POLÍTICA INTEGRADA DE GESTIÓN

IUS GENTIUM ABOGADOS

APROBACIÓN DEL DOCUMENTO	
Aprobado por: FRANCISCO JAVIER TORNOS MARTIN-FERNANDEZ Firmado digitalmente por FRANCISCO JAVIER TORNOS MARTIN-FERNANDEZ Fecha: 2026.07.07 17:11:30 +02'00' Javier Tornos (Alta Dirección y Responsable SGSI)	**Fecha** 23/06/2026

HISTORIAL DE VERSIONES		
Versión	**Fecha**	**Modificación**
1	17/11/2025	Creación del documento para adaptación a la norma UNE-ISO/IEC 27001:2023 y UNE-EN-ISO 9001:2015.
2	05/01/2026	Integración de la norma UNE-EN-ISO 9001:2015.
3	23/06/2026	Integración de las normas UNE-EN-ISO 14001:2015 y 45001:2018.

CLASIFICACIÓN DEL DOCUMENTO	PROPIETARIO DEL DOCUMENTO
Público	Comité de Seguridad y Alta Dirección

REFERENCIAS DEL DOCUMENTO

Este documento ha sido preparado utilizando los siguientes requerimientos como referencia:

De la Cláusula 5: Liderazgo – de la norma UNE-ISO/IEC 27001:2023: 5.2 Política.

Del Anexo A - Controles Organizacionales -de la norma UNE-ISO/IEC 27001:2023: A.5.1: Políticas para la seguridad de la información.

De la Cláusula 5: Liderazgo – de la norma UNE-EN-ISO9001:2015: 5.2. Política de la Calidad.

De la Cláusula 5.2 – de la norma UNE-EN-ISO 14001:2015: 5.2. Política ambiental.

De la Cláusula 5.2 – de la norma UNE-EN-ISO 45001:2018: 5.2. Política de la seguridad y salud en el trabajo.

Política Integrada de Gestión de Ius Gentium Abogados

1. Propósito y alineación estratégica

La presente política establece el marco general para la gestión de la seguridad de la información, calidad, gestión ambiental y seguridad y salud en el trabajo en Ius Gentium Abogados, alineándose con los objetivos estratégicos del despacho y contribuyendo a la excelencia, confianza y competitividad en el sector jurídico. Su finalidad es proteger la confidencialidad, integridad y disponibilidad de la información, así como garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables.

2. Alcance

Esta política aplica a todos los empleados, colaboradores, proveedores y partes interesadas que accedan, procesen o gestionen información de la organización, así como a todos los sistemas, procesos y activos de información definidos en el alcance del Sistema de Gestión de Seguridad de la Información, calidad, gestión ambiental y seguridad y salud en el trabajo

3. Definiciones

En el marco de la seguridad de la información, calidad, gestión ambiental y seguridad y salud en el trabajo de Ius Gentium Abogados, y conforme a la normativa ISO/IEC 27001:2023 y UNE-EN-ISO 9001:2015, se establecen las siguientes definiciones para garantizar la comprensión y correcta aplicación de las políticas y procedimientos:

- **Activo de información:** Cualquier dato, documento, sistema o recurso que tenga valor para la organización y cuya protección es esencial para la prestación de servicios jurídicos y el cumplimiento normativo.
- **Incidente de seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de la información gestionada por el despacho, incluyendo accesos no autorizados, fugas de información, pérdida de datos o interrupciones de servicio.
- **Riesgo:** Posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo en los activos de información, afectando a la operativa, la reputación o el cumplimiento legal de la organización.

4. Principios

La seguridad de la información en Ius Gentium Abogados se fundamenta en los siguientes principios básicos, que garantizan la protección de los activos de información y el cumplimiento de los requisitos legales y contractuales:

- **Confidencialidad:** La información solo será accesible por personas autorizadas, asegurando que los datos jurídicos y personales de clientes, empleados y colaboradores estén protegidos frente a accesos no autorizados.
- **Integridad:** La información será precisa, completa y estará protegida contra modificaciones no autorizadas, garantizando la fiabilidad de los expedientes, documentos y comunicaciones.
- **Disponibilidad:** La información estará disponible cuando sea requerida por los procesos de negocio, permitiendo la continuidad de los servicios jurídicos y el acceso oportuno a los datos necesarios para la operativa del despacho.

5. Compromiso de la Dirección

La Alta Dirección se compromete a proporcionar los recursos necesarios para la implantación, mantenimiento y mejora continua del SIG, liderando y apoyando la cultura de seguridad en la organización, calidad, gestión ambiental y seguridad y salud en el trabajo. Esta política es aprobada y firmada por la dirección, evidenciando su compromiso.

La gestión de la seguridad de la información, calidad, gestión ambiental y seguridad y salud en el trabajo en Ius Gentium Abogados se apoya en una estructura de gobierno clara y definida, que garantiza la responsabilidad, el liderazgo y la supervisión efectiva de todas las medidas y controles implantados. Es por ello, que el despacho ha nombrado un Comité de Seguridad, compuesto por un equipo multidisciplinar, que se encarga de coordinar la implantación del SIG, encargado de la implantación y mantenimiento del SIG y de tomar decisiones estratégicas y revisar de forma continua de la eficacia del sistema, asegurando la protección de los activos de información y el cumplimiento normativo.

La Alta Dirección se compromete a proporcionar condiciones de trabajo seguras y saludables para la prevención de lesiones y deterioro de la salud relacionados con el trabajo y que sea apropiada al propósito, tamaño y contexto de la organización y a la naturaleza específica de sus riesgos y oportunidades para la SST.

6. Objetivos del Sistema Integrado de Gestión

Los objetivos de seguridad de la información, calidad, gestión ambiental y seguridad y salud en el trabajo de Ius Gentium Abogados están alineados con la estrategia del despacho y los requisitos de la norma ISO 27001, ISO 9001, ISO 14001 e ISO 45001. Estos objetivos orientan todas las acciones y controles del SIG, asegurando la protección de los activos de información y la mejora continua del sistema integrado de gestión. Concretamente:

- Proteger los activos de información frente a amenazas internas y externas.

- Cumplir con los requisitos legales, reglamentarios y contractuales.
- Promover la concienciación y formación en seguridad de la información, calidad, gestión ambiental y seguridad y salud en el trabajo.
- Gestionar los riesgos de seguridad de la información de forma sistemática.
- Eliminar los peligros y reducir los riesgos para la seguridad y salud en el trabajo.
- Fomentar la mejora continua del SGSI.
- Promover un compromiso para la consulta y la participación de los trabajadores, y cuando existan, de los representantes de los trabajadores
- Promover un compromiso para la protección del medio ambiente, incluida la prevención de la contaminación, y otros compromisos específicos al contexto de la organización.

7. Roles y Responsabilidades

La correcta implantación y funcionamiento del SGSI y del SIG requiere que todos los miembros del despacho conozcan y asuman sus roles y responsabilidades en materia de seguridad de la información, calidad, gestión ambiental y seguridad y salud en el trabajo.

El cumplimiento de esta política es obligatorio para todo el personal, y su incumplimiento podría derivar acciones disciplinarias, civiles y/o penales oportunas.

8. Gestión de Riesgos

La organización realizará evaluaciones periódicas de riesgos de seguridad de la información y aplicará controles adecuados para su tratamiento, conforme al Anexo A de la ISO 27001 y conforme a la ISO 9001, ISO 14001 e ISO 45001, conforme al requisito 6.1. Los resultados se documentarán y los controles se revisarán ante cambios relevantes en el entorno, la legislación o tras incidentes significativos.

9. Cumplimiento y mejora continua

La organización se compromete a cumplir con la legislación vigente y a revisar periódicamente esta política y el SIG, promoviendo la mejora continua y la adaptación a nuevas amenazas, requisitos legales o lecciones aprendidas de auditorías e incidentes.

10. Comunicación

Esta política será comunicada a todo el personal y estará disponible para las partes interesadas relevantes.

11. Revisión

Esta política será revisada al menos una vez al año o cuando se produzcan cambios significativos en la organización, en los requisitos legales o en el entorno de amenazas.