PSGSI-00 Política de seguridad de la información

03 ABRIL 2025 – V2.7

ISO **9001** ISO **27001** ISO **14001** ISO **27018**

Integrity360 PCI DSS APPROVED

CNMC COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

Índice

Control documental

Control de cambios

VERSIÓN	FECHA	ANOTACIONES / CAMBIOS	AUTOR	CARGO
00	26/10/2010	Edición inicial.	-	-
01	26/10/2010	Revisión. Sin cambios.	-	-
02	22/10/2012	Cambio de razón social a Atiun Comunicaciones S.L.U.	-	-
1.3	04/05/2013	Revisión. Sin cambios.	-	-
1.4	20/09/2013	Inclusión de la gestión y el análisis del riesgo como parte del compromiso de Atiun.	-	-
1.5	24/04/2015	Revisión. Sin cambios.	-	-
1.6	26/08/2016	Revisión. Sin cambios.	-	-
1.7	09/05/2018	Actualización de las líneas de actividad	-	-
2.0	06/06/2018	Cambio de razón social a ALISYS DIGITAL S.L.U	JMMP	Técnico de RRHH, Organización y Excelencia
2.1	04/06/2019	Revisión anual. Sin cambios.	JMMP	Técnico de RRHH, Organización y Excelencia
2.2	10/05/2020	Revisión anual. Sin cambios.	JMMP	Técnico de RRHH, Organización y Excelencia
2.3	05/02/2021	Inclusión del alcance del sistema, principios fundamentales, comité de Seguridad de la Información, compromiso de mejora continua. Inclusión del estándar PCI DSS como referencia dentro de los objetivos de seguridad	IVLL	Resp. Sistema de Gestión
2.4	29/09/2022	Adaptación de la política a los requisitos marcados por el Esquema Nacional de seguridad. Adición de los puntos: 2.4.1, 2.6, 2.9.1, 2.10, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.19 y 2.20.	ACC IVLL	Ingeniero de procesos
2.5	15/05/2023	Inclusión las correspondientes referencias a la norma ISO 27018. Inclusión compromisos relacionados con la norma ISO 27018. Actualización legislación de referencia.	ACC	Ingeniero de procesos

		Incluido requisito de homologación de proveedores sobre la ISO 27018.		
2.6	12/03/2024	Actualización referencia ENS 2022. Actualización documentación aplicable. Actualización logos y dirección social. Actualización legislación aplicable: inclusión RD311/2022.	ACC	Ingeniero de procesos
2.7	03/04/2025	Revisión sin Cambios	IVLL	Resp. SIG

Revisión

FECHA	NOMBRE	ÁREA	CARGO
03/04/2025	Irene Villar Llera	RRHH, Org y Exxc.	Resp. SIG

Aprobación

FECHA	NOMBRE	ÁREA	CARGO
03/04/2025	Comité SGSI		

Distribución

NOMBRE	ÁREA	CARGO	EMAIL
Plantilla Alisys	Alisys Digital, S.L.U.		Intranet Corporativa

Documentación de referencia

TIPO DOC.	CÓDIGO	DESCRIPCIÓN
REGISTRO	-	LISTADO DE DOCUMENTOS Y REGISTROS
MANUAL	**MSGSI**	MANUAL DE SEGURIDAD DE LA INFORMACIÓN
POLÍTICA	**PRH-02**	POLÍTICA DE PROCESO DISCIPLINARIO
POLÍTICA	**PRH-03**	POLÍTICA DE USO ACEPTABLE Y RESPONSABILIDAD DEL USUARIO
POLÍTICA	**PSGSI-10**	POLÍTICA ANTICORRUPCIÓN
POLÍTICA	**PPCIDSS-00**	POLÍTICA DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS DE TARJETA

POLÍTICA	**PPCIDSS-09**	POLÍTICA DE ACCESO REMOTO
PROCEDIMIENTO	**PR-03_02**	GESTIÓN DE INCIDENTES DE SEGURIDAD
PROCEDIMIENTO	**PR-05**	METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS
PROCEDIMIENTO	**PR-05_02**	METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS ENS
PROCEDIMIENTO	**PR-07**	PLAN DE CONTINUIDAD DEL NEGOCIO
PROCEDIMIENTO	**PR-09**	CONTROL DE ACCESOS
PROCEDIMIENTO	**PR-12**	CLASIFICACIÓN DE LA INFORMACIÓN
PROCEDIMIENTO	**PR-13**	PROTECCIÓN DE DATOS. DOCUMENTO DE SEGURIDAD
PROCEDIMIENTO	**PR-15**	GESTIÓN DE COMPRAS Y APROVISIONAMIENTOS
PROCEDIMIENTO	**PR-24**	DIRECTIVA DE SEGURIDAD IOP
PROCEDIMIENTO	**PR-31**	MONITORIZACIÓN Y RESPUESTA ANTE EVENTOS DE SEGURIDAD
PROCEDIMIENTO	**PR-33**	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN. REGLAMENTO DE FUNCIONAMIENTO.
PROCEDIMIENTO	**PR-60**	GESTIÓN DE PROVEEDORES
PROCEDIMIENTO	**PR-64**	PLAN DE RECUPERACIÓN ANTE DESASTRES
TODA LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN PARA ALISYS (RESTO DE POLÍTICAS Y PROCEDIMIENTOS APLICACBLES A LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)		

1 Introducción

Alisys Digital, como empresa dedicada al ***análisis, diseño, desarrollo y mantenimiento de sistemas de información que dan soporte a los servicios de telecomunicaciones y a diferentes soluciones de transformación digital***, para alcanzar sus objetivos asume un firme compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de la misma, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la gestión de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el **Esquema Nacional de Seguridad**, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Asimismo, para todos los servicios que impliquen la gestión de datos personales en infraestructuras desplegadas en la nube las medidas aplicadas cumplen con la normativa legal exigible en materia de protección de datos personales.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

La organización contempla acciones para prevenir, detectar y responder, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información y los servicio de la compañía, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.).

2 Alcance y ámbito de aplicación del Sistema de Seguridad de la Información

Esta política contempla toda la información utilizada por Alisys Digital S.L.U. (en adelante, Alisys) para el desarrollo de sus actividades y es aplicable, con carácter obligatorio a todas las líneas de negocio, así como, para otras entidades colaboradoras o terceros involucrados en la utilización de la información y sistemas que la soportan. Las relaciones con dichas entidades colaboradoras deben estar amparadas en todo momento por los contratos de prestación de servicios correspondientes, incluyendo cláusulas de confidencialidad en el uso de la información.

Las políticas, estándares, procedimientos y guías que se desarrollen, son de aplicación en todas las fases del ciclo de vida de la información: generación, distribución, almacenamiento, procesamiento, transporte, acceso, consulta y destrucción; en los sistemas que la soportan, así como de los espacios físicos que les afecten.

Esta política persigue la adopción de acciones destinadas a proteger los cuatro componentes básicos de la seguridad, aplicados a la información:

- Confidencialidad: Garantizar que el acceso a la información y sistemas que la soportan sólo sea por entidades debidamente autorizadas.
- Integridad: Garantizar la exactitud de la información y los sistemas que la soportan contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Disponibilidad: Garantizar que la información y los sistemas que la soportan puedan ser utilizados por personal autorizado en la forma y el tiempo requeridos.
- Cumplimiento: Garantizar cumplimiento de la legislación vigente y estándares de la industria en materia de protección y seguridad de la información en todos sus procesos de negocio.
- Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad/activo/sistema pueden ser imputadas a dicho sujeto.
- Autenticidad: Identificar y garantizar que el origen y destinatario de la información son quien dicen ser.

El alcance del Sistema de Gestión de Seguridad de la Información de Alisys Digital S.L.U. es el siguiente:

Análisis, diseño y desarrollo de sistemas de telecomunicaciones y soluciones de transformación digital, como servicio de alojamiento, gestión y mantenimiento de sistemas informáticos, cloud computing, redes, servicios de telefonía, red inteligente, voz sobre IP, Fax, SMS, streaming de audio y video, blockchain, inteligencia artificial y servicios especializado en soluciones estratégicas de comunicación interactiva y marketing online.

2.1. Alcance del Esquema Nacional de Seguridad

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

Sistema de Información que soporta los servicios, diseñados, desarrollados y mantenimientos por ALISYS DIGITAL, de soluciones tecnológicas basadas en Software orientado, entre otros, a

- Servicios de telecomunicaciones, comunicaciones omnicanal y gestión de clientes
- Servicios de certificación y servicios de pago electrónico,
- Plataformas para la gestión, monitorización y operación de dispositivos IoT y robots
- Servicios de desarrollo de aplicaciones "ad-hoc" así como otras, orientadas a:
    - Modelos de Inteligencia Artificial incluyendo aplicaciones de:
        - Procesamiento de lenguaje natural
        - Visión artificial,
        - Biometría
        - Resolución de problemas de optimización, predicción y generación de contenido
    - Sistemas de registro distribuido como blockchain

3 Objetivos de Seguridad de la Información

Alisys dispone de un Sistema de Gestión de Seguridad de la Información, basado en los estándares de las Normas UNE ISO/IEC 27001, PCI DSS, ISO/IEC 27018 y Esquema Nacional de Seguridad, como herramienta de mejora continua de sus procesos.

El Sistema de Gestión de Seguridad de la Información da soporte al firme compromiso asumido por la Dirección en dar cumplimiento a los siguientes objetivos de seguridad de la información:

1. Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz

2. Asegurar la recuperación rápida y eficiente de los servicios frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.

3. Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.

4. Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información

5. Priorizar la satisfacción y el cumplimiento de los requisitos del cliente, en materia de seguridad de la información, interpretando sus necesidades y proporcionando los recursos necesarios para darles respuesta.

6. Alinear el diseño de los procesos de la compañía con los requerimientos de seguridad de nuestros clientes, los requisitos legales, la legislación aplicable y las buenas prácticas de nuestro sector.

7. Promover el compromiso de toda la organización con la Gestión de Seguridad de la Información, facilitando la sensibilización de su personal en la materia, así como potenciando su participación en todos los procesos de generación de ideas innovadoras.

8. Mejorar continuamente la eficacia del Sistema de Gestión de Seguridad de la Información, con el objeto de aumentar nuestra competitividad en el mercado, a través de la utilización de herramientas de control de procesos, auditorias, análisis de riesgos y vulnerabilidades, planes de contingencia y continuidad de negocio, capacitaciones, así como la concienciación, sensibilización y formación al personal sobre su uso y aplicación.

9. Gestionar de forma adecuada los incidentes de seguridad, a través de herramientas que faciliten la identificación de los mismos, así como su tratamiento posterior.

10. Asegurar la protección de los datos de personales en todos los entornos que comporten su almacenamiento en servicios de nube, así como proporcionar cuantas medidas sean oportunas para conseguirlo.

El objetivo principal de la Seguridad de la Información en ALISYS es garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información y mantener su adecuado sustento en entornos seguros mediante políticas, estándares, procedimientos y guías adecuadas que contemplen todo el ciclo de vida de la información, sus sistemas, y los espacios físicos donde éstos se encuentran.

Adicionalmente, el presente documento está orientado a:

- prevenir los incidentes de seguridad de la información y mitigar los riesgos de seguridad de la información generados por nuestras actividades

- crear y fomentar una conciencia de seguridad, identificándose como un medio más para que la empresa logre sus objetivos.

4 Marco jurídico y normativo

Alisys se compromete al cumplimiento con los requisitos legales aplicables y con cualesquiera otros requisitos que fueran de aplicación. A esto se suman los compromisos adquiridos con los clientes, así como la actualización continua de los mismos.

Alisys adquiere el compromiso de velar por el cumplimiento de la legislación vigente y estándares de la industria en materia de protección y seguridad de la información, de las bases de datos de carácter personal y de los sistemas aplicables a todos sus procesos de negocio:

Para ello, el marco legal y regulatorio en el que desarrollamos nuestras actividades es:

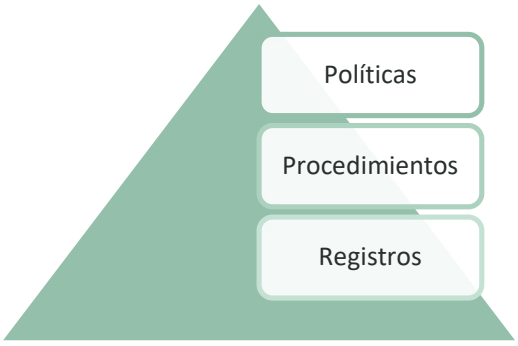
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley Orgánica 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.
- Ley 2/2019, de 1 de marzo, por la 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).
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Ver también **MSGSI MANUAL DE SEGURIDAD DE LA INFORMACIÓN**, Aptdo 2. “Referencias Normativas”

5 Necesidades para alcanzar el cumplimiento de objetivos

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información.
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:



6 Directrices Generales

Con el fin de garantizar la protección de la información, se establece un conjunto de directrices generales, aplicables a todo sistema informático, en el sentido más amplio, accesibles directa o remotamente a través de redes y comunicaciones. Estas directrices son:

- La **PSGSI -00 Política de seguridad de la información** se rige en primera instancia, por las disposiciones legales, aplicables y vigentes, así como en lo dispuesto en los tratados internacionales en los que España sea participante.

- La información, los sistemas que la soportan y sus componentes son propiedad de las empresas de Alisys y su uso se restringe a fines autorizados y de negocio.

- Cualquier utilización de la información y sistemas que la soportan para actividades ajenas a la empresa queda prohibida.

- Todo activo generado para la compañía o proporcionado a consultores, empresas externas o personal para la realización de un desarrollo o actividad, es propiedad de Alisys y tiene que ser entregado o destruido a la finalización del proyecto o actividad.

- Deben existir inventarios actualizados de los sistemas de información y de los activos que los sustentan, de sus responsables o propietarios.

- El área de la empresa que solicita un sistema informático como apoyo a una actividad de la cual es responsable, se convierte en el propietario de dicho sistema y de la información que genera.

- El responsable funcional, es aquella persona en la cual el propietario delega la integridad y seguridad de los programas e información del sistema y para lo cual debe: gestionar y autorizar los cambios al sistema, administrar los niveles de confidencialidad, establecer los criterios de accesos, determinar y revisar las medidas de protección y requerimientos legales, negociar y autorizar las interfaces y extracciones de datos para otros sistemas.

- El custodio es el departamento que mantiene el sistema en un entorno íntegro y seguro, para lo cual debe: implementar las medidas de seguridad físicas y lógicas acordes a las necesidades definidas por el propietario, proveer de control de accesos y monitorización del sistema, mantener y velar por la integridad de los elementos que componen el sistema e informar al propietario del sistema de anomalías, incidentes o riesgos de seguridad.

- El usuario es la persona que hace uso de sistemas informáticos y la información que soportan para la realización de sus actividades en la organización. Es responsable de proteger la información y mecanismos de acceso, seguir los procedimientos establecidos por el

responsable funcional, mantener el secreto profesional e informar de cualquier mal uso o riesgo de seguridad.

- Todos los contratos, licencias y acuerdos con proveedores o consultores deben incluir cláusulas relativas a la propiedad intelectual y derechos de uso, a la confidencialidad y a los requerimientos de seguridad, exigibles por imperativos legales o de negocio.

- El propietario del sistema es responsable de la clasificación de la información manejada y almacenada por el sistema, así como de definir su caducidad. Dicha clasificación y caducidad debe de estar en la etiqueta, para todo archivo o medio de almacenamiento.

- Todo el personal está obligado a velar por el cumplimiento de la legislación vigente en materia de privacidad y seguridad de la información, derechos de propiedad intelectual y del cumplimiento de los acuerdos contractuales adquiridos con terceros.

- Los sistemas informáticos, especialmente los que manejan información reservada o protegida por la Ley, requieren de accesos individualizados y de mecanismos de auditoría que permitan saber, de manera inequívoca, quién y cuando accedió al sistema.

- La interconexión de la red o redes de Alisys con otras redes debe realizarse por medios seguros y controlados. Asimismo, los accesos externos deben ser identificados, autenticados y registrados.

- La instalación de cualquier elemento de comunicaciones en un equipo conectado a la red de Alisys requiere de la aprobación del Comité de Seguridad de la Información para su análisis y control.

- Todo el software comprado para su uso en sistemas informáticos debe estar apoyado en una licencia en donde se determine los derechos de uso y sus limitaciones.

- El personal debe acatar las especificaciones de dichas licencias y no debe hacer copias ilegales del software.

- La salida de equipos o elementos de sistemas fuera de las dependencias y del control de Alisys, requieren de la aprobación del **Comité de Seguridad de la Información**, así como del responsable de sistemas y deberán ir acompañados de los requerimientos de seguridad especificados por Alisys.

- Todo medio magnético que se vaya a desechar tiene que ser debidamente tratado para eliminar los datos residuales que contenga, con el fin de no exponer la información de la compañía que se hubiera almacenado. En este sentido, se deben tomar las medidas oportunas de seguridad

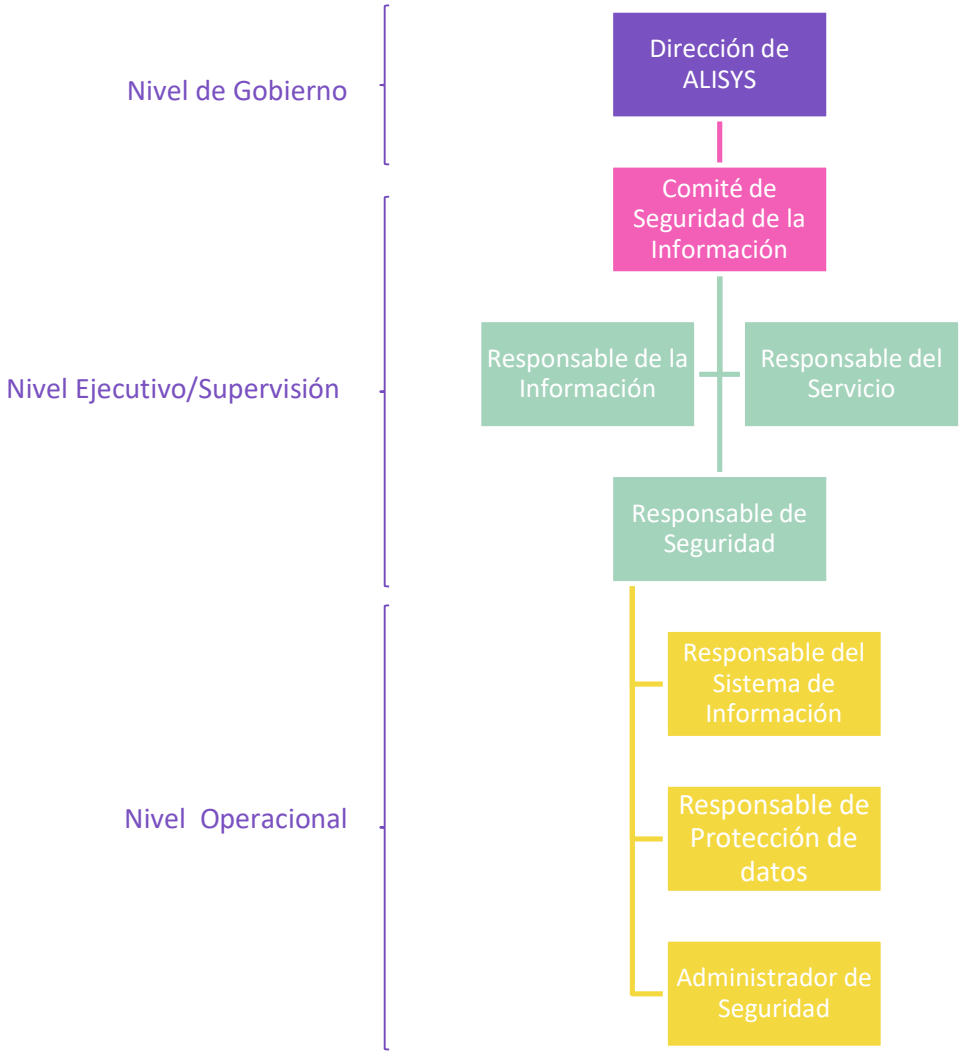
y control en la reparación de equipos fuera de las dependencias de ALISYS.

- La implantación de medidas de seguridad se hará de forma progresiva, de acuerdo con las directrices estratégicas y tácticas del **Responsable de Seguridad**.

Cualquier excepción, modificación o sugerencia sobre esta política debe remitirse al **Responsable de Seguridad**, quien, con una evaluación previa, procederá en su caso a la propuesta de aprobación y/o modificación que corresponda.

7 Organización y estructura de la seguridad

La Dirección General de Alisys delega la organización de la Seguridad en varios actores que, con diferentes funciones y responsabilidades, tienen como misión principal la coordinación de la seguridad, canalizando las directrices y políticas hacia las distintas unidades de negocio.



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 de seguridad de la información

Todos los directivos de la compañía y mandos intermedios 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 al personal de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento

a través de la presente **PSGSI-00 Política de seguridad de la información**.

Los roles o funciones de seguridad definidos son:

ROLES	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 de Información	Coordinar la implantación del sistema Mejorar el sistema de forma continua
Responsable de Protección de Datos	Velar por el cumplimiento legal durante la gestión de datos personales. Asistir al resto de miembros en materia de protección de datos sensibles.
Administrador de Seguridad	Implantación, gestión y mantenimiento de las medidas de seguridad.

La designación de las personas que ocupan los puestos de responsabilidades dentro de esta estructura organizativa de la seguridad de Alisys, así como la definición de sus deberes y responsabilidades se completa en:

- **MSGSI - Manual de seguridad de la información**
- **PR-33 Comité de seguridad de la información: reglamento de funcionamiento**
- Descripción de perfiles de puesto

7.1. Resolución de conflictos

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

8 Comité de seguridad de la información

Se designará un Comité de Seguridad de la Información cuyos miembros serán las personas responsables de las áreas estratégicas de la organización y directamente relacionadas con la seguridad de la información.

El procedimiento para la designación y renovación del Comité será la ratificación en el Comité de Seguridad de la Información.

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 de la compañía, a excepción de la Dirección General.

Los miembros del comité de seguridad de la información serán, al menos, los siguientes:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de la Seguridad
- Responsable del Sistema
- Responsable de Protección de Datos

Su régimen de funcionamiento, así como su composición, objetivos, funciones y responsabilidades está detallado en el **PR-33 Comité de seguridad de la información: reglamento de funcionamiento.**

9 Gestión de personal

Todos los miembros de ALISYS tienen la obligación de conocer y cumplir esta **PSGSI-00 Política de seguridad de la información** y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Alisys establecerá un programa de concienciación continua para atender a todos los miembros de la compañía, en particular a los de nueva incorporación. Dicho programa contemplará el uso, operación y/o administración de sistemas TIC.

9.1. Responsabilidades del personal

Todo el personal de la organización asume su responsabilidad y compromiso con el cumplimiento de esta **PSGSI-00 Política de seguridad de la información,** de acuerdo con la aplicabilidad de la misma a cada una de las áreas y departamentos de la compañía.

Todo el personal de Alisys es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente, de acuerdo con lo establecido en el **PR-03_02 Gestión de incidentes de seguridad.**

Asimismo, Alisys gestionará Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

9.2. Profesionalidad y seguridad de los recursos humanos

Esta Política se aplica a todo el personal de Alisys y el personal externo que realiza tareas dentro de la empresa.

RRHH incluirá funciones de seguridad de la información en las descripciones de los puestos de trabajo, informará a todo el personal que contrate sobre sus obligaciones con respecto al cumplimiento de la **PSGSI-00 Política de seguridad de la información**, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

El Responsable de Seguridad es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarlos al Comité de Seguridad de la Información y a los propietarios de información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.

El Responsable de Gestión de la Seguridad (RGS) [CISO] participará en la preparación del Compromiso de Confidencialidad que firmará los empleados y terceros que desempeñen funciones en Alisys, en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.

Profesionalidad del Departamento de Recursos Humanos:

- Determinar la competencia necesaria del personal para llevar a cabo el trabajo que afecta a la Seguridad de la Información
- Asegurar que las personas sean competentes sobre la base de la educación, capacitación o experiencia adecuadas
- Demostrar mediante la información documentada que sea necesaria la competencia del personal en materia de Seguridad de la Información

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Garantizar que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad de la Información de la organización en el curso de sus tareas normales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

9.3. Formación y concienciación

El método más efectivo de mejorar la seguridad es a través de la formación del personal, tanto en el momento de su incorporación a la actividad laboral como a través de programas continuos de capacitación.

Dentro de los planes de formación para el personal se incluirán cursos específicos sobre seguridad de la información, acordes a las áreas destinatarias.

10 Proveedores, subcontratistas

Todos los proveedores, subcontratistas y colaboradores de la organización, cuando tengan acceso a cualquier tipo de información de la compañía o de sus clientes, deben conocer y cumplir con las disposiciones de la **PSGSI-00 Política de seguridad de la información** de Alisys.

Asimismo, Alisys gestionará Compromisos de Confidencialidad con los proveedores, subcontratistas y colaboradores, y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

Se realizarán campañas de concienciación sobre seguridad dirigidas a todo el personal, proveedores y colaboradores de Alisys a través de los medios que se consideren más efectivos.

Para el caso concreto de proveedores que proporcionen, o estén relacionados, con la prestación de servicios en la nube, se les requerirá el cumplimiento de los estándares de seguridad marcados por la norma ISO 27018. Por lo tanto, estos deberán acreditar el cumplimiento durante el proceso de homologación de proveedores. Sin perjuicio de que Alisys pueda llevar a cabo auditorías de segunda parte para verificar el cumplimiento.

11 Clasificación de la información

Toda la información debe estar clasificada en función de su importancia para la organización y en relación con la mayor o menor necesidad de garantizar su confidencialidad, conforme a lo dispuesto en la **PR-12 Clasificación de la información**.

12 Gestión de riesgo

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisa regularmente:

- al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se tendrán en cuenta la metodología de análisis de riesgos desarrollada en los documentos **PR-05 Metodología para el análisis de riesgos,** y **el PR-05_02 Metodología para el análisis de riesgos ENS** para servicio incluidos en el alcance del Esquema Nacional de Seguridad.

13 Autorización y control de accesos a los Sistemas de Información

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de Alisys y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.
- Revisar el comportamiento del personal en relación con los datos de carácter personal.

El control de accesos a los sistemas de información se encuentra recogido en el **PR-09 Control de accesos.**

14 Protección de las instalaciones

Los objetivos de la **PSGSI-00 Política de seguridad de la información** en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de Alisys.
- Proteger el equipo de procesamiento de información crítico de Alisys, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de esta en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de Alisys.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.

Esta **PSGSI-00 Política de seguridad de la información** se aplica a todos los recursos físicos relacionados con los sistemas de información de ALISYS: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El **Responsable de Seguridad** definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de Alisys a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de Alisys cuando lo consideren apropiado.

Todo el personal de Alisys es responsable del cumplimiento de esta política, para la protección de la información relacionada con el trabajo diario en las oficinas.

15 Adquisición de productos

Los diferentes departamentos deben cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad deben ser identificados e incluidos en la planificación de los proyectos y en la solicitud de ofertas a proveedores y subcontratistas.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio, siguiente las disposiciones establecidas en la **PSGSI-14 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas**.

En el caso concreto de las adquisiciones, se seguirá lo establecido en los documentos **PR-15 Gestión de compras** y **PR-60 Gestión de proveedores**, que establecen criterios en materia de seguridad de la información para la selección de proveedores y la compra de componentes.

16 Seguridad por defecto

Alisys considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

17 Integridad y actualización del sistema

Alisys se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por el Área de Sistemas, que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

Ver **PPCIDSS-02 Política de aplicación de parches de seguridad y PR-24 Directiva de seguridad IOP.**

18 Protección de la información almacenada y en tránsito

Alisys establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros.

Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

19 Prevención de sistemas de información interconectados

Alisys establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Ver **PRH-03 Política de uso aceptable y responsabilidad del usuario** y el **PCIDSS-09 Política de accesos remotos.**

20 Registros de actividad

Alisys registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Los objetivos principales de la **Gestión de incidentes** son los de:

- Establecer un sistema de detección y reacción frente a código dañino
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.
- Este registro se empleará para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

La gestión de incidentes de seguridad se realizará de acuerdo con lo establecido en el **PR-03_02 Gestión de incidentes de seguridad** y el **PR-31 Monitorización y respuesta ante eventos de seguridad de la información.**

21 Continuidad de la actividad

Alisys, con el objetivo de garantizar la continuidad de las actividades, establece medidas para que los sistemas dispongan de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Para ello, se seguirá lo establecido en el documento **PR-07 Plan de continuidad de negocio** y **PR-64 Plan de recuperación ante desastres**.

22 Compromiso de mejora continua del proceso de seguridad

Alisys establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales como ISO27001 e ISO27018, así como en el Esquema Nacional de Seguridad.

La Dirección de Alisys se compromete a garantizar que toda la actividad de la compañía se desarrolla bajo los requisitos legales o reglamentarios y las obligaciones de seguridad contractuales, así como cumplir con los requisitos aplicables relacionados con la seguridad de la información.

De igual forma, la Dirección de Alisys se compromete a proporcionar los recursos necesarios para garantizar el desarrollo y mejora continua de la eficiencia del Sistema de Seguridad de la Información.

La Dirección tendrá en cuenta el análisis de riesgos y vulnerabilidades para la identificación y gestión de estos y valorará sus activos teniendo en cuenta los criterios de seguridad como Confidencialidad, Integridad y Disponibilidad.

23 Revisión

Esta **Política de seguridad de la información** será revisada de forma anual para considerar el resultado de los análisis de riesgos, así como para adaptarse a los procesos y activos de información que hayan surgido como parte de las actividades de negocio de Alisys.

24 Auditoría

Los sistemas de información se someterán periódicamente a auditorías internas y/o externas con la finalidad de verificar la correcta implantación de esta política de seguridad y la adecuada ejecución del Plan de Seguridad para determinar grados de cumplimiento y recomendar medidas correctivas.

25 Incumplimiento de la política

Alisys hará responsable al usuario de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento.

Alisys se reserva el derecho de evaluar periódicamente el cumplimiento de este reglamento. Cualquier acción disciplinaria derivada del incumplimiento de esta será considerada de acuerdo con los procedimientos establecidos.

El usuario que no cumpla con la política de almacenamiento de información será directamente responsable de las sanciones legales derivadas de sus propios actos y de los costos y gastos en que pudiera incurrir Alisys en defensa por la posible pérdida de información sensible.

Ver **PRH-02 Política de proceso disciplinario y PRH-03 Política de uso aceptable y responsabilidad del usuario**

26 Aprobación y entrada en vigor

Esta Política se Seguridad de la Información es efectiva desde la fecha de firma y hasta que sea reemplazada por una nueva Política.

En Madrid, a 03 de Abril de 2025

La Dirección

Calle Cronos, Nº63, Planta 2ª, Local 4
28037 Madrid
+34 910 200 000

info@alisys.net
www.alisys.net