

WHITEGURU

Política de seguridad

Índice

Aprobación 3
1 Política de seguridad 4
2 Alcance 4
3 Compromisos de la Dirección 5
4 Objetivos 6
5 Legislación aplicable y requisitos contractuales 7
6 Estructura de seguridad 8
7 Documentación de seguridad del sistema 9
8 Principios y requisitos del ENS 9
8.1 Principios básicos del ENS 9
8.1.1 Seguridad integral 9
8.1.2 Gestión de riesgos 10
8.1.3 Prevención, detección, respuesta y conservación 10
8.1.4 Existencia de líneas de defensa 10
8.1.5 Reevaluación periódica 10
8.1.6 Diferenciación de responsabilidades 10
8.1.7 Vigilancia continua 11
8.2 Requisitos mínimos del ENS 11
9 Datos de carácter personal 12
Control de cambios del documento 13

Aprobación

Este documento es propiedad de Whiteguru S.L. Su reproducción total o parcial queda limitada a la autorización expresa por parte del Administrador Único de la organización.

ELABORADO POR	REVISADO POR	APROBADO POR
Manuel Rodríguez Borrego Responsable de sistema	Rubén Arrevola Diez Responsable de seguridad	Rubén Arrevola Diez Administrador Único

1 Política de seguridad

La Dirección de Whiteguru S.L. establece la presente Política de Seguridad de la Información como expresión formal de su compromiso con la protección de la información y de los servicios prestados, considerando la seguridad como un elemento estratégico y parte esencial de la cultura organizativa.

Whiteguru S.L. tiene como misión la prestación de servicios de desarrollo y mantenimiento de aplicaciones informáticas a sus clientes, incluidas entidades del sector público, para lo cual la información y los sistemas que la tratan constituyen activos esenciales cuya protección resulta imprescindible para la calidad y continuidad de los servicios prestados.

La presente Política se desarrolla en cumplimiento de lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y toma como referencia de buenas prácticas la norma ISO/IEC 27001, así como con las directrices recogidas en las Guías CCN-STIC publicadas por el Centro Criptológico Nacional, en particular la Guía 805 relativa a la Política de Seguridad de la Información.

La organización tiene implantado y mantiene un Sistema de Gestión de la Seguridad de la Información (SGSI), integrado en sus procesos de negocio y orientado a la protección de los activos de información frente a amenazas internas o externas, deliberadas o accidentales, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

La presente Política constituye el marco de referencia para la definición de objetivos, normas y procedimientos en materia de seguridad de la información y es de obligado cumplimiento para todo el personal, con independencia de su modalidad contractual, así como para terceros que tengan acceso a los sistemas o a la información incluida en su alcance.

La Política se comunica a toda la organización y se pone a disposición de las partes interesadas pertinentes. Asimismo, proporciona el marco para el establecimiento de los objetivos de seguridad de la información, incluye el compromiso de cumplimiento de los requisitos legales, reglamentarios, contractuales y normativos aplicables, así como el compromiso de mejora continua del SGSI.

La presente Política entra en vigor desde su aprobación por la Dirección y será revisada al menos con carácter anual, a propuesta del Comité de Seguridad, así como cuando se produzcan cambios significativos que puedan afectar al sistema de seguridad, garantizando su adecuación continua al contexto organizativo y normativo.

2 Alcance

La presente Política de Seguridad es de aplicación al Sistema de Gestión de la Seguridad de la Información (SGSI) de Whiteguru S.L., cuyo alcance comprende los sistemas de

información que dan soporte a los servicios de desarrollo y mantenimiento de aplicaciones informáticas, incluyendo los servicios, procesos y activos asociados. Dichos sistemas se encuentran categorizados, conforme al Anexo I del Real Decreto 311/2022, en la categoría MEDIA.

La Política resulta de obligado cumplimiento para todo el personal de la organización, incluidos directivos, empleados, personal temporal y contratistas, así como para terceros que tengan acceso a los sistemas de información o a la información incluida en el alcance del SGSI.

El alcance incluye tanto los activos de información propios de la organización como aquellos gestionados o tratados por terceros en el marco de relaciones contractuales, con independencia del soporte o medio en el que se encuentren.

3 Compromisos de la Dirección

El Administrador Único de Whiteguru S.L. asume la responsabilidad última sobre la seguridad de la información en la organización y lidera el desarrollo, implantación y mejora continua del Sistema de Gestión de la Seguridad de la Información.

La dirección:

- Comunica a la organización la importancia de satisfacer los requisitos de seguridad, legales, reglamentarios, contractuales y del servicio, así como las obligaciones derivadas del Esquema Nacional de Seguridad.
- Establece y comunica el alcance del SGSI.
- Aprueba la Política de Seguridad, la categorización de los sistemas, la Declaración de Aplicabilidad del ENS, los criterios de aceptación del riesgo y las decisiones relativas al tratamiento de riesgos.
- Asegura la provisión de los recursos necesarios para la implantación, mantenimiento y mejora del SGSI.
- Garantiza la definición y asignación formal de roles y responsabilidades en materia de seguridad de la información.
- Realiza la revisión periódica del SGSI, incluyendo el análisis de resultados de auditorías, incidentes, indicadores y estado general de la seguridad, promoviendo la adopción de acciones correctivas y de mejora cuando resulte necesario.
- Comunica la Política de Seguridad y la importancia de cumplir con ella a clientes y a proveedores (contrato de confidencialidad).
- Asegura el establecimiento y la comunicación de los objetivos de seguridad de la Información.
- Determina las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección se materializa mediante su participación activa en el Comité de Seguridad y en la revisión periódica del estado de la seguridad, y está reflejado en la presente política.

4 Objetivos

Los objetivos del Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización son:

- Mantener una gestión adecuada del SGSI de acuerdo con los estándares de seguridad y las buenas prácticas del sector, llevando a cabo todo esto de manera que se aseguren ventajas competitivas para la organización.
- Garantizar la protección de la información y de los servicios prestados, preservando sus dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Gestionar los riesgos de seguridad de la información de forma sistemática, documentada y continua, adoptando medidas proporcionales a la categoría del sistema y al nivel de riesgo identificado.
- Garantizar la continuidad de los servicios mediante la implantación de medidas preventivas, de detección, respuesta y recuperación ante incidentes de seguridad.
- Asegurar el cumplimiento de los requisitos legales, reglamentarios, contractuales y normativos aplicables, en particular los establecidos en el Esquema Nacional de Seguridad.
- Establecer y mantener una estructura organizativa clara, con roles y responsabilidades definidos y formalmente asignados en materia de seguridad de la información.
- Promover la concienciación, formación y capacitación del personal en materia de seguridad, fomentando una cultura organizativa orientada a la protección de la información. La organización establece programas periódicos de formación y concienciación en seguridad de la información, adecuados a las funciones y responsabilidades del personal, asegurando su actualización continua y dejando evidencia documental de su realización.
- Evaluar de forma periódica la eficacia del Sistema de Gestión de la Seguridad de la Información, mediante procesos de seguimiento, revisión y auditoría, asegurando su mejora continua.

Los objetivos específicos de seguridad de la información se establecen y revisan periódicamente en el marco del SGSI, siendo coherentes con la presente Política y con el contexto estratégico de la organización.

5 Legislación aplicable y requisitos contractuales

Se identifican las siguientes obligaciones legales aplicables a la organización en relación a la seguridad de la información:

- Esquema Nacional de Seguridad:
  - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
  - Instrucciones Técnicas de Seguridad y demás disposiciones dictadas en desarrollo del Esquema Nacional de Seguridad.
  - Guías CCN-STIC y demás documentos técnicos de apoyo publicados por el Centro Criptológico Nacional para el desarrollo e interpretación del Esquema Nacional de Seguridad.
  - Aplicabilidad: alcance del SGSI.
- 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 y por el que se deroga la Directiva 95/46/CE (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
  - Aplicabilidad: tratamiento de datos de carácter personal propios tanto de Whiteguru S.L. como de empresas externas (encargados de tratamiento, destinatarios).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE).
  - Aplicabilidad: actividades comerciales en internet de la organización.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
  - Aplicabilidad: actividad de la empresa.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, y Ley 17/2001, de 7 de diciembre, de Marcas.
  - Aplicabilidad: licencias software, nombres comerciales.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
  - Aplicabilidad: prestación de servicios a entidades del sector público.
- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza (eIDAS), en su redacción dada por el Reglamento (UE) 2024/1183, y Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
  - Aplicabilidad: uso de certificados y firma electrónica por la organización.

Además, se consideran los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de seguridad.

La organización mantiene identificados y actualizados los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad de la información. La revisión de estos requisitos se realiza de forma periódica y siempre que se produzcan cambios normativos

relevantes, quedando documentadas las actualizaciones correspondientes en el marco del Sistema de Gestión de la Seguridad de la Información.

6 Estructura de seguridad

La organización dispone de una estructura organizativa formal en materia de seguridad de la información, conforme a lo establecido en el Real Decreto 311/2022, garantizando la diferenciación de responsabilidades y la ausencia de conflictos de interés.

Se encuentran formalmente designados los roles de seguridad de la información (Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema) en el documento «Estructura de seguridad» y en las correspondientes actas de designación y aceptación, definiendo para cada uno las funciones y responsabilidades de su cargo, así como el procedimiento para su designación y renovación. En este sentido, el Responsable de Seguridad reporta directamente a la Dirección y dispone de la autoridad necesaria para supervisar el cumplimiento de las medidas de seguridad, pudiendo elevar incidencias o incumplimientos sin interferencias operativas.

La organización dispone asimismo de un Comité de Seguridad, como órgano colegiado de coordinación y seguimiento, que supervisa el estado de la seguridad, analiza riesgos e incidentes y promueve la mejora continua del sistema.

El Comité de Seguridad está compuesto por el Responsable del Comité, el Responsable de Seguridad y el Responsable del Sistema, con la participación de la Dirección en su condición de Responsable de la Información y del Servicio. Se reúne con carácter semestral y, de forma extraordinaria, cuando la situación de seguridad lo requiera, dejando constancia de sus decisiones en las correspondientes actas.

Dado el reducido tamaño de la organización, determinados roles recaen en una misma persona. En todo caso, se garantiza la separación entre el Responsable de Seguridad y el Responsable del Sistema exigida por el artículo 11 del Real Decreto 311/2022, y la acumulación del resto de funciones se compensa mediante el registro documentado de las decisiones del Comité de Seguridad y la verificación independiente que aportan las auditorías de seguridad periódicas.

La designación de los responsables se realiza formalmente por la Dirección y queda debidamente documentada.

Los roles y responsabilidades en relación al SGSI son comunicados a las nuevas incorporaciones y recordados periódicamente a todo el personal de la organización.

En caso de conflicto o discrepancia entre los responsables definidos en materia de seguridad de la información, la resolución corresponderá a la Dirección, previo análisis en el seno del Comité de Seguridad, garantizando la adecuada ponderación de los riesgos y el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad.

7 Documentación de seguridad del sistema

El Sistema de Gestión de la Seguridad de la Información dispone de una estructura documental formalmente establecida, organizada en diferentes niveles (política, normativa, procedimientos, instrucciones técnicas y registros asociados).

Cada uno de estos documentos está debidamente identificado, aprobado, revisado y controlado conforme al procedimiento de gestión documental del SGSI.

La documentación del SGSI es aprobada por la Dirección o por el Comité de Seguridad, según corresponda, y se mantiene actualizada para garantizar su coherencia con el Esquema Nacional de Seguridad y con las buenas prácticas de referencia (ISO/IEC 27001).

La documentación se conserva en repositorios de acceso controlado y se comunica al personal cuando resulte aplicable.

En el procedimiento «Gestión de documentación» se establece la gestión que se realiza de la documentación del SGSI (elaboración, aprobación, control de versiones, distribución, archivo y conservación) y en la normativa «Calificación de la información» se especifica la categorización establecida y las condiciones de acceso a cada nivel.

8 Principios y requisitos del ENS

8.1 Principios básicos del ENS

La organización desarrolla y mantiene su Sistema de Gestión de la Seguridad de la Información conforme a los principios básicos establecidos en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

Estos principios rigen de forma permanente la protección de la información y de los servicios prestados, aplicándose de manera proporcional a la categoría de los sistemas y a los riesgos identificados.

8.1.1 *Seguridad integral*

La seguridad se gestiona como un proceso integral que abarca la totalidad de los elementos técnicos, humanos, organizativos y materiales relacionados con los sistemas de información.

La organización protege todas las dimensiones de la seguridad —confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad— garantizando una visión global y coordinada de la protección de los activos de información.

8.1.2 *Gestión de riesgos*

La organización dispone de un proceso formal, continuo y documentado de análisis y tratamiento de riesgos, que permite identificar, evaluar y mitigar las amenazas que pueden afectar a los sistemas de información.

Las medidas de seguridad implantadas son proporcionales a los riesgos identificados y a la categoría del sistema, garantizando un nivel adecuado de protección.

8.1.3 *Prevención, detección, respuesta y conservación*

La organización aplica un enfoque integral de seguridad que contempla medidas de prevención, mecanismos de detección, procedimientos de respuesta ante incidentes y capacidades de recuperación y conservación de la información y los servicios, con el objetivo de minimizar el impacto sobre la información y los servicios y asegurar la continuidad de la actividad.

8.1.4 *Existencia de líneas de defensa*

La organización dispone de una estrategia de protección constituida por múltiples capas de seguridad, de naturaleza organizativa, física y lógica, de modo que, cuando una de ellas resulte comprometida, las restantes permitan desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar su impacto final.

8.1.5 *Reevaluación periódica*

Las medidas de seguridad implantadas son objeto de revisión periódica y siempre que se producen cambios significativos en los sistemas, en el entorno tecnológico, en el marco normativo o en el nivel de riesgo.

Esta reevaluación garantiza la adecuación y eficacia continua del sistema de seguridad.

8.1.6 *Diferenciación de responsabilidades*

Las responsabilidades en materia de seguridad se encuentran claramente definidas, documentadas y formalmente asignadas.

La organización garantiza la separación de funciones y evita conflictos de interés, diferenciando adecuadamente las funciones de supervisión, control y operación de los sistemas.

El Responsable de Seguridad ejerce sus funciones con la independencia necesaria respecto de la operación y administración de los sistemas de información, garantizando la objetividad en la supervisión del cumplimiento de las medidas de seguridad establecidas.

8.1.7 *Vigilancia continua*

La organización mantiene mecanismos de supervisión y monitorización continua del estado de seguridad de los sistemas de información, que permiten detectar desviaciones, incidentes o vulnerabilidades y adoptar las medidas correctoras necesarias. La información derivada de la monitorización es analizada sistemáticamente y utilizada para la mejora preventiva del sistema.

8.2 Requisitos mínimos del ENS

En cumplimiento de lo dispuesto en los artículos 12 a 27 del Real Decreto 311/2022, de 3 de mayo, la organización tiene implantadas las medidas de seguridad del Anexo II necesarias para dar satisfacción a los requisitos mínimos del Esquema Nacional de Seguridad, en función de la categoría del sistema y de los riesgos identificados.

La organización ha realizado la categorización de sus sistemas conforme a los criterios establecidos en el Anexo I del ENS, resultando la categoría MEDIA, aplicando las medidas de seguridad correspondientes de manera proporcional y adecuada al impacto potencial sobre la información y los servicios.

Las medidas de seguridad implantadas se encuentran recogidas en la Declaración de Aplicabilidad del ENS y desarrolladas en la normativa interna, procedimientos y controles operativos del Sistema de Gestión de la Seguridad de la Información. Dichas medidas abarcan, entre otros, los siguientes ámbitos:

- Marco organizativo y responsabilidades en materia de seguridad.
- Análisis y gestión continua de riesgos.
- Gestión de personal y concienciación en seguridad.
- Profesionalidad del personal con responsabilidades en materia de seguridad.
- Control de accesos y protección de identidades.
- Protección de instalaciones, infraestructuras y entornos físicos.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio en la configuración de los sistemas.
- Integridad y actualización del sistema.
- Protección de sistemas, comunicaciones y servicios interconectados.
- Protección de la información en almacenamiento y en tránsito.
- Registro de actividad, monitorización y detección de eventos de seguridad.
- Gestión de incidentes y notificación cuando proceda.

- Continuidad del servicio y recuperación ante desastres.
- Supervisión, auditoría y mejora continua del sistema de seguridad.

La eficacia y adecuación de las medidas implantadas son objeto de seguimiento continuo y de revisión periódica. Asimismo, cuando la categoría del sistema lo requiera, la organización somete el sistema a auditorías de seguridad conforme a lo establecido en el ENS, adoptando las acciones correctoras necesarias para garantizar el mantenimiento del nivel de seguridad exigido.

La organización elabora y mantiene actualizado el informe del estado de la seguridad, que permite evaluar el grado de cumplimiento del ENS y promover la mejora continua del sistema.

Los resultados de las auditorías y revisiones son analizados por la Dirección en el marco de la revisión del SGSI, adoptándose las acciones correctoras y de mejora que resulten necesarias.

9 Datos de carácter personal

Whiteguru S.L. trata datos de carácter personal de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). La organización está cumpliendo con todas las disposiciones del RGPD para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del RGPD, por los cuales son tratados de manera lícita, leal y transparente en relación con el interesado y adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

La organización garantiza que implementa políticas técnicas y organizativas apropiadas para garantizar las medidas de seguridad que establece el artículo 32 del RGPD con el fin de proteger los derechos y libertades de los interesados.

Los riesgos derivados del tratamiento de datos personales se identifican y evalúan en el marco del análisis de riesgos del sistema y, cuando proceda, mediante la correspondiente evaluación de impacto relativa a la protección de datos (artículo 35 del RGPD). La organización mantiene actualizado el Registro de Actividades de Tratamiento y cuenta con asesoramiento externo especializado en protección de datos.

28794912Q RUBEN ARREVOLA (R: B90241753)

Firmado digitalmente por 28794912Q RUBEN ARREVOLA (R: B90241753)
Fecha: 2026.11.24 08:43:30 +01'00'

Sevilla, a 19 de noviembre de 2026

Rubén Arrevola Diez

Administrador Único de Whiteguru S.L.

Control de cambios del documento

Versión	Fecha	Motivo del cambio
1.0	21/10/2026	Creación inicial
1.1	18/11/2026	Incorporación de las correcciones