Objetivo:
Supervisar y analizar de manera continua las actividades en los sistemas de información para detectar comportamientos anómalos, accesos no autorizados y apoyar la respuesta a incidentes de seguridad.

Declaración:
La organización ha implementado procesos, herramientas y controles para el monitoreo efectivo de actividades en redes, sistemas y aplicaciones, garantizando la detección temprana de eventos de seguridad y facilitando la gestión proactiva de riesgos.

Alcance:
Este control aplica a todos los sistemas y activos de información que requieran supervisión para mantener la seguridad y la integridad.

Directrices:

- Se definen las actividades críticas y eventos que deben ser monitoreados.
- Se utilizan herramientas y tecnologías para la recopilación y análisis de datos de actividad.
- Se establecen procedimientos para la revisión periódica y respuesta ante eventos detectados.
- Se documentan y reportan las anomalías y eventos relevantes para la gestión de incidentes.
- Se capacita al personal responsable en técnicas y herramientas de monitoreo.
- Se asegura la confidencialidad y protección de la información generada durante el monitoreo.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- PRO 014 — Procedimiento para el Registro y Supervisión de Accesos
- PSC 002 — Gestión de Incidentes
- PSC 007 — Monitoreo y Medición
- PSC 009 — Sensibilización y Capacitación

Evidencias de implementación:

- Configuraciones y registros de monitoreo de actividades.
- Informes periódicos de análisis y seguimiento de eventos.
- Registros de capacitación del personal de monitoreo.
- Reportes de incidentes detectados y acciones tomadas.
- Auditorías y revisiones relacionadas con el monitoreo de seguridad.

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO

Historial de Versiones