universal
Servicios Gráficos

Política de Seguridad de la Información

PSI 01

16/06/2025

Departamento de Seguridad Informática

-Documento Público-

PSI 01
Versión 02

Control Documental

Revisado y aprobado por Dirección:

Servicios Gráficos Plenos
Imprenta UNIVERSAL, S.L.
Mungialde Etorbidea, 26
48160 DERIO (Bizkaia)
C.I.F.: B48145155

Histórico de modificaciones

CÓDIGO	VERSIÓN	FECHA	COMENTARIO
PSI	1,0	08/05/2023	Creación del documento
PSI	2,0	16/06/25	Documento revisado

-Documento Confidencial-

1 Objeto

Recoger la existencia de las Políticas de Seguridad de la Información de IMPRENTA UNIVERSAL, que proporcionarán las indicaciones para la gestión y soporte de la seguridad de la información, de acuerdo con los requisitos empresariales de la entidad, con la legislación y las normativas aplicables, además de establecer el alcance del SGSI.

Este procedimiento será de aplicación a todo el personal de IMPRENTA UNIVERSAL implicado en el desarrollo, implantación y mantenimiento del Sistema de Gestión de Seguridad de la Información.

2 Responsabilidades

Es responsabilidad de la Dirección de la Empresa establecer las metas de la Seguridad de la Información a fin de garantizar un ambiente controlado, tanto para la empresa como para mantener lo pactado con sus clientes, asumiendo de esta manera su responsabilidad corporativa.

Es Responsabilidad del Comité de Gestión de Seguridad de la Información, revisar una vez al año las Políticas de Seguridad de la Información, siendo el Responsable del SGSI quién controlará que se efectúa la revisión.

Los Usuarios de la Seguridad de la Información, serán responsables de asumir y cumplir con las Políticas de Seguridad.

3 Desarrollo

3.1 Misión y visión

La misión de Imprenta Universal es en la fabricación, impresión y personalización de documentos de seguridad.

Somos una empresa con amplia experiencia y conocimiento, siendo en la actualidad uno de los principales fabricantes de impresos de seguridad de todo el Estado.

Colaboramos con distintas Universidades, siendo proveedores en el suministro de los Títulos Oficiales, SETs, Títulos Propios, y otros Diplomas y Certificados. Nuestras muestras han sido analizadas por el Departamento de Ingeniería, I+D+i y Laboratorio de la Fábrica Nacional de Moneda y Timbre.

Nuestra visión es la de ser un referente nacional por seguridad y calidad.

3.1.1 Políticas para la seguridad de la información

Todas las políticas de seguridad de la información que se encuentran implantadas en IMPRENTA UNIVERSAL, han sido previamente aprobadas por la Dirección de la organización.

-Documento Confidencial-

Las políticas de seguridad de la información son comunicadas al personal a través de la intranet mientras que, para las partes interesadas, la comunicación de las políticas se lleva a cabo a través de correo electrónico.

- *Política Corporativa de Seguridad de la Información*

En IMPRENTA UNIVERSAL la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, IMPRENTA UNIVERSAL implementa un Sistema de Gestión de Seguridad de la Información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales y contractuales vigentes y otros requisitos de nuestros clientes y partes interesadas.

Como punto fundamental de la política está la implantación, operación y mantenimiento de un SGSI basado en ISO 27001.

Aspectos básicos de la política de seguridad de la información de IMPRENTA UNIVERSAL:

- Asegurar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Cumplir todos los requisitos legales aplicables.
- Tener un plan de continuidad que permita recuperarse de un desastre en el menor tiempo posible.
- Formar y concienciar a todos los empleados en materia de seguridad de la información.
- Gestionar adecuadamente todas las incidencias ocurridas.
- Todos los empleados son informados de sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Comunicar a todo el personal de IMPRENTA UNIVERSAL y todo aquel que trabaje en su nombre el obligado cumplimiento de esta Política, incluyendo contratistas y visitantes a nuestras instalaciones.
- Hay un responsable de seguridad encargado del sistema de gestión la seguridad de la información (SGSI) de la organización.
- Mejorar de forma continua el sistema de gestión de seguridad de la información.

Los objetivos de esta Política serán:

a) Garantizar que los activos de información reciban un apropiado nivel de protección.
b) Clasificar la información para señalar su sensibilidad y criticidad.
c) Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Esta Política se aplica a toda la información administrada en la Empresa, cualquiera que sea el soporte en que se encuentre.

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad de la Información es el encargado de asegurar que para la utilización de los recursos de la tecnología de información se contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rotulado de información de su departamento sea cumplimentado de acuerdo a lo establecido en la presente Política.

- ***Política de Seguridad del Personal***

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Información de la Empresa en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos a las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal del Empresa y al personal externo que efectúe tareas dentro del ámbito de la Empresa.

El Departamento de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información y a los propietarios de la información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tendrá conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad de la información.

El Responsable de Seguridad de la Información participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la Empresa, en el

asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad de la información.

Todo el personal de la Empresa es responsable del reporte de debilidades e incidentes de seguridad de la información que oportunamente se detecten.

- *Política de Gestión de Comunicaciones y Sistemas*

Los objetivos de la gestión de comunicaciones y sistemas son:

a) Garantizar el funcionamiento correcto y seguro de las instalaciones y sistemas informáticos y comunicaciones.
b) Establecer responsabilidades y procedimientos para su gestión, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Responsable del Departamento Técnico, determinará los requerimientos para proteger la información de la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

- *Política de Control de Accesos a los Sistemas de Información*

Controlar el acceso a los sistemas de información tiene como objetivos:

a) Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
b) Implementar seguridad en los accesos de usuarios por medio de técnicas de autentificación y autorización.
c) Controlar la seguridad en la conexión entre la red de la Empresa y otras redes públicas o privadas.
d) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
e) Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
f) Garantizar la seguridad de la información cuando se utilizan portátiles y ordenadores personales para trabajo remoto.

- *Política de Desarrollo y Mantenimiento de Sistemas*

La seguridad en el desarrollo y mantenimiento de sistemas tiene como objetivos:

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas informáticos.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de las aplicaciones y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la Empresa.

-Documento Confidencial-

El Responsable de Seguridad de la Información junto con el Propietario de la Información definirá los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la Información definirá junto con el Responsable del Departamento Técnico, los métodos de encriptación a utilizar.

- *Política de Administración de la continuidad de las actividades de la empresa*

La seguridad en la administración de la continuidad de las actividades de la empresa tiene como objetivos:

a) Minimizar los efectos de las posibles interrupciones de las actividades normales de la Empresa (sean éstas resultado de desastres naturales, accidentes, fallos en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
b) Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
c) Maximizar la efectividad de las operaciones de contingencia de la Empresa con el establecimiento de planes que incluyan al menos las siguientes etapas:

    1. Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.

    2. Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

    3. Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

d) Asegurar la coordinación con el personal de la Empresa y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

El Responsable de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos o actividades de la Empresa.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Empresa.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Empresa.

-Documento Confidencial-

- ***Normativa aplicable***

Los requisitos legales aplicables a nuestro sistema son los siguientes:

- 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).

- ***Responsabilidades***

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	❑ Determinar los requisitos de los servicios prestados
Responsable de la seguridad	❑ Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios ❑ Firmar la Declaración de Aplicabilidad ❑ Aprobar, en su caso, las medidas compensatorias
Responsable del sistema	❑ Coordinar la implantación del sistema ❑ Mejorar el sistema de forma continua ❑ Implantación, gestión y mantenimiento de las medidas de seguridad.
Dirección	❑ Proporcionar los recursos necesarios para el sistema ❑ Liderar el sistema

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.

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

- *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 del sistema.

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

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento. La toma de decisiones se realiza por mayoría simple, teniendo la Dirección voto de calidad para el caso de empates.

Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

- *Estructura documental*

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

-Documento Confidencial-

La gestión de nuestro sistema se encomienda al Responsable de Gestión 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.

3.1.2 Revisión de las políticas para la seguridad de la información

Cada Responsable de Departamento, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad de la información establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad de la Información, realizará revisiones periódicas de todas las áreas de la Empresa a efectos de garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.

b) Proveedores de sistemas.

c) Propietarios de información.

d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de las políticas, normas, procedimientos y otros requisitos de seguridad de la información aplicable

-Documento Confidencial-

-Documento Confidencial-