Política del SIG de Tecnosylva

Tecnosylva S.L.U. tiene como objetivo prioritario el alcanzar y mantener una posición relevante en la prestación de servicios de ingeniería del territorio, forestal y medioambiental, mediante el desarrollo y la integración de técnicas avanzadas de apoyo a la gestión (sistemas de información geográfica, teledetección, cartografía digital, GNSS).

Se considera, por tanto, que la adopción de un Sistema Integrado de Gestión fundamentado en la mejora continua es un elemento fundamental para cumplir con nuestros objetivos.

Esta política del Sistema Integrado de Gestión nace de la preocupación por parte de la Dirección de garantizar la plena satisfacción de las partes interesadas, así como la gestión de la seguridad de sus sistemas de información. Además, nuestra organización se siente totalmente identificada con principios orientados a la protección y prevención del medio ambiente y por lo tanto se propone la búsqueda permanente de soluciones encaminadas a evitar o minimizar el impacto ambiental de sus productos, actividades y servicios, contribuyendo a una mejor calidad de vida de la comunidad.

Este compromiso queda reflejado en los siguientes principios:

LIDERAZGO: convertirnos en un referente para los clientes que necesiten soluciones innovadoras en el ámbito de la Ingeniería del Territorio y el desarrollo de servicios basados en herramientas geoespaciales.

VOCACIÓN DE SERVICIO: mantener y fomentar las buenas relaciones con las partes interesadas para conocer y adelantarnos en la satisfacción de sus necesidades.

INNOVACIÓN: esencia de la mejora continua de nuestros servicios, impulsándonos de forma dinámica y ágil para poder adaptarnos a la evolución de las necesidades de nuestros clientes y a los cambios del mercado, garantizando productos innovadores de calidad.

MEJORA PERSONAL: incentivamos a los trabajadores y a los colaboradores para optimizar su aportación a la organización, y que esta les brinde los medios para crecer como profesionales, implicándoles en búsqueda de la excelencia y de servicio al cliente, propiciando los medios formativos y el ambiente laboral para obtenerla.

MOTIVACIÓN: motivamos al personal de Tecnosylva SL para la realización de las actividades propias de las herramientas de innovación (vigilancia, previsión, análisis, creatividad).

MEJORA DE LA GESTIÓN: cumplir con los requisitos y la mejora continua de nuestros procesos, productos y servicios para incrementar la satisfacción de las partes interesadas, definiendo las responsabilidades individuales para su posterior medición y análisis, asegurando, al mismo tiempo, que nuestra política ambiental se aplique de modo que los procesos técnicos y organizativos necesarios sean revisados regularmente y se continúen desarrollando y mejorando.

SENSIBILIDAD MEDIOAMBIENTAL: motivando a nuestro equipo y clientes a mejorar su comportamiento ambiental de manera que se alineen a nuestros principios de protección

del medio, cooperando activamente con las autoridades competentes en la materia, con el fin de alcanzar nuestros objetivos y metas.

PREVENCIÓN: adoptar todas las medidas a nuestro alcance para prevenir riesgos laborales y ambientales.

CUMPLIMENTO DEL MARCO LEGAL: asegurar el cumplimiento de las disposiciones para el desarrollo de nuestros servicios y la protección del medio ambiente que contemplan los impactos ambientales, y optimizar del consumo de energía y recursos.

TRANSFERENCIA DE TECNOLOGÍA: buscar entidades de interés para afrontar nuevos retos de I+D+i que permitan desarrollar proyectos innovadores.

EXPANSIÓN: reinvertir los beneficios obtenidos para fomentar el crecimiento y la autofinanciación continuos de la empresa, asegurando la rentabilidad y el correcto desarrollo de la actividad comercial y de la atención a las necesidades de los clientes.

RESULTADOS E INNOVACIÓN: establecer una metodología de protección y explotación de los resultados, prestando especial atención a aquellos éxitos que no están contemplados en el estado del arte nacional.

SEGURIDAD DE LA INFORMACIÓN: hacer patente el compromiso de la dirección en relación con la seguridad de la información, en consonancia con la estrategia de negocio. Para ello, se procede a definir, desarrollar e implantar los controles técnicos y organizativos que resulten necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por la empresa. La seguridad de la información se entiende como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más avanzados.

PROTECCIÓN DE DATOS: garantizar el cumplimiento de la legislación vigente en materia de protección de datos de carácter personal y sociedad de la información, así como todos los requerimientos legales, reglamentarios y contractuales que resulten aplicables.

CULTURA DE SEGURIDAD: crear una “cultura de seguridad” tanto interna (en relación con todo el personal), como externa (en relación con los clientes y proveedores).

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

La Dirección de TECNOSYLVA SL se compromete a revisar periódicamente esta política, así como a velar por el cumplimiento de los principios establecidos en la misma por parte de toda la organización. Esta política es comunicada y puesta a disposición de todos los afectados, tanto internos como externos.

Alcance

La presente política afecta integralmente a Tecnosylva y al sistema de información que soporta los servicios y los procesos tanto internos como externos necesarios para desarrollar y cumplir con los objetivos de negocio.

En el ámbito del sistema de gestión de la calidad, el alcance:

> afecta a proyectos de ingeniería forestal y medioambiental, trabajos de mediciones y de cartografía digital y diseño, el desarrollo de aplicaciones informáticas relacionadas con las actividades anteriores.

La política de seguridad de la información, será de aplicación a toda la información del sistema con independencia del soporte o medio, a los activos de información, a todo el personal de Tecnosylva incluso a terceros que accedan al sistema.

En el ámbito del Esquema Nacional de Seguridad, se considera como alcance:

> los sistemas de información (administración y operación de infraestructuras de red, comunicaciones, datos y puesto de usuario) que soportan los servicios de consultoría tecnológica de gestión forestal y emergencias, mediante sistemas de información geográfica, teledetección, integración de técnicas avanzadas de modelización, incluyendo el desarrollo de herramientas informáticas para la toma de decisiones, de acuerdo a la categorización vigente.
>
> El nivel de categorización es MEDIO, como se ha determinado en TS_RG_Categorizacón.

En el ámbito de la norma ISO 27001, se considera como alcance:

> el Sistema de información que da soporte a los procesos de: desarrollo de aplicaciones basadas en tecnologías de información geográfica y comunicaciones (geotic's) (sistemas de información geográfica, sistemas de posicionamiento, teledetección y cartografía temática digital) y servicios de ingeniería del territorio (estudios de planificación y ambientales, estudios sectoriales, planificación regional y comarcal, proyectos de ingeniería aplicada). De acuerdo con la declaración de aplicabilidad en vigor.

Compromisos de la Dirección

El Gerente de TECNOSYLVA está comprometido con el desarrollo e implementación del Sistema Integrado de Gestión y con la mejora continua de su eficacia.

El Gerente de TECNOSYLVA está comprometido con la seguridad de la compañía, además de por sus cargos, por formar parte del Comité de Seguridad, y ser así parte activa del mismo.

El Gerente:

- Comunica a la organización la importancia de satisfacer tanto los requisitos del cliente como los de seguridad, los legales, reglamentarios, y las obligaciones contractuales.
- Establece y comunica el alcance del SIG.
- Define y comunica la Política del Sistema Integrado de Gestión, normas y procedimientos.
- Comunica la Política de Seguridad y la importancia de cumplir con ella a clientes y a proveedores.
- Asegura el establecimiento y la comunicación de los objetivos del Sistema Integrado de Gestión.

- Lleva a cabo y dirige las revisiones por la Dirección anuales.
- Vela por que se realicen las auditorías internas del SIG, anualmente.
- Asegura que se revisan los resultados de las auditorías para identificar oportunidades de mejora.
- Asegura la provisión y disponibilidad de recursos.
- Asegura que se gestionan y se evalúan los riesgos de seguridad de la información a intervalos planificados.
- Define el enfoque a tomar para la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos.
- Aprueba los niveles de riesgo aceptables para la organización.
- Establece roles y responsabilidades en materia de seguridad.
- Determina las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección está reflejado en las siguientes políticas.

Política de seguridad

La Política de Seguridad tiene por objeto proteger los activos de información del sistema de información de TECNOSYLVA, así como los activos de información de nuestros clientes con los que exista un acuerdo contractual, ante cualquier amenaza, sea interna o externa, deliberada o accidental. Se busca garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con urgencia a los incidentes para recuperarse lo antes posible y minimizar el impacto.

TECNOSYLVA tiene implantado, y mejora continuamente, un Sistema de Gestión de la Seguridad de la Información acorde con la norma UNE-ISO/IEC 27001:2013 y el RD3/2010 por el que se regula el Esquema Nacional de Seguridad (ENS).

La Política de Seguridad es de aplicación sobre todo el personal de TECNOSYLVA, incluyendo sus contratistas y el personal contratado temporalmente; afecta a cualquier tipo de información, tanto la que sea propiedad de TECNOSYLVA como la que procede de clientes, con independencia del soportes o medio en el que se encuentre, tipología o categoría; y aplica a cualquier activo de información propiedad de la organización que afecte al sistema.

La Seguridad de la Información está implícita en cada uno de los puntos de esta Política, e integrada en los procesos de negocio como herramienta clave para conseguir los objetivos de negocio de TECNOSYLVA. Esta política queda alineada plenamente con los objetivos de negocio e integrada en la estrategia de la organización.

Objetivos

Los objetivos del Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización son:

- Mantener una gestión adecuada del SGSI de acuerdo con los estándares de seguridad y las buenas prácticas del sector, llevando acabo todo esto de manera que se aseguren ventajas competitivas para la organización.

- Proteger la información interna relacionada con la prestación de los servicios, considerando las dimensiones de:
    - *Disponibilidad* para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
    - *Integridad* para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
    - *Confidencialidad* para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva. Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
    - *Autenticidad* que permita verificar y garantizar que el origen de la información a la que se accede o modifica es correcto. Se han establecidos los procedimientos e implementado los sistemas buscando que los accesos a la información no puedan generar dudas en este sentido, pudiendo conocer y contrastar al autor de toda información.
    - *Trazabilidad* de los accesos y modificaciones de la información que permita conocer quién, cuándo y cómo se ha realizado. Para ello se han implantado los sistemas y registros adecuados para la realización de los análisis y detección de accesos no autorizados tanto a nivel informático como físico de manera que toda acción quede registro del autor.
- Establecer anualmente objetivos específicos en relación a la Seguridad de la Información, que garanticen la mejora continua del SGSI, siendo estos consistentes con los presentes objetivos.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo a su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos.
- Establecer los medios necesarios para garantizar la continuidad del negocio de la organización.
- Cumplir con los requisitos del negocio, las obligaciones legales y las obligaciones contractuales de seguridad.
- Asegurar que los activos de la organización solo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, sus perfiles definidos o según asignaciones extraordinarias.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de la organización en relación a los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.
- Reflejar en la Declaración de Aplicabilidad del SGSI los objetivos de control definidos para el SGSI de TECNOSYLVA, basados en los controles recogidos en el Anexo A de la norma 27001:2013.
- Sancionar cualquier violación a esta política, así como a cualquier política o procedimiento del SGSI.

Legislación aplicable y requisitos contractuales

Se identifican las siguientes obligaciones legales aplicables a la organización en relación a la seguridad de la información:

- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) LOPDGDD – Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.**
    - Aplicabilidad: tratamiento de datos de carácter personal propios tanto de Tecnosylva como de empresas externas (encargados de tratamiento, destinatarios).
- **LSSICE – Ley de Servicios de la Sociedad de Información y del Comercio Electrónico.**
    - Aplicabilidad: actividades comerciales en internet de la organización.
- **Copyright – Derecho de autor.**
    - Aplicabilidad: licencias software.
- ***Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.***
- ***Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.***
- ***Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas.***
- ***Convenio Colectivo Nacional de Empresas de Ingeniería y Oficinas de Estudios Técnicos.***
- ***Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad***
- ***Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad***
- ***Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información***
- ***Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad***

Se identifican las siguientes obligaciones empresariales establecidas por la organización:

- **ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI).**
  - Aplicabilidad: alcance del SGSI.
- **UNE EN ISO 9001:2015 – Sistemas de Gestión de la Calidad (SGC).**
  - Aplicabilidad: alcance del SGC.
- ***Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.***
  - Aplicabilidad: alcance del SGSI.

Además, se consideran los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de seguridad.

Estructura de seguridad

Se establecen los roles de seguridad, definiendo para cada uno, los deberes y responsabilidades de su cargo, el procedimiento para su designación y renovación, así como la resolución de conflictos en el documento TS_PR_Estructura_Seguridad_Tecnosylva.

Además, en el TS_MC_Organigrama, se establece la estructura del Comité de Seguridad para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

Los roles y responsabilidades en relación al SGSI son comunicados a las nuevas incorporaciones y recordados periódicamente a todo el personal de la organización.

Principios de seguridad

a) Seguridad como proceso integral.
   TS_MC_Manual
   Documentación de COMUN_SISTEMAS

b) Gestión de la seguridad basada en los riesgos.
   TS_PR_Análisis Gestión riesgos y sus registros asociados TS_RSI_Análisis de riesgos y TS_RSI_Plan Tratamiento_Riesgos.

c) Prevención, detección, respuesta y conservación.
   Documentación de COMUN_SISTEMAS

d) Existencia de líneas de defensa
   TS_PR_Arquitectura_Seguridad

e) Vigilancia continua.
   Documentación de COMUN_SISTEMAS

f) Reevaluación periódica.

TS_PR_Arquitectura_Seguridad, TS_PR_Gestion_Capacidades, revisiones y auditorias programadas

g) Diferenciación de responsabilidades.
TS_PR_Estructura_Seguridad_Tecnosylva

Requisitos mínimos de seguridad

La política de seguridad de Tecnosylva articula la gestión continuada mediante aplicación de los siguientes requisitos mínimos desarrollados en la documentación y procedimientos implementados. Se indican los principales documentos del sistema donde se tratan estos requisitos mínimos, si bien no son os únicos, puesto que como todo sistema se encuentra interrelacionado:

h) Organización e implantación del proceso de seguridad.
TS_RSI_SOA resume y permite trazar toda la documentación e implementación del proceso

i) Análisis y gestión de los riesgos.
TS_PR_Análisis Gestión riesgos y sus registros asociados TS_RSI_Análisis de riesgos y TS_RSI_Plan Tratamiento_Riesgos.

j) Gestión de personal.
TS_PR_RRHH es el procedimiento que recoge los aspectos principales, pero el registro TS_RSI_Clausulas resume los principales aspectos

k) Profesionalidad.
Centrada en la documentación de COMUN_SISTEMAS

l) Autorización y control de los accesos.
TS_PR_Accesos y TS_PR_Autorizaciones

m) Protección de las instalaciones.
TS_PR_Infraestructura

n) Adquisición de productos.
TS_PR_Compras

o) Seguridad por defecto.
TS_PR_Arquitectura_Seguridad

p) Integridad y actualización del sistema.
TS_PR_Arquitectura_Seguridad

q) Protección de la información almacenada y en tránsito.
TS_PR_Arquitectura_Seguridad

r) Prevención ante otros sistemas de información interconectados.
TS_PR_Arquitectura_Seguridad

s) Registro de actividad.

TS_PR_Monitorización

t) Incidentes de seguridad.
TS_PR_Gestion_Incidentes

u) Continuidad de la actividad.
TS_PR_Plan_Autoproteccion

v) Mejora continua del proceso de seguridad.
TS_PR_Arquitectura_Seguridad, TS_PR_Gestion_Capacidades, revisiones y auditorias programadas

Directrices documentación de seguridad del sistema

La documentación generada dentro del SGSI es controlada y aprobada por el Comité de Seguridad.

Esta documentación se encuentra localizada en un directorio de acceso restringido, únicamente haciéndose públicos los documentos que se consideran que deben ser conocidos por todos a través de la Intranet de Tecnosylva.

APROBADO POR
 Gerente En León a 12/02/2024