Política sobre

seguridad de la información

GARRIGUES

GARRIGUES

Edición 04, junio 2025

Índice

1. Introducción

El Grupo Garrigues ha tomado la decisión de gestionar los Sistemas de la Información (en adelante, SGSI) utilizando las mejores prácticas internacionales, conforme al estándar ISO/IEC 27001 y Esquema Nacional de Seguridad (ENS).

Teniendo en cuenta lo anterior, la presente Política de Seguridad de la Información se elabora en cumplimiento de las exigencias legales previstas en las siguientes disposiciones normativas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Norma ISO27001.
- 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 (Reglamento general de protección de datos), y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-gdd).

El tratamiento de la información debe basarse en los principios de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad.

2. Objetivos

Este documento tiene como objeto recoger la Política de Seguridad de la Información del Grupo Garrigues, en la que se especifican los compromisos asumidos por la Dirección en relación al Sistema de Gestión de la Seguridad de la Información aplicado a los sistemas de información que dan soporte a los servicios de Asesoramiento Jurídico y Fiscal, Asesoramiento en Transacciones y en Procedimientos administrativos y/o judiciales, y servicios de Consultoría prestados por las empresas del Grupo Garrigues a sus clientes, definiendo el marco organizativo y ejecutivo que garantice la confidencialidad, integridad y disponibilidad del sistema de información.

La aprobación de la citada Política se enmarca en el proceso de implantación del Sistema de Gestión de la Seguridad de la Información de Garrigues, con el que se persigue garantizar que nuestros Sistemas de Información están siendo gestionados con la seguridad requerida, utilizando para ello las mejores prácticas internacionales conforme el estándar ISO/IEC 27001 y Esquema Nacional de Seguridad (ENS).

El Objetivo de la Política de Seguridad de los Sistemas de Información es doble:

- Por un lado, consiste en definir el **marco de referencia** que permita salvaguardar las características de seguridad de los activos que dan soporte a los procesos del Grupo Garrigues. Y ello, en base a los resultados del análisis de riesgos realizado,

a los requisitos estratégicos del negocio alineados con los requisitos de seguridad, así como a los requisitos legales y contractuales. Como exige el marco de referencia anteriormente mencionado, esta Política de Seguridad sirve para establecer los principios fundamentales de seguridad de los Sistemas de Información que se desarrollan en las normas, procedimientos, instrucciones técnicas, registros u otros documentos necesarios para especificar el uso de la información, de los sistemas y de los activos que los soportan.

- Por otro, la Política de Seguridad de la Información de Garrigues tiene como objetivo establecer las **medidas de seguridad** de naturaleza organizativa, física y lógica que se consideran adecuadas para salvaguardar las características de seguridad de los activos mencionados, partiendo del presupuesto de que la seguridad debe ser concebida como un proceso integral transversal (que comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y comunicaciones), y no debe entenderse como un gasto en la gestión, sino como una inversión en evitar impactos negativos sobre el negocio.

3. Marco legal y regulatorio

El marco legal y regulatorio aplicable se gobierna en el "Procedimiento de gestión del cumplimiento legal y contractual", incorporado en el SGSI como documento "PRG 18.1", en el cual se identifica la legislación aplicable, las implicaciones en la protección de datos de carácter personal y las responsabilidades y obligaciones asignadas.

Adicionalmente, se mantiene un registro detallado de la normativa aplicable en el "Registro de la legislación aplicable y obligaciones contractuales", incorporado en el SGSI como documento "RG 18.01".

4. Alcance

Esta Política es de aplicación a los Sistemas de Información referentes al proceso de clientes que trata el Grupo Garrigues en el desarrollo de sus actividades. Cualquier normativa, procedimiento o documento interno que trate algún aspecto particular de la seguridad referida a los Sistemas de Información debe respetar y cumplir con lo establecido en esta Política.

La Política establecida en este documento es aplicable a todos los empleados, socios y otros miembros de sociedades del Grupo Garrigues integradas en los sistemas de Garrigues, así como a colaboradores y terceros relacionados con las actividades y procesos de negocio definidos dentro del alcance del SGSI, que dan soporte a los procesos relacionados con clientes del Grupo Garrigues (en adelante, "usuarios de la información" o, simplemente, "usuarios").

5. Principios fundamentales de la Política de Seguridad

Dada la importancia que tienen los Sistemas de Información, Garrigues establece a través de su Dirección los siguientes Principios Fundamentales de Seguridad de la Información:

(a) Principio de cumplimiento normativo: todos los Sistemas de Información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

(b) Principio de gestión del riesgo: se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre los controles de seguridad y la naturaleza de la información. Los objetivos de seguridad deben ser establecidos, ser revisados y coherentes con los aspectos de seguridad de la información.

Todos los sistemas afectados por esta Política de Seguridad de la Información están sujetos a un análisis de riesgos para evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando la información y/o servicios gestionados cambien significativamente.
- Cuando ocurra un incidente de seguridad grave o se detecten vulnerabilidades graves.

En el marco de la categorización de los sistemas, se definirán los criterios de determinación de los niveles de seguridad de los sistemas.

(c) Principio de concienciación y formación: se articularán programas de formación, sensibilización y campañas de concienciación para todos los usuarios, adaptados a su perfil profesional, con acceso a la información, en materia de seguridad de la información.

(d) Principios de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad:

- Se debe garantizar **la confidencialidad** de la información, de tal manera que solo tengan acceso a la misma las personas autorizadas.
- Deberá asegurarse **la integridad** de la información con la que se trabaja, de modo que sea concisa y precisa, incidiéndose en la exactitud, tanto de su contenido como de los procesos involucrados.
- Se debe garantizar **la disponibilidad** de la información, asegurándose la continuidad del negocio soportado por los servicios de la información mediante planes de contingencias.

- Se debe garantizar **la trazabilidad** de la información, para asegurar que las actuaciones de una entidad (persona o proceso) puedan ser trazadas de forma indiscutible hasta dicha entidad.

- Se debe garantizar **la autenticidad** de la información, para asegurar la identidad de la entidad (persona o proceso) que trata dicha información.

(e) Principio de proporcionalidad: la implantación de controles que mitiguen los riesgos de seguridad de los activos debe hacerse buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y riesgo.

(f) Principio de responsabilidad: todos los miembros del Grupo Garrigues deben ser responsables en su conducta en cuanto a la seguridad de la información, cumpliendo con las normas y controles establecidos.

(g) Principio de mejora continua: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados en el Despacho para aumentar la capacidad de adaptación a la constante evolución del riesgo y del entorno tecnológico. Dentro de las revisiones que se realizan se tendrá en cuenta anualmente la revisión de servicios e información y su categorización, normas y procedimientos y la realización de auditorías internas o en su caso externas, y la ejecución anual del análisis de riesgos.

6. Responsabilidades

Sin perjuicio de que cada uno de los usuarios es responsable de la información a la que tiene acceso y/o maneja como consecuencia del desempeño de sus funciones, hay personas y/u órganos con funciones concretas en el SGSI de Garrigues a los que se le atribuyen las siguientes responsabilidades específicas en relación con esta Política:

6.1 Dirección

La Dirección es la responsable directa de velar por el cumplimiento de las normas de seguridad, lo que implica que debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información, asegurarse de que se establecen la política y objetivos de seguridad y que éstos son compatibles con la dirección estratégica.

Por ello, entre sus funciones se encuentra la de aprobar esta Política de Seguridad, nombrar al Responsable de Seguridad de los Sistemas de Información y al resto de los roles requeridos por el ENS, aprobar la constitución y composición del Comité de Seguridad y Privacidad y autorizar la Creación de la Oficina Técnica de Seguridad.

Además, la Dirección debe informar y formar a los usuarios de los Sistemas de Información sobre la existencia y el contenido de esta Política, que debe ser conocida por todos en la organización, pues de ella emanan las demás directrices en cuanto a la aplicación de medidas de seguridad para obtener un nivel adecuado de protección.

6.2 Comité de Seguridad y Privacidad

El Comité de Seguridad y Privacidad debe revisar –al menos– una vez al año que la Política de Seguridad sigue siendo adecuada al propósito de la organización, proporciona un marco de coordinación y referencia para el establecimiento de los objetivos de seguridad de la información, incluye el compromiso de mejora continua, está disponible para las partes interesadas y ha sido comunicada a nivel interno. También debe revisar que ha sido aprobada por la Dirección.

En definitiva, el Comité de Seguridad y Privacidad debe revisar anualmente, o siempre que se produzcan cambios significativos, que la Política de Seguridad mantiene su idoneidad, adecuación y eficacia, proponiendo si es necesario mejoras. Además, el Comité de Seguridad y Privacidad es el órgano establecido para la resolución de posibles conflictos.

La composición del Comité de Seguridad y Privacidad de la Información se define en el documento “Normativa Definición roles y responsabilidades”, incorporado en el SGSI como documento“NOR02”,, en su apartado 5.2 Comité de Seguridad y Privacidad.

El nombramiento se revisará cada año o cuando algún puesto quede vacante.

6.3 Oficina Técnica de Seguridad

La Oficina Técnica de Seguridad es la responsable de verificar que todos los proyectos operativos que se desarrollan en Garrigues siguen y respetan los principios fundamentales establecidos en esta Política de Seguridad.

6.4 Roles y responsabilidades Esquema Nacional de Seguridad

En el marco del cumplimiento con el Esquema Nacional de Seguridad (ENS) se definen los siguientes roles y responsabilidades:

- **Responsable de la Información**, que determina los requerimientos de la información procesada.
- **Responsable de Servicio**, que determina los requisitos de los servicios prestados.
- **Responsable de Seguridad**, persona encargada de tomar decisiones de requerimientos de seguridad y supervisar la implantación de las medidas necesarias para garantizar que se satisfacen dichos requisitos.
- **Responsable del Sistema**, persona encargada de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo.

Responsable de la información: Comité de Seguridad y Privacidad

Responsable del servicio: Comité de Seguridad y Privacidad

Responsable de la seguridad: CISO

Responsable del sistema: CIO

El nombramiento y la revisión de los roles ENS se realizará por la Dirección cada año o cuando alguno de los puestos quede vacante.

7. Usuarios

Todos los usuarios deben cumplir con los principios fundamentales establecidos en la Política de Seguridad y en el resto de políticas Internas incluidas en el Sistema Normativo Interno de Garrigues.

En caso de falta de cumplimiento de los usuarios de la política, normas y procedimientos vigentes en materia de seguridad de la información, se procederá con el correspondiente proceso disciplinario.

8. Prevención

Para garantizar el cumplimiento de la política de seguridad, la organización tomará las siguientes medidas de prevención:

- Autorizar los sistemas antes de entrar en funcionamiento para garantizar que cumplan con los requisitos de seguridad.
- Evaluar periódicamente la seguridad, incluidas las evaluaciones de los cambios de configuración realizados rutinariamente.
- Solicitar revisión periódica por parte de terceros para obtener una evaluación independiente.

9. Detección

Se establecerán mecanismos de detección, análisis y reporte, que llegarán periódicamente a los responsables cuando se produzca una desviación significativa de los parámetros que se han preestablecido como normales.

10. Respuesta

Garrigues realiza una serie de acciones de respuesta:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones sobre incidentes detectados en cualquier área de la organización.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye la comunicación bidireccional con el cliente.

11. Recuperación

Garrigues dispone de un plan de continuidad de negocio para garantizar la disponibilidad de los sistemas y servicios críticos. En concreto, Garrigues ha establecido:

- Plan de continuidad de negocio.
- Análisis de impacto de negocio.
- Plan de recuperación ante desastres

El Plan de Continuidad de Garrigues está diseñado para respaldar la operación continua en actividades de soporte clave de Garrigues, reducir el daño y el impacto de incidentes inesperados en los servicios mejorar la capacidad de recuperar rápidamente el negocio.

12. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, Garrigues notificará a sus clientes aquellas incidencias que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización del sistema ENS. Dicha operativa queda referenciada en el del procedimiento de Gestión de Incidentes de seguridad de la información, incorporado en el SGSI como documento “A.16”.

13. Terceras partes

Los principios de esta Política de Seguridad de la Información están publicados en la web de Garrigues para que estén a disposición de clientes, proveedores y terceros interesados.

Cualquier tercero que acceda a información de Garrigues, en el marco de una prestación de servicios a Garrigues, deberá conocer esta Política de Seguridad y la normativa asociada, y comprometerse al debido cumplimiento de las obligaciones derivadas de ella, pudiendo desarrollar en su caso sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se exigirá que el personal de esos terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de 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 los servicios afectados antes de seguir adelante.

14. Aprobación y divulgación de la política de seguridad

Esta Política ha sido aprobada por la Dirección, que ha verificado:

- Que es adecuada con el propósito de la organización;
- Que incluye un marco de referencia para el establecimiento de objetivos de Seguridad de la Información;
- Que incluye el compromiso de cumplir con los requisitos aplicables de seguridad y mejora continua.

Como se indica en el apartado 6.1 anterior, la Dirección debe informar a los usuarios sobre la existencia y el contenido de esta Política, que debe ser conocida por todos en la organización.

Por ello, esta Política de Seguridad permanecerá publicada en la Intranet de Garrigues, junto con el resto de Políticas Internas que forman parte del Sistema Normativo Interno del Despacho, donde podrá ser consultada permanentemente por los usuarios de la información que sean miembros de Garrigues.

Una vez publicada en la Intranet, la Dirección informará de ello a los miembros de la organización mediante el envío de un correo electrónico, de modo que conozcan la existencia de esta Política y dónde pueden consultarla.

Además, el apartado 5 de esta Política, que recoge los Principios Fundamentales de la Política de Seguridad, permanecerá publicado en la web de Garrigues.

15. Revisión de la Política de Seguridad

La Política de Seguridad de la Información será revisada una vez al año, de forma habitual, y cuando existan cambios relevantes, de forma extraordinaria.

El Comité de Seguridad y Privacidad deberá notificar a la Dirección las modificaciones que se introduzcan en la Política de Seguridad, con el fin de asegurar que se mantenga su idoneidad, adecuación y eficacia, y dejar cumplida constancia de tales modificaciones en el registro de “Control documental”.

16. Referencias

En la redacción de esta Política de Seguridad se han tenido en cuenta las siguientes referencias:

- Norma ISO/IEC 27001
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Normativa de protección de datos personales europea y local que resulte de aplicación.

- El documento denominado “Revisión del Sistema de Gestión de Seguridad de la Información por Dirección”, que forma parte del SGSI de Garrigues.

17. Histórico de versiones

Versión	Fecha	Resumen de los cambios producidos
Edición 01	Julio 2017	Versión inicial de la política
Edición 02	Abril 2018	Modificaciones en el alcance y objeto de la política para recoger los compromisos de Garrigues en la implementación del Sistema de Gestión de la Seguridad de la Información y definir el marco organizativo y ejecutivo que garantice la confidencialidad, integridad y disponibilidad del sistema de información.
Edición 03	Octubre 2018	Ajuste de la mención a la normativa de protección de datos de aplicación
Edición 04	Junio 2025	Adaptación de la política al estándar Esquema Nacional de Seguridad (ENS)