

 Safe Comercial Zona Franca S.A.S.	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 1 de 3

1. Objetivo

Establecer un marco para la clasificación de la información, asegurando que reciba un nivel apropiado de protección, conforme a su valor, sensibilidad y criticidad para la organización.

2. Alcance

Aplica a toda la información creada, recibida, almacenada, procesada o transmitida por la organización, sin importar su formato (digital, físico, verbal).

3. Niveles, Etiquetado y Manejo de la Clasificación

Nivel	Descripción	Ejemplos	Acceso	Protección mínima requerida
Público	Información de libre acceso, cuya divulgación no representa riesgo.	Políticas públicas, contenidos del sitio web.	Cualquier persona.	Sin restricciones.
Interno	Uso exclusivo dentro de la organización.	Manuales operativos, actas internas.	Personal autorizado.	Acceso controlado, no enviar a externos.
Confidencial	Información sensible, su divulgación puede generar daño a la organización o a terceros.	Datos personales, contraseñas, correos de clientes.	Sólo personal autorizado con necesidad de conocer.	Acceso restringido, VPN obligatoria.

Etiquetado de la información (A.8.2.2)

Se utilizará **una palabra clave en el nombre del archivo o asunto del correo** para marcar la clasificación:

- Archivos o documentos:
Ejemplo: *usuarios_confidencial.xlsx, manual_interno.docx*

 Safe Comercial Zona Franca S.A.S.	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 2 de 3

- Correos electrónicos:
Asunto: *[CONFIDENCIAL] Acceso de base de datos o [INTERNO] Procedimiento contable*

Manejo de activos (A.8.2.3)

Los activos de información serán tratados según su nivel, de forma práctica:

- **Público:** puede estar en el sitio web o compartirse libremente.
- **Interno:** se almacena en Google Drive o carpetas compartidas internas de trabajo (no públicas).
- **Confidencial:** se guarda en carpetas privadas solo accesibles por personal autorizado (por ejemplo, en una carpeta Drive con permisos restringidos). No se comparte sin autorización del líder de operaciones Y TI o el líder de área.

4. Responsabilidades

- **Todos los colaboradores:** Clasificar correctamente la información según esta política.
- **TI / DevOps:** Aplicar controles técnicos según el nivel.
- **Oficial de Seguridad:** Supervisar cumplimiento, actualizar esta política.

5. Clasificación y Revisión

- La información debe clasificarse al momento de su creación.
- Se debe revisar la clasificación cada 12 meses o cuando cambie su criticidad.

6. Incumplimiento

El incumplimiento de esta política puede dar lugar a medidas disciplinarias y será tratado como un incidente de seguridad de la información.



CARLOS HUMBERTO TRONCOSO AYALDE
GERENTE GENERAL

 Safe Comercial Zona Franca S.A.S.	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 3 de 3

VERSIÓN	CAMBIO	VIGENCIA
1	Primera versión	25/06/2024