POLÍTICA DE GESTIÓN Y ACCESO A LA INFORMACIÓN

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

Esta política tiene como objetivo establecer los lineamientos para la gestión adecuada y el acceso controlado a la información de COMFICA, garantizando su confidencialidad, integridad y disponibilidad, así como el cumplimiento de las normativas vigentes en materia de protección de datos.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas y terceros que tengan acceso a la información de COMFICA, independientemente de su formato (digital o físico) o ubicación (local o remota).

3. Principios de gestión de la información

3.1 Clasificación de la información

Toda la información manejada por COMFICA debe ser clasificada de acuerdo con su nivel de sensibilidad y riesgo. Las categorías de clasificación son:

- **Información Pública:** Puede ser accesible por cualquier persona, sin restricciones.
- **Información Interna:** Información cuyo acceso está limitado a colaboradores autorizados de COMFICA.
- **Información Confidencial:** Datos críticos para la operación y cuyo acceso está restringido a un grupo específico de colaboradores.
- **Información Sensible:** Información que, de ser divulgada o accedida sin autorización, puede causar daños significativos a la empresa o sus clientes.

3.2 Ciclo de vida de la información

La información debe gestionarse a lo largo de su ciclo de vida, que incluye:

- **Creación:** Identificación y clasificación de la información.
- **Almacenamiento:** Protección física y digital de la información según su clasificación.
- **Acceso:** Control de acceso basado en la necesidad de conocer.
- **Transmisión:** Transferencia segura de información dentro y fuera de la empresa.
- **Retención y Destrucción:** Conservación de la información según las políticas de retención y eliminación segura cuando ya no sea necesaria.

3.3 Integridad y disponibilidad

- La información debe mantenerse íntegra, lo que significa que no debe alterarse de manera no autorizada.
- Los sistemas de almacenamiento y acceso a la información deben garantizar su disponibilidad en todo momento, según los niveles de servicio establecidos por COMFICA.

4. Control de acceso

4.1 Control de accesos basado en roles

El acceso a la información se concederá según el principio de "mínimo privilegio", lo que significa que los colaboradores y terceros solo tendrán acceso a la información necesaria para desempeñar sus funciones. Las políticas de acceso se gestionarán mediante un sistema de Control de Acceso Basado en Roles, que incluye:

- Roles definidos: Cada colaborador tendrá un rol asignado que determinará los niveles de acceso a la información.
- Revisión periódica: Los permisos de acceso serán revisados y ajustados periódicamente para asegurar que estén alineados con las responsabilidades actuales de cada persona.
- Segregación de funciones: Se implementará la segregación de funciones para minimizar el riesgo de accesos indebidos.

4.2 Control de acceso físico y lógico

- Acceso físico: Se controlará el acceso a las áreas donde se almacena información sensible, implementando medidas como acceso biométrico, sistemas de seguridad y vigilancia.
- Acceso lógico: El acceso a sistemas y bases de datos se controlará mediante credenciales de usuario, autenticación multifactor (MFA) y políticas de contraseñas seguras.

4.3 Gestión de credenciales

- Contraseñas: Las contraseñas deberán cumplir con los estándares mínimos de complejidad definidos en el procedimiento de uso, creación y gestión de accesos físicos y lógicos, y deberán ser cambiadas cada 6 meses.
- Autenticación multifactor (MFA): Se requerirá autenticación multifactor para acceder a sistemas críticos.
- Revocación de accesos: Los accesos de los colaboradores que dejan la empresa o cambian de función serán revocados inmediatamente para prevenir accesos no autorizados

5. Responsabilidades

5.1 Área de TI

- Gestionar los sistemas de control de acceso y garantizar la seguridad de la infraestructura tecnológica.
- Mantener actualizados los permisos de acceso y realizar auditorías periódicas.
- Gestionar el respaldo y la recuperación de la información, garantizando su disponibilidad ante incidentes.

5.2 Gerentes o líderes de área

- Asegurar que los colaboradores de sus áreas tengan los permisos de acceso adecuados según sus roles.

- Notificar al área de TI cualquier cambio en la estructura del personal que requiera ajustes en los accesos.

Colaboradores

- Utilizar la información de acuerdo con los niveles de acceso que les han sido concedidos y en línea con las políticas de seguridad de COMFICA
- Reportar cualquier acceso no autorizado o incidentes relacionados con la seguridad de la información.

5.3 Terceras partes

- Cumplir con los acuerdos de acceso y confidencialidad firmados con COMFICA, y respetar las políticas de seguridad de la información durante la prestación de servicios.

6. Medidas de seguridad

6.1 Protección de información digital

- Toda la información confidencial o sensible almacenada en sistemas digitales deberá estar protegida mediante cifrado.
- Se utilizarán firewalls y soluciones antivirus para proteger la infraestructura de TI de COMFICA.

6.2 Respaldo y recuperación

- Se realizarán respaldos periódicos de toda la información crítica y se almacenarán en ubicaciones seguras, conforme al Procedimiento de Continuidad del Negocio y Recuperación ante Desastres.
- Los respaldos deberán ser verificados periódicamente para garantizar su integridad y disponibilidad.

6.3 Protección de información física

- La información en formato físico deberá almacenarse en áreas seguras y cerradas con acceso controlado.
- La destrucción de documentos físicos se llevará a cabo mediante procesos seguros, como el triturado de papel.

7. Sanciones

El incumplimiento de esta política podrá resultar en sanciones disciplinarias, incluyendo el despido en casos graves, así como en la revocación de contratos con terceros que no cumplan con los estándares de seguridad de la información de COMFICA.

8. Revisión y actualización

Esta política será revisada anualmente por el área de TI, junto con los Gerentes de Área, para asegurar su efectividad y adecuación a los cambios tecnológicos y normativos.