

Control 5.31 – Requisitos Legales, Estatutarios, Regulatorios y Contractuales

Objetivo:

Garantizar el cumplimiento de todos los requisitos legales, estatutarios, regulatorios y contractuales aplicables relacionados con la seguridad de la información.

Declaración:

La organización ha establecido procesos para identificar, evaluar y cumplir con los requisitos legales y regulatorios vigentes, así como las obligaciones contractuales que impactan en la seguridad de la información.

Alcance:

Este control aplica a todas las áreas y actividades de la organización relacionadas con la gestión y protección de la información.

Directrices:

- Se mantiene un registro actualizado de los requisitos legales, regulatorios y contractuales aplicables.
- Se realiza una evaluación periódica para asegurar el cumplimiento continuo de dichos requisitos.
- Se asignan responsabilidades claras para la gestión del cumplimiento normativo.
- Se integran los requisitos legales y contractuales en las políticas, procedimientos y controles del SGSI.
- Se proporciona capacitación y sensibilización al personal sobre sus obligaciones legales y contractuales.
- Se documentan y gestionan evidencias de cumplimiento y auditorías externas.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- PRO 005 — Gestión de Riesgos y Oportunidades
- PSC 004 — Auditoría Interna
- PSC 008 — Mejora Continua
- DOC 006 — Análisis del Contexto
- DOC 007 — Análisis de Partes Interesadas

Evidencias de implementación:

- Registro formal de requisitos legales, regulatorios y contractuales.
- Informes de auditorías internas y externas que evidencian el cumplimiento.
- Documentación de políticas y procedimientos que incorporan los requisitos normativos.
- Registros de capacitación y sensibilización en temas legales y contractuales.
- Reportes de gestión y seguimiento de acciones correctivas relacionadas con cumplimiento.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO