

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN

Investigación y Consulting es una empresa de seguridad dedicada al diseño, integración, instalación y mantenimiento de sistemas y aplicaciones informáticas y electrónicas de seguridad y control; y al diseño, instalación y mantenimiento de soluciones de protección contra incendios.

Debido al sector en el que opera la empresa, la información es un activo muy valioso para nosotros, por lo que requiere de una protección y gestión adecuadas.

En Investigación y Consulting, S.A., como empresa de seguridad, nos preocupamos de la seguridad de las personas, tanto de nuestros clientes, como de nuestros trabajadores y colaboradores, es por ello que consideramos la Seguridad y Salud en el Trabajo como un factor esencial de nuestra actividad, promoviendo un entorno de trabajo seguro y saludable.

1. Objeto

La presente Política integrada establece los principios y compromisos de la organización para garantizar la calidad de los servicios prestados, la protección del medio ambiente, la seguridad y salud en el trabajo y la seguridad de la información, asegurando la mejora continua de los procesos y el cumplimiento de los requisitos legales y normativos aplicables.

Nuestra **política de calidad, ambiental, seguridad y salud en el trabajo y seguridad de la información** es el motor que conduce a Investigación & Consulting hacia la mejora del desempeño de la organización en todos sus ámbitos, está alineada con el propósito, el tamaño, el contexto de la organización y los riesgos y oportunidades. Constituye el marco de referencia para el Sistema Integrado de Gestión implantado en la organización, que integra:

- Sistema de Gestión de la Calidad
- Sistema de Gestión Ambiental
- Sistemas de Gestión de Seguridad y Salud en el Trabajo (SST)
- Sistema de Gestión de Seguridad de la Información, ciberseguridad y protección de la privacidad
- Sistema de seguridad conforme al Esquema Nacional de Seguridad (ENS)

2. Alcance

El Sistema de Gestión Integrado de Investigación & Consulting comprende la estructura organizativa, los procesos y recursos necesarios para gestionar la Calidad, Medio ambiente y la Seguridad de la Información necesaria para satisfacer los requisitos de gestión interna, de los clientes, los legales y reglamentarios.

Alcance del Sistema de Gestión Integrado:

Diseño e integración de sistemas y aplicaciones informáticas y electrónicas de seguridad y control e instalación y mantenimiento de las mismas.

Diseño, instalación y mantenimiento de soluciones de protección contra incendios:

- *Sistemas de detección y de alarma de incendios.*
- *Sistemas para el control de humos y de calor*
- *Sistemas de señalización luminiscente.*
- *Sistemas de abastecimiento de agua contra incendios.*
- *Sistemas de hidrantes contra incendios.*
- *Sistemas de bocas de incendio equipadas.*
- *Sistemas de columna seca.*
- *Sistemas fijos de extinción por rociadores y agua pulverizada.*
- *Sistemas fijos de extinción por agua nebulizada.*
- *Sistemas fijos de extinción por espuma física.*
- *Sistemas fijos de extinción por polvo.*
- *Sistemas fijos de extinción por agentes extintores gaseosos.*
- *Sistemas de extinción por aerosoles condensados.*
- *Mantas ignífugas.*
- *Alumbrado de emergencia.*

El alcance del sistema de gestión de Seguridad de la Información aplica a los sistemas de información que dan soporte a las actividades descritas anteriormente, de acuerdo al documento de Declaración de Aplicabilidad (SOA) vigente.

La organización categoriza sus sistemas conforme al ENS y aplica las medidas de seguridad correspondientes según el Anexo II.

Todos los procesos internos y externos quedan adscritos y afectos a la presente política o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma. Es la herramienta clave para conseguir los objetivos de negocio y seguridad de la organización, está alineada plenamente con los objetivos de negocio y seguridad e integrada en la estrategia de la organización.

La organización establece objetivos de seguridad de la información alineados con los resultados del análisis de riesgos, medibles cuando sea posible, monitorizados y revisados periódicamente para asegurar la mejora continua del SGSI, en línea con los requisitos del Esquema Nacional de Seguridad.

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 Sistema Integrado de Gestión.

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 la norma ISO/IEC 27001.

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

En PC01 Gestión documental se establece la gestión que se realiza de la documentación del SGSI, especificando la categorización establecida.

3. Marco normativo de referencia

El Sistema Integrado de Gestión se basa en el siguiente marco normativo y de referencia:

Normas internacionales

- **ISO 9001:2015** – Sistemas de Gestión de la Calidad
- **ISO 14001:2015** – Sistemas de Gestión Ambiental
- **ISO 45001:2018** - Sistemas de Gestión de Seguridad y Salud en el Trabajo (SST)
- **ISO/IEC 27001:2022** – Sistemas de Gestión de Seguridad de la Información
- **ISO/IEC 27002:2022** – Controles de seguridad de la información

Normativa nacional

- **Real Decreto 311/2022**, por el que se regula el **Esquema Nacional de Seguridad (ENS)**
- **Guías CCN-STIC** publicadas por el Centro Criptológico Nacional

Legislación aplicable

- **Reglamento (UE) 2016/679 (RGPD)**
- **Ley Orgánica 3/2018 (LOPDGDD)**
- Legislación ambiental aplicable
- Legislación aplicable en materia de prevención de riesgos laborales
- Legislación sectorial aplicable a la actividad de la organización

4. Compromiso de la Dirección

La Dirección de Investigación y Consulting al objeto de alcanzar el liderazgo en la integración de sistemas y ser una empresa reconocida y valorada por la calidad de nuestros productos y servicios, garantizando la satisfacción de las necesidades de las partes interesadas, los requisitos legales y reglamentarios y garantizar el respeto por el medioambiente, la seguridad y salud de trabajadores y colaboradores y la seguridad de la información, ciberseguridad y protección de la privacidad se compromete a liderar y mantener un Sistema de Gestión Integrado en Calidad, Medio Ambiente, Seguridad y Salud en el Trabajo y Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, alineado con la estrategia y los objetivos de la organización..

Para ello, el CEO de la empresa adquiere los siguientes compromisos:

Liderazgo y orientación estratégica

- Analizar el contexto interno y externo de la organización, así como la evolución del mercado, identificando factores relevantes para la toma de decisiones estratégicas.
- Definir y mantener la dirección estratégica de la organización, asegurando la alineación del Sistema de Gestión Integrado con los objetivos de negocio.
- Promover el uso del enfoque a procesos y el pensamiento basado en riesgos.

- Asegurar la integración del sistema en todos los procesos de la organización.
- Comunicar la importancia de una gestión de la seguridad de la información eficaz y conforme a los requisitos del sistema de gestión.
- Representar al máximo nivel a la empresa ante terceros.

Cumplimiento y partes interesadas

- Cumplir con los requisitos legales, reglamentarios y contractuales aplicables a la organización.
- Asegurar la satisfacción de los clientes y demás partes interesadas.
- Garantizar el cumplimiento de los requisitos específicos en materia de calidad, medio ambiente, seguridad y salud en el trabajo y seguridad de la información.

Calidad del servicio

- Garantizar la calidad en el diseño, instalación y mantenimiento de los sistemas de seguridad.
- Asegurar la correcta ejecución de los proyectos mediante su planificación, control y revisión.
- Establecer y mantener al día un sistema de gestión que asegure la conformidad con las especificaciones.
- Mantener permanentemente un proceso de mejora continua y dirigir la revisión periódica del Sistema de Gestión Integrado para asegurar su eficacia y su adecuación
- Procurar un clima favorable a la promoción de la Calidad, que garantice la seguridad de los trabajadores, la seguridad de la información y respeto al Medio ambiente en el seno de la organización, formando y motivando al personal, y fomentando el máximo desarrollo de las capacidades de los miembros integrantes de la organización.

Medio ambiente

- Proteger el medio ambiente, incluyendo la prevención de la contaminación.
- Minimizar los impactos ambientales derivados de la actividad, especialmente los relacionados con residuos electrónicos, consumo de recursos y emisiones indirectas.
- Fomentar el uso eficiente de los recursos y la sostenibilidad.

Seguridad y salud en el trabajo

- Eliminar los peligros y reducir los riesgos para la seguridad y salud en el trabajo, especialmente los derivados de los trabajos en altura, riesgos eléctricos y trabajos en instalaciones de clientes.

- Garantizar la consulta y participación de los trabajadores.
- Integrar la actividad preventiva en el sistema de gestión, en coordinación con el Servicio de Prevención Ajeno.
- Proporcionar condiciones de trabajo seguras y saludables, orientadas a la prevención de lesiones y deterioro de la salud, integrando la prevención de riesgos laborales en todas sus actividades y niveles jerárquicos.

Seguridad de la información

- Proteger la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Gestionar los riesgos de seguridad de la información mediante un enfoque sistemático basado en análisis de riesgos.
- Garantizar la continuidad del negocio y la resiliencia de los sistemas de información.
- Cumplir con los requisitos del Esquema Nacional de Seguridad y normativa aplicable.
- Establecer controles de seguridad adecuados para proteger los activos de información propios y de clientes.
- Establecer y mantener un proceso formal para la gestión de incidentes de seguridad de la información, que garantice su detección, registro, análisis y resolución, así como la comunicación a las partes interesadas cuando sea necesario. Los incidentes son analizados con el fin de adoptar medidas correctivas y prevenir su recurrencia, contribuyendo a la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Garantizar la continuidad de los procesos y servicios críticos mediante la implantación y mantenimiento de planes de continuidad de negocio y recuperación ante desastres, basados en el análisis de impacto y riesgos, asegurando la disponibilidad de la información, la resiliencia de los sistemas y la capacidad de respuesta y recuperación ante incidentes o situaciones de interrupción. Estos planes son revisados y probados periódicamente para asegurar su eficacia.

Recursos, organización y cultura

- Facilitar los recursos necesarios para alcanzar los objetivos propuestos, con la plena convicción de que la implicación de todo el personal es determinante para conseguirlo
- Establecer canales de comunicación apropiados para asegurarse de que todo el personal entienda la importancia de satisfacer los requisitos del cliente, legales y reglamentarios, y de aplicar las directrices que emanan de los documentos que integran el Sistema de Gestión Integrado.
- Determinar la organización de la empresa:
 - Estableciendo los procesos a realizar y sus funciones de cara a la obtención de los resultados.

- Definiendo las responsabilidades y competencias de cada puesto.
 - Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.
 - Asegurándose de que se establecen los canales de comunicación interna apropiados.
- Fomentar una cultura organizativa basada en la calidad, protección del medioambiente, la seguridad, la sostenibilidad y la protección de la información.
 - Gestionar y planificar los recursos financieros de la empresa, proporcionando los recursos técnicos, materiales y humanos necesarios.
 - Establecer un Comité de Seguridad de la Información como órgano de gobierno encargado de supervisar, coordinar y promover el Sistema de Gestión de Seguridad de la Información y el cumplimiento del Esquema Nacional de Seguridad, asegurando la adecuada gestión de riesgos, la toma de decisiones en materia de seguridad y la mejora continua. Este Comité integra y coordina los roles y responsabilidades definidos en materia de seguridad de la información.
El Comité de Seguridad de la Información actúa como órgano de resolución de conflictos en materia de seguridad de la información, garantizando una adecuada toma de decisiones alineada con los objetivos de la organización y los requisitos normativos aplicables. Está formado por el Responsable de Seguridad (CPE), Responsable del Sistema (JGB) y el Responsable del SGSI (IDG).
La composición, funciones y régimen de funcionamiento del Comité se encuentran definidos en el documento de “Estructura de Seguridad”.

El Comité se reunirá con una periodicidad definida y tendrá autoridad para la toma de decisiones en materia de seguridad de la información.
 - Asegurar la formación e información en materia de calidad, medioambiente, PRL y seguridad de la información.

Seguimiento, evaluación y mejora

- Establecer, difundir y mantener al día la Política entre todos los miembros de la organización, asegurándose que es entendida, aplicada y mantenida al día por todos los niveles de la organización.
- Establecer un programa anual de Objetivos de Calidad, de SST, de Seguridad de la Información y Metas Ambientales coherentes con la Política y con la dirección estratégica de la empresa y se asegurará que se establecen en las funciones y niveles pertinentes dentro de la organización.
- Impulsar la mejora continua del Sistema de Gestión Integrado.
- Realizar las revisiones del sistema, fijando los objetivos y mejoras para el siguiente periodo.
- Realizar el seguimiento, medición, análisis y evaluación del desempeño del Sistema de Gestión Integrado mediante indicadores, auditorías internas y revisiones periódicas por la Dirección, asegurando su adecuación, eficacia y alineación con los riesgos y objetivos

establecidos. Los resultados de esta evaluación se utilizan para la toma de decisiones y la mejora continua del sistema.

La Dirección asume la responsabilidad última del Sistema de Gestión Integrado y garantiza su eficacia mediante el seguimiento continuo de su desempeño.

5. Principios de gestión

Las directrices de la política se enfocan en actividades encaminadas a:

- **Asegurar** la adaptación y mejora continua del **Sistema de Gestión Integrado**, manteniendo una gestión adecuada del mismo.
- **Consolidar** el compromiso de toda la organización con la calidad, seguridad y salud en el trabajo, la protección del medioambiente y la prevención de la contaminación, así como con la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- **Cumplir** y hacer cumplir los requisitos legales, reglamentarios, normativos y otros requisitos aplicables a nuestra actividad, ya sean internos o expresados a través de nuestros clientes. Cumplir con los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de calidad, medioambiente seguridad y salud y/o seguridad de la información.
- **Definir y Difundir** los roles y responsabilidades relaciones con el Sistema de Gestión Integrado. Las responsabilidades en seguridad de la información de las personas que forman parte del Comité del SGSI están definidas y asignadas en el documento “Estructura de Seguridad”.
- **Desarrollar** un proceso de análisis del riesgo y gestión de oportunidades, de acuerdo a su resultado, implementar las acciones correspondientes, con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos y aprovechar las oportunidades.
- **Establecer** los controles de seguridad necesarios para salvaguardar la información, así como los medios necesarios para garantizar la continuidad del negocio de la organización.
- **Fomentar y mantener** el buen nombre de la organización en relación a los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, manteniendo la imagen y reputación.
- **Formar** a nuestro personal, capacitándole para que pueda asumir sus responsabilidades en la consecución de la Calidad, prevención de riesgos laborales, seguridad de la información, reducción del impacto ambiental que puedan ocasionar las actividades que desempeñe y su mejora día a día. Sensibilizando y concienciando al personal de manera estable y permanente en cuanto a seguridad de la información.
- **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, al objeto de recuperarse lo antes posible y minimizar el impacto.

- **Identificar** las obligaciones legales aplicables a la organización, estableciendo medidas para asegurar el cumplimiento de los requisitos legales aplicables, recogidos en la Base de Legislación que mantiene actualizada el departamento de Calidad de la empresa.
- **Implantar** medidas de prevención, control y corrección, encaminadas a disminuir el impacto ambiental derivado de nuestra actividad.
- **Promover** el trabajo en equipo como patrón de comportamiento en la organización.
- **Proteger** los activos de información del sistema de información de la empresa, así como los activos de información de nuestros clientes con los que exista un acuerdo contractual, ante cualquier amenaza, sea interna o externa, deliberada o accidental. Asegurando que solo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, sus perfiles definidos o según asignaciones extraordinarias.
- **Proveer** servicios y soluciones de seguridad innovadoras al objeto de lograr la satisfacción y seguridad de nuestros clientes, adaptando continuamente nuestros productos y servicios a sus necesidades.
- **Reflejar** en la Declaración de Aplicabilidad (SoA) las medidas de seguridad y dimensiones definidos.
- **Sancionar** cualquier violación a esta política, así como a cualquier otra política o procedimiento del sistema de gestión de la información.
- **Valorar** los activos de la información bajo las dimensiones de integridad, disponibilidad, confidencialidad, trazabilidad y autenticidad.

La organización adopta y aplica los principios básicos de seguridad establecidos en el Esquema Nacional de Seguridad, que guían la gestión de la seguridad de la información:

- **Seguridad integral**, considerando todos los elementos organizativos, técnicos, humanos y físicos.
- **Gestión de riesgos**, como base para la selección e implantación de medidas de seguridad.
- **Prevención, detección, respuesta y recuperación**, garantizando la resiliencia frente a incidentes de seguridad.
- **Reevaluación periódica**, asegurando la mejora continua y la adaptación a nuevas amenazas y requisitos.
- **Función diferenciada**, estableciendo responsabilidades claras en la gestión y operación de la seguridad.

Estos principios se integran en el Sistema de Gestión de Seguridad de la Información y en el conjunto del Sistema Integrado de Gestión de la organización.

La aplicación de estos principios garantiza un enfoque sistemático, estructurado y alineado con los requisitos del Esquema Nacional de Seguridad.

Nuestros compromisos son asumidos por la Dirección, que se encarga de su supervisión para asegurar que responde en todo momento a las exigencias y expectativas de nuestras partes interesadas, normativos y/o legales de aplicación a la organización.

La presente política tiene vigencia desde la aprobación por la Dirección y se mantendrá vigente mientras no se aprueba una política posterior.

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

Valladolid, a 25 de junio de 2026

Claudio Parrilla Escobar
CEO de Investigación & Consulting

Firmado por ***0525**
CLAUDIO PARRILLA (R:
****1719*) el día 25/06/2026
con un certificado emitido
por AC Representación