analizA
Sociedad de Diagnóstico

Política de Seguridad de la Información

de Analiza Sociedad de Diagnóstico

Aprobación y Vigencia:

La política de seguridad de la información de ANALIZA, efectiva desde el 5 de diciembre de 2023, documentada y aprobada por la Dirección en el documento **R-2001**, se establecen las directrices para proteger los sistemas de información y garantizar la continuidad de los servicios.

Misión:

En ANALIZA, reconocemos la importancia crítica de las Tecnologías de la Información y Comunicaciones (TIC) para alcanzar nuestros objetivos estratégicos y operativos. Nos comprometemos a desarrollar y mantener procedimientos robustos que aseguren la máxima protección de la información utilizada en nuestras operaciones. Nuestro objetivo es ofrecer a todos nuestros grupos de interés, incluidos clientes, proveedores y socios, las mayores garantías en términos de seguridad de la información. Esto implica administrar nuestros sistemas con diligencia, implementando medidas adecuadas para protegerlos contra daños accidentales o deliberados que puedan comprometer la disponibilidad, integridad, autenticidad, trazabilidad o confidencialidad de la información y los servicios prestados. La seguridad de la información es fundamental para garantizar la calidad de nuestros servicios y la continuidad operativa, actuando de manera preventiva, supervisando la actividad diaria y respondiendo rápidamente a los incidentes.

Alcance:

Esta política se aplica a todos los sistemas TIC de ANALIZA y a todos los miembros de la organización involucrados en servicios y proyectos destinados al sector público.

Objetivos:

- Aumentar la resiliencia y capacidad de respuesta ante incidentes.
- Asegurar la recuperación rápida y eficiente de los servicios.
- Prevenir y mitigar incidentes de seguridad de la información.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Marco Normativo:

ANALIZA cumple con los requisitos legales aplicables y los compromisos adquiridos con clientes y partes interesadas, actualizando continuamente su marco regulatorio.

Desarrollo:

La política incluye la mejora continua del sistema de seguridad, la identificación de amenazas, la colaboración con proveedores y la formación del personal para garantizar la competencia técnica y la motivación en la mejora de procesos.

Organización de la Seguridad:

La responsabilidad de la seguridad recae en la Dirección General, que organiza funciones y proporciona recursos. Se definen roles específicos para la gestión de la información, servicios, seguridad y sistemas.

Comité de Seguridad de la Información:

Este comité es el órgano máximo de gestión y coordinación de la seguridad, responsable de tomar decisiones clave y compuesto por responsables de información, servicios, seguridad y sistemas.

Gestión de Riesgos:

Se realiza un análisis de riesgos regular para evaluar amenazas y riesgos, con revisiones anuales o cuando ocurren cambios significativos o incidentes graves.

Gestión de Personal:

Todos los miembros de ANALIZA deben conocer y cumplir la política de seguridad. Se establecen programas de concienciación y formación continua en seguridad TIC.

Control de Acceso:

Se implementan medidas para evitar el acceso no autorizado a sistemas de información, bases de datos y servicios, utilizando técnicas de autenticación y autorización.

Protección de Instalaciones:

Se previene el acceso no autorizado y se protege el equipo crítico de procesamiento de información mediante medidas de seguridad física y ambiental.

Adquisición de Productos:

La seguridad se integra en todas las etapas del ciclo de vida de los sistemas, desde su concepción hasta su retirada, incluyendo decisiones de desarrollo y adquisición.

Seguridad por Defecto:

La seguridad se considera un proceso integral y transversal en todos los sistemas y servicios, desde su creación hasta su retirada.

Integridad y Actualización del Sistema:
Se garantiza la integridad del sistema mediante procesos de gestión de cambios y revisiones periódicas de seguridad.

Protección de la Información:
Se establecen medidas para proteger la información almacenada y en tránsito, especialmente en entornos inseguros.

Prevención de Sistemas Interconectados:
Se implementan medidas de protección para sistemas interconectados, especialmente cuando se conectan a redes públicas.

Registros de Actividad:
Se registran las actividades de los usuarios para monitorizar, analizar e investigar actividades indebidas o no autorizadas.

Continuidad de la Actividad:
Se establecen mecanismos para garantizar la continuidad de las operaciones mediante copias de seguridad y otros medios.

Mejora Continua:
ANALIZA aplica un proceso de mejora continua de la seguridad de la información basado en normas internacionales.

Aprobado por la Dirección