Política De Seguridad de la Información

Política de Seguridad

Introducción

Esta Política de Seguridad de la Información se establece para proteger la confidencialidad, integridad y disponibilidad de los activos de información de Tendios. Cumple con la norma ISO/IEC 27001 y el estándar ENS, y aplica a todos los empleados, contratistas y usuarios externos que accedan o utilicen los activos de información de Tendios.

Propósito

El propósito de esta política es garantizar la protección de los activos de información frente a todas las amenazas, ya sean internas o externas, deliberadas o accidentales. Su objetivo es asegurar el cumplimiento de todas las leyes, regulaciones y obligaciones contractuales aplicables.

La política establece un marco para definir, revisar y alcanzar los objetivos de seguridad de la información, y define las responsabilidades de los empleados, contratistas y usuarios externos en la protección de los activos de información de Tendios.

Adicionalmente, la política busca promover la concienciación, formar a los empleados y guiar los procesos de toma de decisiones relacionados con la seguridad de la información dentro de la organización.

Alcance

Tendios, es una compañía especializada en ofrecer una plataforma impulsada por inteligencia artificial para la contratación pública. Su tecnología ayuda a las empresas a descubrir, analizar y ganar contratos públicos, y a las instituciones públicas a optimizar sus procesos de contratación mediante inteligencia de datos avanzada y automatización. Con el objetivo de mejorar los servicios que presta a sus clientes, Tendios ha decidido implantar un Sistema de Gestión de Seguridad de la Información (SGSI).

Esta política aplica a todos los activos de información propiedad de Tendios, arrendados, gestionados o controlados de cualquier forma, incluyendo información almacenada en medios físicos o electrónicos, la información transmitida a través de redes o de cualquier canal de comunicación, así como la información procesada o manipulada por empleados, contratistas o usuarios externos.

Objetivos

Los principales objetivos de esta política son proteger la confidencialidad de la información, evitando su divulgación no autorizada; garantizar la integridad de la información, previniendo su modificación no autorizada; y asegurar su disponibilidad para los usuarios autorizados cuando sea necesaria.

Adicionalmente, esta política tiene como objetivo garantizar el cumplimiento de las leyes, regulaciones y obligaciones contractuales aplicables, como el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), la Ley 10/2021 de trabajo a distancia, entre otras, al tiempo que promueve la mejora continua del sistema de gestión de seguridad de la información (SGSI).

Organización y Responsabilidades de Seguridad

La Dirección de Tendios es responsable de proporcionar liderazgo y compromiso con la seguridad de la información, asegurándose de que existan recursos adecuados para la implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información

(SGSI), y se compromete a revisar y aprobar las políticas y procedimientos de seguridad de la información.

El Responsable del Sistema de Gestión de Seguridad de la Información (Responsable del SGSI) es responsable de desarrollar, implementar y mantener el sistema de gestión de seguridad de la información. Esto incluye la realización de evaluaciones de riesgos, la implantación de controles adecuados y la presentación de informes sobre la eficacia del sistema a la alta dirección.

Los empleados, contratistas y usuarios externos son responsables de cumplir esta política y todos los procedimientos relacionados con la seguridad de la información. Asimismo, deben informar de cualquier incidente o vulnerabilidad sospechada al Responsable del SGSI y participar en programas de formación y concienciación en seguridad de la información.

Medidas de Seguridad

En línea con nuestro compromiso de salvaguardar los activos de información y mantener la integridad de nuestras operaciones, se ha establecido un conjunto integral de medidas de seguridad. Estas medidas abarcan una variedad de estrategias y tecnologías destinadas a proteger nuestros sistemas, datos y recursos frente a amenazas potenciales, garantizando la confidencialidad, integridad y disponibilidad de la información crítica para el negocio.

- **Recursos Humanos**: Se implementan medidas de seguridad para garantizar que los empleados, contratistas y usuarios externos conozcan sus responsabilidades y estén capacitados para proteger los activos de información.
- **Seguridad Física**: Se aplican medidas de seguridad física para proteger los activos de información frente a accesos no autorizados, daños o interferencias.
- **Gestión de Activos**: Se implementan medidas para garantizar que todos los activos de información estén debidamente identificados, clasificados y protegidos durante todo su ciclo de vida. Esto incluye mantener un inventario actualizado, asignar responsables y definir pautas de uso. Se realizan auditorías y revisiones periódicas para garantizar que los activos estén adecuadamente protegidos.
- **Control de Acceso:** El acceso a los activos de información está limitado únicamente a los usuarios autorizados. Se aplican mecanismos sólidos de autenticación y autorización, y los derechos de acceso se revisan periódicamente.
- **Seguridad de Red:** Se implementan medidas para proteger la infraestructura de red de la empresa frente a accesos no autorizados, brechas y otras amenazas de seguridad. Esto incluye cortafuegos, sistemas de detección de intrusos y monitorización regular.

- **Seguridad en Operaciones**: Se establecen medidas para preservar la integridad de los procesos operativos y garantizar la ejecución segura de las actividades diarias. Esto incluye sistemas robustos de monitorización y registros que permitan identificar y responder rápidamente a actividades sospechosas.
- **Gestión de Configuración:** Se aplica un procedimiento de gestión de configuración para asegurar que todas las configuraciones de sistemas de información y activos relacionados estén gestionadas, documentadas y supervisadas sistemáticamente durante todo su ciclo de vida.
- **Desarrollo Seguro:** Se integran prácticas de seguridad en el ciclo de vida del desarrollo de software para garantizar que las aplicaciones se diseñen, desarrollen y mantengan de forma segura. Esto incluye revisiones de código, evaluaciones de vulnerabilidades y pruebas de seguridad regulares.
- **Gestión de Cambios:** Se establece un procedimiento para controlar y documentar los cambios en los sistemas de información e infraestructuras. Esto asegura que los cambios sean revisados, aprobados e implementados de manera controlada, minimizando riesgos.
- **Gestión de Riesgos**: Se realizan evaluaciones periódicas de riesgos para identificar y evaluar riesgos en los activos de información. Se aplican controles adecuados y se supervisa continuamente la eficacia de estas actividades.
- **Gestión de Datos:** La información se clasifica según su sensibilidad y criticidad. Se definen procedimientos de manejo para cada nivel de clasificación a fin de proteger la información durante todo su ciclo de vida.
- **Gestión de Incidentes**: Se establece y mantiene un proceso de gestión de incidentes para detectar, responder y recuperarse de incidentes de seguridad de la información. Todos los incidentes deben ser reportados de inmediato al equipo de respuesta designado. Los incidentes son investigados para identificar la causa raíz y prevenir su recurrencia.
- **Continuidad de Negocio:** Se establecen y mantienen planes para asegurar la continuidad de las funciones críticas en caso de una interrupción. Dichos planes son revisados, puestos a prueba y actualizados de forma periódica para garantizar su eficacia.
- **Gestión de Terceros:** Se definen y aplican requisitos de seguridad para proveedores y socios externos, realizando evaluaciones y revisiones periódicas para garantizar su cumplimiento.
- **Cumplimiento**: Se asegura el cumplimiento de todas las leyes, regulaciones y obligaciones contractuales relevantes en materia de seguridad de la información. Para ello, se llevan a cabo auditorías y revisiones periódicas para verificar dicho cumplimiento.
- **Concienciación y Comunicación**: Se proporciona formación regular en seguridad de la información a todos los empleados, contratistas y usuarios externos. Asimismo, se

promueve la concienciación sobre políticas, procedimientos y mejores prácticas en toda la organización.

Mejora de la Seguridad

Tendios está comprometida con el principio de mejora continua en sus prácticas de gestión de seguridad de la información. Para ello, se realizan evaluaciones y revisiones periódicas para identificar oportunidades de mejora en el SGSI. Los resultados de auditorías, los informes de incidentes y las sugerencias del personal se analizan de forma sistemática con el fin de implementar acciones correctivas y preventivas.

Se supervisan métricas e indicadores de rendimiento para medir la eficacia de los controles de seguridad de la información e identificar oportunidades de optimización. Estos esfuerzos de mejora continua aseguran que el SGSI se mantenga eficaz, responda adecuadamente a amenazas emergentes y se mantenga alineado con los objetivos estratégicos de Tendios.

Aprobación

Equipo Directivo,

Tendios Technologies

12 de septiembre de 2025