SGSI-N1-001

Política de Seguridad de la Información

Documento de gobierno de nivel N1 — principios y compromiso de la Dirección con la seguridad de la información

Sistema de Gestión de la Seguridad de la Información

Skynet Systems, S.L.U.

Versión 2.0 · 0 - Público

C/ Carril de la Condomina 3, 7ªC
Atalayas Business Center
30006 Murcia, España
Teléfono: +34 968 67 92 90

Control documental

Campo	Valor
Código del documento	SGSI-N1-001
Versión	2.0
Fecha de aprobación	1 de julio de 2026
Clasificación	0 - Público
Elabora	Responsable de la Seguridad
Aprueba	CEO
Marco de referencia	ISO/IEC 27001:2022 · Esquema Nacional de Seguridad (RD 311/2022), categoría ALTA
Próxima revisión	Anual, o antes ante cambios significativos en la estructura, los objetivos o la seguridad de la organización

Aprobación

	Nombre y cargo	Fecha y firma
Elaborado por	José Ángel López Sánchez — Director de Ciberseguridad y Tecnología	01/07/2026
Aprobado por	Manuel Pérez de Castro — CEO	01/07/2026

La versión 2.0 actualiza el marco legal aplicable, incorpora la categoría ALTA del Esquema Nacional de Seguridad y adapta la referencia a la estructura documental a los niveles vigentes del sistema de gestión. Sustituye en su integridad a la versión 1.2, aprobada el 18 de julio de 2025. Es efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva versión.

Índice

1. Introducción

Skynet Systems, S.L.U., en adelante Skynet, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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 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, 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 las áreas deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, en su categoría ALTA, y por la norma de libre adopción ISO/IEC 27001:2022, 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.

Las diferentes áreas de la empresa 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. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación y en la solicitud de ofertas realizadas a proveedores.

Las áreas de Skynet deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del Real Decreto 311/2022.

2. Prevención

Las áreas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS —en su categoría ALTA— y por la ISO/IEC 27001:2022, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, las áreas de Skynet deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los componentes del equipo de seguridad deben vigilar la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia según lo establecido en el artículo 10 del Real Decreto 311/2022.

La vigilancia es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 10 del Real Decreto 311/2022. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los

responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4. Respuesta

Las áreas deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente, incluidas las comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

5. Recuperación

Para garantizar la disponibilidad de los servicios críticos, las áreas deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y de sus actividades de recuperación.

6. Alcance

6.1. Alcance objetivo

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) definido en esta política aplica específicamente a los procesos y recursos relacionados con los servicios de soporte técnico, mantenimiento de sistemas e infraestructura, y desarrollo de software, gestionados por Skynet Systems, S.L.U.

En concreto, el alcance incluye:

- Las actividades de soporte técnico a usuarios internos y externos, incluyendo la gestión de incidencias, solicitudes de servicio, asistencia remota y presencial, y resolución de problemas técnicos.
- Las funciones de mantenimiento preventivo y correctivo de sistemas e infraestructuras TIC, que abarcan servidores, redes, dispositivos de comunicaciones, estaciones de trabajo y otros componentes críticos.
- Los entornos, herramientas y recursos utilizados para el desarrollo, prueba, despliegue y mantenimiento de aplicaciones y soluciones software, tanto internas como desarrolladas para terceros.
- Los activos asociados a estos servicios, incluyendo hardware, software, plataformas cloud, bases de datos, documentación técnica y configuraciones de seguridad.
- El personal implicado, ya sea propio, subcontratado o colaborador, con acceso a la información o a los sistemas bajo el alcance.
- Las instalaciones físicas y los accesos remotos seguros donde se llevan a cabo estas actividades.

Este alcance se ha definido teniendo en cuenta el contexto organizacional, las partes interesadas relevantes, y los requisitos contractuales y legales aplicables, con el objetivo de garantizar la protección de la información manejada en dichos servicios y contribuir a la continuidad operativa de los sistemas soportados.

6.2. Aplicabilidad y ámbito de utilización

La política de seguridad de la información es de obligado cumplimiento en Skynet. Los trabajadores, colaboradores, subcontratistas y proveedores de la compañía deben conocer y cumplir esta política de acuerdo con su rol cuando traten con información de la empresa o de sus participantes.

7. Misión y objetivos de seguridad

Skynet desea proteger sus objetivos de negocio, participantes y demás partes interesadas, ofreciendo a sus trabajadores, colaboradores, proveedores y participantes un entorno de gestión de la información seguro.

Objetivos por cumplir:

- **Confidencialidad**: la información debe ser conocida exclusivamente por las personas autorizadas.
- **Integridad**: la información debe ser completa, exacta, válida y no sujeta a manipulaciones.
- **Disponibilidad**: la información debe ser accesible únicamente por usuarios autorizados y garantizar su persistencia ante cualquier eventualidad.
- **Trazabilidad**: característica consistente en que una acción pueda ser imputada exclusivamente a una entidad.
- **Autenticidad**: característica consistente en que una entidad garantiza la fuente de la que proceden los datos.

La política de seguridad está alineada con la organización del negocio, los requerimientos de seguridad de los clientes, la legislación aplicable y las buenas prácticas del sector.

La política de seguridad se actualiza periódicamente de acuerdo con la gestión de riesgos de la organización y siguiendo un proceso de mejora continua.

La organización dispone de un sistema de gestión de la seguridad de la información aprobado e impulsado por su Dirección.

Las medidas de seguridad garantizan la privacidad de los datos personales de acuerdo con la legislación vigente.

8. Marco normativo

Estándares y marcos de referencia reconocidos en el sector:

- ISO/IEC 27001:2022.

Normativas legales nacionales e internacionales:

- 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.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre los requisitos de ciberseguridad horizontales para productos con elementos digitales (Reglamento de Ciberresiliencia).
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial).
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, categoría ALTA conforme a la categorización del sistema.
- Convenio colectivo aplicable.

Normativas corporativas:

- Normativa de Seguridad y demás normativas y procedimientos internos del Sistema de Gestión de la Seguridad de la Información.

Acuerdos contractuales adquiridos:

- Acuerdos marco y contratos con proveedores y clientes.

9. Organización de la seguridad de la información

9.1. Roles: funciones y responsabilidades

La organización, en cumplimiento de las previsiones del Esquema Nacional de Seguridad y de la UNE-EN ISO/IEC 27001:2022, adopta un modelo organizacional para su SGSI basado en niveles jerárquicos de dirección, supervisión y operación.

La estructura organizativa articulada diferencia las responsabilidades y tareas conforme al principio básico de diferenciación de roles y responsabilidades y a la Guía CCN-STIC-801 sobre responsabilidades y funciones en el ENS.

9.2. Procedimientos de designación

La Alta Dirección es la autoridad competente para la designación formal de los distintos roles vinculados a la seguridad de la información, incluyendo los nombramientos del Comité de Seguridad, del Responsable de la Seguridad, del Responsable del Sistema, y demás funciones relacionadas.

Los nombramientos se realizarán atendiendo a los principios de competencia, idoneidad y confianza, considerando para ello la formación, la experiencia acreditada y las capacidades técnicas del personal. En todo caso, el proceso se desarrollará conforme al procedimiento corporativo de provisión o contratación de personal.

Durante el proceso de asignación o renovación, la Alta Dirección podrá requerir la actualización curricular, la superación de entrevistas internas o la realización de pruebas específicas de competencia cuando lo estime necesario.

10. Compromiso con la protección de datos personales

Skynet únicamente tratará datos de carácter personal cuando estos sean adecuados, pertinentes y no excesivos, en relación con las finalidades legítimas, explícitas y determinadas para las que hayan sido recabados. Este tratamiento se ajustará en todo momento a los principios establecidos por la normativa vigente en materia de protección de datos.

El tratamiento de datos personales se realizará previa obtención del consentimiento expreso, libre, informado e inequívoco de los interesados, salvo en aquellos supuestos en los que una base jurídica habilite su tratamiento sin necesidad de consentimiento.

La organización aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, apoyándose en sus políticas, normativas y procedimientos internos en el marco del Sistema de Gestión de Seguridad de la Información.

Skynet mantendrá una Política de Protección de Datos Personales accesible a los usuarios, mediante la cual se velará por la transparencia, la confidencialidad y el pleno ejercicio de los derechos reconocidos a los titulares de los datos.

La gestión, el mantenimiento, la revisión y la mejora continua de dicha política son responsabilidad del responsable de cumplimiento legal y protección de datos, que actúa como garante del cumplimiento normativo y como punto de contacto ante las autoridades de control y los titulares de derechos. Skynet Systems no ha designado Delegado de Protección de Datos, por no resultar exigible atendiendo a la naturaleza, el alcance y los fines de los tratamientos de datos personales que realiza actualmente.

11. Gestión de riesgos

Todos los sistemas afectados por esta política están sujetos a una gestión de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos la información, los servicios y los sistemas de la organización. El análisis de riesgos se repetirá regularmente:

- Al menos una vez al año.
- Cuando ocurra un cambio significativo en la información o los servicios de la organización.
- Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 311/2022.
- Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 311/2022.

El análisis se realiza siguiendo la metodología MAGERIT 3.0. Para la armonización de los análisis de riesgos, la Alta Dirección establece una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados, y dinamiza la disponibilidad de recursos para atender a las necesidades de seguridad de los distintos sistemas, promoviendo inversiones de carácter horizontal.

12. Desarrollo de la política de seguridad de la información

En el marco del Sistema de Gestión de Seguridad de la Información, la estructura documental constituye la base para implementar y mantener los controles establecidos por el Esquema Nacional de Seguridad, la ISO/IEC 27001:2022 y los demás marcos normativos aplicables. El sistema de gestión de seguridad de la información de Skynet se estructura, a nivel documental, en los siguientes niveles relacionados jerárquicamente:

- El gobierno del sistema, con sus documentos de marco y de gestión del riesgo.
- La política de seguridad de la información, que es este documento.
- La normativa de seguridad y las fichas de control, que desarrollan cada control del sistema.
- Los procedimientos, las guías y los planes que ejecutan esa normativa.
- Los registros y las evidencias que demuestran su cumplimiento.

El desarrollo directo de esta política se articula, en el nivel inmediatamente inferior, en la normativa de seguridad y en las fichas de control, que fijan qué debe cumplirse, y se despliega después en los procedimientos, las guías y los planes que fijan cómo se ejecuta. Cada conjunto cumple una función complementaria en el desarrollo, la aplicación y la mejora continua de las medidas de seguridad.

La política de seguridad estará disponible para su consulta en la web corporativa. Así mismo, todo el personal tendrá acceso a la normativa y a los procedimientos que le sean de aplicación. También existirá una copia impresa en las instalaciones de la empresa.

13. Obligaciones del personal

Todos los miembros de Skynet tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad de la Dirección disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Skynet seguirán el plan de formación y concienciación en materia de seguridad de la información aprobado. En particular, se atenderá principalmente a los perfiles de nueva incorporación.

Las personas con responsabilidad en el uso, la operación o la administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

14. Terceras partes

Cuando Skynet preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para el reporte y la coordinación de los respectivos Responsables de Seguridad o Comités de Seguridad externos, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Skynet utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de las normativas de seguridad que atañan a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. El personal de terceros deberá estar adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

Cuando algún aspecto de la política no pueda ser satisfecho por una tercera parte clasificada como proveedor crítico según lo requerido en los párrafos anteriores, se requerirá un informe del Responsable de la Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y de los servicios afectados antes de seguir adelante.

15. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Las organizaciones están continuamente adaptándose a nuevas tecnologías, de las que surgen amenazas y vulnerabilidades que tratar. Por ello es necesario mantener un proceso de mejora continua que incorpora las siguientes acciones:

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios y de la información, y de su categorización.
- Realización de análisis de riesgos anuales.
- Realización de auditorías internas y externas.
- Revisión de las medidas y los controles de seguridad.
- Revisión de las normas y los procedimientos.

16. Revisión de la política de seguridad de la información

Es misión del CEO, en su condición de máxima autoridad, la revisión anual de esta Política de Seguridad de la Información, quedando la propuesta de su revisión o su mantenimiento bajo responsabilidad del Comité de Seguridad. La política es aprobada por el CEO y difundida para que la conozcan todas las partes afectadas.

Esta revisión puede coincidir con la revisión anual del Sistema de Gestión de Seguridad de la Información de Skynet.

Versión	Fecha	Autor	Descripción del cambio	Aprobación
1.0	02/04/2025	Responsable de la Seguridad	Elaboración inicial y aprobación.	Dirección General
1.1	10/07/2025	Responsable de la Seguridad	Revisión tras auditoría interna: condiciones de cumplimiento de la política para terceras partes alineadas con el objetivo inicial; se suprime la vigencia máxima de designación de puestos.	Dirección General
1.2	18/07/2025	Responsable de la Seguridad	Resumen de contenidos para su publicación en web.	Dirección General

			corporativa..	
2.0	01/07/2026	Responsable de la Seguridad	Nuevo formato corporativo. Actualización del marco legal, incorporación del Reglamento de Ciberresiliencia y del Reglamento de Inteligencia Artificial. Incorporación de la categoría ALTA del ENS. Actualización de la estructura documental de referencia y de los roles de organización de la seguridad.	CEO

Firmado por ***5621** MANUEL PEREZ (R: ****6129*) el día 01/07/2026 con un certificado emitido por AC Representación