

Objetivo:

Garantizar que el desarrollo de software se realice bajo prácticas seguras a lo largo de todo su ciclo de vida, minimizando vulnerabilidades y riesgos de seguridad.

Declaración:

La organización ha establecido políticas, procedimientos y controles que integran aspectos de seguridad en cada fase del ciclo de desarrollo de software, desde el diseño hasta la implementación, prueba y mantenimiento.

Alcance:

Este control aplica a todos los proyectos y actividades de desarrollo, mantenimiento y actualización de software dentro de la organización.

Directrices:

- Se incorporan requisitos de seguridad desde la fase de análisis y diseño.
- Se aplican prácticas de codificación segura para prevenir vulnerabilidades comunes.
- Se realizan revisiones de seguridad, pruebas y auditorías durante el desarrollo.
- Se gestionan adecuadamente los cambios y versiones del software.
- Se capacita al personal de desarrollo en metodologías y herramientas de desarrollo seguro.
- Se documentan y gestionan las incidencias y correcciones 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, procedimientos y estándares de desarrollo seguro.
- Registros de revisiones, pruebas y auditorías de seguridad en el desarrollo.
- Informes de gestión de cambios y versiones.
- Registros de capacitación y sensibilización del personal de desarrollo.
- Reportes de incidentes y acciones correctivas relacionadas con vulnerabilidades en software.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO