

Objetivo:

Garantizar que el desarrollo de software realizado por terceros cumpla con los requisitos de seguridad establecidos para proteger la información y activos de la organización.

Declaración:

La organización ha implementado políticas, procedimientos y controles para gestionar y supervisar el desarrollo tercerizado, asegurando la aplicación de prácticas de seguridad durante todo el proceso.

Alcance:

Este control aplica a todos los proyectos y servicios de desarrollo de software contratados a proveedores externos o colaboradores externos.

Directrices:

- Se establecen criterios claros para la selección y evaluación de proveedores de desarrollo.
- Se incluyen cláusulas de seguridad en los contratos y acuerdos con terceros.
- Se definen requisitos de seguridad para el desarrollo, pruebas y entrega de software.
- Se realiza seguimiento y auditoría del cumplimiento de los proveedores con los requisitos de seguridad.
- Se gestionan los riesgos asociados al desarrollo tercerizado.
- Se capacita al personal involucrado en la gestión y supervisión del desarrollo tercerizado.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- POL 011 — Política de seguridad del proveedor
- PRO 025 — Procedimiento de Desarrollo Seguro (si aplica)
- PSC 002 — Gestión de Incidentes
- PSC 009 — Sensibilización y Capacitación

Evidencias de implementación:

- Contratos y acuerdos con cláusulas de seguridad para desarrollo tercerizado.
- Informes de auditorías y seguimientos a proveedores.
- Documentación de requisitos y especificaciones de seguridad aplicadas.
- Registros de capacitación para responsables y supervisores.
- Reportes de incidentes y acciones correctivas relacionadas con desarrollo tercerizado.

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO



Sistemas de gestión de la seguridad de la información

Rev. 1

A 8. 30 – DESARROLLO TERCERIZADO

Aprobada:
01.05.2024

Crea: COF

Aprueba: CEO

Página 2 de 2

--	--	--	--

Historial de Versiones