Política de seguridad de la información

-GRUPO SISTEPLANT-

B- CONTROL DE CAMBIOS

Rev	Fecha	Descripción de la revisión
1	01/04/2023	Edición inicial
2	19/06/2024	Adaptación al Esquema Nacional de Seguridad
3	23/04/2026	Actualizacion de Roles y Funciones

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

SISTEPLANT es una empresa de servicios líder en el sector de la ingeniería industrial y organización, y nuestra misión es ayudar activamente a prosperar a nuestros clientes utilizando técnicas innovadoras de organización y las más avanzadas tecnologías de información y fabricación. Soñamos, Innovamos y aceptamos desafíos.

Nuestra misión es ayudar activamente a prosperar a nuestros clientes utilizando técnicas innovadoras de organización y tecnologías avanzadas de información y fabricación.

Los objetivos fundamentales de nuestro sistema de gestión de seguridad de la información son:

- Proteger los activos de información conforme a su valor o importancia.
- Garantizar la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información.
- Gestionar los riesgos identificados de manera diligente.
- Preservar la privacidad de clientes, empleados, proveedores y terceras partes.
- Garantizar el cumplimiento de los requisitos aplicables, y en especial los legales.
- Mejorar continuadamente el sistema de seguridad de la información.

Para alcanzar estos objetivos generales la Dirección de esta empresa asume el firme compromiso de optimizar su política de seguridad de la información basada en los siguientes factores:

- **Prevención de Riesgos:** Establecer las directrices y medios necesarios en materia de prevención de riesgos con el objetivo fundamental de eliminarlos o mitigarlos
- **Compromiso con la protección del medio ambiente:** Reducir y prevenir los impactos medio ambientales generados por nuestras actividades, productos o servicios.
- **Requisitos Legales**: Entender los requisitos legales y otro tipo de requisitos especificados por nuestros clientes como un conjunto de mínimos a cumplir.
- **Difusión:** Difundir y promover la mejora de la seguridad de la información.
- **Grupos de interés:** Participación conjunta con todos nuestros STAKEHOLDERS por una mejora de la seguridad de la información.
- **Capacitación:** Capacitación constante de todos nuestros profesionales, en conocimientos técnicos, y habilidades, fomentando su participación y compromiso con esta política, la mejora del sistema y la seguridad de la información.
- **Seguimiento**: Establecer indicadores a todos los niveles que nos permitan tomar decisiones basadas en la evidencia.
- **Mejora continua:** Establecer y revisar periódicamente objetivos y metas, que proporcionen un marco de referencia para la mejora continua de los procesos y del desarrollo sostenible.
- **Analizar**: Analiza y evaluar las desviaciones que puedan producirse en materia de seguridad de la información y establecer las acciones correctivas y oportunidades de mejora necesarias.
- **Sistema integrado:** Elaboración participativa de todos los grupos de la organización, a todos los niveles, siendo conscientes de la aportación a los objetivos del sistema y las repercusiones de los incumplimientos.

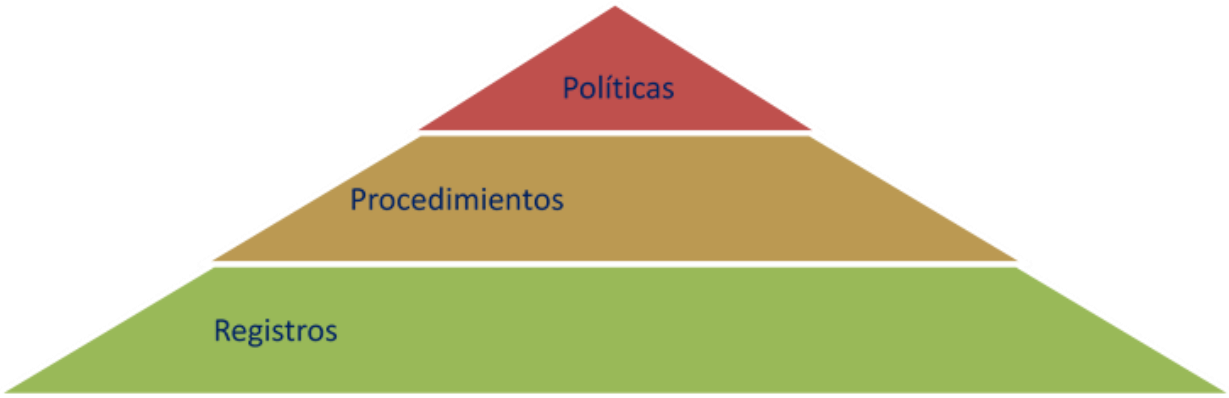
Legislación aplicable

Uno de los objetivos debe ser el de cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. Para ello, el marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- 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
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
- Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)
- REGLAMENTO (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- 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 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 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
- 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

Estructura documental

Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:



La gestión de nuestro sistema se encomienda al Responsable de Sistemas Informáticos y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

Organización de seguridad

La responsabilidad esencial recae sobre la Dirección General de la organización, ya que esta es responsable de organizar las funciones y responsabilidades y de facilitar los recursos adecuados para conseguir los objetivos del ENS. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información	-Tomar las decisiones relativas a la información tratada
Responsable de los servicios	-Coordinar la implantación del sistema -Mejorar el sistema de forma continua
Responsable de la seguridad	-Determinar la idoneidad de las medidas técnicas -Proporcionar la mejor tecnología para el servicio
Responsable del sistema	-Implantación, gestión y mantenimiento de las medidas de seguridad.
Responsable de Personas	Definir las políticas en relación con el personal
Responsable del Sistema de Gestión de la Seguridad de la Información	-Garantizar el cumplimiento de la normativa y coordinar el correcto funcionamiento del sistema.
Dirección	-Proporcionar los recursos necesarios para el sistema -Liderar el sistema

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema Registro de responsables, roles y responsabilidades, así como con la Guía CCN 801

Comité de Seguridad

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad.

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité.

Los miembros del comité de seguridad de la información son:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de la Seguridad
- Responsable de Personas
- Responsable del Sistema
- Responsable del Sistema de Gestión de la Seguridad de la Información

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

Toma de decisiones

Las decisiones que impliquen cualquier cambio en el sistema, se tomarán por votación a mayoría simple en el seno del Comité de Seguridad.

Resolución de conflictos

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección General.

La Dirección

A 05 de Febrero de 2026