

	<b>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>		
	<b>POLÍTICA DE MEDIDAS DE SEGURIDAD PARA TELÉFONOS CORPORATIVOS</b>		
<b>VIGENCIA: 25/06/2024</b>	<b>VERSIÓN: 1</b>		<b>PÁG. 1 de 4</b>

## 1. Objetivo

Establecer las medidas de seguridad obligatorias para el uso, administración y soporte de los teléfonos móviles **corporativos** brindados por Safe Comercial, con el fin de proteger la información de la organización, garantizar la operatividad y minimizar riesgos de pérdida o exposición de datos.

## 2. Alcance

Esta política aplica **exclusivamente** a los **teléfonos móviles entregados por Safe Comercial** a su personal operativo, comercial o administrativo, y que sean utilizados en el cumplimiento de funciones laborales.

## 3. Requisitos de Seguridad

### 3.1. Autenticación y Bloqueo

- Todos los teléfonos deben contar con un método de autenticación seguro (PIN, contraseña, huella o reconocimiento facial).
- El bloqueo automático debe estar configurado con un tiempo máximo de inactividad de **2 minutos**.

### 3.2. Encriptación

- Los teléfonos deben tener el cifrado de almacenamiento habilitado (por defecto en versiones recientes de Android/iOS).
- Toda información confidencial almacenada debe estar protegida mediante cifrado a nivel de aplicación o sistema.

### 3.3. Gestión Remota (MDM)

- Todos los dispositivos estarán registrados bajo un sistema de **Gestión de Dispositivos Móviles (MDM)** que permita:

	<b>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>		
	<b>POLÍTICA DE MEDIDAS DE SEGURIDAD PARA TELÉFONOS CORPORATIVOS</b>		
<b>VIGENCIA:</b> 25/06/2024	<b>VERSIÓN:</b> 1		<b>PÁG. 2 de 4</b>

- Monitoreo de uso.
- Aplicación de políticas.
- Restricción de aplicaciones.

### 3.5. Actualizaciones y Mantenimiento

- Los dispositivos deben mantenerse actualizados con los últimos parches de seguridad. Las actualizaciones podrán ser gestionadas de forma centralizada por el área de TI.

### 3.6. Uso de Redes

- Está prohibido conectarse a redes Wi-Fi públicas sin autorización. Se priorizará el uso de VPN corporativa para acceso remoto a sistemas internos.(Si aplica)

### 3.7. Almacenamiento y Respaldos

- No se permite el almacenamiento prolongado de archivos sensibles en el dispositivo. Los dispositivos deberán sincronizar automáticamente los datos con servidores seguros o la nube.

## 4. Protocolo en Caso de Pérdida o Robo

- El colaborador deberá reportar el incidente **de forma inmediata** al área de Soporte TI.
- Se procederá al bloqueo y borrado remoto del dispositivo, utilizando la aplicación de google (<https://www.google.com/android/find/about>) que deberá estar configurada en cada dispositivo corporativo.  
Se investigará si existió riesgo de fuga o acceso no autorizado.

## 5. Restricciones de Uso

- Queda prohibido el uso del teléfono corporativo para fines personales que impliquen riesgos de seguridad (apps de mensajería no corporativas, etc.).

	<b>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>		
	<b>POLÍTICA DE MEDIDAS DE SEGURIDAD PARA TELÉFONOS CORPORATIVOS</b>		
<b>VIGENCIA:</b> 25/06/2024	<b>VERSIÓN:</b> 1		<b>PÁG. 3 de 4</b>

- Las aplicaciones de redes sociales están autorizadas solo al personal autorizado.(Personal de Marketing y publicidad, Personal Comercial.).
- No se permite modificar el sistema operativo (rooting o jailbreak).

## 6. Responsabilidades

Área / Persona	Responsabilidad
Usuario final	Cumplir con la política, mantener el dispositivo seguro, reportar incidentes.
Área de TI	Configurar, gestionar y mantener la seguridad de los dispositivos.
Seguridad de la Información	Realizar evaluaciones de cumplimiento.

## 7. Sanciones

El incumplimiento de esta política podrá resultar en:

- Suspensión temporal del uso del dispositivo.
- Retiro del dispositivo asignado.
- Medidas disciplinarias conforme al reglamento interno.

## 8. Revisión

Esta política será revisada y actualizada anualmente o cuando se identifiquen nuevas amenazas, tecnologías o cambios normativos relevantes.



**CARLOS HUMBERTO TRONCOSO AYALDE**  
**GERENTE GENERAL**

	<b>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>		
	<b>POLÍTICA DE MEDIDAS DE SEGURIDAD PARA TELÉFONOS CORPORATIVOS</b>		
<b>VIGENCIA: 25/06/2024</b>	<b>VERSIÓN: 1</b>		<b>PÁG. 4 de 4</b>

<b>VERSIÓN</b>	<b>CAMBIO</b>	<b>VIGENCIA</b>
1	Primera versión	25/06/2024