Índice

Control de Versiones

Versión	Fecha	Autor	Comentarios
0	20/12/2013	Responsable de Calidad	Creación del documento
1	09/07/2021	JG	Creación del documento
2	25/04/2024	TU	Revisión del documento y adecuación
3	31/01/2025	TU	Adecuación del documento
4	23/03/2026	TU	Revisión del documento y adecuación

1. Introducción

Este documento expone la política de seguridad de la información de INTEPLAST, como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de la norma ISO 27001.

La **información** es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Este activo debe ser adecuadamente protegido, mediante las medidas de seguridad necesarias, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas o personas que intervengan en su conocimiento, procesado o tratamiento.

La **seguridad de la información** es la protección de este activo, con la finalidad de asegurar la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio. Es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos. Es fundamental la máxima colaboración e implicación de **todo el personal de la empresa.**

La Dirección de INTEPLAST demuestra su compromiso explícito con el Sistema de Gestión de Seguridad de la Información (SGSI), liderando y apoyando la implantación, mantenimiento y mejora continua del mismo conforme a los requisitos de la norma ISO/IEC 27001:2022

2. Propósito

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de la empresa, asegurando para ello la disponibilidad, integridad y confidencialidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

Esta política establece el marco de referencia para definir los objetivos de seguridad de la información y para la aplicación coherente de controles y medidas de seguridad dentro del SGSI.

3. Alcance

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de INTEPLAST abarca los sistemas de información que dan soporte a las actividades de negocio relacionadas con la producción de piezas plásticas de precisión mediante inyección de materiales termoplásticos, sobremoldeados sobre componentes metálicos, así como montaje y operaciones de acabado.

El SGSI se aplica a todos los procesos, personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información gestionada o propiedad de INTEPLAST dentro del marco de estos procesos. Esto incluye datos confidenciales, información comercial, propiedad intelectual y cualquier otro activo de información relevante para la organización.

El cumplimiento de esta política de seguridad de la información es obligatorio para todas las personas con acceso a la información descrita, independientemente del soporte en el que se

encuentre y de la relación contractual con la empresa. Esto incluye a empleados, proveedores, clientes y cualquier otra tercera parte que tenga acceso a los sistemas o información de INTEPLAST.

Como parte del SGSI, se llevará a cabo la identificación, evaluación y tratamiento de los riesgos de seguridad de la información de acuerdo con las necesidades de la organización. Asimismo, INTEPLAST se compromete a la mejora continua del sistema, asegurando su efectividad a través de revisiones periódicas, auditorías y la aplicación de controles adecuados para mitigar riesgos y garantizar la protección de la información.

El alcance del SGSI se revisa periódicamente para asegurar su adecuación frente a cambios organizativos, tecnológicos, legales o contractuales.

4. Contexto de la organización

INTEPLAST opera en un entorno altamente competitivo y regulado, donde la seguridad de la información es fundamental para garantizar la continuidad del negocio.

INTEPLAST identifica y analiza los factores internos y externos que pueden influir en la consecución de los objetivos del SGSI, así como las necesidades y expectativas de las partes interesadas relevantes.

Las principales partes interesadas incluyen, entre otras: clientes, empleados, proveedores, socios tecnológicos, entidades reguladoras y auditores, cuyos requisitos de seguridad de la información son considerados dentro del SGSI.

Se han identificado factores externos como el cumplimiento de normativas de seguridad y privacidad, así como amenazas cibernéticas crecientes. A nivel interno, la empresa debe gestionar la capacitación del personal, la infraestructura tecnológica y la implementación de controles de acceso adecuados para mitigar riesgos.

Adicionalmente, INTEPLAST considera el cambio climático como un factor externo relevante que puede impactar en la disponibilidad de los servicios, la continuidad del negocio y la seguridad de la información, especialmente en lo relativo a interrupciones de suministro eléctrico, afectación a infraestructuras, disponibilidad de proveedores críticos y variaciones en el entorno operativo. Estos factores son tenidos en cuenta dentro del análisis de contexto y en el proceso de gestión de riesgos del SGSI.

5. Objetivos y fundamentos

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

1) **Cumplimiento normativo:** todos los sistemas de información se ajustan a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

2) **Gestión del riesgo:** se minimizan los riesgos hasta niveles aceptables y se busca el equilibrio entre los controles de seguridad y la naturaleza de la información. Los objetivos de seguridad son establecidos, revisados y coherentes con los aspectos de seguridad de la información.

   La organización tiene en cuenta los impactos potenciales derivados del cambio climático en la disponibilidad de la información, la resiliencia de los sistemas y la continuidad del negocio, incorporando estos factores en los procesos de análisis de riesgos, continuidad y toma de decisiones en materia de seguridad de la información.

3) **Formación y concienciación:** se articulan programas de formación, sensibilización y campañas de concienciación para todos los usuarios con acceso a la información, en materia de seguridad de la información.

4) **Disponibilidad, integridad y confidencialidad:**

   - Se garantiza la **disponibilidad** de la información, asegurándose la continuidad del negocio soportado por los servicios de la información mediante planes de contingencia.
   - Se asegura la **integridad** de la información con la que se trabaja, de modo que sea concisa y precisa, incidiéndose en la exactitud, tanto de su contenido como de los procesos involucrados.
   - Se garantiza la **confidencialidad** de la información, de tal manera que solo tengan acceso a la misma las personas autorizadas.

5) **Proporcionalidad:** la implantación de controles que mitiguen los riesgos de seguridad de los activos se hace buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el riesgo.

6) **Responsabilidad:** todos los miembros de INTEPLAST son responsables en su conducta en cuanto a la seguridad de la información, cumpliendo con las normas y controles establecidos.

7) **Mejora continua:** se revisa de manera recurrente el grado de eficacia de los controles de seguridad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución del riesgo y del entorno tecnológico.

8) **Forma medible**: Los objetivos de seguridad de la información se definen de forma medible, alineados con los riesgos identificados y revisados al menos anualmente

6. Roles y resposabilidades

La Dirección de INTEPLAST asigna los roles y responsabilidades necesarios para una correcta gestión de la seguridad de la información, incluyendo:

- **Responsable de Seguridad**, encargado de coordinar, mantener y mejorar el sistema.
- **Responsables de activos de información**, responsables de la protección adecuada de los mismos.
- Todo el personal, que debe cumplir esta política y los procedimientos derivados.

7. Requisitos

Las políticas de seguridad de la información consideran los requisitos desde 3 enfoques:

7.1. La estrategia del negocio

En la actualidad la información se ha convertido en uno de los activos más importantes para las empresas, por lo que podríamos afirmar que estas basan su actividad en sistemas de información con soporte tecnológico. Por eso mismo debemos tener muy presente que **proteger la información de la empresa es proteger el negocio** y que es necesario llevar a cabo una gestión planificada de actuaciones en materia de ciberseguridad.

INTEPLAST ha tomado la decisión de **gestionar los sistemas de la información utilizando las mejores prácticas nacionales e internacionales en Seguridad de la información** y es por ello que ha tomado la decisión de seguir las directrices conforme al estándar ISO 27001:2022, con el fin de alcanzar los siguientes objetivos:

1) **Incrementar el valor añadido de su cartera de servicios** tanto en el apartado proyectos como en el de servicios, donde INTEPLAST está haciendo un gran esfuerzo para posicionarse como un referente de calidad en el mercado.
2) Alinearse con todo aquello que se está definiendo en su plan estratégico: La **apuesta decidida por la protección de los activos de negocio propios y los de sus clientes**.
3) **Reforzar la confianza en la seguridad de sus sistemas de información** tanto para aquellos clientes que ya llevan tiempo trabajando con INTEPLAST, como para todos aquellos que decidan apostar por sus servicios en el futuro.

7.2. La normativa, legislación y contratos

Para INTEPLAST **es esencial el cumplimiento de toda la normativa y legislación vigente** aplicable a la misma, ya que es la base para evitar sanciones administrativas que podrían perjudicar la continuidad de las actividades de la organización.

Principalmente se considera:

- 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 esos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Asimismo, también lo es el **cumplimiento de los compromisos contractuales** con otras organizaciones.

En cuanto al **compliance legal**, el departamento responsable del seguimiento y cumplimiento de la normativa vigente es **Recursos Humanos y Financiero**, con el **soporte del departamento legal de Vila Riba**.

8. Gestión de riesgos y controles de seguridad

INTEPLAST realiza de forma periódica la identificación, análisis y tratamiento de los riesgos de seguridad de la información, considerando tanto factores internos como externos, incluyendo aquellos derivados del cambio climático que puedan afectar a la disponibilidad de los sistemas, infraestructuras y servicios críticos.

Los controles de seguridad se seleccionan conforme al Anexo A de la norma ISO/IEC 27001:2022, y su aplicación se documenta en la Declaración de Aplicabilidad (SoA).

9. Gestión de incidentes de seguridad de la información

INTEPLAST establece mecanismos organizativos y técnicos para la detección, notificación, gestión y resolución de incidentes de seguridad de la información, incluyendo la comunicación al Responsable de Seguridad , el registro y análisis de los incidentes, y la adopción de acciones correctivas y preventivas que eviten su recurrencia.

10. Relación con otras políticas y procedimientos

Esta Política de Seguridad de la Información se desarrolla y complementa mediante normas, procedimientos y directrices internas específicas, tales como control de accesos, copias de seguridad, continuidad del negocio, gestión de activos y seguridad física y lógica.

11. Revisión y aprobación

Esta política es aprobada por la Dirección de INTEPLAST y se revisa al menos una vez al año o cuando se produzcan cambios significativos en el negocio, la organización, la tecnología o los riesgos de seguridad de la información.

12. Revisión objetivos anuales

La revisión de los objetivos globales es un proceso fundamental para garantizar su éxito a largo plazo en un mercado altamente competitivo y en constante evolución. Este proceso implica analizar el entorno empresarial, evaluar el rendimiento pasado y establecer nuevos objetivos estratégicos.

Incluyendo la evaluación de tendencias ambientales y factores relacionados con el cambio climático que puedan influir en los objetivos estratégicos y de seguridad de la información.

A continuación, se detallan los pasos para llevar a cabo una revisión efectiva de los objetivos globales para la seguridad de la información.

1- Plan estrategico 2025 → 2028
2- Revisión de la misión y visión de Inteplast
3- Análisis del entorno
4- Análisis DAFO (Fortalezas , Oportunidades , Debilidades y Amenazas)
5- Revisión de los objetivos anteriores
6- Establecimiento de nuevos objetivos
7- Desarrollo de estrategias
8- Evaluación y seguimiento.
9- Comunicación de los objetivos