DOCUMENTO DEL SGSI · ISO/IEC 27001:2022 · CLÁUSULA 5.2

Política de Seguridad de la Información

Documento marco del Sistema de Gestión de Seguridad de la Información

Código del documento	HK-SGSI-POL-000
Versión	v1.0
Fecha de emisión	31/07/2026
Organización	HSI KITERIS, S.L. — H&K
Clasificación	Público · publicada en la web corporativa
Propietario del documento	Responsable del SGSI
Aprobación	Dirección de HSI KITERIS, S.L.
Ámbito de aplicación	Todo el personal, personal en prácticas y de ETT, y colaboradores externos
Norma de referencia	ISO/IEC 27001:2022, cláusula 5.2
Ciclo del SGSI	2026
Próxima revisión	Anual, o antes ante cambios significativos

Versión	Fecha	Autor	Descripción del cambio
0.1	23/06/2026	Ubimia — J. D. Méndez	Borrador inicial alineado con la actividad de la organización.
0.2	23/06/2026	Ubimia — J. D. Méndez	Se distingue el Responsable del SGSI del Responsable de IT.
1.0	31/07/2026	Ubimia — J. D. Méndez	Primera versión aprobada. Se incorporan la identificación de la persona jurídica, el alcance con sus exclusiones, el marco de objetivos, la referencia a la metodología de riesgos y a la Declaración de Aplicabilidad, y la firma de la Dirección.

Índice

1. Objeto

La Dirección de **HSI KITERIS, S.L.** (en adelante H&K) establece esta Política de Seguridad de la Información como documento marco de su Sistema de Gestión de Seguridad de la Información (en adelante, el SGSI), implantado conforme a la norma ISO/IEC 27001:2022.

La información es uno de los activos principales de H&K. La compañía presta servicios tecnológicos que implican el acceso a sistemas y a información de sus clientes, y esa relación se sostiene sobre la confianza. Proteger la información propia y la que los clientes confían a H&K no es únicamente una exigencia legal o contractual: es una condición para poder seguir prestando el servicio.

Esta política fija los principios que orientan esa protección, establece el marco para definir los objetivos de seguridad y expresa el compromiso de la Dirección con el cumplimiento de los requisitos aplicables y con la mejora continua del sistema.

2. Alcance

Esta política se aplica a todas las actividades comprendidas en el alcance del SGSI de H&K: la comercialización y gestión de licenciamiento y de consumos de servicios en la nube, la prestación de servicios gestionados de tecnologías de la información, el desarrollo y mantenimiento de soluciones de software, y los procesos internos de soporte necesarios para todo ello.

Es de obligado cumplimiento para todo el personal de H&K, para el personal en prácticas y de empresas de trabajo temporal, y para los colaboradores externos que accedan a sistemas o a información de la compañía o de sus clientes.

La declaración de alcance completa, con la relación de sedes, servicios, activos y exclusiones justificadas, figura en el documento de Contexto y Alcance del SGSI.

3. Compromiso de la Dirección

La Dirección de H&K asume la responsabilidad última sobre la seguridad de la información y se compromete a:

- **Liderar el SGSI** e integrarlo en la estrategia, en los procesos de negocio y en la toma de decisiones, en lugar de tratarlo como una función aislada.
- **Proporcionar los recursos** —humanos, técnicos, formativos y económicos— necesarios para implantar, operar, mantener y mejorar el sistema.

- **Cumplir los requisitos** legales, reglamentarios y contractuales aplicables, incluidos los relativos a la protección de datos personales.
- **Establecer y revisar objetivos de seguridad** medibles, coherentes con esta política y con los objetivos de negocio.
- **Gestionar la seguridad en función del riesgo**, aceptando de forma expresa y documentada los riesgos residuales que la organización decide asumir.
- **Promover la formación y la concienciación** de todas las personas de la organización, y una cultura de seguridad coherente con la forma de trabajar de H&K.
- **Mejorar el sistema de forma continua**, tratando las no conformidades y las oportunidades de mejora que se detecten.

> **COMUNICAR NO TIENE CONSECUENCIAS**
>
> La Dirección quiere dejar constancia expresa de un principio que considera esencial: **notificar un incidente o un error propio no acarrea consecuencias disciplinarias**. Un sistema de seguridad solo funciona si las personas avisan pronto, y las personas solo avisan pronto si saben que hacerlo no les perjudica.
>
> Lo que sí resulta inaceptable es ocultar un incidente conocido, porque el daño se multiplica con cada hora que pasa.

4. Principios de seguridad de la información

La actuación de H&K en materia de seguridad de la información se sustenta en los principios siguientes:

Principio	Qué significa en H&K
Confidencialidad	La información, y muy especialmente la de los clientes, solo es accesible para quien está autorizado y la necesita para su trabajo.
Integridad	La información y los sistemas se mantienen exactos, completos y libres de alteraciones no autorizadas.
Disponibilidad	La información y los servicios están disponibles cuando el negocio y los clientes los necesitan, dentro de los tiempos comprometidos.
Mínimo privilegio y necesidad de conocer	Los accesos se conceden según las funciones de cada persona, por el tiempo necesario, y se retiran cuando dejan de serlo.
Gestión basada en riesgos	Las decisiones de seguridad se toman en función del riesgo evaluado, no de la percepción ni de la costumbre.
Seguridad desde el diseño	Los requisitos de seguridad se identifican al inicio de los proyectos y de los desarrollos, cuando corregir todavía es barato.
Responsabilidad de las personas	La seguridad no es responsabilidad exclusiva del área técnica: cada persona responde del uso adecuado de la información y de los recursos que se le confían.
Continuidad del servicio	La organización se prepara para seguir prestando sus servicios esenciales ante una interrupción, y comprueba periódicamente que puede hacerlo.

5. Marco para el establecimiento de objetivos

La Dirección establece anualmente objetivos de seguridad de la información medibles, coherentes con esta política, con los riesgos identificados y con los objetivos de negocio. Cada objetivo tiene asignados un responsable, una meta, una fuente de medición y un plazo de revisión.

Los objetivos del ciclo en curso, sus indicadores y su seguimiento se documentan en el registro de Objetivos e Indicadores del SGSI, y se revisan en la revisión por la Dirección.

6. Requisitos aplicables

H&K identifica, mantiene actualizados y cumple los requisitos aplicables a su actividad, en particular:

- El Reglamento (UE) 2016/679 General de Protección de Datos y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.
- La Ley 10/2021 de trabajo a distancia, en lo relativo a los medios y a la protección de la información en el trabajo en remoto.
- Los requisitos contractuales acordados con clientes, incluidos los acuerdos de confidencialidad, los encargos de tratamiento y los niveles de servicio comprometidos.
- Los requisitos derivados de los acuerdos con proveedores y colaboradores.

La relación detallada de requisitos y su seguimiento se mantienen en el registro de legislación y requisitos aplicables del SGSI.

7. Organización y responsabilidades

La Dirección impulsa el SGSI y delega su gestión operativa conforme al esquema siguiente. La asignación nominal de estos roles se documenta en el documento de Roles y Responsabilidades del SGSI.

Rol	Responsabilidad principal
Dirección	Aprueba esta política, asigna los recursos, acepta los riesgos residuales y celebra la revisión por la Dirección.
Comité de Seguridad de la Información	Órgano de seguimiento del SGSI. Revisa los riesgos, los objetivos, los incidentes y las acciones de mejora.
Responsable del SGSI	Gestiona el sistema: mantiene la documentación, coordina el análisis de riesgos, sigue los objetivos y decide sobre los incidentes.
Responsable de IT	Aplica y opera los controles técnicos, y responde de la seguridad de la infraestructura y de los servicios.
Responsables de área	Aplican la política en su ámbito, identifican los riesgos de sus procesos y trasladan las necesidades de seguridad.
Delegado de Protección de Datos	Vela por el cumplimiento en materia de datos personales y coordina la respuesta ante brechas que los afecten.
Todo el personal	Cumple esta política y las normas que la desarrollan, y notifica los incidentes y las debilidades de seguridad que detecte.

8. Gestión de riesgos

H&K identifica, analiza, evalúa y trata los riesgos de seguridad de la información mediante una metodología documentada, que valora cada escenario en función de su probabilidad y de su impacto y determina un nivel de riesgo inherente y residual.

Los riesgos y su tratamiento se mantienen en el registro de análisis y tratamiento de riesgos. La selección de los controles aplicables y la justificación de las exclusiones se documentan en la Declaración de Aplicabilidad, aprobada por la Dirección.

Los riesgos residuales que superan el nivel aceptable definido requieren **aceptación expresa y documentada de la Dirección**.

9. Desarrollo de esta política

Esta política se desarrolla en políticas específicas, procedimientos, normas y registros que concretan cómo se aplican sus principios. Entre ellos, y sin carácter exhaustivo: el control de accesos, el uso aceptable de recursos y dispositivos, la criptografía, el desarrollo seguro, la gestión de activos, la gestión de incidentes, la continuidad del negocio, la gestión de proveedores, las copias de seguridad y la gestión documental.

Todos los documentos que desarrollan esta política son de obligado cumplimiento en su ámbito y están disponibles para el personal en el repositorio documental del SGSI.

10. Cumplimiento, excepciones e incumplimiento

El cumplimiento de esta política y de los documentos que la desarrollan es obligatorio para todas las personas incluidas en su ámbito de aplicación.

Excepciones. Cuando una necesidad justificada del negocio impida cumplir un requisito, la excepción debe solicitarse de forma expresa al Responsable del SGSI, quedar documentada con su justificación, su plazo y las medidas compensatorias adoptadas, y ser aprobada por el nivel que corresponda según el riesgo asumido. No existen excepciones tácitas.

Incumplimiento. Cuando una persona de la organización cause un perjuicio a la seguridad de la información, la Dirección valorará las medidas a adoptar sobre sus privilegios de acceso y las eventuales medidas disciplinarias, en el marco de la normativa laboral y del convenio colectivo aplicables. Cuando el perjuicio provenga de un colaborador externo, se estará a lo previsto en el contrato suscrito con él.

11. Comunicación y disponibilidad

Esta política se comunica a todo el personal en el momento de su incorporación y cada vez que se actualiza, a través de los canales internos de la compañía, y permanece disponible de forma permanente en el repositorio documental del SGSI.

Se pone a disposición de las partes interesadas que lo requieran —clientes, auditores, organismos de certificación y proveedores— cuando exista una razón legítima para ello.

12. Revisión

Esta política se revisa como mínimo con periodicidad anual dentro de la revisión por la Dirección, y siempre que se produzcan cambios significativos en la organización, en su actividad, en los riesgos identificados o en los requisitos legales o contractuales aplicables.

13. Aprobación

La Dirección de HSI KITERIS, S.L. aprueba la presente Política de Seguridad de la Información, asume los compromisos que en ella se expresan y ordena su difusión y cumplimiento en toda la organización.

	Aprobado por la Dirección
Nombre y apellidos	Manuel José Peña Marco
Cargo	Associate Managing Director
En calidad de	En representación de la Dirección de HSI KITERIS, S.L.
Entidad	HSI KITERIS, S.L. — CIF B58573965
Firma	18957440N MANUEL JOSE PEÑA (R: B58573965) — Firmado digitalmente por 18957440N MANUEL JOSE PEÑA (R: B58573965) Fecha: 2026.08.07 09:57:52 +02'00'
Fecha de firma	6 de agosto de 2026