

Objetivo:

Incorporar principios de ingeniería y arquitectura que aseguren la construcción de sistemas seguros, robustos y resistentes a amenazas y vulnerabilidades.

Declaración:

La organización ha establecido políticas, directrices y controles para integrar principios de seguridad en el diseño y arquitectura de sus sistemas, garantizando su protección durante todo su ciclo de vida.

Alcance:

Este control aplica a todos los sistemas de información desarrollados, adquiridos o mantenidos por la organización.

Directrices:

- Se adoptan principios como defensa en profundidad, mínimo privilegio, segregación de funciones y diseño modular.
- Se diseñan arquitecturas que soporten la identificación, mitigación y respuesta a riesgos de seguridad.
- Se promueve la utilización de estándares y buenas prácticas en ingeniería de software y sistemas.
- Se realizan revisiones y auditorías de seguridad en las etapas de diseño y arquitectura.
- Se capacita al personal técnico en principios de ingeniería y arquitectura segura.
- Se documentan los criterios y decisiones arquitectónicas relacionadas con la seguridad.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- PRO 025 — Procedimiento de Desarrollo Seguro (si aplica)
- PSC 009 — Sensibilización y Capacitación

Evidencias de implementación:

- Documentación de políticas, directrices y estándares de diseño seguro.
- Informes de revisiones y auditorías de arquitectura y diseño.
- Registros de capacitación del personal técnico.
- Documentación técnica de arquitectura que incluye aspectos de seguridad.
- Reportes de incidentes y acciones correctivas relacionadas con fallos arquitectónicos.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO