Control 5.21 – Gestión de la Seguridad de la Información en la Cadena de Suministro de las Tecnologías de la Información y Comunicación (TIC)

Objetivo:

Asegurar que los riesgos relacionados con la seguridad de la información derivados de la cadena de suministro de las tecnologías de la información y comunicación (TIC) sean gestionados adecuadamente para proteger los activos y la información de la organización.

Declaración:

La organización ha implementado políticas, procedimientos y controles que permiten identificar, evaluar y mitigar riesgos asociados a proveedores, subcontratistas y terceros involucrados en la cadena de suministro de TIC, garantizando la continuidad y seguridad de los servicios.

Alcance:

Este control aplica a todos los proveedores y actores que forman parte de la cadena de suministro de TIC, incluyendo hardware, software, servicios y soporte técnico.

Directrices:

- Se realiza una evaluación de riesgos específica para la cadena de suministro de TIC antes y durante la relación contractual.
- Se establecen requisitos contractuales que contemplan aspectos de seguridad de la información para proveedores de TIC.
- Se implementan controles para la supervisión y monitoreo continuo del cumplimiento de proveedores en materia de seguridad.
- Se gestionan planes de contingencia y continuidad en caso de fallos o incidentes relacionados con proveedores de TIC.
- Se capacita al personal responsable en gestión y supervisión de la cadena de suministro TIC.
- Se documentan y registran todas las actividades relacionadas con la gestión de la seguridad en la cadena de suministro.

Referencias relacionadas:

- POL 011 — Política de seguridad del proveedor
- PRO 012 — Procedimiento para la Comunicación de Incidentes de Seguridad

- PSC 002 — Gestión de Incidentes
- PSC 003 — Plan de Continuidad del Negocio
- DOC 023 — Lista de proveedores críticos
- FOR 031 — Registro de comunicado de incidente y seguimiento

Evidencias de implementación:

- Evaluaciones de riesgos documentadas específicas para proveedores de TIC.
- Contratos y acuerdos que incluyen cláusulas de seguridad para proveedores de TIC.
- Informes de auditorías y monitoreos de cumplimiento de proveedores TIC.
- Planes de contingencia y continuidad actualizados y probados.
- Registros de capacitaciones y sensibilización en gestión de la cadena de suministro TIC.
- Documentación y registros de incidentes y acciones correctivas relacionadas con proveedores TIC.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO