Política de Gestión de Incidentes de Seguridad de la Información

Fecha: 10/11/2022
Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
10/11/2022	1.0	Creación del Documento	Comité de Seguridad de la Información

Contenido

1 Revisiones

Fecha	Versión	Descripción	Autor
10/11/2022	1.0	Creación del Documento	Comité de Seguridad de la Información

2 Objetivo

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información con el fin de prevenir y limitar el impacto de los mismos.

3 Alcance

La política de gestión de incidentes de seguridad de la información está dirigida a toda persona que tenga legítimo acceso a los activos de información de ISA, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

4 Vigencia

La presente norma entra en vigor a partir de su aprobación y publicación por parte del Directorio de la empresa.

Esta política será revisada en un período no mayor a tres años, o ante cambios que así lo ameriten.

5 Responsabilidades

- Referentes de Seguridad - determinan en consulta con el Comité de Seguridad y el área de Infraestructura / Operaciones, la gravedad de los incidentes y el procedimiento a aplicar
- Comité de Seguridad de la Información - gestionar los incidentes de seguridad de la información promoviendo el reporte de estos, su tratamiento con las áreas involucradas y su cierre, aprendiendo de los mismos.
- Referentes de Seguridad - Gestionar los incidentes de seguridad informática y comunicarlos en forma oportuna al Comité de Seguridad de la Información y a la Gerencia del área.

- Personal de ISA Paraguay - reportar los eventos o incidentes de seguridad de la información que detecte a los Referentes de Seguridad y/o a Mesa de Ayuda en el caso de eventos o incidentes de seguridad informática.

6 Desarrollo

Es política de ISA:

- Adoptar medidas de seguridad eficientes para proteger sus activos de información
- Analizar los eventos de seguridad para determinar si se trata de un incidente de seguridad.
- Ejecutar procedimientos de repuesta a incidentes para contener y mitigar las consecuencias del incidente.
- Investigar, documentar y clasificar los incidentes de seguridad de la información.
- Aprender de los incidentes de seguridad de la información, para prevenir nuevas ocurrencias.
- Procurar la reparación y la mitigación de las consecuencias de los incidentes de seguridad de la información, siempre que sea posible.
- Emprender actividades posts-incidentes, como ser mejoras a los procesos operativos de gestión de incidentes de seguridad de la información y asegurar la retención de evidencias.

Fases del ciclo de vida de un evento o incidente:

- Detección y registro
- Categorización del Evento
- Investigación y diagnóstico
- Tratamiento
- Cierre del evento o incidente

Detección y registro

Todos los eventos o incidentes que se detectan deben ser registrados en el sistema informático. El registro se almacena con un código único de referencia del evento o incidente, la fecha, los datos de la persona que hace el registro y la descripción del evento o incidente, entre otros datos.

Categorización del Evento

El evento o incidente debe ser clasificado de acuerdo con el criterio que se establezca.

Investigación

En esta tarea pueden intervenir diferentes actores según el caso, incluyendo (de ser necesario), el apoyo y soporte de terceras partes. El área de Infraestructura /Operaciones en conjunto con los referentes de seguridad son responsables de identificar y resguardar cualquier evidencia asociada a los eventos o incidentes, que pueda ser luego utilizada a los efectos de un proceso disciplinario o acciones legales.

Tratamiento

En primera instancia se debe establecer cuál será el tratamiento para el evento o incidente. El evento o incidente es resuelto en base a la solución brindada y a la realización de acciones de recuperación requeridas. Los detalles del evento o incidente incluyendo la forma en que fue resuelto quedan registrados.

Cierre del evento o incidente

El cierre se produce cuando el evento o incidente ha sido resuelto. El acceso al cierre de eventos o incidentes es restringido y debidamente controlado por la Jefatura de Seguridad de la Información.

Registro de Lecciones Aprendidas

Una vez cerrado el incidente se debe analizar el mismo y definir lecciones aprendidas que permitan la mejora de los procedimientos, definición de nuevos procedimientos y/o políticas en la organización.

FIRMADO DIGITALMENTE tuid CERTIFICACIÓN DIGITAL AVANZADA

LEONARDO NOACH