

Política de Gestión de incidentes de seguridad de la información

Versión	3.0	Categoría	Política
Última actualización	22/06/2023	Estado	

Objetivo

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y mitigar el impacto de los mismos; basándose en el contexto de la organización, concientización, reducción en tiempos de respuesta, estrategias para la recuperación y la generación de una base de conocimientos con lecciones aprendidas de eventos e incidentes.

Alcance

Toda persona que tenga legítimo acceso a los activos de información de la organización, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

Responsabilidades

Dirección de la organización es responsable por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o su relación contractual y de brindar los recursos necesarios para el cumplimiento de la misma.

Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de esta política y realizar las revisiones periódicas y oportunas.

Equipo de respuesta es responsable por la ejecución de los planes y demás actividades vinculadas a la gestión de incidentes.

Personal de la organización es responsable por dar cumplimiento a la presente política y reportar los eventos de seguridad que detecte al RSI, siguiendo los procedimientos operativos establecidos para tal fin.

Políticas relacionadas

Política de Seguridad de la Información

Política de Gestión de Riesgos de Seguridad de la Información



Descripción

Al aprobar la presente política, la organización debe planificar y preparar el proceso de gestión de incidentes asignando los recursos de gestión, técnicos y humanos necesarios.

Todo evento o incidente de seguridad que sea reportado o detectado debe ser registrado, quedando registro de cada actividad realizada en su proceso de gestión.

La organización debe realizar la gestión de cada incidente contemplando todas las etapas de su ciclo de vida: Detectar y reportar; Evaluar y decidir; Responder y Lecciones aprendidas.

Anualmente se debe definir un plan de capacitación para el equipo de respuesta que permita mantener sus capacidades actualizadas.

Detectar y reportar

El proceso de gestión de incidentes debe explicitar de manera clara y sin ambigüedades los mecanismos y métodos para realizar los reportes de incidentes de seguridad, así como también la información mínima a proporcionar; manteniendo la confidencialidad de la información suministrada, así como su anonimato y respetando la cadena de custodia de las evidencias recabadas.

Evaluar y decidir

Los incidentes de seguridad de la información se deben clasificar, conforme la taxonomía definida por el CERTuy (o la [taxonomía de ENISA](#)), para poder realizar una gestión eficaz y definir indicadores de gestión que permitan la mejora continua de la gestión de incidentes.

El equipo de respuesta debe informar de forma completa e inmediata al CERTuy la existencia de un potencial incidente de seguridad informática, conforme lo establece el Decreto N° 451/009.

Responder

Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados. La respuesta debe incluir al menos los procedimientos de: contención, recopilación de evidencia, escalamiento y comunicación oportuna a las partes interesadas.

Lecciones aprendidas

Se debe promover y adoptar las medidas de seguridad pertinentes para proteger los activos de información. Asimismo, se debe aprender de los incidentes de seguridad reportados, identificando nuevos controles a implementar, o la mejora de los existentes; en particular se debe trabajar en la generación de una cultura de seguridad a fin de prevenir nuevas ocurrencias.