Objetivo:
Proteger los sistemas y activos de información contra software malicioso (malware), minimizando riesgos de infección, propagación y daños.

Declaración:
La organización ha implementado políticas, procedimientos y controles técnicos para prevenir, detectar y responder ante amenazas de malware, asegurando la continuidad y seguridad de sus operaciones.

Alcance:
Este control aplica a todos los sistemas, dispositivos y redes gestionados por la organización.

Directrices:

- Se implementan soluciones antivirus y antimalware actualizadas y configuradas adecuadamente.
- Se realizan análisis y escaneos periódicos para detectar software malicioso.
- Se establecen políticas de uso de software, correos electrónicos y dispositivos externos para reducir riesgos.
- Se capacita a los usuarios sobre prácticas seguras para prevenir infecciones.
- Se mantienen procedimientos para la respuesta rápida ante detección de malware.
- Se monitorea y registra la actividad relacionada con malware para análisis y mejora continua.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- PRO 012 — Procedimiento para la Comunicación de Incidentes de Seguridad
- PSC 009 — Sensibilización y Capacitación

Evidencias de implementación:

- Informes de análisis y escaneo antimalware.
- Registros de actualización y configuración de soluciones de protección.
- Documentación de políticas y procedimientos relacionados con malware.
- Registros de capacitación y sensibilización.
- Reportes de incidentes y acciones correctivas relacionadas con malware.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO