05 DE MAYO DEL 2025

1. OBJETIVO

Establecer las directrices para el uso correcto, responsable y seguro de los recursos tecnológicos de **INDUSTRIA SUPERFILT SAS**, incluyendo correos electrónicos, dispositivos, software y redes empresariales, con el fin de proteger la información corporativa, prevenir incidentes de ciberseguridad y asegurar la continuidad operativa.

2. ALCANCE

Esta política aplica a todos los empleados, contratistas, proveedores y cualquier persona que acceda a los sistemas, redes y recursos tecnológicos de la empresa, independientemente del lugar desde el que lo hagan.

3. USO ADECUADO DE TECNOLOGÍAS

3.1 Correos electrónicos corporativos

El correo electrónico institucional debe utilizarse exclusivamente para fines laborales.

- ✓ Está prohibido enviar correos masivos no autorizados, cadenas, archivos maliciosos o contenido ofensivo.
- ✓ No se debe usar el correo corporativo para registrarse en servicios personales o ajenos al trabajo.

3.2 Dispositivos tecnológicos

Los dispositivos entregados por la empresa (computadores, tablets, teléfonos, etc.) deben usarse únicamente para funciones laborales.

- ✓ Se debe evitar la instalación de software no autorizado o el uso de dispositivos de almacenamiento no aprobados (USB, discos externos).
- ✓ El colaborador es responsable del cuidado y conservación de los dispositivos asignados.

3.3 Software

Solo se permitirá el uso de software legal y autorizado por el área de TI. La instalación o modificación de programas debe ser aprobada y realizada por personal autorizado.

Se prohíbe el uso de software pirata, descargas ilegales o aplicaciones que comprometan la seguridad de la empresa.

3.4 Redes y acceso a internet

El acceso a redes internas y externas debe ser realizado mediante las credenciales personales asignadas.

- ✓ El uso de internet debe estar alineado con fines laborales. Está restringido el acceso a sitios de apuestas, contenido para adultos, violencia, piratería o redes de intercambio ilegal.
- ✓ No se debe compartir contraseñas ni dejar sesiones abiertas en equipos de uso compartido.

4. SEGURIDAD INFORMÁTICA Y PREVENCIÓN DEL CIBERCRIMEN

4.1 Medidas de seguridad

- ✓ Todos los usuarios deben utilizar contraseñas seguras, actualizarlas periódicamente y mantenerlas en confidencialidad.
- ✓ Se deberá bloquear el equipo al dejarlo desatendido, incluso por cortos períodos de tiempo.
- ✓ Los equipos deben contar con antivirus actualizado y firewall activo.
- ✓ El acceso remoto debe realizarse únicamente mediante conexiones seguras (VPN autorizadas).

4.2 Prevención del cibercrimen

- ✓ Se debe evitar abrir enlaces o archivos adjuntos sospechosos, incluso si provienen de contactos conocidos.
- ✓ Cualquier intento de phishing, fraude electrónico o acceso no autorizado debe reportarse inmediatamente al área de TI.
- ✓ La empresa realizará campañas de concientización y capacitaciones periódicas sobre ciberseguridad.

5. CONFIDENCIALIDAD Y PRIVACIDAD

Toda la información a la que se accede por medios tecnológicos debe tratarse como confidencial, a menos que sea de dominio público o esté autorizada para su difusión.

- ✓ El uso indebido, filtración o robo de información será considerado falta grave y podrá dar lugar a acciones disciplinarias y/o legales.
- ✓ La empresa se reserva el derecho de auditar el uso de sus recursos tecnológicos cuando lo considere necesario, respetando la legislación vigente.

6. SANCIONES

El incumplimiento de esta política podrá dar lugar a sanciones disciplinarias que incluyen llamados de atención, suspensión del servicio, sanciones contractuales o la terminación del vínculo laboral o comercial, sin perjuicio de las acciones legales correspondientes.

7. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada y actualizada de manera anual o cuando existan cambios significativos en el entorno tecnológico, amenazas informáticas o regulaciones legales.

_____

CARLOS HERNAN LOZANO ARIAS
REPRESENTANTE LEGAL