GrayHats

Política de Seguridad de la Información y Ciberseguridad

Esquema Nacional de Seguridad, ISO/IEC 27001:2022 y NIS2

Documento público

AVISO LEGAL DE VERSIÓN PÚBLICA ANONIMIZADA. *El presente documento es una versión pública y anonimizada de la Política de Seguridad de la Información y de Ciberseguridad de Grayhats S.L.U., publicada con fines de transparencia, divulgación y cumplimiento de los principios de información del Reglamento (UE) 2016/679 (RGPD) y de la Ley Orgánica 3/2018 (LOPDGDD). De conformidad con el principio de minimización de datos (art. 5.1.c RGPD) y con el considerando 26 del RGPD, se han suprimido o sustituido por marcadores los nombres de personas físicas, firmas, fechas concretas, localidad y códigos internos de documentación del Sistema de Gestión de Seguridad de la Información, de modo que no resulte posible la identificación, directa o indirecta, de los interesados ni se expongan elementos sensibles del SGSI. El documento original, completo y firmado, se conserva internamente por Grayhats S.L.U. y se encuentra a disposición de las autoridades competentes y de las partes interesadas que acrediten legítimo interés. La presente versión pública mantiene íntegros los principios, controles, responsabilidades por rol y el contenido normativo y técnico de la Política aprobada. Para cualquier consulta o ejercicio de derechos en materia de protección de datos puede contactarse con el Delegado de Protección de Datos en* ***dpo@grayhats.com****.*

Tabla de contenido

1. Introducción

Este documento expone la Política de Seguridad de la Información y de la Ciberseguridad de Grayhats S.L.U. (en adelante, Grayhats), entendida como el conjunto de principios básicos, compromisos y líneas de actuación estratégicas a los que la organización se compromete y adhiere, para garantizar los máximos niveles de seguridad de la información, ciberseguridad, resiliencia operativa y continuidad de los servicios digitales que presta.

La información y los activos digitales son pilares esenciales para el desarrollo de la actividad de Grayhats y para el cumplimiento de sus objetivos de negocio. Por ello, han de ser protegidos de forma sistemática frente a amenazas internas o externas, incidentes intencionados o accidentales, y vulnerabilidades tecnológicas o humanas. Esta protección debe abarcar todos los formatos, soportes, medios de transmisión, entornos tecnológicos y personas que participen en el ciclo de vida de la información.

La seguridad de la información requiere medios técnicos, humanos, y una adecuada gestión y definición de los procedimientos, y para conseguir esto, es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La seguridad de la información y la ciberseguridad constituyen funciones inseparables dentro de la gestión corporativa. Juntas garantizan la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos y servicios, permitiendo la gestión eficaz del riesgo, la resiliencia frente a ciberamenazas y la continuidad operativa de la empresa, conforme a los principios del ENS, los controles de la ISO/IEC 27001:2022 y las exigencias de NIS2.

En este marco, la ciberseguridad se define como el conjunto coordinado de capacidades, medidas y procesos técnicos y organizativos destinados a proteger los sistemas de información, redes y servicios esenciales frente a ataques, incidentes o usos no autorizados. Grayhats promueve una gestión de la ciberseguridad orientada a:

1. Prevenir, detectar y responder de forma eficaz ante ciberincidentes.
2. Implementar medidas proporcionales al riesgo, atendiendo a los requerimientos de NIS2 (art. 21.2).
3. Reforzar la resiliencia digital y la capacidad de recuperación ante interrupciones o ataques graves.
4. Asegurar la coordinación con su Centro de Operaciones de Seguridad (SOC), responsable de la monitorización continua, el análisis forense y la notificación de incidentes.
5. Garantizar la formación y concienciación del personal, fomentando una cultura organizativa de ciberseguridad responsable.

La dirección de Grayhats, plenamente consciente del valor estratégico de la información y de los riesgos inherentes al entorno digital, asume el compromiso firme de liderazgo, apoyo y mejora continua de esta política.

Dicho compromiso incluye la provisión de recursos adecuados, la definición de responsabilidades claras, y la integración de la ciberseguridad en todo el ciclo de gestión de la empresa, en línea con el modelo de gobernanza exigido por NIS2 y el principio de mejora continua de la ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad.

En consecuencia, esta Política constituye la base del Sistema de Gestión de Seguridad de la Información (SGSI) y del Sistema de Gestión de la Ciberseguridad de Grayhats, ambos orientados a garantizar la convergencia entre

la protección de la información, la defensa digital y la resiliencia del negocio frente a cualquier amenaza o incidente.

1.1. Propósito

El propósito de esta Política de la Seguridad de la Información y de la Ciberseguridad es definir la estrategia para proteger los activos de información de la empresa, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

Esta política establece el marco de referencia para proteger la infraestructura digital y operativa de la empresa, de conformidad con los principios definidos por la Directiva (UE) 2022/2555 (NIS2), que exige a las entidades esenciales y a las entidades importantes la implantación de medidas técnicas, operativas y organizativas adecuadas para gestionar los riesgos de seguridad que afecten a las redes y sistemas de información.

En este sentido, la política contribuye a cumplir con los requisitos del artículo 20 y 21 de NIS2 en relación con la gestión de riesgos y las medidas de seguridad aplicables, entre las que se incluyen:

1. La adopción de políticas de análisis y gestión de riesgos.
2. La implantación de planes de continuidad de negocio y recuperación ante incidentes.
3. La seguridad en la cadena de suministro y la gestión de dependencias externas.
4. La reacción y notificación de incidentes de seguridad ante las autoridades competentes.

Asimismo, esta política se enmarca elemento central del Plan Director de Seguridad de Grayhats y está alineada con el estándar marcado por la ISO/IEC 27001:2022 el cual marca los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI), como con los principios de resiliencia digital y gestión de cibercrisis exigidos por NIS2, garantizando un proceso de mejora continua y un enfoque basado en la gestión del riesgo, lo cual es el propósito vehicular para conseguir los objetivos de seguridad de la información y de la ciberseguridad que persigue esta política.

1.2. Alcance

La presente política es aplicable a todos los sistemas, servicios y procesos tecnológicos incluidos en el Sistema de Gestión de la Seguridad de la Información (SGSI) de Grayhats (servicios que usa y ofrece Grayhats), abarcando también las operaciones internas como los servicios ofrecidos a terceros, en los que la empresa actúe como entidad esencial o importante, según los criterios de clasificación establecidos por NIS2.

La presente Política de Seguridad de la Información y de la Ciberseguridad se aplica a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la empresa para los procesos descritos.

De acuerdo con el artículo 20 de la Directiva NIS2, el alcance de esta política se extiende también a todas las personas, sistemas y activos físicos o lógicos que intervienen directa o indirectamente en el tratamiento, almacenamiento, transmisión o gestión de información y datos esenciales para la prestación de los servicios de Grayhats.

Este ámbito incluye:

1. Empleados, directivos y colaboradores que tengan acceso a la información corporativa.
2. Contratistas, proveedores y socios tecnológicos que gestionen servicios críticos o infraestructura subcontratada (en cumplimiento de los requisitos de seguridad en la cadena de suministro de NIS2).
3. Clientes o terceros que, por razón contractual, accedan a los sistemas o servicios protegidos por Grayhats.

El personal sujeto a esta Política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la empresa. Por lo tanto, también se aplica a los proveedores, contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la empresa.

El alcance abarca tanto los entornos físicos como los entornos en la nube, redes corporativas, equipos de usuario, aplicaciones y cualquier otro componente digital asociado.

Para garantizar que el proceso de seguridad implantado será actualizado y mejorado de forma continua, se implantará y documentará un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a ISO/IEC 27001:2022, complementado con un Sistema de Gestión de Ciberseguridad alineado con NIS2, que será objeto de revisiones periódicas, auditorías internas y actualizaciones frente a cambios tecnológicos, regulatorios o de riesgo. Así, el contenido de esta política general de seguridad de la Información y de Ciberseguridad se desarrollará en otras políticas más especializadas, guías y procedimientos complementarios de seguridad.

1.3. Marco normativo y estándares de referencia

En España, los sistemas de gestión de seguridad de la información se desarrollan dentro de un marco normativo específico que establecen los requisitos fundamentales relacionados con la seguridad de la información y la protección de datos. Este marco normativo incluye varias leyes, regulaciones y normativas que establecen los requisitos y obligaciones para garantizar la seguridad de la información en las organizaciones.

Algunos de los aspectos más relevantes de este marco normativo en España son:

1. **Real Decreto 311/2022, de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

2. **Constitución Española:** La constitución española otorga a todos los ciudadanos, entre los que se encuentran tanto los clientes como los empleados de Grayhats, una serie de derechos fundamentales

y libertades públicas. Entre ellos se encuentran el derecho al secreto en las comunicaciones, derecho a la vida privada, al honor y la propia imagen, así como el de la protección de datos como un derecho diferente al de la intimidad.

3. **Directiva (UE) 2022/2555 (NIS2),** del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad para entidades esenciales e importantes en toda la Unión Europea, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI2).

4. **Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal**. El código penal muestra las actitudes se han tipificado como delito en España. Entre ellos está la estafa electrónica, piratería informática, delitos contra la intimidad, o la corrupción de menores entre otros.

5. **Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**: Esta ley regula el tratamiento de datos personales y establece las obligaciones de las organizaciones en cuanto a la protección de la privacidad y los derechos de las personas en relación con el tratamiento de sus datos personales.

6. **Reglamento 2016/679 General de Protección de Datos (RGPD)**: Aunque es una normativa de la Unión Europea (UE), el RGPD tiene un impacto significativo en España y complementa la LOPDGDD. Establece principios, derechos y obligaciones para el tratamiento de datos personales en toda la UE, incluidas las medidas de seguridad de la información.

7. **Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE)**: Esta ley regula diversos aspectos de la sociedad de la información, incluida la seguridad de los servicios electrónicos y la protección de la información en línea.

8. **Norma UNE-ISO/IEC 27001:2022**: La adopción de la ISO 27001 en España se basa en la versión internacional de la norma, que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI).

Estas leyes, regulaciones y normativas forman un marco normativo sólido que establece las bases legales y los requisitos para la implementación de la ISO 27001 en España. Las organizaciones que operan en el país deben cumplir con estos requisitos y adoptar medidas adecuadas para garantizar la seguridad de la información y la protección de datos personales.

2. Misión

2.1. Misión de Grayhats

La misión de GrayHats es proteger la información y los activos digitales propios y de sus clientes mediante la aplicación de controles técnicos, organizativos y procedimentales que garanticen la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos.

GrayHats busca consolidarse como un referente en ciberseguridad gestionada, ofreciendo servicios basados en la excelencia técnica, la mejora continua y la confianza digital, contribuyendo así a la resiliencia y soberanía tecnológica de las organizaciones con las que colabora.

La seguridad de la información y la Ciberseguridad son pilares estratégicos y transversales que orientan todas las actividades de la empresa, integrándose en sus procesos, proyectos y relaciones con terceros, conforme a los principios del Esquema Nacional de Seguridad (ENS) y los estándares internacionales de gestión de la seguridad y ciberseguridad.

2.2. Objetivos específicos de esta política

La mayoría de los procesos de Grayhats tienen una fuerte dependencia con activos y procesos TIC, por lo que esta política de seguridad y ciberseguridad tiene como objetivo establecer los principios generales que van a regir la seguridad de la información, ciberseguridad y resiliencia operativa de Grayhats en dichos activos.

Un punto clave de la misión de Grayhats es la mejora constante de su imagen de marca y reputación, por lo que uno de los objetivos fundamentales de esta política es salvaguardarla y que no se vea mermada por un incidente de seguridad de la información o ciberseguridad.

A continuación, se describen los objetivos específicos que persigue esta política:

1. **Establecer un marco de referencia**: Esta política de seguridad de la información y ciberseguridad proporciona un marco de referencia para toda la organización, estableciendo los principios y objetivos generales de seguridad que deben seguirse.

2. **Alinear la seguridad con los objetivos de la organización**: Esta política de seguridad de la información y ciberseguridad se alineará con los objetivos y la dirección estratégica de la organización, asegurando que la seguridad de la información, ciberseguridad y la resiliencia operativa se considere como un componente integral de la gestión empresarial.

3. **Definir responsabilidades y autoridades**: Esta política identificará claramente las responsabilidades y autoridades relacionadas con la seguridad de la información, ciberseguridad y procesos, asegurando que haya una clara asignación de roles y responsabilidades dentro de la organización.

4. **Establecer un compromiso de la alta dirección**: Esta política de seguridad y ciberseguridad demuestra el compromiso de la alta dirección con la seguridad de la información, la ciberseguridad y establece un enfoque de arriba a abajo para fomentar una cultura de seguridad y ciberseguridad en toda la organización.

5. **Guiar la toma de decisiones**: Esta política proporciona un marco para la toma de decisiones relacionadas con la seguridad de la información y la ciberseguridad, asegurando que las decisiones se tomen de manera consistente y alineadas con los objetivos de Grayhats y principios establecidos.

6. **Garantizar el cumplimiento legal y normativo**: Esta política de seguridad y ciberseguridad ayudará a garantizar que la organización cumpla con todas las leyes, regulaciones y requisitos contractuales relacionados con la seguridad de la información, ciberseguridad y servicios digitales.

7. **Mejorar la conciencia y la capacitación**: La política de seguridad de la información y de ciberseguridad puede servir como una herramienta para mejorar la conciencia y la capacitación en seguridad de la información entre los empleados, asegurando que comprendan sus responsabilidades y obligaciones.

3. Organización de la seguridad y de la ciberseguridad

3.1. Requisitos de seguridad de la información y de la Ciberseguridad

Esta Política y todo el SGSI de Grayhats están dirigidas en primer lugar a cumplir los requisitos legales y reglamentarios pertinentes para la organización en el ámbito de la seguridad de la información y de la ciberseguridad, así como las obligaciones contractuales para con sus clientes y proveedores.

Adicionalmente, el SGSI de Grayhats impone requisitos que van más allá de los estrictamente requeridos por la ley. El consejo de administración de Grayhats es el órgano responsable de fijar estos requisitos estos se detallan con más detalle en el documento citado anteriormente

3.2. Principios generales de la seguridad

De acuerdo con el **artículo 5 del Real Decreto 311/2022**, por el que se regula el **Esquema Nacional de Seguridad (ENS)**, **y los principios de control y mejora continua establecidos en la norma ISO/IEC 27001:2022**, GrayHats adopta los siguientes **principios fundamentales** como marco de actuación para la protección de sus sistemas, servicios y activos de información, asegurando la **coherencia entre el marco europeo, nacional e internacional de ciberseguridad y gestión de la información**:

a) Seguridad como proceso integral

La seguridad se concibe como un **proceso transversal y continuo**, integrado en todas las fases del ciclo de vida de los sistemas de información, desde su diseño y desarrollo hasta su operación, mantenimiento y retirada. Cada área funcional de GrayHats debe incorporar medidas de seguridad coherentes con los objetivos globales de protección de la organización.

b) Gestión de la seguridad basada en los riesgos

La gestión de la seguridad se fundamenta en la **identificación, análisis, evaluación y tratamiento de los riesgos** que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. Las medidas de seguridad adoptadas deben ser proporcionales al nivel de riesgo residual aceptable, priorizando los recursos de acuerdo con el impacto potencial de las amenazas.

c) Prevención, detección, respuesta y conservación

El sistema de gestión de seguridad se estructura sobre un **ciclo continuo de mejora** que abarca cuatro fases esenciales:

- **Prevención:** adopción de medidas que eviten o reduzcan la probabilidad de incidentes.

- **Detección:** implementación de mecanismos para identificar en tiempo real eventos anómalos o compromisos de seguridad.
- **Respuesta:** actuación rápida, coordinada y eficaz ante incidentes para minimizar su impacto.
- **Conservación:** mantenimiento de evidencias y registros necesarios para el análisis forense, la mejora continua y el cumplimiento normativo.

d) Existencia de líneas de defensa

GrayHats establece un modelo de **defensa en profundidad**, donde las medidas de protección se implementan en **capas complementarias** y coordinadas, garantizando que la vulneración de una no comprometa el conjunto del sistema. Esta arquitectura permite reforzar la resiliencia y reducir la probabilidad de fallos sistémicos.

e) Vigilancia continua

Se mantendrá una **supervisión permanente de los sistemas y servicios**, utilizando herramientas y procesos que permitan la detección temprana de vulnerabilidades, amenazas o comportamientos anómalos. El Centro de Operaciones de Seguridad (SOC) de GrayHats asegura la monitorización continua y el tratamiento de eventos de seguridad.

f) Reevaluación periódica

La eficacia de las medidas de seguridad y el nivel de riesgo residual se **revisarán periódicamente** para asegurar su adecuación ante cambios tecnológicos, organizativos o normativos. Esta reevaluación forma parte del ciclo de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

g) Diferenciación de responsabilidades

GrayHats garantiza la **separación y asignación clara de funciones y responsabilidades** relacionadas con la seguridad, evitando conflictos de interés y asegurando que los controles y auditorías se realicen de manera independiente. Cada empleado y colaborador debe conocer y asumir sus obligaciones específicas en materia de seguridad de la información.

3.3. Principios generales de ciberseguridad

En coherencia con los requisitos establecidos por la **Directiva (UE) 2022/2555 (NIS2)**, Grayhats adopta los siguientes principios rectores para garantizar un nivel elevado de **ciberseguridad y resiliencia operativa**, especialmente en lo que concierne a la gestión del riesgo y la prestación segura de sus servicios digitales esenciales. Estos principios complementan los establecidos por el Esquema Nacional de Seguridad (ENS) y por el estándar ISO 27001:2022 y constituyen el marco de referencia europeo para la estrategia de ciberseguridad corporativa.

a) Enfoque basado en la gestión del riesgo

De conformidad con el artículo **21.2.a) de NIS2**, Grayhats implanta un modelo de actuación fundamentado en la **identificación, análisis y tratamiento** continuo de riesgos relativos a sus redes y sistemas de información.

Las medidas de seguridad se aplican de forma proporcional al nivel de riesgo detectado, priorizando los activos e infraestructuras más críticos para la continuidad del negocio.

b) Integración de la seguridad desde el diseño y por defecto

La **ciberseguridad por diseño y por defecto (security by design & default)** constituye un principio esencial derivado de NIS2, aplicable a todos los sistemas, servicios y proyectos tecnológicos de Grayhats.
Las medidas de seguridad deben concebirse desde la fase inicial de diseño y mantenerse activas durante todo el ciclo de vida del sistema, garantizando la prevención y resiliencia frente a ciberamenazas.

c) Protección de la cadena de suministro

El artículo **21.2.d) de NIS2** exige que las entidades implementen mecanismos para **asegurar la ciberseguridad de terceros y proveedores críticos.**
Por ello, Grayhats supervisa los riesgos derivados de la cadena de suministro y establece **controles y cláusulas de seguridad en los acuerdos de servicio** (SLA, NDA, contratos de mantenimiento, outsourcing), exigiendo niveles de protección equivalentes a los internos.

d) Respuesta y notificación de incidentes

Conforme a los artículos **23 a 28 de NIS2**, Grayhats debe contar con **procedimientos documentados de detección, gestión y notificación de incidentes de ciberseguridad a las autoridades nacionales competentes y a los clientes afectados.**
El **Centro de Operaciones de Seguridad (SOC)** supervisa los sistemas de forma continua y coordina la comunicación inmediata de eventos significativos, asegurando trazabilidad, conservación de evidencias y cumplimiento de los plazos legales de notificación.

e) Resiliencia operativa y continuidad del servicio

La NIS2 refuerza los principios de **resiliencia operacional**, obligando a las entidades a garantizar la disponibilidad y recuperación de los servicios esenciales.
Grayhats dispone de **Planes de Continuidad de Negocio (BCP) y Planes de Recuperación ante Desastres (DRP)**, revisados periódicamente, que aseguran la prestación de servicios incluso ante incidentes graves o cibercrisis.

f) Supervisión, auditoría y mejora continua

En línea con el artículo **21.3 de NIS2**, la empresa mantiene un **régimen de supervisión y revisión continua del Sistema de Gestión de Seguridad de la Información y de Ciberseguridad**, apoyado en auditorías internas, revisiones directivas y controles técnicos automatizados.
Este principio consolida un enfoque de **mejora continua (PDCA)** tanto en la gestión del riesgo como en la adaptación a nuevas amenazas o cambios normativos.

g) Responsabilidad de la dirección y cultura de ciberseguridad

NIS2 refuerza la responsabilidad directa de los órganos de dirección sobre las políticas y medidas de ciberseguridad **(artículo 20.2)**.
Grayhats asegura la implicación ejecutiva en la toma de decisiones de seguridad y promueve una **cultura de ciberseguridad organizativa**, garantizando la formación continua, la concienciación y la rendición de cuentas a todos los niveles.

3.4. Principios directores

Además, Grayhats seguirá los siguientes principios directores básicos:

- ✓ **Principio de confidencialidad**: Los sistemas de información deberán ser accedidos sólo por personas que la organización decida que deban hacerlo, y en su caso órganos, entidades o procesos autorizados para ello, respetando las obligaciones de secreto y sigilo profesional.

- ✓ **Principio de integridad y calidad:** Se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de esta, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

- ✓ **Principio de disponibilidad y continuidad:** Se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias tanto leves como graves.

- ✓ **Principio de gestión del riesgo:** Se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

- ✓ **Principio de proporcionalidad en coste**: La implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información se deberá hacer bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se disponga de recursos necesarios para el sistema de gestión de seguridad de la información.

- ✓ **Principio de concienciación y formación:** Se articularán iniciativas que permitan a las personas usuarias de los sistemas de información, conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. Se prestará especial atención a la concienciación a la propiedad, gerencia, así como a la dirección y altos cargos ya que deben conocer tanto los riesgos a los que se enfrentan, así como su responsabilidad personal ante la justicia que incluso puede llegar a ser penal.

  De igual forma, se fomentará la formación específica en materia de ciberseguridad a todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

- ✓ **Principio de prevención:** Se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir incidentes, fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

- ✓ **Principio de detección temprana y respuesta:** Los sistemas y servicios se deben monitorizar de manera continua para detectar anomalías e indicadores de compromiso en su fase más temprana posible, para así actuar en consecuencia respondiendo eficazmente, mediante los mecanismos y planes de contingencia establecidos.

- ✓ **Principio de mejora continua:** Se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Empresa.

- ✓ **Principio de ciberseguridad en el ciclo de vida de los sistemas de información:** Las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

- ✓ **Principio de función diferenciada:** La responsabilidad de la seguridad de los sistemas de información, estará diferenciada de la responsabilidad sobre la prestación de los servicios de TI. Esto es así porque existe un conflicto de intereses entre ambas funciones.

Esta política de seguridad de la Información ha sido aprobada por el consejo de administración de la empresa por lo que su contenido y el de las normas y procedimientos anexos que la desarrollan, es de obligado cumplimiento para todo el personal de la empresa.

En particular:

- ✓ Todos los usuarios con acceso a la información tratada, gestionada, o propiedad de la empresa tienen la obligación de custodiarla y protegerla.

- ✓ La política y las normas de seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas de la norma ISO/IEC 27001:2022.

- ✓ Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el documento de aplicabilidad. La dirección de la empresa establecerá una planificación para su implantación y control.

- ✓ Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.

- ✓ Las y los usuarios que incumplan la política de seguridad de la Información, o las normas y procedimientos complementarios, podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con la empresa y con la legislación vigente y aplicable.

3.5. Roles, responsabilidades y deberes

En esta sección definiremos un marco de funciones y responsabilidades que es fundamental para un buen gobierno de la seguridad y salud de los sistemas que mantienen la información y soportan los servicios ofrecidos

por la organización y ayudará a ordenar y legitimar las acciones en materia de seguridad de la información y servicios.

Este marco definirá roles y responsabilidades a 3 niveles:

1. **Roles de Gobierno**: Son los responsables y propietarios del sistema de información y los riesgos de estos. Estos roles desempeñan funciones clave en la dirección estratégica y el cumplimiento de los objetivos, tanto de la empresa, como del sistema de seguridad de la información. Dentro de esta categoría típicamente se encuentra el Consejo de Administración, CEO, CIO o CFO entre otros.

2. **Roles Ejecutivos**: Son los responsables de diseñar y supervisar el sistema de gestión de seguridad de la información, así como los planes de resiliencia y contingencia. Dentro de esta categoría típicamente se encuentra el CISO o el DPO.

3. **Roles de Operaciones**: Son los encargados del desarrollo y operaciones diarias que comprenden tanto el sistema de información como sus procesos de seguridad. Dentro de esta categoría típicamente se encuentran puestos como el CTO, desarrolladores de software y técnicos de sistemas.

En otro nivel estarían los empleados y colaboradores externos que son parte también del sistema pero que no se encuentran dentro de la sección organizativa de la seguridad.

3.5.1. El responsable de la información y el servicio

El responsable de la información y el servicio (abreviado **RINF**) es habitualmente una persona que ocupa un alto cargo en la dirección de la organización, o un comité con poderes suficientes a tal efecto. Este cargo tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. El responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Ya que es responsable del riesgo, este tiene la potestad de establecer los requisitos materia de seguridad de la información, así como los requisitos de la resiliencia operativa y continuidad de negocio. Estos requisitos se establecerán de manera clara y de manera cuantificable mediante métricas como RTO, RPO ó MTTR.

Específicamente y respecto a esta política el responsable de la información y servicio se compromete a los siguiente:

- ✓ Demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información y de la ciberseguridad.
- ✓ Recibir formación periódica sobre el estado del arte de los riesgos de ciberseguridad y de sus posibles impactos.
- ✓ Asegurar que se establece una política que establezca los objetivos de seguridad de la información y de la ciberseguridad y que estos son, no sólo compatibles, si no impulsores de los objetivos estratégicos de la organización.

- ✓ Aprobar y comunicar esta política de seguridad de la Información y de la ciberseguridad, las normas de uso de los sistemas de información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.
- ✓ Reunirse al menos una vez al trimestre, y cuando cualquier evento o solicitud extraordinaria lo demande, con los responsables de Seguridad y de Sistemas, para ser informado sobre el SGSI y actualizar la estrategia en materia de Seguridad de la Información.
- ✓ Fomentar, mediante las acciones pertinentes, una cultura corporativa de seguridad de la informacióny de ciberseguridad.
- ✓ Apoyar con recursos, la mejora continua de los procesos de seguridad de la información y de ciberseguridad.
- ✓ Asegurar que estén disponibles los recursos necesarios para el cumplimiento de la política de seguridad de la información y de ciberseguridad, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de seguridad de la información y de la ciberseguridad.
- ✓ Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y de la ciberseguridad y los criterios para asumir los riesgos y asegurar la evaluación de estos al menos con una periodicidad anual.
- ✓ Asegurar que se realizan auditorías internas de seguridad de la información y de ciberseguridad y que se revisan sus resultados para identificar oportunidades de mejora.
- ✓ Dotar y controlar el presupuesto para seguridad de la información y ciberseguridad.
- ✓ Aprobar los planes de formación y las mejoras y proyectos relacionados con la seguridad de la información.
- ✓ Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad y ciberseguridad.

El consejo de administración de Grayhats ha designado que tanto el rol de responsable de la información como del servicio, será desempeñado por [redacted] **(Datos Disponibles en Anexo Independiente con clasificación Interna)**.

3.5.2. El responsable del sistema

El responsable del sistema (abreviado **RSIS**) es la persona cuyas responsabilidades principales es supervisar y operar los sistemas de información de la empresa y sus operaciones:

- ✓ Desarrollar, operar y mantener los sistemas de Información y ciberseguridad durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- ✓ Definir la topología y sistema de gestión del Sistema de Información y de ciberseguridad estableciendo los criterios de uso y los servicios disponibles en el mismo.
- ✓ Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y ciberseguridad y los planes de continuidad existentes.
- ✓ Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- ✓ Implantar las medidas necesarias para garantizar la seguridad de los sistemas durante todo su ciclo de vida, de acuerdo con el responsable de seguridad.
- ✓ Aprobar toda modificación sustancial de la configuración de cualquier elemento de los sistemas.

- ✓ Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el responsable de Seguridad y la dirección.
- ✓ Realizar con la colaboración del responsable de seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al responsable de seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- ✓ Elaborar, en colaboración con el responsable de Seguridad, la documentación de seguridad y de ciberseguridad de tercer nivel (Guías. Procedimientos Operativos e Instrucciones Técnicas).
- ✓ La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información y de ciberseguridad.
- ✓ La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información y de ciberseguridad.
- ✓ La gestión de las autorizaciones concedidas a los usuarios del sistema en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- ✓ La aplicación de los procedimientos operativos de seguridad.
- ✓ Aprobar y aplicar los cambios de configuración del sistema de información y ciberseguridad.
- ✓ Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información y ciberseguridad.
- ✓ Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- ✓ Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- ✓ Informar a los respectivos responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

El responsable de la información ha designado para este puesto al director tecnología, [redacted] **(Datos Disponibles en Anexo Independiente con clasificación Interna).**

3.5.3. El responsable de la seguridad

El responsable de la seguridad (abreviado **RSEC**) es la persona cuyas responsabilidades fundamentales son la de diseñar y supervisar el plan director de seguridad de la información y resiliencia operativa de Grayhats.

Específicamente y respecto a esta política el responsable de seguridad de Grayhats se compromete a los siguiente:

- ✓ Definir la estrategia de seguridad de la información, ciberseguridad y resiliencia de servicios electrónicos alineada con los objetivos del negocio.
- ✓ Establecer y supervisar planes de respuesta ante incidentes.
- ✓ Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los responsables del servicio y de la información.
- ✓ Promover las actividades de concienciación y formación en materia de seguridad y ciberseguridad en su ámbito de responsabilidad.

- ✓ Coordinar el análisis, contención, notificación y recuperación ante ciberataques.
- ✓ Dirigir y supervisar las actividades del equipo técnico del SOC.
- ✓ Evaluar la seguridad de los proveedores y otros socios comerciales.
- ✓ Realizar con la colaboración del responsable del sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al responsable del sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.
- ✓ Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y ciberseguridad y analizar los informes de auditoría, elaborando las conclusiones a presentar al responsable del sistema para que adopte las medidas correctoras adecuadas.
- ✓ Coordinar el proceso de gestión de la seguridad, en colaboración con el responsable de sistemas.
- ✓ Diseñar campañas de concienciación interna sobre buenas prácticas de seguridad y ciberseguridad.
- ✓ Formar a empleados en detección de phishing y uso seguro de sistemas.
- ✓ Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el responsable de sistemas.
- ✓ Verificar que las medidas de seguridad y de ciberseguridad son adecuadas para la protección de la información y los servicios.
- ✓ Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el responsable del Sistema, aportando información puntual para la toma de decisiones.

Respecto a la documentación, y apoyándose en el responsable del Sistema, son funciones del responsable de seguridad:

- ✓ Determinar la categorización del Sistema de gestión de Seguridad de la Información, siendo los responsables de la información y el servicio y el responsable del sistema los que la valorarán.
- ✓ Proponer al responsable de la información, y al responsable de sistemas para su aprobación, la documentación de seguridad de segundo nivel (Políticas específicas) y firmar dicha documentación.
- ✓ Aprobar la documentación de seguridad y ciberseguridad de tercer nivel (Guías, Procedimientos Operativos e Instrucciones Técnicas).
- ✓ Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

El responsable de la información ha designado para este puesto a, [redacted] **(Datos Disponibles en Anexo Independiente con clasificación Interna)**.

3.5.4. Responsabilidades y funciones del comité de seguridad

- ✓ Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- ✓ Informar regularmente del estado de la seguridad de la información y de la Ciberseguridad a la Dirección.
- ✓ Promover la mejora continua del sistema de gestión de la seguridad de la información y de la ciberseguridad.
- ✓ Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la Información y de la ciberseguridad.

- ✓ Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información y ciberseguridad, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- ✓ Elaborar (y revisar regularmente) la Política de Seguridad de la Información y de la Ciberseguridad para su aprobación por la Dirección.
- ✓ Aprobar la Normativa de Seguridad de la información y de la Ciberseguridad.
- ✓ Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información y de la ciberseguridad.
- ✓ Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- ✓ Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- ✓ Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad y ciberseguridad.
- ✓ Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- ✓ Priorizar las actuaciones en materia de seguridad y ciberseguridad cuando los recursos sean limitados.
- ✓ Velar porque la seguridad de la información y de la ciberseguridad se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- ✓ Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

3.5.5. Procedimientos de designación

El responsable de la información y los servicios ha sido nombrado por el consejo de administración de Grayhats. Los responsables de seguridad y sistemas han sido nombrados por el responsable de la información y servicio.

3.5.6. Procedimiento de resolución de conflictos

En caso de conflicto entre el responsable del sistema y el responsable de la seguridad, tendrá prevalencia los designios del responsable de la seguridad.

3.5.7. Otros roles en el sistema

Empleado

Toda persona vinculada con la empresa mediante un contrato laboral, que acceda a la información tratada, gestionada o propiedad de la empresa se considerará un empleado. Los empleados son responsables de su

conducta cuando acceden a la información o utilizan los sistemas informáticos de la empresa. El empleado es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los empleados tienen la obligación de:

- ✓ Cumplir la Política de Seguridad de la Información y de la Ciberseguridad y las normas, procedimientos e instrucciones complementarias.
- ✓ Proteger y custodiar la información de la empresa, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- ✓ Conocer y aplicar la política de seguridad de la Información y de la Ciberseguridad, las normas de uso de los sistemas de Información y el resto de las políticas, normas, procedimientos y medidas de seguridad aplicables.
- ✓ Reportar cualquier incidente de seguridad de la información o de ciberseguridad que observen o del que sean conscientes. Esto puede incluir intentos de acceso no autorizado, pérdida de información o violaciones de las políticas de seguridad de la información y de la ciberseguridad.
- ✓ Participar en las formaciones y actividades de concienciación sobre la seguridad de la información y ciberseguridad proporcionadas por la empresa.
- ✓ Utilizar las herramientas y recursos proporcionados por la empresa para realizar su trabajo de manera segura.
- ✓ Formarse de manera proactiva en materia de concienciación de seguridad de la información, ciberseguridad, reconocimiento de técnicas de ingeniería social y resiliencia de procesos.

Colaborador Externo

Los colaboradores externos son todas aquellas personas o entidades que, sin tener un contrato laboral con la empresa, pueden tener uno mercantil, o no, pero interactúan de alguna forma con los activos de información, procesos o sistemas de la organización. Esto puede incluir a proveedores, clientes, consultores, socios comerciales, entre otros.

Los colaboradores externos tienen la obligación de:

- Firmar un Acuerdo de Confidencialidad con la empresa.
- Cumplir con todas las políticas y procedimientos relacionados con la seguridad de la información y de la ciberseguridad que sean aplicables a su relación o interacción con la empresa. Esto incluye respetar los términos y condiciones de los acuerdos de confidencialidad o los contratos de servicio, que pueden incluir cláusulas relacionadas con la seguridad de la información.
- Proteger la información a la que tienen acceso como parte de su colaboración con la empresa. Esto incluye prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información, ya sea accidental o deliberada.
- Reportar cualquier incidente de seguridad de la información o ciberseguridad que observen o del que sean conscientes en el contexto de su trabajo con la empresa. Esto puede incluir intentos de acceso no autorizado, pérdida de información o violaciones de las políticas de seguridad de la información.

- Cooperar con la empresa en cualquier actividad relacionada con la seguridad de la información o ciberseguridad, como auditorías de seguridad o investigaciones de incidentes.
- Utilizar las herramientas y recursos proporcionados por la empresa de manera segura y solo para los fines permitidos como parte de su colaboración.

Delegado de Protección de Datos

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el delegado de Protección de Datos (abreviado **DPD**) tendrá como mínimo las siguientes funciones:

- ✓ Difundir buenas prácticas, políticas y concienciación sobre la protección de datos en toda la organización.
- ✓ Asegurar que la empresa responda adecuadamente a solicitudes de derechos de los usuarios: acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad.
- ✓ Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación con el RGPD y otras disposiciones de protección de datos.
- ✓ Revisar bases legales, cláusulas informativas y contratos con encargados del tratamiento.
- ✓ Supervisar el cumplimiento de lo dispuesto en el presente reglamento y Ley Orgánica de protección de datos, de otras disposiciones de protección de datos de la Unión o de los estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- ✓ Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- ✓ Actuar como punto de contacto de la autoridad de control (AEPD) para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
- ✓ Verificar que el Registro de Actividades de Tratamiento (RAT) esté actualizado.

En Grayhats el puesto de Delegado de Protección de Datos lo ocupa [redacted] **(Datos Disponibles en Anexo Independiente con clasificación Interna)**.

3.6. Evaluación y Gestión de Riesgos

GrayHats establece un proceso continuo de evaluación y gestión de riesgos, conforme a los principios del Esquema Nacional de Seguridad (ENS), la ISO 27001:2022 y NIS2, y emplea como marco metodológico la metodología MAGERIT v3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

3.6.1. Objetivo

El objetivo de este proceso es identificar, analizar, valorar y tratar los riesgos que afectan a los sistemas de información, activos y servicios esenciales para el cumplimiento de las funciones de la organización, garantizando un nivel de seguridad adecuado al nivel de riesgo asumible.

3.6.2. Enfoque metodológico

El análisis se desarrolla conforme a los siguientes principios clave de MAGERIT v3:

- **Identificación de activos**: Se inventarían los activos tanto físicos como lógicos, y se establece su valoración en función de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- **Identificación de amenazas y vulnerabilidades**: Se consideran amenazas intencionadas y accidentales, internas y externas, junto con las vulnerabilidades existentes en los activos identificados.
- **Análisis de riesgos**: Se evalúa el impacto potencial (económico, reputacional, legal y operativo) de la materialización de las amenazas, y se determina la probabilidad de ocurrencia.
- **Valoración del riesgo**: Se calcula el nivel de riesgo resultante de la combinación entre el impacto y la probabilidad, clasificando los riesgos según niveles (aceptable, tolerable, no tolerable).
- **Tratamiento del riesgo**: Se seleccionan e implementan medidas de seguridad (técnicas, organizativas y procedimentales) proporcionales al nivel de riesgo identificado, de acuerdo con el catálogo de medidas del ENS.

3.6.3. Evaluación continua

El análisis de riesgos se revisará y actualizará al menos una vez al año, o siempre que se produzcan cambios significativos en los sistemas, servicios o amenazas conocidas.

Se mantendrá un registro actualizado de riesgos, sus responsables y el estado de aplicación de medidas correctoras. Se realizarán actividades de seguimiento y monitorización para verificar la eficacia de las medidas implantadas y detectar nuevos riesgos.

Los resultados del análisis se integrarán en la planificación de la seguridad, el plan de mejora continua, y en la toma de decisiones estratégicas de la organización.

3.7. Documentos de desarrollo de la seguridad y de la ciberseguridad

Esta política general de seguridad de la Información y de la ciberseguridad se desarrollará por medio de distintos documentos e instrumentos que afronten y amplíen aspectos específicos.

Se usarán los siguientes instrumentos:

1. **Políticas de seguridad específicas**: Uniformizan el uso de aspectos concretos del sistema. Son documentos que indican el uso correcto y las responsabilidades del usuario a alto nivel y no suelen entrar en detalles técnicos. Son de carácter obligatorio.
2. **Estándar:** Describe el uso específico de una tecnología en la empresa. Por ejemplo; todos los ordenadores personales deben tener el sistema operativo Windows 10 Profesional o superior. Son de carácter obligatorio.
3. **Guías de seguridad**: Tienen un carácter informativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos. Ayudan a prevenir que se pasen por alto aspectos importantes de

seguridad que pueden materializarse de varias formas. Estas guías pueden ofrecerse a los usuarios en forma de curso o aplicación interactiva.

4. **Procedimientos operativos de seguridad (POS)**: Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.
5. **Instrucciones técnicas (IT):** Desarrollan los POS llegando al máximo nivel de detalle, indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas.
6. **Baselines (Benchmarks):** Son medidas comparativas que se utilizan para evaluar el rendimiento, la eficiencia, el nivel de seguridad o la calidad de un sistema, dispositivo, componente o proceso en relación con otros similares. Son de carácter obligatorio.

3.8. Controles de seguridad de la información

GrayHats adopta y aplica un conjunto de **medidas de seguridad organizativas, operativas y técnicas**, conforme al Catálogo de Medidas del Esquema Nacional de Seguridad (ENS) recogidas en el Anexo II del RD 311/2022 de 3 de Mayo, con el objetivo de garantizar la protección adecuada de la información y los servicios, en función de su nivel de seguridad definido a nivel medio.

Estas medidas se agrupan en tres dominios principales:

- **Marco organizativo**: medidas relacionadas con la gobernanza, la planificación, la gestión de riesgos y el aseguramiento del cumplimiento.
- **Marco operacional**: medidas para la explotación segura de los sistemas, protección contra amenazas, control de accesos y gestión de incidentes.
- **Medidas de protección**: controles técnicos específicos para la seguridad lógica, física y ambiental, comunicaciones seguras y protección de la información.

La aplicación de estas medidas estará sujeta a la "*Declaración de Aplicabilidad de Medidas del ENS*" que forma parte del plan director de seguridad de Grayhats.

Además, GrayHats cumple y aplica los controles de seguridad correspondientes al estándar ISO 27001:2022. Esta aplicación de medidas está recogida en la "*Declaración de Aplicabilidad de Medidas de la ISO 27001*" que también forma parte del plan director de seguridad.

Grayhats armonizará la implantación de estas medidas para estar conforme con los estándares mencionados de manera eficiente y racionalizada, así como con otros que pudieran ser de aplicación como NIS2, SOC2 o PCI-DSS.

3.9. Gestión de vulnerabilidades

Grayhats realizará de manera periódica una identificación proactiva de vulnerabilidades técnicas y superficie de ciber exposición de los sistemas de información y aplicaciones empleadas en la organización. Una vez realizada, y de acuerdo con su exposición a dichas vulnerabilidades, se adoptarán las medidas adecuadas para mitigar, tanto dicha vulnerabilidad como su riesgo asociado.

3.10. Gestión de incidentes

Todos los empleados de Grayhats tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad, de cualquier incidente o anomalía que pudiera comprometer la seguridad de sus activos de información.

Asimismo, Grayhats implementará procedimientos para la correcta gestión de los incidentes detectados siguiendo el marco de gestión de incidentes: *Procedimiento de Gestión de Ciberincidentes para el sector privado y la ciudadanía* de INCIBE, y en caso de que haya que notificar dicho incidente a la autoridad competente, se usará como referencia la *Guía Nacional de Notificación y Gestión de Ciberincidentes* del Consejo Nacional de Ciberseguridad del Gobierno de España.

Esto se definirá con más detalle en la política específica sobre gestión de incidentes.

3.11. Obligaciones del personal

Todo el personal de la empresa tiene la obligación de conocer y cumplir esta política de seguridad de la Información y de la ciberseguridad y sus instrumentos de desarrollo. Si algún punto no llegase a quedar claro para alguna persona, esta deberá pedir al responsable de seguridad que se la aclare.

Todos los miembros la empresa atenderán a una sesión de concienciación en materia de seguridad TIC y de ciberseguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la empresa, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC y de ciberseguridad recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

3.12. Contrataciones internas y externas

Todas las contrataciones, laborales o mercantiles, que requieran acceso o tratamiento de información clasificada como no pública, se realizarán amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

En aquellos casos en los que los proveedores de servicios contratados necesiten acceso a datos de carácter personal, se incluirá en el contrato, el clausulado requerido para el cumplimiento de la LOPDGDD y sus desarrollos.

Las empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, conocerán la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las empresas y personas externas que accedan a la información de la empresa considerarán dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

3.13. Registro de actividad

Grayhats de manera generalizada, registrará las actividades de su personal con el fin de monitorizar, analizar, investigar y documentar actividades indebidas que pudiesen violar esta política y su espíritu, permitiendo identificar en cada momento a la persona infractora. Todo ello con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, de acuerdo con los derechos fundamentales de la persona, y la normativa sobre protección de datos personales y demás disposiciones que resulten de aplicación.

3.14. Proceso disciplinario y régimen sancionador

Cualquier violación de la presente Política de Seguridad de la Información y de la Ciberseguridad o alguna de las políticas derivadas de esta, procedimientos o estándares, puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de Grayhats. Es responsabilidad de todos los empleados de Grayhats notificar al responsable de Seguridad de la Información cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

Grayhats dispone de un proceso disciplinario formal, documentado y comunicado a todo el personal, que se activa ante cualquier incumplimiento de la presente Política, de las políticas y procedimientos derivados o del resto del marco normativo del SGSI. Este proceso da cumplimiento al control 6.4 «Proceso disciplinario» de la Norma UNE-EN ISO/IEC 27001:2022 y a la medida mp.per.2.1 del Esquema Nacional de Seguridad, y se ejerce siempre en el marco del texto refundido de la Ley del Estatuto de los Trabajadores y del convenio colectivo de aplicación.

Los incumplimientos se clasifican, en función de su gravedad, intencionalidad, reincidencia e impacto sobre la confidencialidad, la integridad o la disponibilidad de la información, en faltas leves, graves y muy graves. Tienen la consideración de muy graves, entre otros, la revelación o el uso indebido de información confidencial, el sabotaje de sistemas, el acceso no autorizado deliberado, la sustracción de información o de credenciales y el incumplimiento doloso de las obligaciones de seguridad.

El proceso disciplinario se sustancia de forma garantista conforme a las siguientes fases: detección y comunicación del posible incumplimiento; instrucción e investigación con recopilación de evidencias; notificación escrita a la persona afectada de los hechos imputados y de las posibles sanciones; trámite de audiencia, en el que la persona puede formular alegaciones y aportar pruebas; resolución motivada; aplicación de una sanción proporcional a la gravedad; y registro documentado del expediente.

El proceso se rige por los principios de proporcionalidad de la sanción, presunción de inocencia, derecho de audiencia y defensa, confidencialidad y discreción en su tramitación, ausencia de represalias frente a quien notifica de buena fe, e igualdad de trato. Su desarrollo operativo (tipificación de faltas, catálogo de sanciones y

procedimiento detallado) se recoge en la Política de Gestión de Recursos Humanos y en el Procedimiento de Gestión del Personal.

3.15. Acuerdos de confidencialidad y no divulgación

Toda persona (empleados, becarios, personal en prácticas, personal contratado a través de terceros, proveedores y visitantes) que pueda acceder a información no pública de Grayhats o de sus clientes asume formalmente, con carácter previo a dicho acceso, un deber expreso de confidencialidad y no divulgación, materializado mediante la firma de un acuerdo de confidencialidad o no divulgación (NDA). Esta exigencia da cumplimiento al control 6.6 «Acuerdos de confidencialidad o no divulgación» de la Norma UNE-EN ISO/IEC 27001:2022 y a la medida mp.per.2.3 del Esquema Nacional de Seguridad.

Grayhats mantiene tres modelos de acuerdo, gestionados y revisados con periodicidad anual: un modelo específico para empleados, incorporado como anexo al contrato de trabajo y firmado antes de la entrega de credenciales; un modelo específico para terceros y proveedores, vinculado a los contratos de prestación de servicios y a los acuerdos de tratamiento de datos del artículo 28 del RGPD; y un modelo específico para visitantes y candidatos con acceso a información no pública.

El deber de confidencialidad abarca toda la información a la que se acceda durante la relación, subsiste tras su finalización por tiempo indefinido respecto de los secretos empresariales y se ejerce conforme a la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, al deber de secreto del artículo 5 de la LOPDGDD y al artículo 5 del Estatuto de los Trabajadores. Su incumplimiento se gestiona conforme al proceso disciplinario del apartado anterior, sin perjuicio de las responsabilidades civiles o penales que correspondan. El desarrollo operativo de los modelos de NDA y de su ciclo de vida se recoge en el Procedimiento de Gestión del Personal y en la Política de Gestión de Recursos Humanos.

3.16. Teletrabajo y trabajo a distancia

Grayhats admite la prestación de servicios en régimen de teletrabajo o trabajo a distancia, tanto de forma regular (estructural) como ocasional (movilidad, viajes o situaciones excepcionales), siempre que se garantice un nivel de seguridad equivalente al del trabajo presencial. Esta modalidad se regula conforme al control 6.7 «Trabajo a distancia» de la Norma UNE-EN ISO/IEC 27001:2022 y a la Ley 10/2021, de 9 de julio, de trabajo a distancia.

El teletrabajo regular requiere autorización previa y la formalización del correspondiente acuerdo de trabajo a distancia. El personal que desempeñe funciones fuera de las instalaciones corporativas debe emplear exclusivamente equipos corporativos bastionados, con cifrado de disco, protección antimalware/EDR y conexión a los sistemas internos a través de la VPN corporativa con autenticación multifactor; debe mantener un entorno de trabajo privado y seguro, aplicar la política de puesto de trabajo despejado y pantalla limpia, y notificar de inmediato cualquier incidente, pérdida o robo de equipos.

El desarrollo técnico, organizativo y físico de las medidas de teletrabajo se recoge en el Procedimiento de Gestión del Personal y en la Normativa de Uso Aceptable de Recursos TIC, y su cumplimiento es objeto de formación específica obligatoria con carácter previo al inicio de la actividad a distancia.

3.17. Gestión de excepciones

Cualquier excepción a la presente Política de Seguridad de la Información y de la Ciberseguridad será registrada e informada al responsable de la Seguridad de la Información de Grayhats. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la organización y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

3.18. Mejora continua del proceso de seguridad y de la ciberseguridad

El sistema de gestión de seguridad y de la ciberseguridad implantado es actualizado y mejorado de manera continua, según establecen las especificaciones de la norma ISO 27001:2022, el esquema nacional de seguridad y la directiva NIS2.

3.19. Comunicación de la política

El responsable de Seguridad apoyado por el departamento de Recursos Humanos debe asegurarse de que todos los empleados de Grayhats, así como las partes externas apropiadas, conozcan y estén familiarizados con esta política.

4. Clasificación de la información

Para alinear con ambos marcos, se proponen 4 niveles de clasificación alineados con los habitualmente usados para empresas comerciales. Son los siguientes:

Información Confidencial (Nivel 4)

Características:

- Información altamente sensible que causaría daño significativo si se divulga.
- Acceso muy limitado, solo personal específico con "Necesidad de Saber".
- Requiere máximas medidas de protección.

Ejemplos:

- **Estrategia de Negocio**: Planes de adquisición, estrategias competitivas, roadmaps de productos.
- **Información Financiera**: Estados financieros no públicos, proyecciones de ingresos, costos detallados.
- **Propiedad Intelectual**: Fórmulas secretas, algoritmos propietarios, patentes en desarrollo.
- **Datos de Clientes**: Información de clientes de alto perfil, contratos exclusivos o datos personales de tratamiento especial. Información de configuración o acceso a cuentas de clientes.
- **Investigación y Desarrollo**: Proyectos en desarrollo, resultados de investigación no publicados
- **Información Legal**: Estrategias de litigio, acuerdos confidenciales, due diligence de M&A

Información Sensible (Nivel 3)

Características:

- Información que requiere cuidado especial en su manejo.
- Puede incluir datos personales o información regulada.
- Es interna a la empresa y le aplica el principio “Necesidad de Saber”. No se comparte entre departamentos.
- Nivel medio-alto de protección.

Ejemplos:

- **Datos Personales**: PII (Personally Identifiable Information), información de contacto de clientes.
- **Información de Recursos Humanos**: Información de nómina (no detallada), beneficios, datos básicos de empleados.
- **Datos de Clientes**: Listas de clientes, preferencias de compra, historial de transacciones básico.
- **Información Regulatoria**: Reportes de compliance, auditorías internas, documentación regulatoria.
- **Datos de Salud**: PHI (Protected Health Information) en organizaciones de salud.
- **Información Financiera Personal**: Datos de tarjetas de crédito (enmascarados), información bancaria básica.

Información Interna (Nivel 2)

Características:

- Información para uso interno de la organización.
- Daño moderado si se divulga externamente.
- No debe compartirse fuera de la organización sin autorización.

Ejemplos:

- **Información Organizacional**: Organigramas detallados, políticas internas, procedimientos operativos.
- **Datos de Empleados**: Directorios internos, información de contacto, evaluaciones de desempeño.
- **Información Operacional**: Métricas de rendimiento interno, reportes de KPIs, análisis de procesos.
- **Documentación Técnica**: Manuales de sistemas internos, configuraciones de red, procedimientos IT.
- **Información de Proveedores**: Contratos con vendors, evaluaciones de proveedores, términos comerciales.
- **Comunicaciones Internas**: Emails corporativos, memorandums, actas de reuniones internas.

Información Pública (Nivel 1)

Características:

- Información que puede ser divulgada al público sin restricciones

- No causa daño a la organización si se comparte
- Disponible para uso general

Ejemplos:

- **Marketing y Publicidad**: Materiales promocionales, folletos, campañas publicitarias.
- **Información Corporativa**: Misión, visión, valores corporativos, historia de la empresa.
- **Reportes Públicos**: Estados financieros públicos (empresas cotizadas), reportes anuales, comunicados de prensa.
- **Información de Productos**: Especificaciones públicas de productos, precios públicos, catálogos.
- **Contenido Web**: Información en sitio web corporativo, redes sociales oficiales, blogs corporativos.
- **Información Regulatoria Pública**: Filings de SEC, reportes regulatorios públicos, licencias públicas.

5. Apoyo a la implantación del SGSI y de la Ciberseguridad

Por la presente, el director general y responsable de la información y servicio, declara que la implantación del SGSI, el mantenimiento adecuado de la ciberseguridad y la mejora continua serán apoyadas con los recursos adecuados para alcanzar todos los objetivos establecidos en esta política, así como para satisfacer todos los requisitos identificados.

5.1. Compromiso de la dirección

Además del director general y consejo de administración, el resto de los directores y mandos intermedios son conscientes de la importancia de la seguridad de la información y de la ciberseguridad para llevar a cabo con éxito su misión y objetivos de negocio. Por ello se comprometen a:

- ✓ Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información y de la ciberseguridad.
- ✓ Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información y de la ciberseguridad.
- ✓ Impulsar la divulgación y la concienciación de la política de seguridad de la Información y de la ciberseguridad entre los empleados.
- ✓ Exigir el cumplimiento de la política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información y de la ciberseguridad.
- ✓ Considerar los riesgos de seguridad de la información y de la ciberseguridad en la toma de decisiones.
- ✓ Dotar del presupuesto y recursos adecuados para, de manera proporcionada, conseguir el desarrollo e implementación de este sistema de gestión de seguridad de la información y de la ciberseguridad.

6. Cobertura y trazabilidad con ISO/IEC 27001:2022

La presente Política, como documento central del SGSI de GrayHats, materializa el control 5.1 «Políticas para la seguridad de la información» de ISO/IEC 27001:2022: ha sido definida y aprobada por la dirección, publicada al

personal pertinente y a las partes interesadas y se revisa con periodicidad anual o ante cambios significativos. A continuación, se relaciona, de forma agregada, la cobertura ofrecida a los controles del Anexo A de la norma.

6.1. Liderazgo y organización (5.1, 5.2 y 5.4)

Los apartados 3.5 «Roles, responsabilidades y deberes» y 3.5.4 «Responsabilidades y funciones del Comité de Seguridad» dan cumplimiento al control 5.2 mediante la asignación formal de roles (Responsable de la Información, Responsable del Servicio, Responsable de Seguridad, Responsable del Sistema, Comité de Seguridad). El compromiso de la dirección con el cumplimiento de la Política y la asignación de recursos (control 5.4) queda formalizado en el apartado de aprobación y validación de versiones por el Comité.

6.2. Contactos externos e inteligencia de amenazas (5.5 y 5.7)

GrayHats establece y mantiene contactos con las autoridades competentes (control 5.5): CCN-CERT, INCIBE-CERT, AEPD, autoridad NIS2 y, en su caso, Fuerzas y Cuerpos de Seguridad. El contacto con grupos de interés especial y foros profesionales se desarrolla, de forma independiente, en el apartado siguiente, dedicado en exclusiva al control 5.6. El control 5.7 «Inteligencia de amenazas» se cubre mediante la suscripción a feeds CTI, MITRE ATT&CK, boletines del CCN-CERT y publicaciones del SOC de GrayHats, cuya información alimenta los análisis de riesgos y los planes de tratamiento.

6.3. Contacto con grupos de interés especial (5.6)

En cumplimiento del control 5.6 «Contacto con grupos de interés especial» de la Norma UNE-EN ISO/IEC 27001:2023 (ISO/IEC 27001:2022), GrayHats establece y mantiene de forma proactiva los contactos apropiados con grupos de interés especial, foros y asociaciones profesionales especializados en seguridad de la información y ciberseguridad. Esta participación, complementaria y diferenciada del contacto formal con autoridades regulado por el control 5.5, tiene como finalidad asegurar un flujo de información adecuado y actualizado en materia de seguridad, mejorar el conocimiento de las mejores prácticas del sector y mantener una comprensión completa y vigente del entorno de amenazas.

La participación activa en estos grupos persigue, en particular, los siguientes objetivos:

- ✓ Recibir alertas tempranas, avisos y boletines sobre vulnerabilidades, amenazas emergentes y parches de seguridad.
- ✓ Obtener acceso a asesoramiento especializado y a la experiencia de profesionales y organizaciones de referencia en seguridad de la información.
- ✓ Compartir e intercambiar conocimiento sobre nuevas tecnologías, productos, técnicas, amenazas y vulnerabilidades.
- ✓ Conocer, evaluar y adoptar las mejores prácticas y los estándares del sector.
- ✓ Disponer de puntos de enlace cualificados para la coordinación y la cooperación durante la gestión de incidentes de seguridad de la información.

Con carácter enunciativo y no limitativo, GrayHats participa o mantiene contacto con los siguientes grupos, foros y comunidades: la comunidad y los foros del **CCN-CERT**, incluyendo las plataformas de intercambio e información (REYES, LUCIA y similares); los servicios y la comunidad de **INCIBE e INCIBE-CERT**; **ISMS Forum Spain**; los capítulos nacionales de **ISACA** y de **(ISC)²**; la **Cloud Security Alliance (CSA)**; la comunidad **OWASP**; el **FIRST** (Forum of Incident Response and Security Teams); los **ISAC** y grupos de intercambio sectoriales pertinentes a la actividad de la organización y de sus clientes; y las comunidades de intercambio de indicadores de compromiso basadas en **MISP**.

El **Responsable de Seguridad de la Información (RSEG)**, con el apoyo del equipo del SOC y del equipo de seguridad, es el encargado de mantener y coordinar estos contactos. La organización mantiene un registro actualizado de las membresías, foros y comunidades en los que participa, identificando para cada uno el punto de contacto interno designado, el alcance de la participación y su vigencia. La pertinencia y el valor de estas membresías se revisan, como mínimo, con periodicidad anual, de forma coordinada con la revisión de la presente Política.

La información obtenida a través de estos grupos alimenta directamente el ciclo de inteligencia de amenazas (control 5.7), los análisis de riesgos y los planes de tratamiento, y refuerza la capacidad de planificación, detección y respuesta ante incidentes (controles 5.24 a 5.28). El intercambio de información en estos foros se realiza respetando en todo momento la clasificación de la información de GrayHats y de sus clientes, aplicando el Protocolo de Semáforo (Traffic Light Protocol, TLP) y los acuerdos de confidencialidad aplicables (control 6.6), de modo que la participación en grupos externos no comprometa en ningún caso la confidencialidad de la información corporativa o de terceros.

6.4. Inventario, uso aceptable, devolución y clasificación (5.9 a 5.14)

El control 5.9 «Inventario de información y otros activos asociados» se desarrolla en el Catálogo e Inventario de Activos y la Política de inventario de activos. El uso aceptable de los activos (control 5.10) se rige por la Política de Uso Aceptable de Recursos TIC. La devolución de activos al cese o cambio de empleo (control 5.11) se aplica conforme al procedimiento de gestión de personal . La clasificación (5.12), etiquetado (5.13) y transferencia (5.14) de la información se desarrollan en la Política integral de Protección de la información y en los procedimientos asociados.

6.5. Relaciones con proveedores y cadena de suministro TIC (5.19, 5.20, 5.21 y 5.22)

El apartado 3.12 «Contrataciones internas y externas» establece el marco general que dan cumplimiento a los controles 5.19 (Seguridad en las relaciones con proveedores), 5.20 (Requisitos pactados con proveedores), 5.21 (Cadena de suministro TIC) y 5.22 (Seguimiento, revisión y gestión del cambio de servicios de proveedores), desarrollados en detalle en la Política de contratación y acuerdos de nivel de servicio, en la Política de protección de la cadena de suministro y los procedimientos de gestión de proveedores.

6.6. Gestión de incidentes (5.24, 5.25, 5.26, 5.27, 5.28 y 6.8)

El apartado 3.10 «Gestión de incidentes» establece el marco para todo el ciclo de incidentes y se desarrolla en la Política de Gestión de Incidentes y los procedimientos correspondientes. Cubre: planificación y preparación (control 5.24), evaluación y decisión sobre eventos (5.25), respuesta (5.26), aprendizaje organizacional (5.27) y recopilación de evidencias (5.28). El mecanismo de notificación de eventos por parte del personal (control 6.8) se canaliza a través del buzón info@grayhats y la formación obligatoria recogida en el apartado 3.11 «Obligaciones del personal».

6.7. Propiedad intelectual, registros y revisión independiente (5.32, 5.33 y 5.35)

Los procedimientos de gestión de licencias y de código fuente, así como las cláusulas contractuales con empleados y proveedores, dan cobertura al control 5.32 «Derechos de propiedad intelectual». Los registros del SGSI (actas, evidencias, informes, hojas de cálculo de análisis y tratamiento) se protegen conforme al apartado 3.13 «Registro de actividad», cubriendo el control 5.33 «Protección de los registros». El control 5.35 «Revisión

independiente de la seguridad de la información» se materializa mediante las auditorías internas anuales del SGSI y las auditorías externas de certificación ENS Alto e ISO/IEC 27001.

6.8. Personal: disciplina, confidencialidad y teletrabajo (6.4, 6.6 y 6.7)

El apartado «Proceso disciplinario y régimen sancionador» da cumplimiento al control 6.4 mediante un proceso disciplinario formal y comunicado al personal, con clasificación de los incumplimientos, fases garantistas y catálogo de sanciones, aplicable ante incumplimientos materiales de la Política; su desarrollo operativo se encuentra en la Política de Gestión de Recursos Humanos y en el Procedimiento de Gestión del Personal. El apartado «Acuerdos de confidencialidad y no divulgación» materializa el control 6.6, exigiendo a empleados y terceros la firma de un acuerdo de confidencialidad con carácter previo al acceso a información no pública, con revisión anual y vigencia indefinida respecto de los secretos empresariales. El apartado «Teletrabajo y trabajo a distancia» da cobertura al control 6.7, fijando las condiciones de autorización y las medidas técnicas, organizativas y físicas exigibles al trabajo fuera de las instalaciones corporativas, desarrolladas en el Procedimiento de Gestión del Personal y en la Normativa de Uso Aceptable de Recursos TIC.

7. Revisión y Aprobación de la Política

La aprobación de esta Política implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

La presente Política de Seguridad de la Información y de la Ciberseguridad, será revisada y aprobada anualmente por la dirección de la organización. No obstante, si tuvieran lugar cambios relevantes en la organización o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de Grayhats.