ALAMCIA, S.L.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento de uso público

Referencia: PS-001/2025

Versión 2.0

21 de mayo de 2026

CONTROL DE VERSIONES

Fecha	Realizado por	Versión	Descripción
09/02/2026	Responsable de Seguridad	1.0	Versión inicial
21/05/2026	Responsable de Seguridad	2.0	Revisión de forma y publicación en web

APROBACIÓN

Realizado por	Revisado por	Aprobado por
Responsable de Seguridad	Comité de Seguridad	Dirección

ÍNDICE

1. Aprobación y entrada en vigor

La presente Política de Seguridad de la Información es efectiva desde la fecha de su firma y permanecerá en vigor hasta que sea reemplazada por una versión posterior debidamente aprobada por la Dirección de ALAMCIA, S.L.

2. Misión de la Organización

ALAMCIA, S.L. asume el compromiso con la seguridad de la información como elemento esencial para alcanzar sus objetivos, garantizando a todos sus grupos de interés las mayores cotas de protección sobre la información que trata.

La misión de la organización es fomentar el desarrollo sostenible mediante la integración de tecnología avanzada y estrategias de emprendimiento que respondan a las necesidades específicas de cada contexto, tanto rural como urbano, con especial atención a las comunidades rurales.

Los sistemas de información de la organización deben ser administrados con diligencia, adoptando 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 de los servicios prestados.

El objetivo 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 ante los incidentes.

Los sistemas TIC deben estar protegidos frente a amenazas en constante evolución que pueden afectar a la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas se requiere una estrategia capaz de adaptarse a los cambios del entorno y de garantizar la prestación continuada de los servicios. Esto implica aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, realizar un seguimiento continuo de los niveles de prestación, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes.

La seguridad TIC debe ser parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, contemplando las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben identificarse e incluirse en la planificación, en la solicitud de ofertas y en los pliegos de licitación de los proyectos TIC.

La organización estará preparada para prevenir, detectar, reaccionar y recuperarse de los incidentes de seguridad, conforme al artículo 8 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.

3. Alcance

La presente política es de aplicación 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 del Esquema Nacional de Seguridad, sin excepción.

4. Objetivos

La Dirección establece los siguientes objetivos en materia de seguridad de la información:

- Proporcionar un marco que aumente la capacidad de resistencia y resiliencia frente a incidentes para ofrecer una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios ante cualquier desastre o contingencia que pudiera comprometer la continuidad de las operaciones.
- Prevenir incidentes de seguridad en la medida en que sea técnica y económicamente viable, mitigando los riesgos derivados de la actividad.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

5. Marco Normativo

ALAMCIA, S.L. desarrolla su actividad dentro del siguiente marco legal y regulatorio, sin perjuicio de la actualización continua del mismo y del cumplimiento de los compromisos adquiridos con los clientes:

- 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 (RGPD).
- 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, por el que se aprueba el texto refundido de la 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 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Resolución de 7 de octubre de 2016, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, 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, 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, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial).
- Reglamento (UE) 2024/2847, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Reglamento de Ciberresiliencia).

6. Desarrollo

Para alcanzar los objetivos enunciados, ALAMCIA, S.L. asume los siguientes compromisos:

- Mejorar continuamente su sistema de seguridad de la información.
- Identificar las amenazas potenciales y el impacto que su materialización podría causar en las operaciones de negocio.
- Preservar los intereses de las principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar conjuntamente con suministradores y subcontratistas para mejorar la prestación de servicios TI, su continuidad y la seguridad de la información.
- Evaluar y garantizar la competencia técnica del personal, asegurando su motivación y proporcionando la formación y comunicación interna adecuadas.
- Garantizar el correcto estado de las instalaciones y del equipamiento, en correspondencia con la actividad, los objetivos y las metas de la empresa.
- Analizar de forma continua todos los procesos relevantes, introduciendo las mejoras pertinentes en función de los resultados obtenidos.
- Estructurar el sistema de gestión de forma comprensible y accesible.

La gestión del sistema documental se encomienda al Responsable del Sistema, y la documentación estará disponible en el repositorio corporativo conforme a los perfiles de acceso definidos en el procedimiento de gestión de accesos vigente.

La documentación referida a la seguridad del sistema se estructura en carpetas dentro del repositorio corporativo, organizadas por puntos de norma y marcos de operación, con acceso restringido al personal autorizado.

La documentación de seguridad se estructura en:

- Política de Seguridad.
- Normativa de Seguridad: documentos que describen el uso de equipos, servicios e instalaciones, lo que se considera uso indebido, la responsabilidad del personal y las medidas disciplinarias aplicables conforme a la legislación vigente.
- Documentos específicos: documentación desarrollada según las guías CCN-STIC que resulten de aplicación.

- Procedimientos de Seguridad: documentos que detallan cómo operar los elementos del sistema.

Esta política se complementa con el resto de políticas, procedimientos y documentos vigentes en el sistema de gestión de ALAMCIA, S.L.

7. Organización de la Seguridad

La responsabilidad esencial recae sobre la Dirección de la organización, a la que corresponde organizar las funciones y responsabilidades y facilitar los recursos necesarios para alcanzar los objetivos del Esquema Nacional de Seguridad. La Dirección es asimismo responsable de dar buen ejemplo cumpliendo las normas de seguridad establecidas.

Estos principios son asumidos por la Dirección, que dota a sus empleados de los recursos necesarios para su cumplimiento, plasmándolos y dándolos a conocer públicamente a través de la presente Política.

Los roles o funciones de seguridad definidos son los siguientes:

Función	Deberes y responsabilidades
Responsable de la Información	Tomar las decisiones relativas a la información tratada.
Responsable del Servicio	Coordinar la implantación del sistema y mejorarlo de forma continua.
Responsable de Seguridad	Determinar la idoneidad de las medidas técnicas y proporcionar la mejor tecnología para el servicio.
Responsable del Sistema	Coordinar la implantación del sistema y mejorarlo de forma continua.
Dirección	Proporcionar los recursos necesarios para el sistema y liderarlo.
Administrador de Seguridad	Implantación, gestión y mantenimiento de las medidas de seguridad.

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en el documento Registro de responsables, roles y responsabilidades.

Resolución de conflictos

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

8. Comité de Seguridad

El procedimiento para la designación y renovación de los miembros del Comité será la ratificación por el propio 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. Todas las decisiones relevantes en materia de seguridad se acuerdan en este Comité.

Los miembros del Comité de Seguridad de la Información son:

- Responsable de Seguridad.
- Responsable del Sistema.
- Responsable del Servicio.
- Responsable de la Información.

Estos miembros son designados por el Comité, único órgano facultado para nombrarlos, renovarlos y cesarlos.

El Comité de Seguridad es un órgano autónomo y ejecutivo, con capacidad para la toma de decisiones, sin subordinación a ningún otro órgano de la empresa.

La organización de la seguridad de la información se desarrolla en el documento complementario a esta Política, denominado Organización de la Seguridad.

9. Gestión de Riesgos

Todos los sistemas sujetos a esta Política realizarán un análisis de riesgos en el que se evaluarán las amenazas y los riesgos a los que están expuestos. Este análisis se revisará periódicamente:

- 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 establecerá una valoración de referencia para los distintos tipos de información manejada y los servicios prestados. El Comité dinamizará la disponibilidad de recursos para atender las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se aplicará la metodología desarrollada en el procedimiento Análisis de Riesgos.

10. Gestión del Personal

Todos los miembros de ALAMCIA, S.L. tienen la obligación de conocer y cumplir la presente Política y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la organización asistirán al menos una vez al año a una sesión de concienciación en materia de seguridad TIC. Se establecerá un programa de concienciación continua que atenderá a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán la formación necesaria para el manejo seguro de los sistemas. La formación será obligatoria antes de asumir una responsabilidad, tanto en una primera asignación como en un cambio de puesto.

11. Profesionalidad y Seguridad de los Recursos Humanos

Esta Política se aplica a todo el personal de ALAMCIA, S.L. y al personal externo que realice tareas dentro de la empresa.

El área de Recursos Humanos incluirá funciones de seguridad de la información en las descripciones de los puestos, informará al personal de sus obligaciones respecto al cumplimiento de la Política, gestionará los Compromisos de Confidencialidad y coordinará las tareas de capacitación de los usuarios.

El Responsable de Seguridad monitoriza, documenta y analiza los incidentes de seguridad reportados, y comunica los resultados al Comité de Seguridad y a los propietarios de la información.

El Comité de Seguridad implementa los medios y canales necesarios para que el Responsable de Seguridad maneje los informes de incidentes y anomalías del sistema. El Comité supervisa la investigación, la evolución de la información y promueve la resolución de los incidentes.

El Responsable de Seguridad participa en la elaboración del Compromiso de Confidencialidad que firmarán los empleados y terceros que desempeñen funciones en ALAMCIA, S.L., en el asesoramiento sobre las sanciones aplicables por incumplimiento y en el tratamiento de los incidentes.

Todo el personal de la organización es responsable de informar oportunamente sobre las debilidades e incidentes de seguridad que detecte.

Profesionalidad de los 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 información documentada, la competencia del personal en materia de seguridad de la información.

Objetivos del control de la seguridad del personal

- Reducir los riesgos de error humano, irregularidades, uso indebido de instalaciones y recursos y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la fase de reclutamiento e incluirlas en los acuerdos a firmar, verificando su cumplimiento durante el desempeño de las tareas.
- Asegurar que los usuarios conocen las amenazas y preocupaciones de seguridad y están capacitados para apoyar la Política en el desarrollo de sus tareas habituales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios externos a las instalaciones de tratamiento.
- Disponer de herramientas y mecanismos para la comunicación de debilidades e incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

12. Autorización y Control de Acceso a los Sistemas de Información

El control del acceso a los sistemas de información tiene los siguientes objetivos:

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

13. Protección de las Instalaciones

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, los daños y las interferencias en la sede, instalaciones e información de ALAMCIA, S.L.
- Proteger el equipo crítico de tratamiento de información, ubicándolo en áreas protegidas dentro de un perímetro de seguridad definido, con medidas y controles de acceso adecuados, contemplando también su protección en traslados y fuera de las áreas protegidas.
- Controlar los factores ambientales que pudieran perjudicar el buen funcionamiento de los equipos.
- Implementar medidas para proteger la información manejada por el personal en sus tareas habituales.
- Proporcionar una protección proporcional a los riesgos identificados.

Esta política se aplica a todos los recursos físicos relacionados con los sistemas de información: instalaciones, equipos, cableado, expedientes y soportes de almacenamiento, entre otros.

El Responsable de Seguridad, junto con los responsables de la información cuando proceda, 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 y cumplimiento.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal a las áreas restringidas bajo su responsabilidad. Los responsables de la información autorizarán formalmente el trabajo fuera del sitio cuando lo consideren apropiado.

Todo el personal es responsable del cumplimiento de la política de mesa limpia y pantalla limpia para la protección de la información relacionada con el trabajo diario.

14. Adquisición de Productos

La seguridad TIC es parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada, contemplando las decisiones de desarrollo o adquisición y las actividades de

explotación. Los requisitos de seguridad y las necesidades de financiación se identifican e incluyen en la planificación, las solicitudes de oferta y los pliegos de licitación de los proyectos TIC.

Asimismo, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas, limitando y gestionando los cambios.

La política de desarrollo y adquisición se desarrolla en el documento Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.

15. Seguridad por Defecto

ALAMCIA, S.L. considera estratégico que sus procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas y servicios incluirán la seguridad por defecto desde su creación hasta su retirada, contemplando la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades de explotación, configurando la seguridad como un proceso integral y transversal.

16. Integridad y Actualización del Sistema

ALAMCIA, S.L. 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 autorización previa a su instalación. La evaluación corresponde principalmente al Responsable del Sistema, que valorará el impacto en la seguridad antes de realizar los cambios y controlará de forma documentada aquellos cambios calificados como importantes o con implicaciones para la seguridad.

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

17. Protección de la Información Almacenada y en Tránsito

ALAMCIA, S.L. establece medidas de protección para la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

18. Protección de Sistemas de Información Interconectados

ALAMCIA, S.L. establece medidas de protección para la seguridad de la información, especialmente para proteger el perímetro de los sistemas, en particular cuando se conecten a redes públicas, y sobre todo si éstas se utilizan de forma total o principal 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 con otros sistemas a través de redes, y se controlarán sus puntos de unión.

19. Continuidad de la Actividad

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

20. Mejora Continua del Proceso de Seguridad

ALAMCIA, S.L. establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y la metodología establecidos en normas internacionales como ISO/IEC 27001.

En Alcorcón, a 21 de mayo de 2026.

29794353S ALBERTO JAVIER ARROYO (R: B85132496)

Firmado digitalmente por 29794353S ALBERTO JAVIER ARROYO (R: B85132496)
Fecha: 2026.05.21 21:42:40 +02'00'

Fdo.

La Dirección