HODEITEK

POLÍTICA CORPORATIVA · SGSI

Política de Seguridad de la Información

Sistema de Gestión de Seguridad de la Información — Esquema Nacional de Seguridad (categoría MEDIA)

PREPARADO PARA **Hodeitek, S.L.U.**

REFERENCIA **HDT- SGSI- POL- 01**

FECHA **4 de junio de 2026**

PREPARADO POR **Dirección de Hodeitek**

Control documental

Versión	Fecha	Autor	Revisor	Aprobador	Descripción del cambio
1.0	4 jun 2026	Dirección de Hodeitek	Ingertec	Dirección de Hodeitek	Primera versión aprobada por la Dirección. Adaptada a la realidad operativa de Hodeitek (sociedad unipersonal, sin CPD propio, infraestructura en nube certificada ENS) y al alcance ENS de categoría MEDIA. Amplía la plantilla base con datos identificativos, marco normativo actualizado, gobierno de la cadena de suministro, protección de datos, gestión de incidentes y régimen de cumplimiento.

Índice

1. Aprobación y entrada en vigor

La presente Política de Seguridad de la Información es aprobada por la Dirección de Hodeitek y entra en vigor desde la fecha de su firma. Permanecerá vigente hasta que sea reemplazada por una versión posterior aprobada por la Dirección.

Constituye el documento de máximo nivel del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) de Hodeitek y expresa el compromiso de la Dirección con la protección de la información y de los servicios prestados. Todo el contenido del SGSI —normativas, procedimientos y registros— se subordina a los principios aquí establecidos.

> **Marco de referencia**
>
> Esta Política se alinea con el Esquema Nacional de Seguridad (RD 311/2022) en categoría MEDIA y toma como referencia la norma ISO/IEC 27001:2022. Su aplicación es de obligado cumplimiento para todo el personal propio y externo que opere bajo el alcance del SGSI.

2. Datos identificativos de la organización

A efectos del SGSI, la organización responsable del tratamiento de la información y de la prestación de los servicios incluidos en el alcance es:

RAZÓN SOCIAL	Hodeitek, S.L.U.
FORMA JURÍDICA	Sociedad de Responsabilidad Limitada Unipersonal
CIF	B56478027
DOMICILIO SOCIAL	Markole, 17 — 20550 Aretxabaleta (Gipuzkoa), España
SITIO WEB	www.hodeitek.com
ACTIVIDAD	Inteligencia Artificial aplicada a negocio, ciberseguridad y automatización de procesos

Hodeitek es una sociedad unipersonal. Esta condición es relevante para la organización de la seguridad descrita en el apartado 8 y se ha tenido en cuenta de forma expresa en la asignación de roles, en la constitución del Comité de Seguridad y en las medidas compensatorias asociadas.

3. Misión y compromiso de la Dirección con la seguridad

Hodeitek asume su compromiso con la seguridad de la información, comprometiéndose a su adecuada gestión con el fin de ofrecer a clientes, proveedores y demás grupos de interés las máximas garantías sobre la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información que maneja y de los servicios que presta.

Los sistemas de información deben administrarse con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados. El objetivo de la seguridad es garantizar la calidad de la información y la prestación continuada de los servicios, actuando de forma preventiva, supervisando la actividad diaria y reaccionando con prontitud ante los incidentes.

Los sistemas TIC deben estar protegidos frente a amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y de los servicios. Para ello, Hodeitek aplica las medidas mínimas exigidas por el Esquema Nacional de Seguridad, realiza un seguimiento continuo de los niveles de prestación de servicio, analiza las vulnerabilidades reportadas y mantiene una capacidad de respuesta efectiva ante incidentes que garantice la continuidad de los servicios.

La seguridad TIC se integra como parte de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación asociadas se identifican e incluyen en la planificación. Hodeitek se prepara para prevenir, detectar, reaccionar y recuperarse de los incidentes conforme al artículo 8 del ENS (prevención, detección, respuesta y conservación).

4. Alcance del SGSI

Esta Política se aplica a toda la actividad de Hodeitek, a la totalidad de sus sistemas TIC y a todas las personas —propias o externas— que operen bajo su responsabilidad. El alcance no se limita a los servicios destinados al sector público: la conformidad con el ENS se asume como marco de gobierno aplicable a toda la organización y como argumento de confianza también ante clientes privados.

Dentro de este alcance general, se identifican como servicios certificables conforme al ENS los siguientes cinco servicios, que constituyen el subconjunto sometido a certificación:

- Plataforma SaaS HodeiShield (inteligencia de cadena de suministro digital y gestión de cumplimiento normativo).
- Servicios de pentesting y auditoría de seguridad.
- Consultoría en ciberseguridad y consultoría TIC.
- Consultoría en Inteligencia Artificial.
- Consultoría en automatización de procesos de negocio.

El sistema ha sido categorizado en nivel MEDIA en las cinco dimensiones de seguridad (confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad), conforme al documento de Categorización del sistema. Los controles de nivel ALTO previstos por el ENS quedan, por tanto, fuera del alcance de certificación, sin perjuicio de que algunas de las soluciones implantadas ya proporcionen capacidades superiores a las exigidas en nivel MEDIA.

> **Modelo operativo**
>
> Hodeitek opera bajo un modelo distribuido sin centro de proceso de datos propio. La infraestructura productiva, incluida la plataforma HodeiShield, se aloja en un proveedor de nube certificado conforme al ENS. La actividad del personal se desarrolla en modalidad remota. Este modelo se refleja de forma explícita en las medidas de protección de los apartados 14, 18, 19 y 21.

5. Objetivos de seguridad

Para dar cumplimiento a su misión, la Dirección establece los siguientes objetivos de seguridad de la información:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada y de los servicios prestados.
- Proporcionar un marco que aumente la capacidad de resistencia y resiliencia de la organización para dar una respuesta eficaz ante incidentes.
- Asegurar la recuperación rápida y eficiente de los servicios frente a cualquier desastre o contingencia que ponga en riesgo la continuidad de las operaciones.
- Prevenir los incidentes de seguridad en la medida en que sea técnica y económicamente viable, y mitigar los riesgos generados por la actividad de Hodeitek.
- Cumplir los requisitos legales, regulatorios y contractuales aplicables, y mantener su actualización continua.
- Gobernar la seguridad de la cadena de suministro, sobre la que se apoya la totalidad de la operación de Hodeitek.

6. Marco normativo y de referencia

Uno de los objetivos de Hodeitek es cumplir con los requisitos legales aplicables, con los compromisos adquiridos con clientes y con cualesquiera otros requisitos suscritos. El marco se estructura distinguiendo, de forma deliberada, la legislación de obligado cumplimiento de los marcos y normas adoptados como referencia o aplicables en función del contexto del servicio.

6.1. Legislación de obligado cumplimiento

- Reglamento (UE) 2016/679 (RGPD) y Ley Orgánica 3/2018 (LOPDGDD), en materia de protección de datos personales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 910/2014 (eIDAS), en materia de identificación electrónica y servicios de confianza (firma electrónica y sellado de tiempo).
- Ley 34/2002 (LSSI-CE), de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996 y Ley 2/2019, en materia de propiedad intelectual.
- Leyes 39/2015 y 40/2015, de procedimiento administrativo común y de régimen jurídico del sector público, en las relaciones con las Administraciones Públicas.

6.2. Marcos y normas adoptados o aplicables según el contexto

Los siguientes marcos se adoptan como referencia de buenas prácticas o resultan de aplicación en función del tipo de cliente o servicio. Hodeitek evita afirmar una aplicabilidad directa cuando esta no existe:

- ISO/IEC 27001:2022, e ISO/IEC 27017 e ISO/IEC 27018 para la seguridad en servicios de nube: normas de referencia para la estructura y mejora continua del SGSI.
- Directiva (UE) 2022/2555 (NIS2): adoptada como referencia de buenas prácticas. Su aplicabilidad directa dependerá de la transposición nacional y de la condición de Hodeitek como proveedor de servicios gestionados de seguridad, así como de su relación con clientes sujetos a la norma.
- Reglamento (UE) 2024/1689 (Reglamento Europeo de IA): en particular el deber de alfabetización en IA (artículo 4, aplicable desde febrero de 2025), por la actividad de consultoría y desarrollo de soluciones basadas en Inteligencia Artificial.

- Reglamento (UE) 2022/2554 (DORA): no resulta directamente aplicable a Hodeitek, que no es entidad financiera. Se adopta como marco de referencia cuando se presten servicios TIC a entidades sujetas a DORA.
- Recomendaciones y guías CCN-STIC aplicables al ENS, en particular las series 800, 801, 803, 807 y 808.

7. Estructura documental del SGSI

Para alcanzar sus objetivos, Hodeitek implementa un sistema de gestión fácil de comprender, mantenido y actualizado de forma continua. La documentación del SGSI se conserva en un repositorio documental controlado, con acceso restringido según los perfiles de acceso autorizados, y se organiza por puntos de norma y marcos de operación. El acceso de personal externo no autorizado a dicho repositorio queda prohibido.

La documentación de seguridad se estructura en cuatro niveles:

- Política de Seguridad de la Información: el presente documento, de máximo nivel.
- Normativa de seguridad: documentos que describen el uso aceptable de equipos, servicios e instalaciones, lo que se considera uso indebido y las responsabilidades, derechos, deberes y medidas disciplinarias del personal.
- Procedimientos de seguridad: documentos que detallan cómo operar los elementos del sistema.
- Documentos específicos y registros: documentación desarrollada según las guías CCN-STIC aplicables y evidencias de la operación del sistema.

Esta Política se complementa, entre otros, con los siguientes documentos del SGSI, que se irán desarrollando y aprobando progresivamente:

- Política de Organización de la Seguridad.
- Normativa de uso aceptable (incluye puesto de trabajo despejado y comunicación de robo o pérdida de dispositivos).
- Procedimiento y registro de Análisis de Riesgos, y planes de tratamiento.
- Política de control de acceso y política de contraseñas.
- Política de clasificación de la información.
- Política de controles criptográficos.
- Procedimiento de gestión de la configuración y de hardening.
- Procedimiento de mantenimiento, actualizaciones de seguridad y gestión de cambios.
- Procedimiento de gestión de incidentes de seguridad.
- Evaluación de la cadena de suministro e inventario de proveedores.
- Plan de continuidad de la actividad y análisis de impacto.
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Plan de concienciación y plan de formación.
- Procedimiento de gestión de soportes, y de borrado y destrucción seguros.

8. Organización de la seguridad y roles ENS

La responsabilidad esencial sobre la seguridad recae en la Dirección de Hodeitek, responsable de organizar las funciones y responsabilidades y de facilitar los recursos adecuados para alcanzar los objetivos del ENS. La Dirección dota de los medios necesarios para el cumplimiento de esta Política y la pone en conocimiento público a través de su versión publicable.

El Esquema Nacional de Seguridad exige la diferenciación de los siguientes roles de seguridad:

Rol	Deberes y responsabilidades
Responsable de la Información (RINFO)	Toma las decisiones relativas a la información tratada y a sus requisitos de seguridad.
Responsable del Servicio (RSER)	Establece los requisitos de los servicios y los niveles de prestación; coordina la implantación del sistema.
Responsable de Seguridad (RSEG / CISO)	Determina la idoneidad de las medidas de seguridad, supervisa su aplicación y gestiona los incidentes.
Responsable del Sistema (RSIS)	Opera y mantiene el sistema de información; aplica las medidas técnicas de seguridad.
Dirección	Proporciona los recursos necesarios, lidera el sistema y asume la rendición de cuentas última.
Administrador de Seguridad (AS)	Implanta, gestiona y mantiene las medidas de seguridad en el día a día.

Tabla 1. *Roles de seguridad definidos conforme al ENS.* Fuente: elaboración propia conforme a RD 311/2022 y CCN-STIC-801.

8.1. Asignación de roles en una organización unipersonal

Por su condición de sociedad unipersonal con un único integrante, en el momento de aprobación de esta Política la Dirección asume personalmente los cuatro roles ENS (Responsable de la Información, del Servicio, de Seguridad y del Sistema), así como las funciones de Administrador de Seguridad. La separación entre estos roles se mantiene a nivel lógico y documental mediante la correspondiente matriz de responsabilidades.

> **Conflicto de interés declarado y aceptado por la Dirección**
>
> La acumulación de roles —en particular la coincidencia entre el Responsable de Seguridad y el Responsable del Sistema —genera un conflicto de interés que la Dirección

> reconoce y acepta de forma expresa como riesgo, en tanto persista la condición unipersonal. Para mitigarlo se establece una medida compensatoria consistente en la revisión y validación independiente de las decisiones de seguridad por un tercero externo (asesoría especializada / CISO externo), formalizada en el documento de Organización de la Seguridad. La Dirección asume el compromiso de revisar esta asignación cuando se incorpore personal a la organización.

8.2. Resolución de conflictos

Las diferencias de criterio que pudieran derivar en conflicto se tratarán en el seno del Comité de Seguridad de la Información. En todo caso prevalecerá el criterio de la Dirección, sin perjuicio de la incorporación documentada de las recomendaciones del asesoramiento externo.

9. Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el órgano de mayor responsabilidad dentro del SGSI: en él se acuerdan las decisiones más relevantes en materia de seguridad. Sus cometidos incluyen la armonización de los análisis de riesgos, la disposición de recursos para atender las necesidades de seguridad y la supervisión de los incidentes.

Dada la condición unipersonal de Hodeitek, las funciones del Comité de Seguridad son asumidas por la Dirección, que las ejerce con el apoyo del asesoramiento externo en seguridad (CISO externo / consultoría especializada) y, cuando proceda, de otros asesores. Esta singularidad se documenta como medida compensatoria en el documento de Organización de la Seguridad, de modo que las decisiones de seguridad cuenten con un contraste independiente. La organización de la seguridad se desarrolla en dicho documento complementario a esta Política.

10. Gestión de riesgos

Todos los sistemas sujetos a esta Política se someten a un análisis de riesgos que evalúa las amenazas a las que están expuestos, conforme a una metodología reconocida (MAGERIT). Este análisis se revisa con regularidad y, como mínimo:

- almenos una vezalaño;
- cuando cambie la información manejada;
- cuando cambien los servicios prestados;
- cuando ocurra un incidente grave de seguridad;
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establece una valoración de referencia para los distintos tipos de información manejados y servicios prestados, y promueve las inversiones de seguridad de carácter horizontal. La metodología se detalla en el procedimiento de Análisis de Riesgos.

11. Gestión y concienciación del personal

Todas las personas vinculadas a Hodeitek tienen la obligación de conocer y cumplir esta Política y la Normativa de Seguridad. Es responsabilidad de la Dirección, en su función de Comité de Seguridad, disponer los medios para que esta información llegue a los afectados.

El personal recibirá, al menos una vez al año, una sesión de concienciación en materia de seguridad TIC, dentro de un programa de concienciación continua que atenderá de forma específica a las nuevas incorporaciones. Las personas con responsabilidad en el uso, operación o administración de los sistemas TIC recibirán la formación necesaria para su manejo seguro, con carácter obligatorio antes de asumir la responsabilidad correspondiente, tanto en la primera asignación como ante un cambio de puesto.

12. Profesionalidad y seguridad de los recursos humanos

Esta Política se aplica a todo el personal de Hodeitek y al personal externo que realice tareas para la organización. Las funciones de seguridad de la información se incorporan a la descripción de los puestos de trabajo. Antes de proporcionar credenciales, se informa a las personas de sus obligaciones respecto al cumplimiento de esta Política y se gestionan los compromisos de confidencialidad correspondientes.

El Responsable de Seguridad (CISO) es responsable de monitorizar, documentar y analizar los incidentes de seguridad reportados, así como de comunicarlos a la Dirección y a los propietarios de la información. Participa en la elaboración de los compromisos de confidencialidad que firman el personal y los terceros, asesora sobre las sanciones aplicables por incumplimiento y coordina el tratamiento de los incidentes. Toda persona vinculada a Hodeitek es responsable de informar oportunamente sobre las debilidades e incidentes de seguridad que detecte.

En materia de profesionalidad de los recursos humanos, Hodeitek determina la competencia necesaria para el trabajo que afecta a la seguridad de la información, asegura dicha competencia sobre la base de la formación y la experiencia adecuadas y la documenta. Los objetivos de control de la seguridad del personal son reducir los riesgos de error humano, uso indebido de recursos y manejo no autorizado de la información; explicitar las responsabilidades de seguridad desde la incorporación; establecer compromisos de confidencialidad; y disponer de mecanismos para comunicar debilidades e incidentes con el fin de minimizar sus efectos y prevenir su reincidencia.

13. Autorización y control de acceso a los sistemas

El control de acceso a los sistemas de información persigue: evitar el acceso no autorizado a sistemas, bases de datos y servicios; implantar la seguridad en el acceso mediante técnicas de autenticación y autorización; controlar la seguridad de las conexiones con redes externas; revisar los eventos críticos y la actividad de los usuarios; concienciar sobre el uso responsable de credenciales y equipos; y garantizar la seguridad de la información en el trabajo remoto.

Hodeitek opera con cuentas nominales, con separación entre cuentas de administración y de usuario, autenticación multifactor obligatoria en todos los accesos y gestión centralizada de credenciales mediante un gestor corporativo cifrado. La política de control de acceso y la política de contraseñas —orientadas a las recomendaciones vigentes (longitud y robustez junto a doble factor)— se desarrollan en los documentos específicos del SGSI.

14. Protección de las instalaciones y del puesto de trabajo

Hodeitek no dispone de centro de proceso de datos propio. La infraestructura productiva se aloja en un proveedor de nube certificado conforme al ENS, sobre el que recaen los controles de seguridad física y ambiental (control de accesos, climatización, suministro eléctrico redundante, protección frente a incendios e inundaciones y registro de entrada y salida de equipamiento), cubiertos por su certificación. Hodeitek mantiene evidencia documental de la conformidad de dicho proveedor.

La actividad del personal se desarrolla en modalidad remota. El entorno de trabajo se considera una zona no controlada y se protege mediante medidas compensatorias sobre el puesto: cifrado completo de disco, solución gestionada de protección frente a código dañino, autenticación multifactor en todos los accesos, bloqueo automático por inactividad y aplicación de la política de puesto de trabajo despejado. Los objetivos de esta sección —prevenir accesos no autorizados, proteger el equipamiento crítico, controlar los factores ambientales y proporcionar una protección proporcional a los riesgos— se cumplen mediante esta combinación de controles del proveedor y del puesto.

15. Adquisición, desarrollo y mantenimiento de sistemas

La seguridad TIC es parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada, incluyendo las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación asociadas se identifican e incluyen en la planificación y en la solicitud de ofertas. En la selección de productos y servicios se prioriza, cuando es posible, el uso de componentes certificados (catálogo CPSTIC del CCN); cuando no existan, se documenta un análisis de equivalencia funcional. La política de desarrollo y adquisición se desarrolla en el documento de Adquisición, Desarrollo y Mantenimiento de Sistemas.

16. Principios y directrices técnicas de seguridad

16.1. Seguridad por defecto

Hodeitek considera estratégico que los procesos integren la seguridad de la información a lo largo de su ciclo de vida. Los sistemas y servicios incorporan la seguridad por defecto desde su creación hasta su retirada, incluyéndola en las decisiones de desarrollo y/o adquisición y en todas las actividades de explotación, como proceso integral y transversal.

16.2. Integridad y actualización del sistema

Hodeitek garantiza la integridad del sistema mediante un proceso de gestión de cambios que controla la actualización de los elementos físicos y lógicos previa autorización a su instalación. Se evalúa el impacto en la seguridad antes de realizar los cambios y se documentan aquellos relevantes o con implicaciones de seguridad. Mediante revisiones periódicas se evalúa el estado de seguridad de los sistemas frente a las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo.

16.3. Protección de la información almacenada y en tránsito

Hodeitek establece medidas de protección para la información almacenada o en tránsito a través de entornos no confiables, empleando algoritmos y parámetros conformes con las recomendaciones del CCN (CCN-STIC-807): cifrado completo de disco en los equipos, cifrado en reposo de los datos en la infraestructura de nube y cifrado en tránsito mediante TLS en su versión vigente.

16.4. Protección del perímetro e interconexión de sistemas

Hodeitek protege el perímetro de sus servicios, en particular en las conexiones con redes públicas, mediante soluciones de protección perimetral (WAF, mitigación de denegación de servicio y filtrado) y monitorización. Toda interconexión con otros sistemas se autoriza previamente y se documenta de forma explícita (características de la interfaz, requisitos de seguridad y protección de datos, y naturaleza de la información intercambiada); todo flujo de información queda prohibido salvo autorización expresa.

17. Continuidad de la actividad

Con el objetivo de garantizar la continuidad de la actividad, Hodeitek establece copias de seguridad de los sistemas y los mecanismos necesarios para mantener la operación en caso de pérdida de los medios habituales de trabajo. El alcance de la continuidad —incluido el análisis de impacto y, en su caso, los medios alternativos— se desarrolla en el Plan de Continuidad de la Actividad, de forma coherente con la categoría MEDIA del sistema.

18. Gestión de la cadena de suministro y servicios en la nube

La operación de Hodeitek se apoya de forma estructural en proveedores tecnológicos externos. La Dirección reconoce la cadena de suministro como un elemento crítico de gobierno y establece su evaluación y seguimiento periódicos. Los proveedores que sustentan la infraestructura y los servicios incluidos en el alcance se inventarían y evalúan en el documento de Evaluación de la Cadena de Suministro, atendiendo a su criticidad y a la naturaleza de la información tratada.

Cuando se utilicen servicios en la nube de terceros, estos deberán ser conformes con el ENS o cumplir las medidas equivalentes establecidas en la guía CCN-STIC correspondiente, atendiendo en particular a la realización de pruebas de penetración, la transparencia, el cifrado y la gestión de claves, y la jurisdicción de los datos. Hodeitek exige conformidad con el ENS a sus proveedores de infraestructura y ofimática críticos y, cuando un proveedor no disponga de dicha certificación, documenta un análisis de equivalencia y las medidas suplementarias aplicables. Los tratamientos de datos personales por terceros se amparan en los correspondientes acuerdos de encargo de tratamiento.

19. Protección de datos personales

Hodeitek trata datos personales conforme al RGPD y a la LOPDGDD. La organización mantiene el registro de actividades de tratamiento, aplica los principios de minimización y limitación de la finalidad, formaliza los acuerdos de encargo de tratamiento con los proveedores que acceden a datos personales y garantiza el ejercicio de los derechos de las personas interesadas. Las medidas técnicas y organizativas derivadas de esta Política contribuyen directamente a la seguridad del tratamiento exigida por la normativa de protección de datos. El detalle se desarrolla en la documentación específica de protección de datos.

20. Gestión de incidentes y notificación

Hodeitek dispone de un proceso de gestión de incidentes de seguridad que cubre su detección, registro, análisis, contención, resolución y aprendizaje posterior. La detección se apoya en la monitorización continua (SIEM y servicio gestionado de detección y respuesta) y en la capacidad de respuesta asociada. Los incidentes se documentan y, cuando proceda, se notifican a las autoridades competentes —CCN-CERT/INCIBE en el ámbito del ENS y la Agencia Española de Protección de Datos en caso de brechas de datos personales— dentro de los plazos legalmente establecidos, así como a los clientes afectados conforme a los compromisos contractuales. El detalle operativo se desarrolla en el Procedimiento de Gestión de Incidentes.

21. Cumplimiento y consecuencias del incumplimiento

El cumplimiento de esta Política es obligatorio para todo el personal propio y externo dentro del alcance del SGSI. Su incumplimiento podrá dar lugar a las medidas disciplinarias previstas en la legislación laboral vigente, a la resolución de las relaciones contractuales con terceros y, en su caso, a las responsabilidades administrativas, civiles o penales que correspondan. La verificación del cumplimiento se realiza mediante auditorías internas periódicas y mediante las auditorías externas exigidas por el ENS.

22. Mejora continua del proceso de seguridad

Hodeitek establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y la metodología de normas internacionales como ISO/IEC 27001, mediante el ciclo de planificación, implantación, verificación y actuación. Para ello identifica las amenazas potenciales y su impacto en el negocio, preserva los intereses de sus partes interesadas, trabaja de forma conjunta con sus proveedores y subcontratistas para mejorar la prestación y la seguridad de los servicios, evalúa y garantiza la competencia del personal y analiza de forma continua los procesos relevantes para establecer las mejoras pertinentes en función de los resultados y de los objetivos fijados.

23. Vigencia, aprobación y revisión

Esta Política es aprobada por la Dirección y entra en vigor desde su firma. Se revisará, como mínimo, con periodicidad anual, así como cuando se produzcan cambios significativos en la organización, en los servicios prestados, en la normativa aplicable o tras un incidente grave de seguridad. Cualquier modificación será aprobada por la Dirección y comunicada al personal afectado, manteniéndose el control de versiones recogido en el front-matter de este documento.

Esta Política se publica en su versión pública en el portal corporativo de Hodeitek, en cumplimiento de las exigencias de transparencia del ENS. La presente versión, de uso interno, constituye la copia autorizada y firmada por la Dirección.

Aprobada por la Dirección de Hodeitek, S.L.U.