3HASH®

DOSSIER DE CIBERSEGURANÇA E CONFORMIDADE

Conformidade NIS2, RGPD e EU AI Act

Documentação institucional de governação, cibersegurança, gestão de risco e conformidade regulatória, em alinhamento com o Decreto-Lei n.º 125/2025 (transposição NIS2), Regulamento (UE) 2016/679 (RGPD), Regulamento (UE) 2024/1689 (EU AI Act) e os quadros voluntários NIST CSF, ISO/IEC 27001 e EU AI Pact.

ENTIDADE

FORTUNEWEEK – UNIPESSOAL LDA
NIPC 515 084 182

MARCA COMERCIAL

3HASH®
Marca Nacional INPI nº 711 356

SEDE

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

VERSÃO E DATA

v1.0 · 2 de Maio de 2026
Próxima revisão: Maio de 2027

Dossier de Cibersegurança e Conformidade — 3HASH

Entidade: FORTUNEWEEK – UNIPESSOAL LDA **Marca comercial:** 3HASH® (Marca Nacional INPI nº 711356) **NIPC:** 515 084 182 **Sede:** Rua Cardoso Marta 14 Cave, 3080-012 Figueira da Foz, Portugal

Objectivo

O presente dossier reúne, num único conjunto institucional, a documentação interna de **cibersegurança, governação e conformidade regulatória** da 3HASH, em alinhamento com:

- O regime jurídico nacional de cibersegurança transposto pelo **Decreto-Lei n.º 125/2025**, de 4 de Dezembro (NIS2), em vigor desde 3 de Abril de 2026;
- O **Regulamento (UE) 2022/2555** (Diretiva NIS2);
- O **Regulamento (UE) 2016/679** (RGPD) e a **Lei n.º 58/2019** de execução em Portugal;
- O **Regulamento (UE) 2024/1689** (EU AI Act) e o compromisso voluntário **EU AI Pact** subscrito pela 3HASH em Abril de 2026;
- Os quadros de referência técnicos adoptados voluntariamente: **NIST Cybersecurity Framework 2.0**, **NIST SP 800-61** (Resposta a Incidentes), **ISO/IEC 27001/27005** e **OWASP**.

Aplicabilidade da NIS2 à 3HASH

A FORTUNEWEEK – UNIPESSOAL LDA é uma **microempresa** (≤10 colaboradores, facturação anual <€2M) que **poderá não estar abrangida directamente** pelo perímetro obrigatório do regime jurídico nacional NIS2 — o qual incide tipicamente sobre médias e grandes entidades em sectores essenciais ou importantes definidos no Anexo do Decreto-Lei n.º 125/2025.

Não obstante, a 3HASH adopta voluntariamente os princípios e controlos do regime, pelas seguintes razões:

1. **Governação interna** — alinhamento com boas práticas internacionais de cibersegurança, independentemente de obrigação legal directa;
2. **Conformidade na cadeia de fornecimento** — vários clientes da 3HASH estão directamente abrangidos pelo perímetro NIS2 (sectores de educação, saúde, transportes e administração pública), sendo legalmente obrigados a fazer due diligence sobre os seus fornecedores tecnológicos;
3. **Diferenciação competitiva** — em concursos públicos, propostas comerciais e candidaturas a fundos europeus (Portugal 2030, PRR, Horizonte Europa);

4. **Responsabilidade civil e reputacional** — mitigação de risco de incidentes que possam afectar clientes ou terceiros.

Índice de documentos

#	Documento	Estado	Versão
01	Política de Cibersegurança 3HASH	Em vigor	1.0
02	Plano de Resposta a Incidentes	Em vigor	1.0
03	Avaliação de Risco	Em vigor	1.0
04	Designação de Responsável de Cibersegurança e Auditoria Externa	Em vigor	1.0
05	Registo de Formação em Cibersegurança	Em vigor	1.0
06	Inventário de Activos e Soberania Tecnológica	Em vigor	1.0

Quadros de referência aplicados

Quadro europeu

Referência	Aplicação
Regulamento (UE) 2022/2555 (Diretiva NIS2)	Art. 7.º (estratégia nacional), Art. 21.º (medidas de gestão de risco), Art. 23.º (notificação de incidentes), Art. 24.º (uso voluntário de esquemas de cibersegurança certificada)
Regulamento (UE) 2016/679 (RGPD)	Art. 5.º (princípios), Art. 25.º (privacidade por concepção), Art. 32.º (segurança), Art. 33.º-34.º (notificação de violações), Art. 35.º (DPIA)
Regulamento (UE) 2024/1689 (EU AI Act)	Art. 5.º (práticas proibidas), Art. 50.º (transparência)
Regulamento (UE) 2019/881 (Cybersecurity Act)	Esquemas europeus de certificação de cibersegurança

Quadro nacional português

Referência	Aplicação
Decreto-Lei n.º 125/2025, de 4 de Dezembro	Transposição da Diretiva NIS2 para a ordem jurídica nacional. Aplicável desde 3 de Abril de 2026. Art. 17.º (responsável de cibersegurança), Art. 21.º (medidas técnicas e organizativas), Art. 27.º (notificação de incidentes ao CNCS)
Lei n.º 46/2018, de 13 de Agosto	Regime jurídico da segurança do ciberespaço (versão anterior, complementar)
Lei n.º 58/2019, de 8 de Agosto	Lei nacional de execução do RGPD
Decreto-Lei n.º 65/2021, de 30 de Julho	Regulamenta a Lei 46/2018 (medidas de segurança e notificação de incidentes)

Quadro técnico voluntário (auto-adopção)

Referência	Aplicação
NIST Cybersecurity Framework 2.0 (2024)	Identificar · Proteger · Detectar · Responder · Recuperar
NIST SP 800-61 r2 (Computer Security Incident Handling)	Estrutura do Plano de Resposta a Incidentes
ISO/IEC 27001:2022	Sistema de Gestão de Segurança da Informação
ISO/IEC 27005:2022	Gestão de risco de segurança da informação
OWASP Top 10 (2021) + OWASP ASVS v4.0.3	Segurança aplicacional
OWASP Top 10 for LLM Applications (2025)	Segurança em sistemas baseados em modelos de linguagem
EU AI Pact — Pillar I	Compromisso voluntário da 3HASH (Abril 2026) com a Comissão Europeia
Cisco Ethical Decision Framework (Networking Academy 2026)	Anexo à Política de Cibersegurança (documento 01)
QNRCS — Quadro Nacional de Referência para a Cibersegurança (Nível Básico)	Alinhamento voluntário declarativo com os princípios do quadro publicado pelo CNCS. Não envolve, neste momento, certificação formal por entidade acreditada.

Modelo de governação

Função	Quem assume
Responsabilidade última	Gerência
Implementação operacional	Equipa técnica 3HASH
Auditoria de cibersegurança	Auditoria externa independente — elemento com Mestrado em Informática pela Universidade de Coimbra e MBA
Comunicação com o CNCS em caso de incidente significativo	Gerência (a 3HASH não tem registo formal de PCP por estar fora do âmbito obrigatório do regime)

Detalhe completo no documento 04.

Notas de versão e revisão

Versão	Data	Alterações
1.0	2026-05-02	Versão inicial. Criação do dossier integral.

Revisão calendarizada: **Anual**, no mês de Maio, ou sempre que ocorra alteração legal relevante ou incidente significativo.

Política de circulação

Este dossier é classificado como **Uso Interno**. As versões redigidas em conformidade com este índice **podem ser partilhadas com clientes e parceiros mediante acordo de não-divulgação (NDA)** previamente assinado, no âmbito de processos de due diligence ou auditoria de fornecedor. Não é destinado a publicação aberta.

Pedidos de cópia devem ser dirigidos a: **geral@3hash.pt** (assunto: «Pedido de documentação de conformidade — [Nome do solicitante]»).

Política de Cibersegurança 3HASH

Versão: 1.0 **Entidade:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Data de aprovação:** 2 de Maio de 2026 **Próxima revisão:** Maio de 2027 (revisão anual obrigatória) **Responsável:** Responsável de Cibersegurança (ver documento 04)

1. Objecto e âmbito

A presente Política de Cibersegurança estabelece os princípios, regras e responsabilidades aplicáveis à protecção dos sistemas de informação, dados e infraestruturas operados pela FORTUNEWEEK – UNIPESSOAL LDA, no exercício da sua actividade enquanto agência digital sob a marca 3HASH®.

Aplica-se a:

a) Todos os colaboradores, prestadores de serviços e subcontratados da entidade; b) Todos os sistemas, dispositivos, aplicações, servidores e serviços operados directa ou indirectamente pela 3HASH; c) Todo o tratamento de dados pessoais efectuado no âmbito de projectos próprios ou prestados a clientes; d) Todas as parcerias com terceiros que envolvam acesso a dados, sistemas ou redes da entidade.

2. Quadro de referência

Esta política dá cumprimento ao disposto no:

- **Artigo 21.º do Decreto-Lei n.º 125/2025**, de 4 de Dezembro (transposição NIS2), no que se refere às medidas técnicas, operacionais e organizativas adequadas e proporcionais para gerir o risco para a segurança das redes e sistemas de informação;
- **Artigo 32.º do Regulamento (UE) 2016/679** (RGPD), no que se refere à segurança do tratamento de dados pessoais;
- **NIST Cybersecurity Framework 2.0** (5 funções centrais: Identificar, Proteger, Detectar, Responder, Recuperar);
- **EU AI Pact — Pillar I**, no que se refere à governação responsável de sistemas de inteligência artificial.

2.1. Postura proactiva e adesão voluntária

A 3HASH é uma microempresa que poderá não estar abrangida directamente pelo perímetro obrigatório do regime jurídico nacional NIS2. A adopção dos controlos descritos nesta política é, portanto, **voluntária e proactiva**, traduzindo um compromisso institucional com:

- Boas práticas internacionais de cibersegurança;
- Protecção dos dados de clientes e de utilizadores finais sob nossa responsabilidade;
- Diferenciação competitiva em propostas comerciais e candidaturas a fundos europeus;
- Antecipação a obrigações legais futuras.

No mesmo espírito, a 3HASH **alinha voluntariamente a sua postura de cibersegurança com os princípios do Quadro Nacional de Referência para a Cibersegurança (QNRCS) — Nível Básico**, publicado pelo Centro Nacional de Cibersegurança. Este alinhamento é declarativo e não envolve, neste momento, processo formal de certificação por entidade acreditada. A 3HASH reserva-se o direito de evoluir para certificação formal QNRCS quando tal se justifique pela maturidade dos controlos ou por exigência de cliente ou concurso.

---

3. Princípios fundamentais

A 3HASH adopta os seguintes princípios estruturantes em matéria de cibersegurança:

3.1. Tríade CIA — Confidencialidade, Integridade e Disponibilidade

Todos os sistemas e processos da entidade são concebidos e operados de modo a assegurar:

- **Confidencialidade** — os dados são acessíveis apenas a quem deles necessite (princípio do need-to-know);
- **Integridade** — os dados são protegidos contra alteração não autorizada;
- **Disponibilidade** — os serviços críticos mantêm-se acessíveis dentro dos parâmetros de SLA assumidos.

3.2. Segurança por concepção e por defeito (security by design / by default)

Todos os sistemas novos são concebidos com cibersegurança e privacidade como requisito desde a fase de desenho, e configurados com a opção mais restritiva por defeito.

3.3. Defesa em profundidade (defense in depth)

A protecção dos sistemas assenta em **múltiplas camadas independentes** de controlos — perímetro, rede, host, aplicação, dados, identidade — de modo a que a falha de uma camada não comprometa as restantes.

3.4. Princípio do menor privilégio

Cada utilizador, processo ou serviço opera com **o conjunto mínimo de permissões** necessário ao seu propósito. Acessos administrativos são restritos, registados e periodicamente revistos.

3.5. Verificabilidade e auditabilidade

Os controlos implementados são **verificáveis**, **registados em log** e disponíveis para auditoria interna ou externa por entidades competentes (CNCS, CNPD, auditores contratados por clientes).

3.6. Adopção antecipada de regulação europeia

A 3HASH adopta voluntariamente os princípios do AI Act (via EU AI Pact) e da Diretiva NIS2 antes da sua aplicabilidade obrigatória directa, enquanto entidade signatária do **EU AI Pact** (Pillar I, Abril de 2026).

---

4. Responsabilidades

4.1. Gerência

Responsável último pela aprovação da presente política, pela alocação de recursos necessários à sua implementação e pelo cumprimento das obrigações legais decorrentes da NIS2 e do RGPD. Nos termos do **artigo 21.º, n.º 6 do DL 125/2025**, a gerência é pessoalmente responsável pelo cumprimento do regime, podendo incorrer em sanção própria em caso de incumprimento doloso ou por negligência grosseira.

4.2. Responsável designado de Cibersegurança

Conforme o documento 04, a responsabilidade pela cibersegurança é assumida directamente pela **Gerência**, apoiada operacionalmente pela equipa técnica e por **auditoria externa independente** prestada por elemento com Mestrado em Informática pela Universidade de Coimbra e MBA. A 3HASH, por se encontrar fora do âmbito obrigatório do regime jurídico nacional NIS2, **não procedeu ao registo formal de Ponto de Contacto Permanente** junto do CNCS. Em caso de incidente significativo que justifique comunicação ao CNCS, esta é assegurada pela Gerência através dos canais públicos disponíveis.

4.3. Colaboradores e prestadores de serviços

Cumprem as regras desta política e participam na formação contínua. Reportam incidentes ou suspeitas no prazo máximo de **4 horas úteis** após detecção, ao Responsável de Cibersegurança.

4.4. Fornecedores e subcontratados

Aceitam contratualmente cláusulas mínimas de cibersegurança e protecção de dados, sujeitas ao processo de due diligence descrito no documento 06.

---

5. Domínios de controlo (alinhamento com NIS2 Art. 21.º, n.º 2)

5.1. Identificar

- Inventário actualizado de **activos** críticos, serviços e dados (documento 06);
- **Avaliação de risco** anual, com revisão extraordinária após incidentes significativos (documento 03);
- Mapeamento de **dependências externas** (cloud, DNS, fornecedores SaaS, certificados).

5.2. Proteger

5.2.1. Controlo de acessos

- Autenticação **multifactor (MFA)** obrigatória em todos os sistemas críticos: administração de servidores, painéis de gestão, repositórios de código, contas de correio electrónico administrativas e gestão de domínios e DNS;
- Palavras-passe com mínimo de **12 caracteres**, mistura de tipos, geridas em **gestor de palavras-passe profissional** — sem reutilização entre sistemas;
- **Princípio do menor privilégio** aplicado em sistemas operativos, bases de dados e aplicações;
- **Revogação imediata** de acessos quando colaborador ou prestador cessa funções.

5.2.2. Cifragem

- Cifragem **em trânsito** obrigatória (TLS 1.2+ / TLS 1.3) para todos os serviços expostos à internet;
- Cifragem **em repouso** para volumes que contenham dados pessoais ou credenciais, em servidores e estações de trabalho;
- Chaves criptográficas geridas separadamente dos dados que protegem.

5.2.3. Endpoints e estações de trabalho

- Sistema operativo **actualizado mensalmente** (no máximo 30 dias após disponibilização de patch crítico);
- **Antivírus e firewall** activos e configurados;
- Cifragem de disco activa em todas as estações de trabalho, conforme recomendado pela formação Cisco Introduction to Cybersecurity (módulo System Safeguards);
- Bloqueio automático de ecrã após 5 minutos de inactividade;

- Sem instalação de software de fonte não confiável (validação prévia obrigatória).

5.2.4. Servidores e infraestrutura

- Sistemas de produção em **infraestrutura própria localizada em Portugal**, sob jurisdição da União Europeia;
- **Perímetro de rede protegido** por firewall com regras explícitas de allow-list e logging;
- Mecanismos de **mitigação de força bruta** activos em serviços de administração e autenticação;
- **Acesso administrativo apenas por chave criptográfica** (sem autenticação por palavra-passe simples), com chaves protegidas por passphrase;
- **Patches de segurança** aplicados no prazo máximo de 7 dias para vulnerabilidades classificadas como critical, 30 dias para high;
- **Segregação aplicacional** por containers, com volumes persistentes isolados e limites de recursos.

5.2.5. Backups e continuidade

- **Backups encriptados diários** dos dados críticos, com retenção mínima de 30 dias;
- **Backups off-site** em sistema de armazenamento segregado, fisicamente independente, para mitigação de risco de ransomware;
- **Teste anual de restauro**, com registo do resultado e validação da integridade.

5.2.6. Segurança aplicacional

- Validação rigorosa de **input** em todas as APIs e formulários (mitigação de OWASP Top 10);
- **Cabeçalhos de segurança** HTTP configurados (CSP, X-Frame-Options, Strict-Transport-Security, Permissions-Policy, Referrer-Policy);
- **Dependências auditadas** periodicamente, sem vulnerabilidades conhecidas críticas em produção;
- **Revisão de código** obrigatória antes de promoção para produção em sistemas críticos;
- **Rate limiting** em endpoints públicos.

5.3. Detectar

Conforme recomendado pelo módulo Network Defense da formação Cisco Introduction to Cybersecurity e pelo NIST Cybersecurity Framework (função **Detect**):

- **Centralização de logs** de servidores, perímetro de rede e aplicações, com retenção mínima de 90 dias;
- **Monitorização contínua e automatizada** da integridade dos sistemas e dos sites alojados, com **alertas em tempo real** para o Responsável de Cibersegurança;

- **Verificação periódica de presença de malware** em servidores partilhados, com mecanismos de quarentena automática;
- **Monitorização de reputação** dos endereços e domínios da entidade (listas negras, abuse reports, threat intelligence feeds).

5.4. Responder

- Procedimento detalhado no documento 02 — **Plano de Resposta a Incidentes**;
- Notificação ao **CNCS** dentro dos prazos legais (early warning até 24 horas; notificação até 72 horas; relatório final até 30 dias) para incidentes de segurança nos termos do **artigo 27.º do DL 125/2025**;
- Notificação à **CNPD** dentro de 72 horas em caso de violação de dados pessoais nos termos do **artigo 33.º do RGPD**;
- Comunicação à pessoa singular afectada quando a violação seja susceptível de implicar elevado risco para os seus direitos e liberdades (**artigo 34.º do RGPD**).

5.5. Recuperar

- Restauro a partir do backup mais recente verificado;
- Análise post-mortem documentada, com identificação de causa-raiz e medidas de prevenção;
- Actualização do registo de incidentes e revisão da Avaliação de Risco.

---

6. Quadro de Decisão Ética 3HASH

Em qualquer dilema ético — incluindo decisões com impacto em segurança, privacidade ou utilização de IA — qualquer colaborador ou prestador de serviços deve aplicar o seguinte quadro, **adaptado do Cisco Ethical Decision Framework** (Cisco Networking Academy 2026):

```
Em qualquer dilema ético, pergunte-se:

1. É legal?
   ├─ Não  → STOP (pode ter consequências legais graves)
   ├─ Sim  → Avançar para 2
   └─ Não sei → AGUARDAR (consultar Officer / jurista)

2. Cumpre a Política e os princípios éticos da 3HASH?
   ├─ Não  → STOP
   ├─ Sim  → Avançar para 3
   └─ Não sei → AGUARDAR

3. Tenho a certeza que não causa dano à 3HASH, aos clientes
   ou a terceiros?
   ├─ Não  → STOP
   ├─ Sim  → Avançar para 4
   └─ Não sei → AGUARDAR

4. Seria aceitável se toda a equipa da 3HASH agisse assim?
   ├─ Não  → STOP
   ├─ Sim  → Avançar para 5
   └─ Não sei → AGUARDAR

5. Sentir-me-ia confortável a ler sobre isto na primeira
   página de um jornal nacional?
   ├─ Não  → STOP
   ├─ Sim  → A decisão está alinhada com esta política
   └─ Não sei → AGUARDAR
```

«AGUARDAR» implica suspender a acção e consultar o Responsável de Cibersegurança, a Gerência ou apoio jurídico externo antes de prosseguir.

«STOP» implica não prosseguir com a acção. Se o dilema persistir, escalar para a gerência.

---

7. Formação e sensibilização

7.1. Obrigação geral

Nos termos do **artigo 21.º, n.º 2, alínea g) do DL 125/2025**, todos os colaboradores e a gerência devem participar em formação periódica em cibersegurança, dimensionada à sua função.

7.2. Currículo mínimo

Cada colaborador deve completar, no prazo de **6 meses após início de funções**, e renovar de acordo com o calendário definido no 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 funções de maior responsabilidade técnica, formação avançada complementar (C-Academy CNCS, Cisco Specialist, equivalente).

7.3. Registo

O registo nominal de formação concluída é mantido pelo Responsável de Cibersegurança no documento 05.

---

8. Inteligência artificial — princípios complementares

A 3HASH é **signatária do EU AI Pact** (Pillar I, Abril de 2026). Em todos os sistemas que utilizem ou desenvolvam componentes de inteligência artificial, aplicam-se cumulativamente:

- **Transparência** — utilizadores são informados de que interagem com sistema baseado em IA (artigo 50.º do EU AI Act);
- **Modelos próprios em infraestrutura nacional** — para projectos sensíveis (saúde, educação, menores), é privilegiada a utilização de modelos executados em servidores próprios em Portugal, sem dependência de API externa (3HASH Local AI);
- **Não tratamento de dados pessoais sensíveis em prompts a fornecedores cloud externos** sem base legal e contratual adequada;
- **Governação documentada** — sistemas de IA críticos são acompanhados de documento de arquitectura técnica, alinhamento com NIST AI RMF e (quando aplicável) DPIA preliminar;
- **Sem práticas proibidas** — não desenvolvemos nem operamos sistemas que se enquadrem nas práticas proibidas do **artigo 5.º do EU AI Act** (manipulação subliminar, exploração de vulnerabilidades, classificação social, etc.).

---

9. Revisão e versionamento

A presente política é objecto de **revisão anual obrigatória** pelo Responsável de Cibersegurança, com aprovação pela gerência. Revisões extraordinárias ocorrem sempre que:

- Surja alteração legal aplicável (NIS2, RGPD, AI Act, regulamentação CNCS);
- Ocorra incidente de cibersegurança classificado como significativo;
- Sejam introduzidas alterações estruturais nos sistemas ou na infraestrutura;

- O EU AI Pact, NIST CSF ou outros frameworks adoptados sejam objecto de actualização material.

Versão	Data	Alterações	Responsável
1.0	2026-05-02	Versão inicial. Criação.	Gerência

10. Aprovação

Documento aprovado pela Gerência em **2 de Maio de 2026**.

A versão assinada e datada é mantida em registo controlado da entidade.

Anexos

- Cisco Ethical Decision Framework (PDF original)
- Documento 04 — Modelo de Governação e Auditoria Externa
- Documento 05 — Registo de Formação
- Comprovativo de adesão ao EU AI Pact

Plano de Resposta a Incidentes de Cibersegurança

Versão: 1.0 **Entidade:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Data de aprovação:** 2 de Maio de 2026 **Próxima revisão:** Maio de 2027 (revisão anual obrigatória) **Responsável:** Responsável de Cibersegurança (ver documento 04)

1. Objecto

O presente plano estabelece o procedimento formal de resposta a incidentes de cibersegurança que afectem ou possam afectar os sistemas, dados ou serviços operados pela 3HASH, incluindo aqueles operados em nome de clientes.

A sua estrutura está alinhada com:

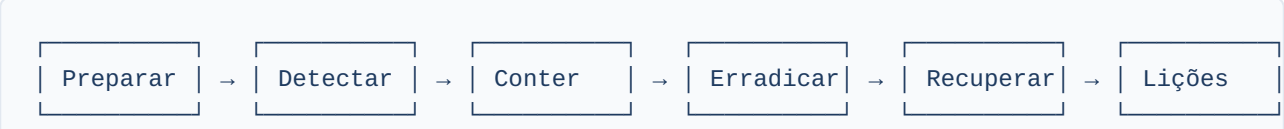
- O **NIST SP 800-61 r2** — Computer Security Incident Handling Guide;
- O **artigo 27.º do Decreto-Lei n.º 125/2025**, de 4 de Dezembro, no que se refere às obrigações de notificação ao Centro Nacional de Cibersegurança (CNCS);
- Os **artigos 33.º e 34.º do Regulamento (UE) 2016/679 (RGPD)**, no que se refere a violações de dados pessoais;
- Os princípios apreendidos no módulo Threat Analysis da formação Cisco Introduction to Cybersecurity.

2. Definições

Termo	Definição
Evento	Ocorrência observável num sistema ou rede, sem necessariamente impacto em segurança.
Alerta	Evento que merece atenção e investigação.
Incidente	Evento ou conjunto de eventos com impacto adverso confirmado ou provável na confidencialidade, integridade ou disponibilidade dos sistemas ou dados.
Incidente significativo	Incidente que cumpre os critérios definidos no n.º 4 do artigo 27.º do DL 125/2025: causa ou é susceptível de causar perturbação operacional grave ou perdas financeiras consideráveis; ou afecta ou é susceptível de afectar pessoas singulares ou colectivas, causando danos materiais ou imateriais consideráveis.
Violação de dados pessoais	Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, perda, alteração, divulgação ou acesso não autorizados a dados pessoais (artigo 4.º, n.º 12 do RGPD).
Early warning	Aviso prévio ao CNCS, dentro de 24 horas após detecção.
Notificação	Comunicação ao CNCS dentro de 72 horas após detecção (incidentes significativos).
Relatório final	Relatório completo ao CNCS dentro de 30 dias após o incidente.

3. Estrutura do plano

O ciclo de resposta a incidentes adoptado pela 3HASH segue as **6 fases do NIST SP 800-61**:



4. Fase 1 — Preparação

A fase de preparação é contínua e ocorre antes de qualquer incidente.

Elemento	Estado
Política de Cibersegurança aprovada	✅ Documento 01
Avaliação de Risco actualizada	✅ Documento 03
Responsável de Cibersegurança designado	✅ Documento 04
Backups encriptados, segregados e testados	✅ Verificável
Logs centralizados com retenção mínima de 90 dias	✅ Verificável
Lista de contactos críticos disponível	✅ Secção 9 deste documento
Equipa formada em fundamentos de cibersegurança	✅ Documento 05
Inventário de activos actualizado	✅ Documento 06

5. Fase 2 — Detecção e análise

5.1. Fontes de detecção

- Alertas automatizados de monitorização contínua;
- Sistemas de detecção de intrusão e de integridade de ficheiros;
- Análise de logs centralizados;
- Reporte por colaborador, cliente, fornecedor ou terceiro;
- Comunicação proveniente do CNCS, de CSIRTs, ou de fontes de threat intelligence.

5.2. Triagem inicial

Após detecção, o Responsável de Cibersegurança ou colaborador de plantão executa, no prazo máximo de **2 horas úteis**:

a) Confirmação de ocorrência (descartar falso positivo); b) Classificação preliminar (severidade, impacto, escopo); c) Decisão de escalonamento.

5.3. Classificação de severidade

Nível	Critério	Exemplos
P1 — Crítico	Comprometimento confirmado de sistemas críticos, exfiltração de dados pessoais ou indisponibilidade total de serviço.	Ransomware, exfiltração massiva, defacement de site institucional.
P2 — Alto	Comprometimento parcial ou risco elevado, sem perda de dados confirmada.	Conta comprometida, malware confinado, ataque DDoS limitado.
P3 — Médio	Tentativa de ataque com mitigação automática activa.	Brute-force bloqueado, phishing detectado e barrado.
P4 — Baixo	Anomalia menor sem impacto operacional.	Tentativa de scan externo.

5.4. Documentação

Cada incidente abre um **registo formal** contendo: identificador único, data e hora de detecção, fonte, descrição inicial, sistemas afectados, severidade preliminar, responsável atribuído.

---

6. Fase 3 — Contenção

A contenção tem por objectivo **limitar o impacto** sem destruir evidência forense.

6.1. Acções imediatas (P1 e P2)

- Isolar os sistemas afectados da rede sem desligar (preservar memória volátil);
- Revogar credenciais comprometidas ou suspeitas;
- Bloquear endereços IP e contas atacantes ao nível do perímetro;
- Acionar backups verificados como fonte de verdade paralela;
- **Preservar evidência** — capturar logs, snapshots, dumps de memória, tráfego de rede.

6.2. Comunicação interna

Notificação imediata da gerência. Para incidentes P1, ponto de situação a cada 4 horas até à contenção total.

---

7. Fase 4 — Erradicação

- Remoção da causa-raiz: malware, contas comprometidas, vulnerabilidades exploradas;
- Aplicação de patches críticos pendentes;
- Reconstrução completa de sistemas comprometidos a partir de imagem limpa quando a confiança no sistema esteja em causa;
- Rotação total de credenciais relacionadas (palavras-passe, chaves de API, tokens, certificados).

8. Fase 5 — Recuperação

- Restauro dos serviços a partir de backups verificados;
- Validação funcional antes de regresso a produção;
- Monitorização reforçada durante 30 dias após o incidente;
- Comunicação a clientes ou utilizadores quando aplicável.

9. Fase 6 — Lições aprendidas

Reunião post-mortem obrigatória dentro de **15 dias úteis** após resolução, com:

a) Reconstrução cronológica do incidente; b) Identificação da causa-raiz (técnica, processual, humana); c) Identificação de falhas nos controlos preventivos e de detecção; d) Acções correctivas com responsáveis e prazos; e) Actualização da Avaliação de Risco (documento 03) e desta política se aplicável.

10. Notificação a entidades externas

10.1. Centro Nacional de Cibersegurança (CNCS) — incidentes significativos

Nos termos do **artigo 27.º do DL 125/2025**, a 3HASH cumprirá os seguintes prazos quando aplicável:

Prazo	Acção
Até 24 horas	Early warning — comunicação preliminar ao CNCS, indicando se o incidente é potencialmente malicioso e se pode ter impacto transfronteiriço.
Até 72 horas	Notificação completa — actualização do early warning, com avaliação inicial, indicadores de comprometimento e medidas tomadas.
Até 30 dias	Relatório final — descrição detalhada do incidente, causa-raiz, gravidade, impactos transfronteiriços, medidas implementadas.
Sob solicitação	Relatório intercalar — em incidentes prolongados, mediante pedido do CNCS.

Canal: portal oficial do CNCS (https://www.cncs.gov.pt) e, em duplicado, por correio electrónico para o endereço institucional indicado pela autoridade.

10.2. Comissão Nacional de Protecção de Dados (CNPD) — violações de dados

Nos termos do **artigo 33.º do RGPD**, em caso de violação de dados pessoais a notificação é feita à CNPD dentro de **72 horas** após o conhecimento. Quando a violação seja susceptível de implicar **elevado risco** para os direitos e liberdades das pessoas singulares afectadas, é-lhes feita comunicação directa nos termos do **artigo 34.º do RGPD**.

Canal: plataforma electrónica da CNPD.

10.3. Cliente

Se o incidente afectar dados ou sistemas tratados em nome de um cliente, a 3HASH notifica esse cliente, na qualidade de subcontratante, no prazo máximo de **24 horas** após o conhecimento, conforme exigido pelo **artigo 33.º, n.º 2 do RGPD**.

10.4. Autoridades policiais

Em caso de suspeita de crime informático nos termos da **Lei do Cibercrime (Lei n.º 109/2009)**, é apresentada queixa à Polícia Judiciária — Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

11. Contactos críticos

Entidade	Contacto	Quando contactar
Gerência da 3HASH	(registo controlado interno)	Sempre, em primeiro lugar; coordena toda a resposta.
Auditoria externa de cibersegurança	(registo controlado interno)	Para incidentes P1, apoio à análise técnica.
CNCS — CERT.PT	cert@cert.pt · +351 210 497 399	Incidentes significativos; early warning até 24 h.
CNPD	geral@cnpd.pt · +351 213 928 400	Violação de dados pessoais; até 72 h.
Polícia Judiciária — UNC3T	cibercrime@pj.pt	Suspeita de crime informático.
Apoio jurídico externo	(a contratualizar pontualmente)	Incidentes com possível responsabilidade civil ou criminal.

12. Comunicação pública

A comunicação pública sobre incidentes obedece aos seguintes princípios:

- **Não comunicar prematuramente** — só após contenção e validação dos factos;
- **Linguagem factual**, evitando especulação;
- **Coordenação prévia com cliente** quando a comunicação envolva sistemas operados em seu nome;
- **Proibição de divulgar detalhes técnicos** que possam facilitar ataques subsequentes;
- **Direito à informação dos titulares de dados** quando aplicável (RGPD artigo 34.º).

13. Revisão

Versão	Data	Alterações	Responsável
1.0	2026-05-02	Versão inicial. Criação.	Gerência

Avaliação de Risco de Cibersegurança

Versão: 1.0 **Entidade:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Data de avaliação:** 2 de Maio de 2026 **Próxima revisão:** Maio de 2027 (revisão anual obrigatória); ou após incidente significativo **Responsável pela avaliação:** Responsável de Cibersegurança (ver documento 04)

1. Objecto

A presente Avaliação de Risco identifica, analisa e classifica os principais riscos de cibersegurança a que a 3HASH está exposta, em cumprimento do disposto no **artigo 21.º, n.º 2, alínea a) do Decreto-Lei n.º 125/2025**.

A metodologia adoptada segue a estrutura do **NIST AI Risk Management Framework** (Frame · Assess · Respond · Monitor) — apreendida na formação Cisco Introduction to Cybersecurity (módulo Threat Analysis) — e as orientações da **ISO/IEC 27005:2022**.

2. Metodologia

2.1. Etapas

2.2. Escala de probabilidade

Nível	Descrição	Frequência indicativa
1 — Muito baixa	Improvável que ocorra	< uma vez em 5 anos
2 — Baixa	Pode ocorrer ocasionalmente	uma vez em 2-5 anos
3 — Média	Ocorrência expectável	uma vez por ano
4 — Alta	Ocorrência frequente	várias vezes por ano
5 — Muito alta	Ocorrência constante	tentativa diária

2.3. Escala de impacto

Nível	Operacional	Legal/Regulatório	Financeiro	Reputacional
1 — Muito baixo	Sem impacto	Sem impacto	< 100 €	Sem impacto
2 — Baixo	Degradação menor, < 1 h	Sem violação	100-1.000 €	Limitado
3 — Médio	Indisponibilidade parcial, < 1 dia	Notificação interna	1.000-10.000 €	Cliente afectado
4 — Alto	Indisponibilidade significativa, > 1 dia	Notificação obrigatória CNCS/ CNPD	10.000-100.000 €	Cobertura mediática negativa
5 — Muito alto	Paralisação total	Sanção administrativa	> 100.000 €	Dano reputacional grave

2.4. Cálculo do risco

Risco = Probabilidade × Impacto (escala 1–25)

Score	Classificação	Acção
1–4	Baixo	Aceitar; monitorizar.
5–9	Moderado	Tratar com controlos existentes; reavaliar.
10–15	Alto	Reduzir com novos controlos; prazo definido.
16–25	Crítico	Reduzir imediatamente; escalar à gerência.

3. Frame — Contexto e perímetro

A 3HASH é uma microempresa portuguesa de serviços digitais. Os seus principais activos sujeitos a risco cibernético são:

Categoria	Descrição genérica
Infraestrutura própria	Sistemas computacionais e de armazenamento localizados em Portugal, sob controlo directo da entidade.
Plataforma de email empresarial	Serviços de correio para a entidade e clientes alojados.
Plataforma de DNS e domínios	Gestão de domínios próprios e de clientes.
Bases de dados aplicacionais	Aplicações próprias com persistência (sistema de gestão de arrendamento, sistema de afiliados, sistema de prospecção, etc.).
Modelo proprietário 3HASH Local AI	Sistemas de inteligência artificial executados em infraestrutura própria, sem dependência de cloud externa.
Repositórios de código	Código-fonte de aplicações próprias e de clientes.
Estações de trabalho	Equipamentos da equipa.
Credenciais de acesso a sistemas de clientes	Acessos delegados pelos clientes para gestão de marketing, hosting e correio.
Dados pessoais	Dados de clientes, prospects e utilizadores finais (no âmbito de subcontratação RGPD).

4. Assess — Identificação e classificação de riscos

4.1. Riscos técnicos

#	Ameaça	Activo afectado	Probab.	Impacto	Risco	Controlos existentes
T1	**Ransomware** sobre servidores/ estações	Infraestrutura própria, bases de dados	3	5	**15 — Alto**	Backups encriptados off-site diários, segregação por containers, MFA em consolas, restauro testado.
T2	**Comprometimento de credenciais administrativas**	Todos	3	5	**15 — Alto**	MFA obrigatório, rotação periódica, gestor de palavras-passe profissional, revogação imediata em saídas.
T3	**Phishing direccionado** à equipa	Credenciais, estações	4	4	**16 — Crítico**	Formação Cisco + CNCS, MFA, alertas de email, política de verificação de remetente.
T4	**DDoS** sobre serviços expostos	Sites de clientes, plataformas próprias	4	3	**12 — Alto**	Protecção de perímetro contra negação de serviço fornecida pelo CDN, rate limiting.
T5	**Exploração de vulnerabilidade aplicacional** (OWASP Top 10)	Aplicações próprias	3	4	**12 — Alto**	Validação de input, headers de segurança, auditoria de dependências, revisão de código antes de produção.
T6	**Violação de cadeia de fornecimento**	Aplicações próprias	2	4	**8 — Moderado**	Pinning de versões, auditoria periódica, due

#	Ameaça	Activo afectado	Probab.	Impacto	Risco	Controlos existentes
	(compromisso de dependência)					diligence (documento 06).
T7	**Acesso físico não autorizado** à infraestrutura	Infraestrutura própria	1	5	**5 — Moderado**	Acesso físico restrito, sem partilha de chaves.
T8	**Fuga de dados** por má configuração (S3, DB exposto)	Bases de dados	2	5	**10 — Alto**	Princípio do menor privilégio, revisão de configurações, auditoria periódica.
T9	**Perda ou roubo de equipamento da equipa**	Estações	3	3	**9 — Moderado**	Cifragem de disco em todas as estações, bloqueio automático, MDM em desenvolvimento.
T10	**Comprometimento de modelo de IA** (prompt injection, model theft)	3HASH Local AI	2	3	**6 — Moderado**	Modelo executado em infraestrutura própria, sem exposição directa, alinhamento com OWASP Top 10 for LLM Applications.

4.2. Riscos organizacionais e processuais

#	Ameaça	Probab.	Impacto	Risco	Controlos existentes
O1	**Indisponibilidade prolongada** do Responsável de Cibersegurança	2	4	**8 — Moderado**	Documentação centralizada, partilha de procedimentos, plano de sucessão.
O2	**Erro humano** em operação crítica	4	3	**12 — Alto**	Procedimentos documentados, 4-eyes em mudanças críticas, ambientes de teste.
O3	**Ausência de formação actualizada**	2	3	**6 — Moderado**	Calendário de formação no documento 05, mínimo de 4 cursos certificados por colaborador.
O4	**Incumprimento contratual de fornecedor** crítico	2	4	**8 — Moderado**	Due diligence prévia, contratos com cláusulas de SLA e segurança (documento 06).

4.3. Riscos legais e regulatórios

#	Ameaça	Probab.	Impacto	Risco	Controlos existentes
L1	**Violação de dados pessoais** com dever de notificação CNPD	2	4	**8 — Moderado**	Política RGPD, plano de resposta a incidentes (documento 02), DPIA quando aplicável.
L2	**Incumprimento NIS2** com sanção	2	4	**8 — Moderado**	Adopção voluntária do regime, dossier de conformidade actualizado.
L3	**Não conformidade com EU AI Act** em projecto de cliente	2	3	**6 — Moderado**	Adesão ao EU AI Pact, alinhamento NIST AI RMF, DPIA quando aplicável.
L4	**Reclamação ou processo judicial** por cliente	2	3	**6 — Moderado**	Contratos formais, SLAs definidos, comunicação documentada.

5. Respond — Tratamento dos riscos

5.1. Estratégias de tratamento

Para cada risco identificado, a 3HASH adopta uma das seguintes estratégias:

- **Aceitar** — risco baixo, custo de mitigação superior ao impacto.
- **Reduzir** — implementar controlos adicionais.
- **Transferir** — seguro de cibersegurança ou contratualização.
- **Evitar** — não realizar a actividade que gera o risco.

5.2. Plano de acção para riscos críticos e altos

Risco	Estratégia	Acção	Responsável	Prazo
T3 — Phishing direccionado	Reduzir	Simulação anual de phishing à equipa; reforço de formação a colaboradores que falhem.	Responsável de Cibersegurança	2026 Q4
T1 — Ransomware	Reduzir	Verificação trimestral do restauro de backups; implementação de regra de imutabilidade.	Responsável de Cibersegurança	Contínuo
T2 — Credenciais comprometidas	Reduzir	Estender MFA aos sistemas restantes; auditoria semestral de privilégios.	Responsável de Cibersegurança	2026 Q3
T4 — DDoS	Transferir/ Reduzir	Manter protecção de perímetro activa; avaliar serviço premium para clientes maiores.	Responsável de Cibersegurança	2026 Q4
T5 — OWASP Top 10	Reduzir	Auditoria de segurança aplicacional anual a aplicações críticas; bug bounty informal.	Equipa técnica	2027 Q1
T8 — Má configuração	Reduzir	Lista de verificação obrigatória pré-deploy; auditoria trimestral.	Equipa técnica	2026 Q4
O2 — Erro humano	Reduzir	Formalizar regra 4-eyes em todas as mudanças críticas.	Responsável de Cibersegurança	2026 Q4

5.3. Risco residual

Após implementação dos controlos previstos, o risco residual mantém-se em níveis **moderado a baixo** para todos os cenários identificados.

---

6. Monitor — Revisão e actualização

A presente avaliação é objecto de **revisão anual obrigatória**. Revisões extraordinárias ocorrem sempre que:

a) Se verifique incidente significativo; b) Se introduza alteração estrutural na infraestrutura ou na actividade da entidade; c) Sejam identificadas novas categorias de ameaças relevantes; d) Surja alteração legal aplicável.

Indicadores monitorizados (KPI):

- Número de incidentes por trimestre, por categoria;
- Tempo médio de detecção (MTTD) e de resposta (MTTR);
- Percentagem de colaboradores com formação em dia;
- Número de tentativas de intrusão bloqueadas no perímetro;
- Estado dos backups (sucesso/falha) e do teste de restauro.

---

7. Anexos

- **Anexo A** — Plano de Resposta a Incidentes (documento 02)
- **Anexo B** — Inventário de Activos e Fornecedores (documento 06)
- **Anexo C** — Registo de Formação (documento 05)

Designação de Responsável de Cibersegurança e Auditoria Externa

Versão: 1.0 **Entidade:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Sede:** Rua Cardoso Marta 14 Cave, 3080-012 Figueira da Foz, Portugal **Documento:** 04 / Conformidade **Data de emissão:** 2 de Maio de 2026

1. Enquadramento legal

Em cumprimento do disposto no **artigo 17.º do Decreto-Lei n.º 125/2025**, de 4 de Dezembro, que transpõe para a ordem jurídica nacional a Diretiva (UE) 2022/2555 (NIS2), em vigor desde 3 de Abril de 2026, a FORTUNEWEEK – UNIPESSOAL LDA estabelece o seu modelo de governação de cibersegurança.

Embora a FORTUNEWEEK – UNIPESSOAL LDA seja uma microempresa que poderá não estar abrangida directamente pelo perímetro obrigatório do regime jurídico nacional NIS2, a entidade adopta voluntariamente o regime enquanto:

- Boa prática de governação interna;
- Garantia de conformidade na cadeia de fornecimento dos seus clientes (alguns dos quais abrangidos directamente);
- Diferenciação competitiva em propostas comerciais e candidaturas a fundos europeus.

2. Modelo de governação adoptado

A 3HASH adopta um **modelo misto** de responsabilidade interna pela cibersegurança, complementado por **auditoria externa independente**:

2.1. Responsabilidade interna

A **gerência da FORTUNEWEEK – UNIPESSOAL LDA** assume directamente a responsabilidade última pela cibersegurança da entidade, nos termos do artigo 21.º, n.º 6, do Decreto-Lei n.º 125/2025, sendo apoiada pela equipa técnica da 3HASH na implementação operacional dos controlos previstos na Política de Cibersegurança (documento 01).

2.2. Auditoria externa independente

A entidade contrata, em regime pontual e independente, **serviços de auditoria de cibersegurança** prestados por elemento externo com as seguintes qualificações académicas e profissionais:

- **Mestrado em Informática** pela Universidade de Coimbra;
- **MBA — Master of Business Administration**;
- Habilitação para auditoria de sistemas de informação.

A escolha deste perfil — combinação de competência técnica avançada (Mestrado em Informática por uma das principais instituições de ensino superior nacionais) com competência de gestão (MBA) — foi deliberada, garantindo que a auditoria abrange tanto a dimensão técnica como a dimensão organizativa da segurança.

A identidade nominal do auditor externo encontra-se documentada em registo controlado, sob acesso restrito da gerência, e pode ser disponibilizada a clientes ou autoridades mediante NDA prévia ou ordem legal. Para todos os efeitos externos (referência em propostas, comunicação com clientes, candidaturas), a designação utilizada é **«Auditoria externa por elemento com Mestrado em Informática pela Universidade de Coimbra e MBA»**.

---

3. Atribuições

3.1. Gerência (responsabilidade interna)

a) Aprovação e revisão anual da Política de Cibersegurança (documento 01); b) Aprovação do Plano de Resposta a Incidentes (documento 02); c) Aprovação da Avaliação de Risco anual (documento 03); d) Decisão sobre alocação de recursos para implementação dos controlos; e) Em caso de incidente significativo que justifique comunicação ao Centro Nacional de Cibersegurança (CNCS), assegurar essa comunicação através dos canais públicos disponíveis, observando os prazos do **artigo 27.º do Decreto-Lei n.º 125/2025** (early warning até 24 horas, notificação até 72 horas, relatório final até 30 dias). A 3HASH **não procedeu ao registo formal de Ponto de Contacto Permanente** junto do CNCS, por se encontrar fora do âmbito obrigatório do regime; f) Em caso de violação de dados pessoais, articular a notificação à **Comissão Nacional de Protecção de Dados (CNPD)**, no prazo de **72 horas** previsto no artigo 33.º do RGPD.

3.2. Equipa técnica (operacionalização)

a) Aplicação operacional dos controlos definidos na Política; b) Manutenção do Inventário de Activos (documento 06); c) Manutenção do Registo de Formação (documento 05); d) Resposta de primeira linha a alertas e incidentes, nos termos do documento 02; e) Comunicação imediata à gerência de incidentes que excedam a sua capacidade de resposta autónoma.

3.3. Auditoria externa independente

a) Revisão crítica anual da Política de Cibersegurança e dos restantes documentos do dossier; b) Avaliação da implementação efectiva dos controlos previstos; c) Identificação de lacunas e recomendação de medidas correctivas; d) Apoio na resposta a pedidos de due diligence apresentados por clientes ou autoridades; e) Acompanhamento da evolução do quadro regulatório aplicável (NIS2, RGPD, AI Act, normas técnicas).

4. Não notificação ao CNCS

A 3HASH, por ser microempresa fora dos sectores essenciais e importantes definidos nos Anexos I e II do **Decreto-Lei n.º 125/2025**, **não está abrangida pelas obrigações de identificação e notificação** previstas no regime jurídico nacional NIS2.

Em consequência, o presente modelo de governação **não foi formalmente comunicado ao Centro Nacional de Cibersegurança (CNCS)**. Trata-se de instrumento interno e voluntário.

A 3HASH reserva-se o direito de proceder, no futuro, ao registo formal junto do CNCS caso passe a ser legalmente abrangida ou caso tal seja exigido por cliente ou concurso público.

5. Validade e revisão

O presente modelo de governação é válido por tempo indeterminado, sendo revisto sempre que ocorra:

- Alteração do auditor externo contratado;
- Alteração estrutural relevante na entidade;
- Alteração legal aplicável.

Revisão calendarizada: **anual**, no mês de Maio.

6. Aprovação

Documento aprovado pela Gerência em **2 de Maio de 2026**.

A versão assinada e datada é mantida em registo controlado da entidade.

Anexos

- Cópia da publicação do Decreto-Lei n.º 125/2025 (Diário da República)
- Documentação curricular do auditor externo (sob registo controlado)

Registo de Formação em Cibersegurança

Versão: 1.0 **Entidade:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Data de actualização:** 2 de Maio de 2026 **Próxima revisão:** Trimestral; revisão completa em Maio de 2027 **Responsabilidade:** Gerência, com apoio de auditoria externa (ver documento 04)

1. Objecto

O presente registo documenta a formação concluída pela equipa da 3HASH em matéria de cibersegurança, em cumprimento do disposto no **artigo 21.º, n.º 2, alínea g) do Decreto-Lei n.º 125/2025**, que exige a implementação de práticas básicas de higiene cibernética e formação em cibersegurança aplicadas à totalidade da equipa, incluindo a gerência.

2. Currículo de referência

A 3HASH adopta o seguinte currículo de formação fundamental em cibersegurança, recorrendo a recursos credíveis emitidos por entidades públicas e por instituições internacionais reconhecidas (CNCS, Cisco Networking Academy):

2.1. Tronco comum (todas as funções)

Curso	Entidade emissora	Duração	Validade	Verificação
Cidadão Ciberinformado	Centro Nacional de Cibersegurança (CNCS) / Lusa / NAU	~3 horas	Sem expiração	Certificado PDF emitido pela plataforma NAU
Cidadão Ciberseguro	Centro Nacional de Cibersegurança (CNCS) / NAU	~3 horas	Sem expiração	Certificado PDF emitido pela plataforma NAU
Consumidor Ciberseguro	Centro Nacional de Cibersegurança (CNCS) / NAU	~4 horas	Sem expiração	Certificado PDF emitido pela plataforma NAU
Introduction to Cybersecurity	Cisco Networking Academy	~15 horas	Sem expiração	Badge digital verificável no Credly

2.2. Funções de marketing digital (complementar)

Curso	Entidade emissora	Validade	Verificação
Google Ads AI-Powered Performance Ads	Google Skillshop	12 meses (renovação anual)	Credencial pública no Skillshop
Google Analytics Certification	Google Skillshop	12 meses (renovação anual)	Credencial pública no Skillshop

2.3. Roadmap de formação avançada

A 3HASH inscreveu-se ou tem em preparação as seguintes formações avançadas, a concluir nos próximos 18 meses:

Curso	Entidade emissora	Estado
Hacking e Testes de Penetração — Nível E (70h)	C-Academy CNCS, em parceria com a Universidade de Coimbra	Em lista de espera
Cisco Certified Cybersecurity Specialist	Cisco	Planeado 2026/27
EU AI Pact — Pillar II	Comissão Europeia	Em preparação

3. Síntese de certificações detidas pela equipa em Maio de 2026

Em Maio de 2026, a equipa da 3HASH detém certificações activas e verificáveis nas duas frentes seguintes:

3.1. Cibersegurança e literacia digital

#	Certificação	Entidade	Data de conclusão	Quantidade detida
F01	Cidadão Ciberinformado	CNCS / Lusa / NAU	02 / 05 / 2026	1
F02	Cidadão Ciberseguro	CNCS / NAU	02 / 05 / 2026	1
F03	Consumidor Ciberseguro	CNCS / NAU	02 / 05 / 2026	1
F04	Cisco Introduction to Cybersecurity (Cisco Networking Academy) — inclui 5 módulos certificados individualmente: Resource Specialist, Network Defense, System Safeguards, Threat Analysis, Cybersecurity Administration	Cisco	02 / 05 / 2026	1

Badge Cisco verificável publicamente em: https://www.credly.com/earner/earned/badge/deb0b114-4678-415a-93ab-4f2980ed5a2c

3.2. Marketing digital

#	Certificação	Entidade	Data
F05	Google Ads AI-Powered Performance Ads	Google Skillshop	Março de 2026 (renovação anual)
F06	Google Analytics Certification	Google Skillshop	Renovada desde 2024

Credenciais verificáveis em: - https://skillshop.credential.net/4f863186-5368-4c6e-9686-160e643455b7 - https://skillshop.credential.net/a7537b03-ef24-493b-937d-b26f750abf5c

3.3. Auditoria externa

A função de auditoria de cibersegurança é exercida por auditor externo independente, com **Mestrado em Informática pela Universidade de Coimbra** e **MBA**, conforme descrito no documento 04. Esta qualificação assegura competência técnica avançada e capacidade de avaliação organizativa.

4. Sensibilização contínua

Adicionalmente à formação certificada, a 3HASH adopta como prática:

- Acompanhamento dos boletins de cibersegurança publicados pelo CNCS, ENISA e CSIRT.PT;
- Análise de incidentes notórios da indústria, com aplicação de lições à operação interna;
- Reforço periódico de boas práticas em matéria de identificação de tentativas de phishing e gestão de credenciais.

5. Revisão e versionamento

O presente registo é actualizado **trimestralmente** pelo responsável designado pela gerência, sempre que:

- Um colaborador conclua novo curso;
- Caduque a validade de uma certificação (e renovação seja programada);
- Entre ou saia colaborador da equipa.

Versão	Data	Alterações
1.0	2026-05-02	Versão inicial. Inclui registo dos 4 cursos de cibersegurança concluídos em 2 de Maio de 2026 (Cisco Introduction to Cybersecurity + 3 cursos do Centro Nacional de Cibersegurança).

Inventário de Activos e Soberania Tecnológica

Versão: 1.0 **Entidade:** FORTUNEWEEK – UNIPESSOAL LDA (marca comercial: 3HASH®) **NIPC:** 515 084 182 **Data de actualização:** 2 de Maio de 2026 **Próxima revisão:** Trimestral; revisão completa em Maio de 2027 **Responsável:** Responsável de Cibersegurança (ver documento 04) **Classificação:** Uso interno · Partilha com clientes apenas mediante NDA

1. Objecto

O presente documento estabelece o inventário das categorias de activos da 3HASH e descreve o modelo de **soberania tecnológica** da entidade, em cumprimento do disposto no:

- **Artigo 21.º, n.º 2, alínea d) do Decreto-Lei n.º 125/2025** — segurança da cadeia de fornecimento;
- **Artigo 21.º, n.º 2, alínea i)** — controlo de activos;
- **ISO/IEC 27001:2022** — controlo A.5.9 (inventário de informação e activos associados).

> Por razões de segurança operacional e protecção de propriedade intelectual, o presente documento descreve categorias de activos sem identificação de modelos específicos, versões, endereços, configurações ou identidades comerciais. A informação detalhada está disponível ao Responsável de Cibersegurança e à Gerência, sob registo controlado.

2. Modelo de soberania tecnológica 3HASH

2.1. Princípio fundamental

A 3HASH opera segundo um modelo de **integração vertical** e **soberania tecnológica nacional**, deliberadamente distinto do modelo dominante na indústria — que assenta na subcontratação intensiva de plataformas cloud internacionais. Em concreto:

> **A 3HASH não depende de fornecedores cloud externos para o processamento, armazenamento ou inferência sobre dados de clientes ou de utilizadores finais.**

Esta opção é estratégica, não acidental, e materializa-se em todas as dimensões críticas da operação:

Função	Modelo dominante na indústria	Modelo 3HASH
Inferência de IA	API de fornecedores cloud (OpenAI, Anthropic, Google)	**Modelo proprietário 3HASH Local AI**, executado em infraestrutura própria em Portugal
Alojamento aplicacional	AWS, Google Cloud, Azure	**Servidores próprios em Portugal**, sob jurisdição UE
Bases de dados	Cloud DB managed (RDS, Cloud SQL, Atlas)	**Bases de dados em servidores próprios**, sem dependência cloud externa
Correio electrónico	Microsoft 365, Google Workspace	**Plataforma de email auto-alojada** em infraestrutura própria
Backups	Cloud storage de fornecedor (S3, GCS)	**Sistema de backup próprio**, com cópia off-site em armazenamento físico segregado
Repositórios de código	GitHub, GitLab.com	Repositórios privados em infraestrutura própria
Monitorização e logs	Datadog, New Relic, CloudWatch	Sistemas de monitorização próprios em infraestrutura local

2.2. Implicações para os clientes

Da soberania tecnológica decorrem benefícios verificáveis e comercializáveis:

a) **Os dados dos clientes não saem do território português** salvo necessidade operacional excepcional, sob acordo escrito;

b) **Não há transferência de dados pessoais para países terceiros** sem base legal adequada nos termos do Capítulo V do RGPD;

c) **O conteúdo de prompts e conversas com sistemas de IA não é enviado para fornecedores cloud externos** — o modelo proprietário 3HASH Local AI executa inteiramente em servidores próprios, sem dependência de OpenAI, Anthropic, Google ou outro fornecedor internacional;

d) **A 3HASH é simultaneamente responsável pelo tratamento e pela infraestrutura** que o suporta, eliminando a dispersão de responsabilidade típica do modelo cloud-as-a-service;

e) **Os clientes podem auditar fisicamente** a infraestrutura, mediante NDA prévia.

2.3. Implicações para o cumprimento NIS2 e RGPD

A soberania tecnológica simplifica e reforça o cumprimento dos regimes aplicáveis:

- **Cadeia de fornecimento (NIS2 Art. 21.º, n.º 2, alínea d)** — o número de dependências externas críticas é minimizado por concepção;

- **Transferência internacional de dados (RGPD Cap. V)** — não aplicável na maioria dos casos por inexistência de transferência;
- **AI Act (Regulamento UE 2024/1689)** — a 3HASH retém controlo integral sobre os sistemas de IA que opera, podendo cumprir requisitos de transparência, supervisão humana e auditabilidade sem dependência de terceiros;
- **Soberania digital europeia** — alinhamento com prioridades estratégicas da União Europeia em matéria de autonomia tecnológica.

3. Categorias de activos próprios

3.1. Infraestrutura computacional própria

Categoria	Localização	Função	Criticidade
Sistemas computacionais de produção	Portugal (jurisdição UE)	Operação de aplicações próprias e de clientes; modelo proprietário 3HASH Local AI	Crítica
Sistemas de armazenamento segregados	Portugal (jurisdição UE)	Backups encriptados off-site	Alta
Estações de trabalho da equipa	Portugal	Desenvolvimento, gestão, comunicação	Média

3.2. Plataformas aplicacionais próprias

Todas as plataformas listadas operam **integralmente em infraestrutura própria em Portugal**, sem dependência de cloud externa para processamento ou armazenamento de dados.

Plataforma	Função	Dados tratados	Criticidade
Sistema de gestão de arrendamento	Operação completa de empresa cliente em modo SaaS	Dados pessoais de inquilinos e proprietários	Crítica
Sistema de afiliados	Gestão de parceiros comerciais	Dados pessoais de afiliados	Alta
Sistema de prospecção comercial	Identificação e qualificação de leads	Dados profissionais públicos de prospects	Média
Plataforma de envios de ficheiros grandes	Transferência segura de ficheiros para clientes	Conteúdo enviado pelos clientes	Alta
Sistema de tickets de suporte	Gestão de incidentes de cliente	Dados de contacto e histórico de comunicação	Alta
Sistema de inventário de domínios	Monitorização de WHOIS, SSL e billing	Metadados de domínios	Média
Modelo proprietário **3HASH Local AI**	Inferência de modelos de linguagem em infraestrutura própria, sem dependência de fornecedores cloud externos	Sem persistência de prompts; ver políticas de privacidade dos projectos	Crítica

3.3. Bases de dados aplicacionais

Cada uma das plataformas listadas em 3.2 mantém base de dados própria, segregada por aplicação. Todas as bases são:

- Operadas em **infraestrutura própria** (sem dependência de fornecedor cloud externo);
- Cifradas em repouso quando contenham dados pessoais ou credenciais;
- Sujeitas a backups encriptados diários, retidos durante um mínimo de 30 dias, com cópia off-site em armazenamento físico segregado;
- Acessíveis apenas a partir da rede aplicacional da própria plataforma (sem exposição directa à internet).

3.4. Repositórios de código-fonte

Código-fonte de aplicações próprias e de projectos de cliente é mantido em **repositórios privados em infraestrutura própria**, com:

- Acesso restrito por princípio do menor privilégio;

- MFA obrigatório;
- Branch protection nos ramos de produção;
- Auditoria periódica de dependências.

3.5. Credenciais e segredos

Credenciais de acesso a sistemas próprios e de clientes, chaves de API, tokens e certificados são geridos em **gestor de palavras-passe profissional**, com:

- MFA obrigatório no acesso ao próprio gestor;
- Segregação por projecto/cliente;
- Política de revogação imediata em saída de colaborador ou suspeita de comprometimento.

4. Dependências externas residuais

A integração vertical da 3HASH minimiza, mas não elimina por completo, a existência de dependências externas. Estas restringem-se ao seguinte conjunto reduzido, correspondente a **infraestruturas comuns da internet** sem alternativa funcional viável a uma microempresa:

Categoria	Tipo de dependência	Risco principal	Plano de mitigação
Conectividade internet	Operador nacional licenciado pela ANACOM	Indisponibilidade da rede	Operador alternativo identificado para activação rápida.
Resolução DNS internacional e protecção de perímetro	Plataforma internacional reconhecida	Indisponibilidade ou redireccionamento malicioso	Configuração documentada para migração para alternativa equivalente em < 24 h.
Registar de domínios	Entidade acreditada pela ICANN/DNS.PT	Hijack de domínios	MFA obrigatório, registry lock activo nos domínios críticos.
Autoridade certificadora TLS pública	Autoridade reconhecida pelos browsers	Não emissão	Autoridade alternativa identificada; cadeia de emissão automatizada.

> **Importante:** Estas dependências residuais **não envolvem o tratamento de dados de clientes nem de utilizadores finais** — limitam-se ao plano da conectividade e da identidade dos serviços públicos da 3HASH. Os dados aplicacionais permanecem sempre em infraestrutura própria em Portugal.

Cláusulas mínimas exigidas a estas dependências

a) Conformidade com o RGPD (operador estabelecido na UE ou com mecanismos válidos de transferência); b) Notificação à 3HASH no prazo máximo de **24 horas** após detecção de incidente; c) Possibilidade de migração assistida em caso de cessação contratual; d) Histórico operacional sem incidentes graves nos últimos 24 meses.

5. Comparação com modelo dominante da indústria

A título ilustrativo, a tabela abaixo compara o número e natureza das dependências críticas do modelo 3HASH com as de uma agência digital típica que assenta em arquitectura cloud.

Indicador	Agência típica baseada em cloud	3HASH (modelo soberano)
Fornecedores cloud com acesso a dados de cliente	5 a 15 (hosting, DB, IA, email, storage, CDN, monitorização, etc.)	**0**
Países onde os dados de cliente podem ser processados	EUA + UE + outros (variável)	**Portugal (UE)**
Cumprimento sem cláusulas de transferência internacional	Difícil	**Por concepção**
Tempo médio de migração entre fornecedores cloud	Semanas a meses	Não aplicável
Capacidade de auditoria física pelo cliente	Limitada ou nula	**Possível mediante NDA**
Capacidade de operar em modo air-gapped (offline)	Não	**Sim, para subconjunto crítico**

6. Revisão

Versão	Data	Alterações
1.0	2026-05-02	Versão inicial. Inventário de activos próprios e enquadramento da soberania tecnológica 3HASH.

Revisão **trimestral** pelo Responsável de Cibersegurança. Revisão completa anual em conjunto com a Avaliação de Risco (documento 03).