

	Sistemas de gestión de la seguridad de la información	Rev. 1
	A - 5.26 – Respuesta a Incidentes de Seguridad de la Información	Aprobada: 01.05.2024
	Crea: COF Aprueba: CEO	Página 1 de 2

Objetivo:

Establecer un proceso estructurado para responder de manera eficaz y oportuna a los incidentes de seguridad de la información, minimizando su impacto y facilitando la recuperación.

Declaración:

La organización ha implementado procedimientos claros para la detección, reporte, análisis, contención, erradicación y recuperación ante incidentes de seguridad de la información, asegurando la continuidad operativa y la protección de activos.

Alcance:

Este control aplica a todos los tipos de incidentes que afecten la seguridad de la información en la organización, incluyendo aquellos relacionados con sistemas, redes, aplicaciones y personal.

Directrices:

- Se define un proceso formal para la gestión integral de incidentes, incluyendo roles, responsabilidades y flujos de comunicación.
- Se establecen mecanismos para la detección temprana y reporte inmediato de incidentes.
- Se implementan acciones rápidas para contener y mitigar los efectos de los incidentes.
- Se documentan todas las etapas del manejo de incidentes para análisis y aprendizaje.
- Se realiza la recuperación de los sistemas afectados y la restauración de la operación normal.
- Se comunica de forma adecuada con las partes interesadas internas y externas.
- Se lleva a cabo un análisis post-incidente para identificar causas raíz y mejoras.

Referencias relacionadas:

- PSC 002 — Gestión de Incidentes
- PRO 012 — Procedimiento para la Comunicación de Incidentes de Seguridad
- FOR 010 — Registro de Incidentes de Seguridad
- FOR 031 — Registro de comunicado de incidente y seguimiento
- PSC 008 — Mejora Continua

Evidencias de implementación:

- Documentación formal del proceso de respuesta a incidentes.
- Registros completos de incidentes gestionados (FOR 010, FOR 031).
- Informes de análisis post-incidente y acciones correctivas implementadas.
- Registros de capacitación y simulacros relacionados con respuesta a incidentes.
- Comunicaciones oficiales y reportes de gestión ante incidentes.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO