Objetivo:

Implementar un proceso sistemático para la recopilación, análisis y distribución de información sobre amenazas actuales y emergentes que puedan afectar la seguridad de la información de la organización, permitiendo una respuesta proactiva y efectiva.

Declaración:

La organización mantiene un programa activo de inteligencia de amenazas que permite identificar, evaluar y anticipar riesgos relacionados con la seguridad de la información, facilitando la toma de decisiones informadas para la protección de sus activos.

Alcance:

Este control aplica a todas las áreas y sistemas que gestionan, procesan o almacenan información crítica, así como al personal responsable de la seguridad de la información.

Directrices:

- Se establecen fuentes confiables y actualizadas para la recopilación de información sobre amenazas internas y externas.
- Se realiza un análisis continuo y contextualizado de las amenazas para determinar su impacto potencial en la organización.
- La inteligencia obtenida se distribuye oportunamente a las áreas responsables para la adopción de medidas preventivas o correctivas.
- Se integran los resultados de la inteligencia de amenazas en la gestión de riesgos y en los planes de respuesta a incidentes.
- Se mantiene la confidencialidad y la integridad de la información manejada durante el proceso.
- Se capacita al personal clave para interpretar y utilizar la inteligencia de amenazas de manera efectiva.

Referencias relacionadas:

- PSC 002 — Gestión de Incidentes
- PRO 012 — Procedimiento para la Comunicación de Incidentes de Seguridad
- PSC 007 — Monitoreo y Medición
- PSC 009 — Sensibilización y Capacitación
- POL 001 — Política de Seguridad de la Información

Evidencias de implementación:

- Reportes periódicos de análisis de inteligencia de amenazas.

- Registros de acciones tomadas basadas en la información de amenazas detectadas.
- Documentación de fuentes y métodos utilizados para la recopilación de inteligencia.
- Registros de capacitaciones y sensibilización en inteligencia de amenazas.
- Integración documentada de inteligencia de amenazas en la gestión de riesgos y respuesta a incidentes.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.05.2024	Original	CEO