

Política General de Seguridad de la Información - Signature/Ingeniox

Objetivo y Alcance

- Establecer los lineamientos que se deben seguir para implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información en Signature/Ingeniox, mediante el cual se desarrollarán los controles necesarios que permiten salvaguardar los principios de:
 - Confidencialidad: Asegurar que sólo quienes estén autorizados puedan acceder a la información.
 - Integridad: Asegurar que la información y sus métodos de proceso sean exactos y completos.
 - Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.
- Mantener la imagen y prestigio de la organización, evitando cualquier incidente que comprometa la seguridad de la información.
- Adelantarse a los requerimientos y mejores prácticas en materia de Seguridad de clientes y partes interesadas.
- Establecer buenas prácticas respecto a la seguridad de la información en las operaciones propias y con terceros.

La Política de Seguridad de la Información es de cumplimiento obligatorio para todo colaborador o tercero involucrado en los procesos donde se gestione información de la empresa.

Desarrollo

Signature/Ingeniox debe seguir los siguientes lineamientos para garantizar la seguridad de la información:

- Establecer objetivos anuales relacionados con la seguridad de la información, así como elaborar y actualizar un plan de acción para lograr dichos objetivos.
- Desarrollar un proceso integral de evaluación y gestión de riesgos de seguridad, implementando acciones correctivas y preventivas apropiadas según los resultados obtenidos.
- Adoptar una política de gestión de incidentes de seguridad de la información en consonancia con los lineamientos establecidos por el CERTuy (Centro de Respuesta a Incidentes de Seguridad Informática de Uruguay).
- Garantizar la continuidad de las operaciones mediante la implementación de planes de continuidad elaborados conforme a las mejores prácticas del mercado.

- Todo el personal es responsable de informar sobre cualquier violación de seguridad, ya sea confirmada o sospechada, de acuerdo con los procedimientos establecidos.
- Implementar políticas y procedimientos de seguridad necesarios para gestionar eficaz y seguramente todos los activos de información.
- Clasificar y proteger la información conforme a la normativa vigente y a criterios de valoración basados en su importancia para la organización.
- Cumplir con los requisitos aplicables a la seguridad de la información, legales o reglamentarios, así como con las obligaciones contractuales en materia de seguridad.
- Generar, almacenar y transferir información, tanto interna como externamente, únicamente con el propósito de cumplir con los objetivos de la organización, siempre respetando los principios de confidencialidad e integridad de la información.
- Implementar un proceso continuo de gestión de proveedores, quienes deben adherirse a los principios de esta política y a los procedimientos derivados de la misma para garantizar la seguridad de la información de la organización.
- Fomentar una cultura organizacional orientada hacia la seguridad de la información.
- Comprometer a la Dirección en la difusión, consolidación y cumplimiento de la política de seguridad de la información.
- Proporcionar concientización y formación en materia de seguridad de la información a todo el personal.
- Mantener actualizadas las políticas, normativas y procedimientos para garantizar su vigencia y efectividad.
- En la organización se debe tener un completo compromiso con la mejora continua. La ciberseguridad, como un concepto amplio de protección, será implementada como un proceso continuo y permanente dentro de Signature/Ingeniox, abarcando la protección de todas las operaciones de la organización en sus diversas funciones.
- El incumplimiento de esta política será sujeto a las sanciones administrativas correspondientes, según lo establecido en el reglamento interno.