POLÍTICA DE CAPACITACIÓN Y GESTIÓN DE TERCERAS PARTES

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 propósito de esta política es garantizar que los colaboradores de COMFICA cuenten con la capacitación adecuada y actualizada en seguridad informática, así como establecer los lineamientos para la selección, contratación y monitoreo de terceros que tengan acceso a los activos de información de la empresa.

2. Alcance

Esta política es aplicable a todos los colaboradores, contratistas y terceros que interactúan con los sistemas de información de COMFICA, incluyendo personal temporal y proveedores que accedan a los activos de información de la empresa.

3. Capacitación en seguridad informática

3.1 Objetivo de la capacitación

El objetivo de la capacitación es proporcionar a los colaboradores los conocimientos y habilidades necesarios para:

- Comprender y aplicar las políticas de seguridad de la información de COMFICA.
- Identificar, prevenir y reaccionar ante amenazas de seguridad informática.
- Fomentar una cultura de seguridad dentro de la empresa.

3.2 Frecuencia y modalidad

- **Frecuencia:** Se realizarán capacitaciones al menos una vez al año para todo el personal, cada vez que ingrese un colaborador o cada vez que haya una actualización significativa en las políticas de seguridad de la empresa.
- **Modalidad:** Las capacitaciones podrán realizarse de manera presencial o en línea, dependiendo de las necesidades y disponibilidad del personal.

3.3 Contenido de las capacitaciones

El contenido debe incluir, pero no se limitará a:

- Políticas de seguridad informática de COMFICA (uso aceptable, clasificación de la información, uso de dispositivos móviles, etc.).
- Procedimientos de respuesta ante incidentes de seguridad.
- Buenas prácticas para el manejo seguro de contraseñas y autenticación.
- Identificación de correos electrónicos de phishing y otras formas de ciberataques.
- Uso seguro de redes sociales y gestión de la privacidad en entornos digitales.

3.4 Evaluación

Al final de cada capacitación, se realizará una evaluación para medir la comprensión de los conceptos presentados. Esta evaluación será utilizada para determinar la efectividad de la formación y detectar posibles áreas de mejora.

4. Gestión de terceras partes

4.1 Selección de Terceras Partes

COMFICA seleccionará cuidadosamente a los terceros que tengan acceso a la información sensible o sistemas de la empresa. Los criterios de selección incluirán:

- Evaluación de la capacidad del proveedor para cumplir con las normativas de seguridad informática.
- Revisión de políticas y procedimientos de seguridad implementados por el tercero.
- Verificación de antecedentes y reputación del proveedor.

4.2 Contratos y Acuerdos

Todo tercero que tenga acceso a la información de COMFICA deberá firmar acuerdos de confidencialidad y cumplir con las políticas de seguridad de la información. Los contratos deben especificar:

- Las responsabilidades del tercero respecto a la protección de la información.
- Los protocolos de respuesta ante incidentes de seguridad.
- Los derechos de COMFICA para auditar al proveedor en caso de incumplimiento de las políticas de seguridad.
- Las sanciones por incumplimiento.

4.3 Monitoreo de Terceras Partes

El acceso y las actividades de los terceros serán monitoreados de forma continua para garantizar el cumplimiento de las políticas de seguridad. Esto incluirá:

- Auditorías periódicas a los procesos y medidas de seguridad de los terceros.
- Revisión de los registros de acceso y actividades en los sistemas de COMFICA.
- Evaluación del desempeño de los proveedores en la protección de la información de la empresa.

4.4 Revisión de contratos

Los contratos con terceros serán revisados periódicamente para asegurar que continúan cumpliendo con las normativas de seguridad y los objetivos de COMFICA en términos de protección de la información.

5. Responsabilidades

5.1 Área de recursos humanos

- Coordina las capacitaciones de seguridad informática para todo el personal.
- Registra la participación y los resultados de las evaluaciones de los colaboradores.

5.2 Área de TI

- Proporciona el contenido técnico de las capacitaciones en seguridad informática.
- Monitorea y audita el acceso de terceros a los sistemas de COMFICA.
- Evalúa el desempeño de los terceros en materia de seguridad.

- Realiza las capacitaciones.

5.3 Gerentes o líderes de área

- Aseguran que su personal participe en las capacitaciones de seguridad informática.
- Supervisan el cumplimiento de las políticas de seguridad por parte de los terceros con los que interactúan.

6. Sanciones

El incumplimiento de esta política, tanto por parte de los colaboradores como de terceros, puede resultar en sanciones que incluyen:

- La suspensión de accesos a sistemas o información de COMFICA.
- Medidas disciplinarias, incluyendo el despido en casos graves.
- Terminación de contratos y acciones legales contra terceros que no cumplan con los acuerdos de seguridad.

7. Revisión y actualización

Esta política será revisada al menos una vez al año o en caso de cambios importantes en las operaciones de COMFICA que afecten la seguridad de la información o la relación con terceros.