Control 5.20 – Abordar la Seguridad de la Información dentro de los Acuerdos con Proveedores

Objetivo:
Incorporar requisitos y controles específicos de seguridad de la información en los acuerdos con proveedores para garantizar la protección de los activos y la información de la organización durante toda la relación contractual.

Declaración:
La organización asegura que todos los acuerdos y contratos con proveedores incluyan cláusulas claras relacionadas con la seguridad de la información, estableciendo responsabilidades, requisitos y controles para la protección de los datos y activos compartidos.

Alcance:
Este control aplica a todos los contratos y acuerdos formales con proveedores que impliquen el manejo, acceso o procesamiento de información o activos de la organización.

Directrices:

- Se definen requisitos mínimos de seguridad que deben ser cumplidos por los proveedores como parte de los acuerdos contractuales.
- Los contratos incluyen cláusulas sobre confidencialidad, protección de datos, manejo de incidentes y auditorías.
- Se establece un proceso para la revisión y aprobación de acuerdos que contemple los aspectos de seguridad de la información.
- Se monitorea el cumplimiento de los proveedores respecto a las obligaciones de seguridad establecidas en los contratos.
- Se gestionan y documentan los incumplimientos y se aplican medidas correctivas o sanciones según corresponda.
- Se capacita al personal responsable de la negociación y gestión de proveedores sobre los requisitos de seguridad.

Referencias relacionadas:

- POL 011 — Política de seguridad del proveedor
- PRO 012 — Procedimiento para la Comunicación de Incidentes de Seguridad
- PSC 002 — Gestión de Incidentes
- DOC 023 — Lista de proveedores críticos
- FOR 031 — Registro de comunicado de incidente y seguimiento

Evidencias de implementación:

- Contratos y acuerdos con cláusulas específicas de seguridad de la información.
- Registros de revisión y aprobación de contratos.
- Informes y resultados de auditorías y seguimientos a proveedores.
- Registros de capacitaciones relacionadas con seguridad en la gestión de contratos.
- Reportes de incidentes y acciones correctivas vinculadas a proveedores.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO