Objetivo:
Registrar y monitorear las actividades relevantes en los sistemas y redes para detectar accesos no autorizados, actividades anómalas y apoyar la investigación de incidentes de seguridad de la información.

Declaración:
La organización ha establecido políticas, procedimientos y controles para la generación, almacenamiento, protección y análisis de logs (registros de actividad) en los sistemas y dispositivos, asegurando su integridad y disponibilidad para fines de seguridad.

Alcance:
Este control aplica a todos los sistemas, aplicaciones, dispositivos y redes gestionados por la organización que generan registros de eventos y actividades.

Directrices:

- Se definen los eventos y actividades que deben ser registrados según su criticidad y relevancia.
- Los logs se generan de manera segura, garantizando su integridad y protección contra modificaciones no autorizadas.
- Se establece un periodo de retención adecuado para los registros de actividad.
- Se implementan mecanismos para la revisión y análisis periódico de logs, detectando eventos sospechosos o anómalos.
- Se capacita al personal responsable en el manejo y análisis de logs.
- Se asegura la disponibilidad y accesibilidad controlada de los registros para auditorías e investigaciones.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- PRO 014 — Procedimiento para el Registro y Supervisión de Accesos
- PSC 007 — Monitoreo y Medición
- PSC 009 — Sensibilización y Capacitación
- FOR 004 — Registro de Seguridad

Evidencias de implementación:

- Configuraciones y políticas documentadas para generación y almacenamiento de logs.
- Registros de eventos y actividades almacenados y protegidos.
- Informes de análisis y monitoreo de logs.
- Registros de capacitación para personal encargado.
- Reportes de incidentes detectados a través del análisis de logs y acciones correctivas.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO