

Objetivo

Asegurar que las aplicaciones y sistemas sean evaluados mediante pruebas de seguridad durante las fases de desarrollo y aceptación para identificar y mitigar vulnerabilidades antes de su implementación.

Declaración:

La organización ha implementado procesos y controles que integran pruebas de seguridad en el ciclo de vida del desarrollo, garantizando que los sistemas cumplan con los requisitos de seguridad antes de entrar en producción.

Alcance:

Este control aplica a todas las aplicaciones y sistemas desarrollados o adquiridos por la organización.

Directrices:

- Se planifican y ejecutan pruebas de seguridad, incluyendo análisis estático y dinámico, pruebas de penetración y revisiones de código.
- Se documentan los resultados de las pruebas y las vulnerabilidades detectadas.
- Se gestionan las correcciones y mitigaciones antes de la aceptación y despliegue.
- Se definen criterios claros para la aceptación basada en resultados de seguridad.
- Se capacita al personal involucrado en técnicas y herramientas de pruebas de 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:

- Planes y reportes de pruebas de seguridad realizadas.
- Registros de vulnerabilidades detectadas y acciones correctivas aplicadas.
- Documentación de criterios y resultados de aceptación.
- Registros de capacitación del personal involucrado.
- Informes de auditoría relacionados con pruebas de seguridad.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO