
- El tratamiento de los datos personales y otros datos sensibles debe cumplir con la **política de protección de datos personales (SGSI-PR-06).** y **la política de tratamiento de la información (SGSI-PR-01).**

9. Concientización y capacitación

- Todo el personal de COMFICA Colombia deberá recibir formación continua en materia de seguridad informática y protección de la información, conforme al **política de capacitación y gestión de terceras partes (SGSI-PR-04).**
- Los colaboradores serán responsables de seguir las políticas y procedimientos establecidos para la seguridad de la información.

10. Auditorias y mejora continua

- Se realizarán auditorías internas periódicas para garantizar el cumplimiento de esta política y de los procedimientos asociados, conforme al **Procedimiento de Auditorías Internas (SGSI-PR-08).**
- Los resultados de las auditorías serán evaluados y se tomarán las medidas correctivas necesarias para la mejora continua.

11. Revisión y actualización

- Esta política será revisada al menos una vez al año, o cuando haya cambios significativos en los sistemas o regulaciones, para garantizar su vigencia y adecuación a las necesidades de COMFICA Colombia.

12. Responsabilidades

- **Gerente General:** Responsable de la supervisión y aprobación de esta política y de asegurar que la empresa cumpla con las normativas de seguridad de la información.
- **Área de TI:** Responsable de la implementación y mantenimiento de los controles de seguridad informática, según el Procedimiento de Seguridad Física y el Procedimiento de Respuesta a Incidentes. También de la recuperación técnica de la información ante incidentes.
- **Gerentes de Área:** Responsables de asegurar que la información dentro de su área esté protegida y gestionada conforme a esta política y los procedimientos relacionados.
- **Coordinadores y Supervisores:** Responsables de la comunicación y ejecución de medidas de seguridad en sus respectivas áreas.
- **Todos los colaboradores:** Responsables de cumplir con las políticas y procedimientos de seguridad de la información.