3HASH®

DOSIER DE CIBERSEGURIDAD Y CUMPLIMIENTO

Cumplimiento NIS2, RGPD y EU AI Act

Documentación institucional de gobernanza, ciberseguridad, gestión de riesgos y cumplimiento normativo, en alineación con la Directiva (UE) 2022/2555 (NIS2) y la normativa nacional de transposición aplicable, el Reglamento (UE) 2016/679 (RGPD), el Reglamento (UE) 2024/1689 (Reglamento Europeo de Inteligencia Artificial) y los marcos voluntarios NIST CSF, ISO/IEC 27001 y EU AI Pact.

ENTIDAD

FORTUNEWEEK – UNIPESSOAL LDA
NIPC 515 084 182

MARCA COMERCIAL

3HASH®
Marca Nacional INPI n.º 711 356

DOMICILIO SOCIAL

Rua Cardoso Marta 14 Cave
3080-012 Figueira da Foz · Portugal

VERSIÓN Y FECHA

v1.0-ES · septiembre de 2026
Próxima revisión: mayo de 2027

Dosier de Ciberseguridad y Cumplimiento — 3HASH

Entidad: FORTUNEWEEK – UNIPESSOAL LDA **Marca comercial:** 3HASH® (Marca Nacional INPI n.º 711356) **NIPC:** 515 084 182 **Domicilio social:** Rua Cardoso Marta 14 Cave, 3080-012 Figueira da Foz, Portugal

Objetivo

El presente dosier reúne, en un único conjunto institucional, la documentación interna de **ciberseguridad, gobernanza y cumplimiento normativo** de 3HASH, en alineación con:

- La **Directiva (UE) 2022/2555** (Directiva NIS2) y la normativa nacional de transposición aplicable en cada jurisdicción en la que la entidad opera;
- El **Reglamento (UE) 2016/679** (RGPD) y la normativa nacional de desarrollo aplicable;
- El **Reglamento (UE) 2024/1689** (Reglamento Europeo de Inteligencia Artificial, EU AI Act) y el compromiso voluntario **EU AI Pact**, suscrito por 3HASH en abril de 2026;
- Los marcos de referencia técnicos adoptados voluntariamente: **NIST Cybersecurity Framework 2.0**, **NIST SP 800-61** (Respuesta a Incidentes), **ISO/IEC 27001/27005** y **OWASP**.

Aplicabilidad de la NIS2 a 3HASH

FORTUNEWEEK – UNIPESSOAL LDA es una **microempresa** (10 empleados, facturación anual <2 M€) que **podría no estar sujeta directamente** al perímetro obligatorio del régimen NIS2 — régimen que recae normalmente sobre entidades medianas y grandes de los sectores esenciales o importantes definidos en los Anexos I y II de la Directiva (UE) 2022/2555.

No obstante, 3HASH adopta voluntariamente los principios y controles del régimen, por las siguientes razones:

1. **Gobernanza interna** — alineación con las buenas prácticas internacionales de ciberseguridad, con independencia de que exista o no una obligación legal directa;
2. **Cumplimiento en la cadena de suministro** — varios clientes de 3HASH sí están sujetos directamente al perímetro NIS2 (sectores de educación, sanidad, transporte y administración pública) y están legalmente obligados a realizar la debida diligencia sobre sus proveedores tecnológicos;
3. **Diferenciación competitiva** — en licitaciones públicas, propuestas comerciales y candidaturas a fondos europeos;

4. **Responsabilidad civil y reputacional** — mitigación del riesgo de incidentes que puedan afectar a clientes o a terceros.

Índice de documentos

#	Documento	Estado	Versión
01	Política de Ciberseguridad 3HASH	En vigor	1.0
02	Plan de Respuesta a Incidentes	En vigor	1.0
03	Evaluación de Riesgos	En vigor	1.0
04	Designación de Responsable de Ciberseguridad y Auditoría Externa	En vigor	1.0
05	Registro de Formación en Ciberseguridad	En vigor	1.0
06	Inventario de Activos y Soberanía Tecnológica	En vigor	1.0

Marcos de referencia aplicados

Marco europeo

Referencia	Aplicación
Directiva (UE) 2022/2555 (NIS2)	Art. 7 (estrategia nacional), Art. 20 (gobernanza y responsabilidad de los órganos de dirección), Art. 21 (medidas de gestión de riesgos), Art. 23 (notificación de incidentes), Art. 24 (uso voluntario de esquemas de certificación de ciberseguridad)
Reglamento (UE) 2016/679 (RGPD)	Art. 5 (principios), Art. 25 (protección de datos desde el diseño), Art. 32 (seguridad del tratamiento), Art. 33-34 (notificación de violaciones), Art. 35 (evaluación de impacto)
Reglamento (UE) 2024/1689 (EU AI Act)	Art. 5 (prácticas prohibidas), Art. 50 (obligaciones de transparencia)
Reglamento (UE) 2019/881 (Cybersecurity Act)	Esquemas europeos de certificación de la ciberseguridad

Marco nacional de transposición

La Directiva (UE) 2022/2555 es objeto de transposición por cada Estado miembro mediante su propia normativa nacional. 3HASH aplica, en cada jurisdicción en la que opera o presta servicios, **la normativa nacional de transposición aplicable**, así como la normativa nacional de desarrollo del RGPD que resulte aplicable.

En materia de protección de datos, las obligaciones de notificación previstas en los artículos 33 y 34 del RGPD se cumplen ante **la autoridad de control competente**. Cuando el tratamiento afecte a interesados en España, la autoridad de control de referencia es la **Agencia Española de Protección de Datos (AEPD)**.

En materia de notificación de incidentes de ciberseguridad, la comunicación se dirige a **la autoridad nacional competente y al CSIRT de referencia** que correspondan en cada caso, dentro de los plazos previstos en el artículo 23 de la Directiva (UE) 2022/2555 y en la normativa nacional que la transponga.

Marco técnico voluntario (autoadopción)

Referencia	Aplicación
NIST Cybersecurity Framework 2.0 (2024)	Identificar · Proteger · Detectar · Responder · Recuperar
NIST SP 800-61 r2 (Computer Security Incident Handling)	Estructura del Plan de Respuesta a Incidentes
ISO/IEC 27001:2022	Sistema de Gestión de Seguridad de la Información
ISO/IEC 27005:2022	Gestión de riesgos de seguridad de la información
OWASP Top 10 (2021) + **OWASP ASVS v4.0.3**	Seguridad de aplicaciones
OWASP Top 10 for LLM Applications (2025)	Seguridad en sistemas basados en modelos de lenguaje
EU AI Pact — Pillar I	Compromiso voluntario de 3HASH (abril de 2026) ante la Comisión Europea
Cisco Ethical Decision Framework (Networking Academy 2026)	Anexo a la Política de Ciberseguridad (documento 01)
Marco nacional de referencia de ciberseguridad, nivel básico (QNRCS, publicado por el Centro Nacional de Cibersegurança de Portugal)	Alineación voluntaria y declarativa con los principios de dicho marco. No implica, por el momento, certificación formal por entidad acreditada.

Modelo de gobernanza

Función	Quién la asume
Responsabilidad última	Órgano de administración
Implementación operativa	Equipo técnico de 3HASH
Auditoría de ciberseguridad	Auditoría externa independiente — profesional con Máster en Informática por la Universidade de Coimbra y MBA
Comunicación con la autoridad competente en caso de incidente significativo	Órgano de administración (3HASH no dispone de registro formal de Punto de Contacto Permanente por encontrarse fuera del ámbito obligatorio del régimen)

Detalle completo en el documento 04.

Notas de versión y revisión

Versión	Fecha	Cambios
1.0	2026-05-02	Versión inicial. Creación del dosier íntegro.
1.0-ES	2026-09	Versión en español. Traducción íntegra y adaptación de las referencias normativas nacionales a formulación europea y neutra. Sin cambios en los controles, hechos, fechas ni datos de la entidad.

Revisión programada: **anual**, en el mes de mayo, o siempre que se produzca una modificación legal relevante o un incidente significativo.

Política de circulación

Este dosier se clasifica como de **uso interno**. Las versiones redactadas conforme a este índice **pueden compartirse con clientes y socios previa firma de un acuerdo de confidencialidad (NDA)**, en el marco de procesos de debida diligencia o de auditoría de proveedores. No está destinado a publicación abierta.

Las solicitudes de copia deben dirigirse a: **geral@3hash.pt** (asunto: «Solicitud de documentación de cumplimiento — [Nombre del solicitante]»).

Política de Ciberseguridad 3HASH

Versión: 1.0 **Entidad:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Fecha de aprobación:** 2 de mayo de 2026 **Próxima revisión:** mayo de 2027 (revisión anual obligatoria) **Responsable:** Responsable de Ciberseguridad (véase el documento 04)

1. Objeto y ámbito de aplicación

La presente Política de Ciberseguridad establece los principios, reglas y responsabilidades aplicables a la protección de los sistemas de información, datos e infraestructuras operados por FORTUNEWEEK – UNIPESSOAL LDA en el ejercicio de su actividad como agencia digital bajo la marca 3HASH®.

Se aplica a:

a) Todos los empleados, prestadores de servicios y subcontratistas de la entidad; b) Todos los sistemas, dispositivos, aplicaciones, servidores y servicios operados directa o indirectamente por 3HASH; c) Todo tratamiento de datos personales efectuado en el marco de proyectos propios o prestados a clientes; d) Todas las colaboraciones con terceros que impliquen acceso a datos, sistemas o redes de la entidad.

2. Marco de referencia

Esta política da cumplimiento a lo dispuesto en:

- El **artículo 21 de la Directiva (UE) 2022/2555** (NIS2) y en la normativa nacional de transposición aplicable, en lo relativo a las medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información;
- El **artículo 32 del Reglamento (UE) 2016/679** (RGPD), en lo relativo a la seguridad del tratamiento de datos personales;
- El **NIST Cybersecurity Framework 2.0** (5 funciones centrales: Identificar, Proteger, Detectar, Responder, Recuperar);
- El **EU AI Pact — Pillar I**, en lo relativo a la gobernanza responsable de los sistemas de inteligencia artificial.

2.1. Postura proactiva y adhesión voluntaria

3HASH es una microempresa que podría no estar sujeta directamente al perímetro obligatorio del régimen NIS2. La adopción de los controles descritos en esta política es, por tanto, **voluntaria y proactiva**, y expresa un compromiso institucional con:

- Las buenas prácticas internacionales de ciberseguridad;
- La protección de los datos de clientes y de usuarios finales bajo nuestra responsabilidad;
- La diferenciación competitiva en propuestas comerciales y candidaturas a fondos europeos;
- La anticipación a futuras obligaciones legales.

Con el mismo espíritu, 3HASH **alinea voluntariamente su postura de ciberseguridad con los principios del marco nacional de referencia de ciberseguridad de nivel básico** (QNRCS) publicado por el Centro Nacional de Cibersegurança de Portugal. Esta alineación es declarativa y no implica, por el momento, ningún proceso formal de certificación por entidad acreditada. 3HASH se reserva el derecho de avanzar hacia una certificación formal cuando así lo justifique la madurez de los controles o lo exija un cliente o una licitación.

---

3. Principios fundamentales

3HASH adopta los siguientes principios estructurantes en materia de ciberseguridad:

3.1. Tríada CID — Confidencialidad, Integridad y Disponibilidad

Todos los sistemas y procesos de la entidad se diseñan y operan de modo que se asegure:

- **Confidencialidad** — los datos son accesibles únicamente para quien los necesite (principio de need-to-know);
- **Integridad** — los datos están protegidos frente a modificaciones no autorizadas;
- **Disponibilidad** — los servicios críticos se mantienen accesibles dentro de los parámetros de nivel de servicio (SLA) asumidos.

3.2. Seguridad desde el diseño y por defecto (security by design / by default)

Todos los sistemas nuevos se conciben con la ciberseguridad y la privacidad como requisito desde la fase de diseño, y se configuran con la opción más restrictiva por defecto.

3.3. Defensa en profundidad (defense in depth)

La protección de los sistemas se asienta en **múltiples capas independientes** de controles — perímetro, red, host, aplicación, datos, identidad — de modo que el fallo de una capa no comprometa a las restantes.

3.4. Principio de mínimo privilegio

Cada usuario, proceso o servicio opera con **el conjunto mínimo de permisos** necesario para su cometido. Los accesos administrativos están restringidos, registrados y se revisan periódicamente.

3.5. Verificabilidad y auditabilidad

Los controles implantados son **verificables**, quedan **registrados en log** y están disponibles para auditoría interna o externa por parte de las entidades competentes (autoridad nacional de ciberseguridad, autoridad de control en materia de protección de datos, auditores contratados por los clientes).

3.6. Adopción anticipada de la normativa europea

3HASH adopta voluntariamente los principios del Reglamento Europeo de Inteligencia Artificial (a través del EU AI Pact) y de la Directiva NIS2 antes de que le resulten directamente exigibles, en su condición de entidad firmante del **EU AI Pact** (Pillar I, abril de 2026).

---

4. Responsabilidades

4.1. Órgano de administración

Responsable último de la aprobación de la presente política, de la asignación de los recursos necesarios para su implantación y del cumplimiento de las obligaciones legales derivadas de la NIS2 y del RGPD. De acuerdo con el **artículo 20 de la Directiva (UE) 2022/2555**, los órganos de dirección aprueban las medidas de gestión de riesgos de ciberseguridad, supervisan su aplicación y pueden ser considerados responsables de su incumplimiento en los términos previstos en la normativa nacional de transposición aplicable.

4.2. Responsable designado de Ciberseguridad

Conforme al documento 04, la responsabilidad en materia de ciberseguridad la asume directamente el **órgano de administración**, apoyado operativamente por el equipo técnico y por una **auditoría externa independiente** prestada por un profesional con Máster en Informática por la Universidade de Coimbra y MBA. 3HASH, por encontrarse fuera del ámbito obligatorio del régimen NIS2, **no ha efectuado el registro formal de un Punto de Contacto Permanente** ante la autoridad nacional competente. En caso de incidente significativo que justifique su comunicación a dicha autoridad, esta se realiza por el órgano de administración a través de los canales públicos disponibles.

4.3. Empleados y prestadores de servicios

Cumplen las reglas de esta política y participan en la formación continua. Comunican los incidentes o sospechas en un plazo máximo de **4 horas hábiles** desde su detección al Responsable de Ciberseguridad.

4.4. Proveedores y subcontratistas

Aceptan contractualmente cláusulas mínimas de ciberseguridad y protección de datos, sujetas al proceso de debida diligencia descrito en el documento 06.

---

5. Ámbitos de control (alineación con el art. 21, apartado 2, de la Directiva NIS2)

5.1. Identificar

- Inventario actualizado de **activos** críticos, servicios y datos (documento 06);
- **Evaluación de riesgos** anual, con revisión extraordinaria tras incidentes significativos (documento 03);
- Mapeo de **dependencias externas** (nube, DNS, proveedores SaaS, certificados).

5.2. Proteger

5.2.1. Control de accesos

- Autenticación **multifactor (MFA)** obligatoria en todos los sistemas críticos: administración de servidores, paneles de gestión, repositorios de código, cuentas de correo electrónico administrativas y gestión de dominios y DNS;
- Contraseñas de un mínimo de **12 caracteres**, con mezcla de tipos, gestionadas en un **gestor de contraseñas profesional**, sin reutilización entre sistemas;
- **Principio de mínimo privilegio** aplicado en sistemas operativos, bases de datos y aplicaciones;
- **Revocación inmediata** de accesos cuando un empleado o prestador cesa en sus funciones.

5.2.2. Cifrado

- Cifrado **en tránsito** obligatorio (TLS 1.2+ / TLS 1.3) para todos los servicios expuestos a internet;
- Cifrado **en reposo** para los volúmenes que contengan datos personales o credenciales, tanto en servidores como en estaciones de trabajo;
- Claves criptográficas gestionadas de forma separada de los datos que protegen.

5.2.3. Puestos de trabajo y dispositivos finales

- Sistema operativo **actualizado mensualmente** (como máximo, 30 días después de la publicación de un parche crítico);
- **Antivirus y cortafuegos** activos y configurados;
- Cifrado de disco activo en todas las estaciones de trabajo, conforme a lo recomendado por la formación Cisco Introduction to Cybersecurity (módulo System Safeguards);
- Bloqueo automático de pantalla tras 5 minutos de inactividad;
- Prohibición de instalar software de origen no confiable (validación previa obligatoria).

5.2.4. Servidores e infraestructura

- Sistemas de producción en **infraestructura propia ubicada en Portugal**, bajo jurisdicción de la Unión Europea;
- **Perímetro de red protegido** por cortafuegos con reglas explícitas de lista de permitidos y registro de actividad;
- Mecanismos de **mitigación de fuerza bruta** activos en los servicios de administración y autenticación;
- **Acceso administrativo únicamente mediante clave criptográfica** (sin autenticación por contraseña simple), con claves protegidas por passphrase;
- **Parches de seguridad** aplicados en un plazo máximo de 7 días para las vulnerabilidades clasificadas como critical y de 30 días para las high;
- **Segregación aplicativa** mediante contenedores, con volúmenes persistentes aislados y límites de recursos.

5.2.5. Copias de seguridad y continuidad

- **Copias de seguridad cifradas diarias** de los datos críticos, con una retención mínima de 30 días;
- **Copias de seguridad externas** (off-site) en un sistema de almacenamiento segregado y físicamente independiente, para mitigar el riesgo de ransomware;
- **Prueba anual de restauración**, con registro del resultado y validación de la integridad.

5.2.6. Seguridad de aplicaciones

- Validación rigurosa de los datos de **entrada** en todas las API y formularios (mitigación del OWASP Top 10);
- **Cabeceras de seguridad** HTTP configuradas (CSP, X-Frame-Options, Strict-Transport-Security, Permissions-Policy, Referrer-Policy);
- **Dependencias auditadas** periódicamente, sin vulnerabilidades críticas conocidas en producción;
- **Revisión de código** obligatoria antes de la promoción a producción en sistemas críticos;
- **Limitación de tasa** (rate limiting) en los endpoints públicos.

5.3. Detectar

Conforme a lo recomendado por el módulo Network Defense de la formación Cisco Introduction to Cybersecurity y por el NIST Cybersecurity Framework (función **Detect**):

- **Centralización de registros** (logs) de servidores, perímetro de red y aplicaciones, con una retención mínima de 90 días;
- **Monitorización continua y automatizada** de la integridad de los sistemas y de los sitios alojados, con **alertas en tiempo real** al Responsable de Ciberseguridad;
- **Comprobación periódica de la presencia de malware** en servidores compartidos, con mecanismos de cuarentena automática;
- **Monitorización de la reputación** de las direcciones y dominios de la entidad (listas negras, abuse reports, fuentes de threat intelligence).

5.4. Responder

- Procedimiento detallado en el documento 02 — **Plan de Respuesta a Incidentes**;
- Notificación a la **autoridad nacional competente y al CSIRT de referencia** dentro de los plazos legales (alerta temprana hasta 24 horas; notificación hasta 72 horas; informe final hasta 30 días) para los incidentes de seguridad, en los términos del **artículo 23 de la Directiva (UE) 2022/2555** y de la normativa nacional de transposición aplicable;
- Notificación a la **autoridad de control en materia de protección de datos** dentro de las 72 horas en caso de violación de la seguridad de los datos personales, en los términos del **artículo 33 del RGPD**;
- Comunicación a la persona física afectada cuando la violación sea susceptible de entrañar un alto riesgo para sus derechos y libertades (**artículo 34 del RGPD**).

5.5. Recuperar

- Restauración a partir de la copia de seguridad verificada más reciente;
- Análisis post mortem documentado, con identificación de la causa raíz y de las medidas de prevención;
- Actualización del registro de incidentes y revisión de la Evaluación de Riesgos.

---

6. Marco de Decisión Ética 3HASH

Ante cualquier dilema ético — incluidas las decisiones con impacto en la seguridad, la privacidad o el uso de la inteligencia artificial — todo empleado o prestador de servicios debe aplicar el siguiente marco, **adaptado del Cisco Ethical Decision Framework** (Cisco Networking Academy 2026):

```
Ante cualquier dilema ético, pregúntese:

1. ¿Es legal?
   ├─ No  → STOP (puede acarrear consecuencias legales graves)
   ├─ Sí  → Pasar al punto 2
   └─ No lo sé → ESPERAR (consultar al Responsable / a un jurista)

2. ¿Cumple la Política y los principios éticos de 3HASH?
   ├─ No  → STOP
   ├─ Sí  → Pasar al punto 3
   └─ No lo sé → ESPERAR

3. ¿Tengo la certeza de que no causa daño a 3HASH, a los
   clientes o a terceros?
   ├─ No  → STOP
   ├─ Sí  → Pasar al punto 4
   └─ No lo sé → ESPERAR

4. ¿Sería aceptable si todo el equipo de 3HASH actuara así?
   ├─ No  → STOP
   ├─ Sí  → Pasar al punto 5
   └─ No lo sé → ESPERAR

5. ¿Me sentiría cómodo leyendo esto en la primera página
   de un periódico de tirada nacional?
   ├─ No  → STOP
   ├─ Sí  → La decisión está alineada con esta política
   └─ No lo sé → ESPERAR
```

«ESPERAR» implica suspender la acción y consultar al Responsable de Ciberseguridad, al órgano de administración o a un asesor jurídico externo antes de continuar.

«STOP» implica no llevar a cabo la acción. Si el dilema persiste, debe escalarse al órgano de administración.

---

7. Formación y concienciación

7.1. Obligación general

De acuerdo con el **artículo 21, apartado 2, letra g), de la Directiva (UE) 2022/2555**, todos los empleados y el órgano de administración deben participar en formación periódica en ciberseguridad, dimensionada a su función.

7.2. Currículo mínimo

Cada empleado debe completar, en el plazo de **6 meses desde el inicio de sus funciones**, y renovar de acuerdo con el calendario definido en el documento 05:

- **Cidadão Ciberseguro** — Centro Nacional de Cibersegurança / NAU (~3 horas);
- **Cidadão Ciberinformado** — Centro Nacional de Cibersegurança / NAU / Lusa (~3 horas);
- **Consumidor Ciberseguro** — Centro Nacional de Cibersegurança / NAU (~4 horas);
- **Cisco Introduction to Cybersecurity** — Cisco Networking Academy (~15 horas).

Para las funciones de mayor responsabilidad técnica, se exige formación avanzada complementaria (C-Academy, especialista Cisco o equivalente).

7.3. Registro

El registro nominal de la formación completada lo mantiene el Responsable de Ciberseguridad en el documento 05.

---

8. Inteligencia artificial — principios complementarios

3HASH es **firmante del EU AI Pact** (Pillar I, abril de 2026). En todos los sistemas que utilicen o desarrollen componentes de inteligencia artificial se aplican de forma acumulativa:

- **Transparencia** — se informa a los usuarios de que interactúan con un sistema basado en inteligencia artificial (artículo 50 del Reglamento (UE) 2024/1689);
- **Modelos propios en infraestructura nacional** — para los proyectos sensibles (sanidad, educación, menores) se privilegia el uso de modelos ejecutados en servidores propios en Portugal, sin dependencia de API externas (3HASH Local AI);
- **No tratamiento de datos personales sensibles en instrucciones (prompts) enviadas a proveedores externos de nube** sin una base legal y contractual adecuada;
- **Gobernanza documentada** — los sistemas de inteligencia artificial críticos se acompañan de un documento de arquitectura técnica, de la alineación con el NIST AI RMF y, cuando proceda, de una evaluación de impacto preliminar;
- **Sin prácticas prohibidas** — no desarrollamos ni operamos sistemas que se encuadren en las prácticas prohibidas del **artículo 5 del Reglamento (UE) 2024/1689** (manipulación subliminal, explotación de vulnerabilidades, puntuación social, etc.).

---

9. Revisión y control de versiones

La presente política es objeto de **revisión anual obligatoria** por el Responsable de Ciberseguridad, con aprobación del órgano de administración. Se realizan revisiones extraordinarias siempre que:

- Se produzca una modificación legal aplicable (NIS2, RGPD, Reglamento Europeo de Inteligencia Artificial, normativa de las autoridades competentes);
- Se produzca un incidente de ciberseguridad clasificado como significativo;
- Se introduzcan cambios estructurales en los sistemas o en la infraestructura;
- El EU AI Pact, el NIST CSF u otros marcos adoptados sean objeto de una actualización material.

Versión	Fecha	Cambios	Responsable
1.0	2026-05-02	Versión inicial. Creación.	Órgano de administración
1.0-ES	2026-09	Versión en español. Traducción y adaptación de las referencias normativas nacionales a formulación europea y neutra.	Órgano de administración

10. Aprobación

Documento aprobado por el órgano de administración el **2 de mayo de 2026**.

La versión firmada y fechada se conserva en el registro controlado de la entidad.

Anexos

- Cisco Ethical Decision Framework (PDF original)
- Documento 04 — Modelo de Gobernanza y Auditoría Externa
- Documento 05 — Registro de Formación
- Justificante de adhesión al EU AI Pact

Plan de Respuesta a Incidentes de Ciberseguridad

Versión: 1.0 **Entidad:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Fecha de aprobación:** 2 de mayo de 2026 **Próxima revisión:** mayo de 2027 (revisión anual obligatoria) **Responsable:** Responsable de Ciberseguridad (véase el documento 04)

1. Objeto

El presente plan establece el procedimiento formal de respuesta a los incidentes de ciberseguridad que afecten o puedan afectar a los sistemas, datos o servicios operados por 3HASH, incluidos aquellos que se operan por cuenta de clientes.

Su estructura está alineada con:

- El **NIST SP 800-61 r2** — Computer Security Incident Handling Guide;
- El **artículo 23 de la Directiva (UE) 2022/2555** (NIS2) y la normativa nacional de transposición aplicable, en lo relativo a las obligaciones de notificación a la autoridad nacional competente y al CSIRT de referencia;
- Los **artículos 33 y 34 del Reglamento (UE) 2016/679 (RGPD)**, en lo relativo a las violaciones de la seguridad de los datos personales;
- Los principios adquiridos en el módulo Threat Analysis de la formación Cisco Introduction to Cybersecurity.

2. Definiciones

Término	Definición
Evento	Suceso observable en un sistema o red, sin que implique necesariamente un impacto en la seguridad.
Alerta	Evento que merece atención e investigación.
Incidente	Evento o conjunto de eventos con impacto adverso confirmado o probable sobre la confidencialidad, la integridad o la disponibilidad de los sistemas o de los datos.
Incidente significativo	Incidente que cumple los criterios definidos en el artículo 23, apartado 3, de la Directiva (UE) 2022/2555: ha causado o puede causar graves perturbaciones operativas o pérdidas financieras considerables; o ha afectado o puede afectar a personas físicas o jurídicas causando daños materiales o inmateriales considerables.
Violación de datos personales	Violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o el acceso no autorizados a dichos datos (artículo 4, apartado 12, del RGPD).
Alerta temprana (early warning)	Aviso previo a la autoridad competente dentro de las 24 horas siguientes a la detección.
Notificación	Comunicación a la autoridad competente dentro de las 72 horas siguientes a la detección (incidentes significativos).
Informe final	Informe completo a la autoridad competente dentro de los 30 días siguientes al incidente.

3. Estructura del plan

El ciclo de respuesta a incidentes adoptado por 3HASH sigue las **6 fases del NIST SP 800-61**:

4. Fase 1 — Preparación

La fase de preparación es continua y se desarrolla antes de que se produzca cualquier incidente.

Elemento	Estado
Política de Ciberseguridad aprobada	✅ Documento 01
Evaluación de Riesgos actualizada	✅ Documento 03
Responsable de Ciberseguridad designado	✅ Documento 04
Copias de seguridad cifradas, segregadas y probadas	✅ Verificable
Registros centralizados con retención mínima de 90 días	✅ Verificable
Lista de contactos críticos disponible	✅ Apartado 11 de este documento
Equipo formado en fundamentos de ciberseguridad	✅ Documento 05
Inventario de activos actualizado	✅ Documento 06

5. Fase 2 — Detección y análisis

5.1. Fuentes de detección

- Alertas automatizadas de la monitorización continua;
- Sistemas de detección de intrusiones y de integridad de ficheros;
- Análisis de los registros centralizados;
- Comunicación por parte de un empleado, cliente, proveedor o tercero;
- Comunicación procedente de la autoridad nacional competente, de CSIRT o de fuentes de threat intelligence.

5.2. Triaje inicial

Tras la detección, el Responsable de Ciberseguridad o el empleado de guardia ejecuta, en un plazo máximo de **2 horas hábiles**:

a) Confirmación de la ocurrencia (descartar falso positivo); b) Clasificación preliminar (gravedad, impacto, alcance); c) Decisión de escalado.

5.3. Clasificación de gravedad

Nivel	Criterio	Ejemplos
P1 — Crítico	Compromiso confirmado de sistemas críticos, exfiltración de datos personales o indisponibilidad total del servicio.	Ransomware, exfiltración masiva, desfiguración del sitio institucional.
P2 — Alto	Compromiso parcial o riesgo elevado, sin pérdida de datos confirmada.	Cuenta comprometida, malware confinado, ataque DDoS limitado.
P3 — Medio	Intento de ataque con mitigación automática activa.	Fuerza bruta bloqueada, phishing detectado y frenado.
P4 — Bajo	Anomalía menor sin impacto operativo.	Intento de escaneo externo.

5.4. Documentación

Cada incidente abre un **registro formal** que contiene: identificador único, fecha y hora de detección, fuente, descripción inicial, sistemas afectados, gravedad preliminar y responsable asignado.

---

6. Fase 3 — Contención

La contención tiene por objeto **limitar el impacto** sin destruir las pruebas forenses.

6.1. Acciones inmediatas (P1 y P2)

- Aislar los sistemas afectados de la red sin apagarlos (preservar la memoria volátil);
- Revocar las credenciales comprometidas o sospechosas;
- Bloquear las direcciones IP y las cuentas atacantes en el perímetro;
- Activar las copias de seguridad verificadas como fuente de verdad paralela;
- **Preservar las pruebas** — capturar registros, instantáneas, volcados de memoria y tráfico de red.

6.2. Comunicación interna

Notificación inmediata al órgano de administración. Para los incidentes P1, informe de situación cada 4 horas hasta la contención total.

---

7. Fase 4 — Erradicación

- Eliminación de la causa raíz: malware, cuentas comprometidas, vulnerabilidades explotadas;
- Aplicación de los parches críticos pendientes;
- Reconstrucción completa de los sistemas comprometidos a partir de una imagen limpia cuando la confianza en el sistema esté en entredicho;
- Rotación total de las credenciales relacionadas (contraseñas, claves de API, tokens, certificados).

8. Fase 5 — Recuperación

- Restauración de los servicios a partir de copias de seguridad verificadas;
- Validación funcional antes del regreso a producción;
- Monitorización reforzada durante los 30 días siguientes al incidente;
- Comunicación a clientes o usuarios cuando proceda.

9. Fase 6 — Lecciones aprendidas

Reunión post mortem obligatoria dentro de los **15 días hábiles** siguientes a la resolución, con:

a) Reconstrucción cronológica del incidente; b) Identificación de la causa raíz (técnica, procedimental, humana); c) Identificación de los fallos en los controles preventivos y de detección; d) Acciones correctoras con responsables y plazos; e) Actualización de la Evaluación de Riesgos (documento 03) y de esta política, si procede.

10. Notificación a entidades externas

10.1. Autoridad nacional competente en ciberseguridad — incidentes significativos

De acuerdo con el **artículo 23 de la Directiva (UE) 2022/2555** y con la normativa nacional de transposición aplicable, 3HASH cumplirá los siguientes plazos cuando proceda:

Plazo	Acción
Hasta 24 horas	Alerta temprana — comunicación preliminar a la autoridad competente, indicando si el incidente es potencialmente malicioso y si puede tener impacto transfronterizo.
Hasta 72 horas	Notificación completa — actualización de la alerta temprana, con evaluación inicial, indicadores de compromiso y medidas adoptadas.
Hasta 30 días	Informe final — descripción detallada del incidente, causa raíz, gravedad, impactos transfronterizos y medidas implantadas.
A requerimiento	Informe intermedio — en incidentes prolongados, a petición de la autoridad competente.

Canal: portal oficial de la autoridad nacional competente y, en duplicado, por correo electrónico a la dirección institucional indicada por dicha autoridad.

10.2. Autoridad de control en materia de protección de datos — violaciones de datos

De acuerdo con el **artículo 33 del RGPD**, en caso de violación de la seguridad de los datos personales la notificación se dirige a la **autoridad de control competente** dentro de las **72 horas** siguientes a que se haya tenido constancia de ella. Cuando el tratamiento afecte a interesados en España, la autoridad de control de referencia es la **Agencia Española de Protección de Datos (AEPD)**.

Cuando la violación sea susceptible de entrañar un **alto riesgo** para los derechos y libertades de las personas físicas afectadas, se les comunica directamente en los términos del **artículo 34 del RGPD**.

Canal: plataforma electrónica de la autoridad de control competente.

10.3. Cliente

Si el incidente afecta a datos o sistemas tratados por cuenta de un cliente, 3HASH notifica a dicho cliente, en su condición de encargado del tratamiento, en un plazo máximo de **24 horas** desde que tenga constancia del mismo, conforme a lo exigido por el **artículo 33, apartado 2, del RGPD**.

10.4. Autoridades policiales

En caso de sospecha de delito informático, se presenta denuncia ante las autoridades policiales competentes en materia de cibercrimen, con arreglo a la legislación penal aplicable en la jurisdicción correspondiente.

11. Contactos críticos

Entidad	Contacto	Cuándo contactar
Órgano de administración de 3HASH	(registro controlado interno)	Siempre, en primer lugar; coordina toda la respuesta.
Auditoría externa de ciberseguridad	(registro controlado interno)	Para incidentes P1, apoyo al análisis técnico.
CSIRT de referencia de la entidad (CERT.PT)	cert@cert.pt · +351 210 497 399	Incidentes significativos; alerta temprana hasta 24 h.
Autoridad de control de protección de datos	AEPD (España) — www.aepd.es · Autoridad de control competente en el resto de casos	Violación de datos personales; hasta 72 h.
Autoridades policiales competentes en cibercrimen	(jurisdicción de la entidad: Polícia Judiciária — UNC3T · cibercrime@pj.pt)	Sospecha de delito informático.
Asesoría jurídica externa	(a contratar puntualmente)	Incidentes con posible responsabilidad civil o penal.

12. Comunicación pública

La comunicación pública sobre incidentes se rige por los siguientes principios:

- **No comunicar prematuramente** — solo tras la contención y la validación de los hechos;
- **Lenguaje factual**, evitando la especulación;
- **Coordinación previa con el cliente** cuando la comunicación afecte a sistemas operados por su cuenta;
- **Prohibición de divulgar detalles técnicos** que puedan facilitar ataques posteriores;
- **Derecho a la información de los interesados** cuando proceda (artículo 34 del RGPD).

13. Revisión

Versión	Fecha	Cambios	Responsable
1.0	2026-05-02	Versión inicial. Creación.	Órgano de administración
1.0-ES	2026-09	Versión en español. Traducción y adaptación de las referencias normativas nacionales a formulación europea y neutra.	Órgano de administración

Evaluación de Riesgos de Ciberseguridad

Versión: 1.0 **Entidad:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Fecha de la evaluación:** 2 de mayo de 2026 **Próxima revisión:** mayo de 2027 (revisión anual obligatoria); o tras un incidente significativo **Responsable de la evaluación:** Responsable de Ciberseguridad (véase el documento 04)

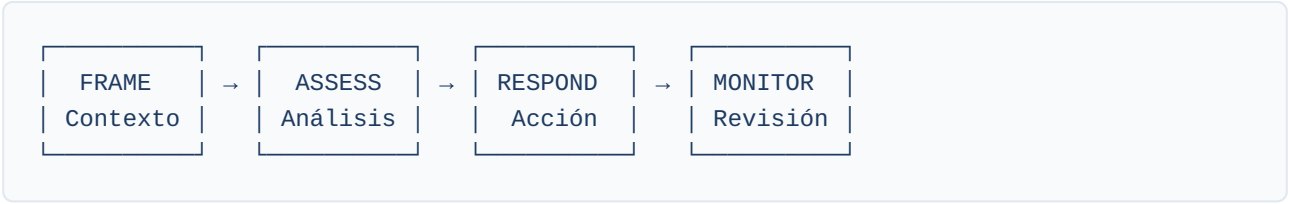
1. Objeto

La presente Evaluación de Riesgos identifica, analiza y clasifica los principales riesgos de ciberseguridad a los que 3HASH está expuesta, en cumplimiento de lo dispuesto en el **artículo 21, apartado 2, letra a), de la Directiva (UE) 2022/2555** y en la normativa nacional de transposición aplicable.

La metodología adoptada sigue la estructura del **NIST AI Risk Management Framework** (Frame · Assess · Respond · Monitor) — adquirida en la formación Cisco Introduction to Cybersecurity (módulo Threat Analysis) — y las orientaciones de la **ISO/IEC 27005:2022**.

2. Metodología

2.1. Etapas



2.2. Escala de probabilidad

Nivel	Descripción	Frecuencia indicativa
1 — Muy baja	Improbable que ocurra	< una vez cada 5 años
2 — Baja	Puede ocurrir ocasionalmente	una vez cada 2-5 años
3 — Media	Ocurrencia esperable	una vez al año
4 — Alta	Ocurrencia frecuente	varias veces al año
5 — Muy alta	Ocurrencia constante	intento diario

2.3. Escala de impacto

Nivel	Operativo	Legal/Regulatorio	Financiero	Reputacional
1 — Muy bajo	Sin impacto	Sin impacto	< 100 €	Sin impacto
2 — Bajo	Degradación menor, < 1 h	Sin infracción	100-1.000 €	Limitado
3 — Medio	Indisponibilidad parcial, < 1 día	Notificación interna	1.000-10.000 €	Cliente afectado
4 — Alto	Indisponibilidad significativa, > 1 día	Notificación obligatoria a las autoridades competentes	10.000-100.000 €	Cobertura mediática negativa
5 — Muy alto	Paralización total	Sanción administrativa	> 100.000 €	Daño reputacional grave

2.4. Cálculo del riesgo

Riesgo = Probabilidad × Impacto (escala 1–25)

Puntuación	Clasificación	Acción
1–4	Bajo	Aceptar; monitorizar.
5–9	Moderado	Tratar con los controles existentes; reevaluar.
10–15	Alto	Reducir con nuevos controles; con plazo definido.
16–25	Crítico	Reducir de inmediato; escalar al órgano de administración.

3. Frame — Contexto y perímetro

3HASH es una microempresa portuguesa de servicios digitales. Sus principales activos sujetos a riesgo cibernético son:

Categoría	Descripción genérica
Infraestructura propia	Sistemas de cómputo y de almacenamiento ubicados en Portugal, bajo control directo de la entidad.
Plataforma de correo electrónico corporativo	Servicios de correo para la entidad y para los clientes alojados.
Plataforma de DNS y dominios	Gestión de dominios propios y de clientes.
Bases de datos de aplicaciones	Aplicaciones propias con persistencia (sistema de gestión de arrendamientos, sistema de afiliados, sistema de prospección comercial, etc.).
Modelo propietario 3HASH Local AI	Sistemas de inteligencia artificial ejecutados en infraestructura propia, sin dependencia de la nube externa.
Repositorios de código	Código fuente de aplicaciones propias y de clientes.
Estaciones de trabajo	Equipos del personal.
Credenciales de acceso a sistemas de clientes	Accesos delegados por los clientes para la gestión de marketing, alojamiento y correo.
Datos personales	Datos de clientes, potenciales clientes y usuarios finales (en el marco del encargo de tratamiento conforme al RGPD).

4. Assess — Identificación y clasificación de riesgos

4.1. Riesgos técnicos

#	Amenaza	Activo afectado	Probab.	Impacto	Riesgo	Controles existentes
T1	**Ransomware** sobre servidores/ estaciones	Infraestructura propia, bases de datos	3	5	**15 — Alto**	Copias de seguridad cifradas off-site diarias, segregación por contenedores, MFA en las consolas, restauración probada.
T2	**Compromiso de credenciales administrativas**	Todos	3	5	**15 — Alto**	MFA obligatorio, rotación periódica, gestor de contraseñas profesional, revocación inmediata en las salidas.
T3	**Phishing dirigido** al equipo	Credenciales, estaciones	4	4	**16 — Crítico**	Formación Cisco y del Centro Nacional de Cibersegurança, MFA, alertas de correo, política de verificación del remitente.
T4	**DDoS** sobre los servicios expuestos	Sitios de clientes, plataformas propias	4	3	**12 — Alto**	Protección perimetral frente a denegación de servicio proporcionada por el CDN, rate limiting.
T5	**Explotación de vulnerabilidad de aplicación** (OWASP Top 10)	Aplicaciones propias	3	4	**12 — Alto**	Validación de entradas, cabeceras de seguridad, auditoría de dependencias, revisión de

#	Amenaza	Activo afectado	Probab.	Impacto	Riesgo	Controles existentes
						código antes de producción.
T6	**Compromiso de la cadena de suministro** (dependencia comprometida)	Aplicaciones propias	2	4	**8 — Moderado**	Fijación de versiones, auditoría periódica, debida diligencia (documento 06).
T7	**Acceso físico no autorizado** a la infraestructura	Infraestructura propia	1	5	**5 — Moderado**	Acceso físico restringido, sin compartición de llaves.
T8	**Fuga de datos** por configuración incorrecta (almacenamiento de objetos o base de datos expuestos)	Bases de datos	2	5	**10 — Alto**	Principio de mínimo privilegio, revisión de configuraciones, auditoría periódica.
T9	**Pérdida o robo de equipos del personal**	Estaciones	3	3	**9 — Moderado**	Cifrado de disco en todas las estaciones, bloqueo automático, MDM en desarrollo.
T10	**Compromiso del modelo de IA** (inyección de instrucciones, robo de modelo)	3HASH Local AI	2	3	**6 — Moderado**	Modelo ejecutado en infraestructura propia, sin exposición directa, alineación con OWASP Top 10 for LLM Applications.

4.2. Riesgos organizativos y de proceso

#	Amenaza	Probab.	Impacto	Riesgo	Controles existentes
O1	**Indisponibilidad prolongada** del Responsable de Ciberseguridad	2	4	**8 — Moderado**	Documentación centralizada, compartición de procedimientos, plan de sucesión.
O2	**Error humano** en una operación crítica	4	3	**12 — Alto**	Procedimientos documentados, regla de doble validación (4-eyes) en cambios críticos, entornos de prueba.
O3	**Ausencia de formación actualizada**	2	3	**6 — Moderado**	Calendario de formación en el documento 05, mínimo de 4 cursos certificados por empleado.
O4	**Incumplimiento contractual de un proveedor** crítico	2	4	**8 — Moderado**	Debida diligencia previa, contratos con cláusulas de nivel de servicio y de seguridad (documento 06).

4.3. Riesgos legales y regulatorios

#	Amenaza	Probab.	Impacto	Riesgo	Controles existentes
L1	**Violación de datos personales** con deber de notificación a la autoridad de control	2	4	**8 — Moderado**	Política de protección de datos, plan de respuesta a incidentes (documento 02), evaluación de impacto cuando proceda.
L2	**Incumplimiento de la NIS2** con sanción	2	4	**8 — Moderado**	Adopción voluntaria del régimen, dosier de cumplimiento actualizado.
L3	**No conformidad con el Reglamento Europeo de Inteligencia Artificial** en un proyecto de cliente	2	3	**6 — Moderado**	Adhesión al EU AI Pact, alineación con el NIST AI RMF, evaluación de impacto cuando proceda.
L4	**Reclamación o procedimiento judicial** por parte de un cliente	2	3	**6 — Moderado**	Contratos formales, niveles de servicio definidos, comunicación documentada.

5. Respond — Tratamiento de los riesgos

5.1. Estrategias de tratamiento

Para cada riesgo identificado, 3HASH adopta una de las siguientes estrategias:

- **Aceptar** — riesgo bajo, con un coste de mitigación superior al impacto.
- **Reducir** — implantar controles adicionales.
- **Transferir** — seguro de ciberseguridad o contratación externa.
- **Evitar** — no realizar la actividad que genera el riesgo.

5.2. Plan de acción para los riesgos críticos y altos

Riesgo	Estrategia	Acción	Responsable	Plazo
T3 — Phishing dirigido	Reducir	Simulación anual de phishing al equipo; refuerzo de la formación de los empleados que no la superen.	Responsable de Ciberseguridad	4.º trimestre de 2026
T1 — Ransomware	Reducir	Verificación trimestral de la restauración de copias de seguridad; implantación de una regla de inmutabilidad.	Responsable de Ciberseguridad	Continuo
T2 — Credenciales comprometidas	Reducir	Extender el MFA a los sistemas restantes; auditoría semestral de privilegios.	Responsable de Ciberseguridad	3.er trimestre de 2026
T4 — DDoS	Transferir/ Reducir	Mantener activa la protección perimetral; evaluar un servicio premium para los clientes de mayor tamaño.	Responsable de Ciberseguridad	4.º trimestre de 2026
T5 — OWASP Top 10	Reducir	Auditoría anual de seguridad de las aplicaciones críticas; bug bounty informal.	Equipo técnico	1.er trimestre de 2027
T8 — Configuración incorrecta	Reducir	Lista de verificación obligatoria previa al despliegue; auditoría trimestral.	Equipo técnico	4.º trimestre de 2026
O2 — Error humano	Reducir	Formalizar la regla de doble validación (4-eyes) en todos los cambios críticos.	Responsable de Ciberseguridad	4.º trimestre de 2026

5.3. Riesgo residual

Tras la implantación de los controles previstos, el riesgo residual se mantiene en niveles **moderado a bajo** para todos los escenarios identificados.

6. Monitor — Revisión y actualización

La presente evaluación es objeto de **revisión anual obligatoria**. Se realizan revisiones extraordinarias siempre que:

a) Se produzca un incidente significativo; b) Se introduzca un cambio estructural en la infraestructura o en la actividad de la entidad; c) Se identifiquen nuevas categorías de amenazas relevantes; d) Se produzca una modificación legal aplicable.

Indicadores monitorizados (KPI):

- Número de incidentes por trimestre, por categoría;
- Tiempo medio de detección (MTTD) y de respuesta (MTTR);
- Porcentaje de empleados con la formación al día;
- Número de intentos de intrusión bloqueados en el perímetro;
- Estado de las copias de seguridad (éxito/fallo) y de la prueba de restauración.

7. Anexos

- **Anexo A** — Plan de Respuesta a Incidentes (documento 02)
- **Anexo B** — Inventario de Activos y Proveedores (documento 06)
- **Anexo C** — Registro de Formación (documento 05)

Designación de Responsable de Ciberseguridad y Auditoría Externa

Versión: 1.0 **Entidad:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Domicilio social:** Rua Cardoso Marta 14 Cave, 3080-012 Figueira da Foz, Portugal **Documento:** 04 / Cumplimiento **Fecha de emisión:** 2 de mayo de 2026

1. Marco legal

En cumplimiento de lo dispuesto en el **artículo 20 de la Directiva (UE) 2022/2555** (NIS2), relativo a la gobernanza y a la responsabilidad de los órganos de dirección, y en la normativa nacional de transposición aplicable, FORTUNEWEEK – UNIPESSOAL LDA establece su modelo de gobernanza de la ciberseguridad.

Aunque FORTUNEWEEK – UNIPESSOAL LDA es una microempresa que podría no estar sujeta directamente al perímetro obligatorio del régimen NIS2, la entidad adopta voluntariamente dicho régimen en tanto que:

- Buena práctica de gobernanza interna;
- Garantía de cumplimiento en la cadena de suministro de sus clientes (algunos de los cuales sí están sujetos directamente);
- Diferenciación competitiva en propuestas comerciales y candidaturas a fondos europeos.

2. Modelo de gobernanza adoptado

3HASH adopta un **modelo mixto** de responsabilidad interna en materia de ciberseguridad, complementado por una **auditoría externa independiente**:

2.1. Responsabilidad interna

El **órgano de administración de FORTUNEWEEK – UNIPESSOAL LDA** asume directamente la responsabilidad última por la ciberseguridad de la entidad, en los términos del artículo 20 de la Directiva (UE) 2022/2555, y cuenta con el apoyo del equipo técnico de 3HASH en la implantación operativa de los controles previstos en la Política de Ciberseguridad (documento 01).

2.2. Auditoría externa independiente

La entidad contrata, con carácter puntual e independiente, **servicios de auditoría de ciberseguridad** prestados por un profesional externo con las siguientes cualificaciones académicas y profesionales:

- **Máster en Informática** por la Universidade de Coimbra;
- **MBA — Master of Business Administration**;
- Habilitación para la auditoría de sistemas de información.

La elección de este perfil — combinación de competencia técnica avanzada (Máster en Informática por una de las principales instituciones de enseñanza superior de Portugal) con competencia de gestión (MBA) — fue deliberada, y garantiza que la auditoría abarque tanto la dimensión técnica como la dimensión organizativa de la seguridad.

La identidad nominal del auditor externo consta en un registro controlado, de acceso restringido al órgano de administración, y puede facilitarse a clientes o autoridades previa firma de un acuerdo de confidencialidad o por mandato legal. A todos los efectos externos (referencia en propuestas, comunicación con clientes, candidaturas), la designación utilizada es **«Auditoría externa por profesional con Máster en Informática por la Universidade de Coimbra y MBA»**.

---

3. Atribuciones

3.1. Órgano de administración (responsabilidad interna)

a) Aprobación y revisión anual de la Política de Ciberseguridad (documento 01); b) Aprobación del Plan de Respuesta a Incidentes (documento 02); c) Aprobación de la Evaluación de Riesgos anual (documento 03); d) Decisión sobre la asignación de recursos para la implantación de los controles; e) En caso de incidente significativo que justifique su comunicación a la autoridad nacional competente en materia de ciberseguridad, asegurar dicha comunicación a través de los canales públicos disponibles, observando los plazos del **artículo 23 de la Directiva (UE) 2022/2555** (alerta temprana hasta 24 horas, notificación hasta 72 horas, informe final hasta 30 días). 3HASH **no ha efectuado el registro formal de un Punto de Contacto Permanente** ante la autoridad competente, por encontrarse fuera del ámbito obligatorio del régimen; f) En caso de violación de la seguridad de los datos personales, articular la notificación a la **autoridad de control competente en materia de protección de datos** en el plazo de **72 horas** previsto en el artículo 33 del RGPD.

3.2. Equipo técnico (operativa)

a) Aplicación operativa de los controles definidos en la Política; b) Mantenimiento del Inventario de Activos (documento 06); c) Mantenimiento del Registro de Formación (documento 05); d) Respuesta de primera línea a alertas e incidentes, en los términos del documento 02; e) Comunicación inmediata al órgano de administración de los incidentes que excedan su capacidad de respuesta autónoma.

3.3. Auditoría externa independiente

a) Revisión crítica anual de la Política de Ciberseguridad y del resto de documentos del dosier; b) Evaluación de la implantación efectiva de los controles previstos; c) Identificación de carencias y recomendación de medidas correctoras; d) Apoyo en la respuesta a las solicitudes de debida diligencia presentadas por clientes o autoridades; e) Seguimiento de la evolución del marco normativo aplicable (NIS2, RGPD, Reglamento Europeo de Inteligencia Artificial, normas técnicas).

---

4. No notificación a la autoridad nacional competente

3HASH, por ser una microempresa ajena a los sectores esenciales e importantes definidos en los Anexos I y II de la **Directiva (UE) 2022/2555**, **no está sujeta a las obligaciones de identificación y notificación** previstas en el régimen NIS2.

En consecuencia, el presente modelo de gobernanza **no ha sido comunicado formalmente a la autoridad nacional competente en materia de ciberseguridad**. Se trata de un instrumento interno y voluntario.

3HASH se reserva el derecho de proceder en el futuro al registro formal ante la autoridad competente en caso de que pase a estar legalmente sujeta al régimen o de que así lo exija un cliente o una licitación pública.

---

5. Vigencia y revisión

El presente modelo de gobernanza tiene vigencia indefinida, y se revisa siempre que se produzca:

- Un cambio del auditor externo contratado;
- Un cambio estructural relevante en la entidad;
- Una modificación legal aplicable.

Revisión programada: **anual**, en el mes de mayo.

6. Aprobación

Documento aprobado por el órgano de administración el **2 de mayo de 2026**.

La versión firmada y fechada se conserva en el registro controlado de la entidad.

Anexos

- Texto de la Directiva (UE) 2022/2555 y referencia a la normativa nacional de transposición aplicable
- Documentación curricular del auditor externo (bajo registro controlado)

Registro de Formación en Ciberseguridad

Versión: 1.0 **Entidad:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Fecha de actualización:** 2 de mayo de 2026 **Próxima revisión:** trimestral; revisión completa en mayo de 2027 **Responsabilidad:** Órgano de administración, con apoyo de la auditoría externa (véase el documento 04)

1. Objeto

El presente registro documenta la formación completada por el equipo de 3HASH en materia de ciberseguridad, en cumplimiento de lo dispuesto en el **artículo 21, apartado 2, letra g), de la Directiva (UE) 2022/2555**, que exige la implantación de prácticas básicas de higiene cibernética y de formación en ciberseguridad aplicadas a la totalidad del equipo, incluido el órgano de administración.

2. Currículo de referencia

3HASH adopta el siguiente currículo de formación fundamental en ciberseguridad, recurriendo a recursos solventes emitidos por entidades públicas y por instituciones internacionales reconocidas (Centro Nacional de Cibersegurança de Portugal, Cisco Networking Academy):

2.1. Tronco común (todas las funciones)

Curso	Entidad emisora	Duración	Validez	Verificación
Cidadão Ciberinformado	Centro Nacional de Cibersegurança (CNCS, Portugal) / Lusa / NAU	~3 horas	Sin caducidad	Certificado en PDF emitido por la plataforma NAU
Cidadão Ciberseguro	Centro Nacional de Cibersegurança (CNCS, Portugal) / NAU	~3 horas	Sin caducidad	Certificado en PDF emitido por la plataforma NAU
Consumidor Ciberseguro	Centro Nacional de Cibersegurança (CNCS, Portugal) / NAU	~4 horas	Sin caducidad	Certificado en PDF emitido por la plataforma NAU
Introduction to Cybersecurity	Cisco Networking Academy	~15 horas	Sin caducidad	Insignia digital verificable en Credly

2.2. Funciones de marketing digital (complementario)

Curso	Entidad emisora	Validez	Verificación
Google Ads AI-Powered Performance Ads	Google Skillshop	12 meses (renovación anual)	Credencial pública en Skillshop
Google Analytics Certification	Google Skillshop	12 meses (renovación anual)	Credencial pública en Skillshop

2.3. Hoja de ruta de formación avanzada

3HASH se ha inscrito o tiene en preparación las siguientes formaciones avanzadas, que se completarán en los próximos 18 meses:

Curso	Entidad emisora	Estado
Hacking y Pruebas de Penetración — Nivel E (70 h)	C-Academy del Centro Nacional de Cibersegurança, en colaboración con la Universidade de Coimbra	En lista de espera
Cisco Certified Cybersecurity Specialist	Cisco	Previsto para 2026/27
EU AI Pact — Pillar II	Comisión Europea	En preparación

3. Síntesis de las certificaciones del equipo en mayo de 2026

En mayo de 2026, el equipo de 3HASH cuenta con certificaciones activas y verificables en los dos frentes siguientes:

3.1. Ciberseguridad y competencia digital

#	Certificación	Entidad	Fecha de finalización	Cantidad
F01	Cidadão Ciberinformado	CNCS (Portugal) / Lusa / NAU	02 / 05 / 2026	1
F02	Cidadão Ciberseguro	CNCS (Portugal) / NAU	02 / 05 / 2026	1
F03	Consumidor Ciberseguro	CNCS (Portugal) / NAU	02 / 05 / 2026	1
F04	Cisco Introduction to Cybersecurity (Cisco Networking Academy) — incluye 5 módulos certificados individualmente: Resource Specialist, Network Defense, System Safeguards, Threat Analysis, Cybersecurity Administration	Cisco	02 / 05 / 2026	1

Insignia de Cisco verificable públicamente en: https://www.credly.com/earner/earned/badge/deb0b114-4678-415a-93ab-4f2980ed5a2c

3.2. Marketing digital

#	Certificación	Entidad	Fecha
F05	Google Ads AI-Powered Performance Ads	Google Skillshop	Marzo de 2026 (renovación anual)
F06	Google Analytics Certification	Google Skillshop	Renovada desde 2024

Credenciales verificables en: - https://skillshop.credential.net/4f863186-5368-4c6e-9686-160e643455b7 - https://skillshop.credential.net/a7537b03-ef24-493b-937d-b26f750abf5c

3.3. Auditoría externa

La función de auditoría de ciberseguridad la ejerce un auditor externo independiente, con **Máster en Informática por la Universidade de Coimbra** y **MBA**, tal como se describe en el documento 04. Esta cualificación asegura una competencia técnica avanzada y capacidad de evaluación organizativa.

---

4. Concienciación continua

Además de la formación certificada, 3HASH adopta como práctica habitual:

- El seguimiento de los boletines de ciberseguridad publicados por el Centro Nacional de Cibersegurança de Portugal, ENISA y CSIRT.PT;
- El análisis de incidentes notorios del sector, con aplicación de las lecciones aprendidas a la operativa interna;
- El refuerzo periódico de las buenas prácticas en materia de identificación de intentos de phishing y de gestión de credenciales.

---

5. Revisión y control de versiones

El presente registro lo actualiza **trimestralmente** el responsable designado por el órgano de administración, y siempre que:

- Un empleado complete un nuevo curso;
- Caduque la validez de una certificación (y se programe su renovación);
- Se incorpore o cause baja un empleado del equipo.

Versión	Fecha	Cambios
1.0	2026-05-02	Versión inicial. Incluye el registro de los 4 cursos de ciberseguridad completados el 2 de mayo de 2026 (Cisco Introduction to Cybersecurity + 3 cursos del Centro Nacional de Cibersegurança).
1.0-ES	2026-09	Versión en español. Traducción; se conservan sin cambios los nombres originales de los cursos, las entidades emisoras, las fechas y las credenciales verificables.

Inventario de Activos y Soberanía Tecnológica

Versión: 1.0 **Entidad:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Fecha de actualización:** 2 de mayo de 2026 **Próxima revisión:** trimestral; revisión completa en mayo de 2027 **Responsable:** Responsable de Ciberseguridad (véase el documento 04) **Clasificación:** Uso interno · Compartición con clientes únicamente previa firma de NDA

1. Objeto

El presente documento establece el inventario de las categorías de activos de 3HASH y describe el modelo de **soberanía tecnológica** de la entidad, en cumplimiento de lo dispuesto en:

- El **artículo 21, apartado 2, letra d), de la Directiva (UE) 2022/2555** — seguridad de la cadena de suministro;
- El **artículo 21, apartado 2, letra i)** — seguridad de los recursos humanos, políticas de control de acceso y gestión de activos;
- La **ISO/IEC 27001:2022** — control A.5.9 (inventario de información y otros activos asociados).

> Por razones de seguridad operativa y de protección de la propiedad intelectual, el presente documento describe categorías de activos sin identificar modelos concretos, versiones, direcciones, configuraciones ni identidades comerciales. La información detallada está a disposición del Responsable de Ciberseguridad y del órgano de administración, bajo registro controlado.

2. Modelo de soberanía tecnológica de 3HASH

2.1. Principio fundamental

3HASH opera conforme a un modelo de **integración vertical** y de **soberanía tecnológica nacional**, deliberadamente distinto del modelo dominante en el sector, que se basa en la subcontratación intensiva de plataformas de nube internacionales. En concreto:

> **3HASH no depende de proveedores de nube externos para el procesamiento, el almacenamiento ni la inferencia sobre datos de clientes o de usuarios finales.**

Esta opción es estratégica, no accidental, y se materializa en todas las dimensiones críticas de la operativa:

Función	Modelo dominante en el sector	Modelo 3HASH
Inferencia de IA	API de proveedores de nube (OpenAI, Anthropic, Google)	**Modelo propietario 3HASH Local AI**, ejecutado en infraestructura propia en Portugal
Alojamiento de aplicaciones	AWS, Google Cloud, Azure	**Servidores propios en Portugal**, bajo jurisdicción de la UE
Bases de datos	Bases de datos gestionadas en la nube (RDS, Cloud SQL, Atlas)	**Bases de datos en servidores propios**, sin dependencia de la nube externa
Correo electrónico	Microsoft 365, Google Workspace	**Plataforma de correo autoalojada** en infraestructura propia
Copias de seguridad	Almacenamiento en la nube de un proveedor (S3, GCS)	**Sistema de copias de seguridad propio**, con copia off-site en almacenamiento físico segregado
Repositorios de código	GitHub, GitLab.com	Repositorios privados en infraestructura propia
Monitorización y registros	Datadog, New Relic, CloudWatch	Sistemas de monitorización propios en infraestructura local

2.2. Implicaciones para los clientes

De la soberanía tecnológica se derivan beneficios verificables y comercializables:

a) **Los datos de los clientes no salen del territorio portugués**, salvo necesidad operativa excepcional y mediante acuerdo escrito;

b) **No se produce transferencia de datos personales a terceros países** sin una base legal adecuada en los términos del Capítulo V del RGPD;

c) **El contenido de las instrucciones (prompts) y de las conversaciones con los sistemas de IA no se envía a proveedores de nube externos** — el modelo propietario 3HASH Local AI se ejecuta íntegramente en servidores propios, sin dependencia de OpenAI, Anthropic, Google ni de ningún otro proveedor internacional;

d) **3HASH es simultáneamente responsable del tratamiento y de la infraestructura** que lo soporta, lo que elimina la dispersión de responsabilidad típica del modelo de nube como servicio;

e) **Los clientes pueden auditar físicamente** la infraestructura, previa firma de un acuerdo de confidencialidad.

2.3. Implicaciones para el cumplimiento de la NIS2 y del RGPD

La soberanía tecnológica simplifica y refuerza el cumplimiento de los regímenes aplicables:

- **Cadena de suministro (art. 21, apdo. 2, letra d), de la Directiva NIS2)** — el número de dependencias externas críticas se minimiza desde el diseño;
- **Transferencia internacional de datos (Capítulo V del RGPD)** — no resulta aplicable en la mayoría de los casos, por inexistencia de transferencia;
- **Reglamento (UE) 2024/1689 (Reglamento Europeo de Inteligencia Artificial)** — 3HASH conserva el control íntegro sobre los sistemas de IA que opera, lo que le permite cumplir los requisitos de transparencia, supervisión humana y auditabilidad sin depender de terceros;
- **Soberanía digital europea** — alineación con las prioridades estratégicas de la Unión Europea en materia de autonomía tecnológica.

3. Categorías de activos propios

3.1. Infraestructura de cómputo propia

Categoría	Ubicación	Función	Criticidad
Sistemas de cómputo de producción	Portugal (jurisdicción UE)	Operación de aplicaciones propias y de clientes; modelo propietario 3HASH Local AI	Crítica
Sistemas de almacenamiento segregados	Portugal (jurisdicción UE)	Copias de seguridad cifradas off-site	Alta
Estaciones de trabajo del equipo	Portugal	Desarrollo, gestión, comunicación	Media

3.2. Plataformas de aplicaciones propias

Todas las plataformas que se enumeran operan **íntegramente en infraestructura propia en Portugal**, sin dependencia de la nube externa para el procesamiento o el almacenamiento de datos.

Plataforma	Función	Datos tratados	Criticidad
Sistema de gestión de arrendamientos	Operación completa de una empresa cliente en modo SaaS	Datos personales de inquilinos y propietarios	Crítica
Sistema de afiliados	Gestión de socios comerciales	Datos personales de afiliados	Alta
Sistema de prospección comercial	Identificación y cualificación de oportunidades	Datos profesionales públicos de potenciales clientes	Media
Plataforma de envío de ficheros de gran tamaño	Transferencia segura de ficheros a clientes	Contenido enviado por los clientes	Alta
Sistema de tiques de soporte	Gestión de incidencias de cliente	Datos de contacto e histórico de comunicaciones	Alta
Sistema de inventario de dominios	Monitorización de WHOIS, SSL y facturación	Metadatos de dominios	Media
Modelo propietario **3HASH Local AI**	Inferencia de modelos de lenguaje en infraestructura propia, sin dependencia de proveedores de nube externos	Sin persistencia de instrucciones; véanse las políticas de privacidad de cada proyecto	Crítica

3.3. Bases de datos de aplicaciones

Cada una de las plataformas enumeradas en el apartado 3.2 mantiene su propia base de datos, segregada por aplicación. Todas las bases de datos:

- Se operan en **infraestructura propia** (sin dependencia de un proveedor de nube externo);
- Están cifradas en reposo cuando contienen datos personales o credenciales;
- Están sujetas a copias de seguridad cifradas diarias, retenidas durante un mínimo de 30 días, con copia off-site en almacenamiento físico segregado;
- Solo son accesibles desde la red de la propia plataforma (sin exposición directa a internet).

3.4. Repositorios de código fuente

El código fuente de las aplicaciones propias y de los proyectos de cliente se mantiene en **repositorios privados en infraestructura propia**, con:

- Acceso restringido conforme al principio de mínimo privilegio;
- MFA obligatorio;

- Protección de ramas (branch protection) en las ramas de producción;
- Auditoría periódica de dependencias.

3.5. Credenciales y secretos

Las credenciales de acceso a sistemas propios y de clientes, las claves de API, los tokens y los certificados se gestionan en un **gestor de contraseñas profesional**, con:

- MFA obligatorio para el acceso al propio gestor;
- Segregación por proyecto/cliente;
- Política de revocación inmediata ante la salida de un empleado o la sospecha de compromiso.

4. Dependencias externas residuales

La integración vertical de 3HASH minimiza, pero no elimina por completo, la existencia de dependencias externas. Estas se limitan al siguiente conjunto reducido, correspondiente a **infraestructuras comunes de internet** sin alternativa funcional viable para una microempresa:

Categoría	Tipo de dependencia	Riesgo principal	Plan de mitigación
Conectividad a internet	Operador nacional autorizado por la autoridad reguladora de telecomunicaciones competente	Indisponibilidad de la red	Operador alternativo identificado para su activación rápida.
Resolución DNS internacional y protección perimetral	Plataforma internacional reconocida	Indisponibilidad o redirección maliciosa	Configuración documentada para la migración a una alternativa equivalente en < 24 h.
Registrador de dominios	Entidad acreditada por la ICANN o por el registro del ccTLD correspondiente	Secuestro de dominios	MFA obligatorio, bloqueo de registro (registry lock) activo en los dominios críticos.
Autoridad de certificación TLS pública	Autoridad reconocida por los navegadores	No emisión de certificados	Autoridad alternativa identificada; cadena de emisión automatizada.

> **Importante:** Estas dependencias residuales **no implican el tratamiento de datos de clientes ni de usuarios finales** — se limitan al plano de la conectividad y de la identidad de los servicios públicos de 3HASH. Los datos de las aplicaciones permanecen siempre en infraestructura propia en Portugal.

Cláusulas mínimas exigidas a estas dependencias

a) Conformidad con el RGPD (operador establecido en la UE o con mecanismos válidos de transferencia); b) Notificación a 3HASH en un plazo máximo de **24 horas** desde la detección de un incidente; c) Posibilidad de migración asistida en caso de resolución del contrato; d) Historial operativo sin incidentes graves en los últimos 24 meses.

5. Comparación con el modelo dominante del sector

A título ilustrativo, la tabla siguiente compara el número y la naturaleza de las dependencias críticas del modelo de 3HASH con las de una agencia digital típica basada en una arquitectura de nube.

Indicador	Agencia típica basada en nube	3HASH (modelo soberano)
Proveedores de nube con acceso a datos de cliente	De 5 a 15 (alojamiento, base de datos, IA, correo, almacenamiento, CDN, monitorización, etc.)	**0**
Países en los que pueden procesarse los datos de cliente	EE. UU. + UE + otros (variable)	**Portugal (UE)**
Cumplimiento sin cláusulas de transferencia internacional	Difícil	**Desde el diseño**
Tiempo medio de migración entre proveedores de nube	De semanas a meses	No aplicable
Capacidad de auditoría física por parte del cliente	Limitada o nula	**Posible previa firma de NDA**
Capacidad de operar en modo aislado (air-gapped, sin conexión)	No	**Sí, para un subconjunto crítico**

6. Revisión

Versión	Fecha	Cambios
1.0	2026-05-02	Versión inicial. Inventario de activos propios y encuadre de la soberanía tecnológica de 3HASH.
1.0-ES	2026-09	Versión en español. Traducción y adaptación de las referencias normativas nacionales a formulación europea y neutra.

Revisión **trimestral** por el Responsable de Ciberseguridad. Revisión completa anual junto con la Evaluación de Riesgos (documento 03).