

**Licenciatura em Segurança Informática  
em Redes de Computadores**

**SGSI**

*Trabalho Prático*

**8230226 - Maria Clara Sameiro**

**8230417 - João Oliveira**

**8230367 - Diogo Batista**

**8210077 - Lécio Almeida**

# Índice

<b>Introdução .....</b>	<b>5</b>
<b>Revisão Bibliográfica.....</b>	<b>6</b>
<b>Caracterização da empresa .....</b>	<b>7</b>
<b>Análise SWOT .....</b>	<b>8</b>
<b>FelgTech.....</b>	<b>9</b>
<b>Internas .....</b>	<b>9</b>
<b>Externas .....</b>	<b>9</b>
<b>Análise Interna e Externa da Empresa .....</b>	<b>10</b>
<b>Análise Interna.....</b>	<b>10</b>
<b>Análise Externa.....</b>	<b>11</b>
<b>Necessidades e Expectativas das Partes Interessadas Relevantes em SI.....</b>	<b>12</b>
<b>Definição do Âmbito do SGSI.....</b>	<b>13</b>
<b>Política de Segurança da Informação.....</b>	<b>14</b>
<b>Objetivos Estratégicos de Segurança da Informação e Metas a Atingir.....</b>	<b>16</b>
<b>Campanhas de Sensibilização em Segurança da Informação .....</b>	<b>17</b>
<b>Política de Classificação da Informação.....</b>	<b>18</b>
<b>Política de Utilização Aceitável de Ativos.....</b>	<b>19</b>
<b>Conclusões .....</b>	<b>20</b>
<b>Bibliografia .....</b>	<b>21</b>

## **Índice de Figuras**

<b>Figura 1 - Organograma FelgTech .....</b>	<b>7</b>
<b>Figura 2 - Análise SWOT .....</b>	<b>8</b>
<b>Figura 3 - Benefícios do SGSI .....</b>	<b>14</b>
<b>Figura 4 - Flayer de sensibilização .....</b>	<b>17</b>
<b>Figura 5 - Outro flayer de sensibilização .....</b>	<b>17</b>

## **Índice de tabelas**

<b>Tabela 1 - Análise Interna .....</b>	<b>11</b>
<b>Tabela 2 - Análise Externa .....</b>	<b>11</b>
<b>Tabela 3 – Necessidades e Expectativas das partes interessadas.....</b>	<b>13</b>

## **Introdução**

Este relatório apresenta o desenvolvimento e implementação do **Sistema de Gestão da Segurança da Informação (SGSI)** na empresa **FelgTech**, em conformidade com a **norma internacional ISO/IEC 27001:2022**. O projeto tem como principal objetivo aplicar, de forma prática e estruturada, os princípios e requisitos de um SGSI, assegurando a **proteção dos ativos de informação**, a **continuidade do negócio** e a **melhoria contínua da cibersegurança organizacional**.

A FelgTech, enquanto empresa tecnológica especializada em **desenvolvimento de software**, **consultoria digital** e **soluções de Internet das Coisas (IoT)**, opera num ambiente altamente competitivo e exposto a riscos crescentes relacionados com a segurança da informação. A proteção de dados sensíveis, a integridade dos sistemas e a confiança dos clientes tornaram-se fatores críticos para a sustentabilidade da organização.

Neste contexto, o projeto visa **analisar o contexto interno e externo da empresa**, **identificar ameaças e vulnerabilidades**, e **definir políticas e objetivos estratégicos** de segurança alinhados com as melhores práticas internacionais. O trabalho inclui a **caracterização da empresa**, uma **análise SWOT**, a **definição do âmbito do SGSI**, bem como a elaboração das principais **políticas internas** — entre as quais se destacam a **Política de Segurança da Informação**, a **Política de Inteligência Artificial**, e as **metas estratégicas de conformidade e resiliência**.

Adicionalmente, o relatório aborda a **sensibilização dos colaboradores** e o desenvolvimento de **campanhas de consciencialização** que reforçam a cultura de segurança dentro da FelgTech. Estas ações visam envolver todas as partes interessadas — colaboradores, clientes, fornecedores e parceiros — num esforço conjunto de proteção da informação, promovendo a **responsabilidade partilhada** e o **cumprimento contínuo da norma ISO/IEC 27001:2022** e do **Regulamento Geral sobre a Proteção de Dados (RGPD)**.

## **Revisão Bibliográfica**

O Sistema de Gestão da Segurança da Informação (SGSI) é um conjunto de políticas e procedimentos que visam proteger os ativos de informação das organizações, assegurando a sua confidencialidade, integridade e disponibilidade (ISO/IEC 27001:2022).

De acordo com autores como Whitman & Mattord (2021), um SGSI eficaz depende não só da tecnologia, mas também da gestão de riscos, da cultura organizacional e da formação contínua.

A adoção da norma ISO/IEC 27001 permite estruturar controlos e medidas que reforçam a resiliência e a conformidade legal das empresas, em particular em contextos tecnológicos complexos como o da FelgTech.

## Caracterização da empresa

A **FelgTech** atua num mercado tecnológico dinâmico, onde a **inovação** e a **segurança da informação** são fundamentais. Reconhecida pela sua experiência em **desenvolvimento de software, consultoria tecnológica e soluções de IoT**, a empresa oferece serviços adaptados às necessidades de cada cliente.

Com uma **estrutura organizacional sólida**, a FelgTech integra departamentos como **Financeiro, Recursos Humanos, Marketing, Vendas, Segurança e Gestão e Desenvolvimento**, garantindo uma gestão eficaz e integrada. A sua **equipa multidisciplinar** reúne profissionais qualificados em diversas áreas, promovendo a **colaboração, a qualidade e a eficiência**.

Localizada na **Avenida Joaquim Silva, Nº 220, 2700-100 Felgueiras, Porto**, a FelgTech posiciona-se como uma **empresa de referência** na área tecnológica, com o apoio de 1000 colaboradores, preparada para enfrentar os desafios de um mercado em constante evolução.

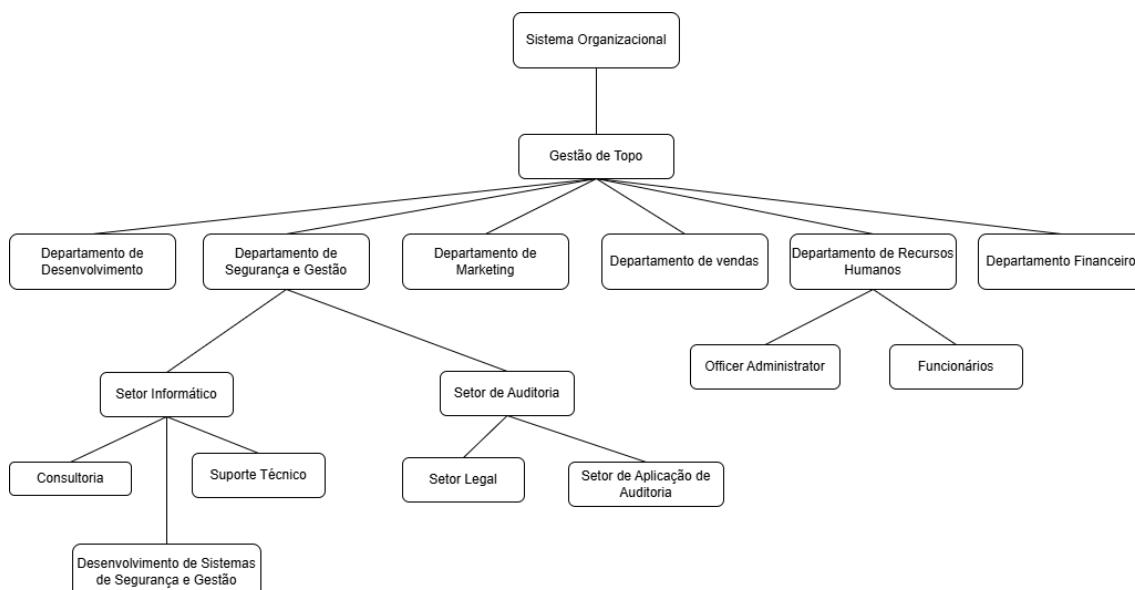


Figura 1 - Organigrama FelgTech

## Análise SWOT

A análise SWOT da FelgTech permite identificar os principais **fatores internos e externos** que influenciam o seu desempenho.

Entre os **pontos fortes**, destacam-se a **equipa técnica especializada** e a **infraestrutura tecnológica moderna**.

Como **fraquezas**, observam-se a **falta de processos formais de gestão de incidentes**, a **dependência de serviços externos** e a **necessidade de sensibilização dos colaboradores** para a segurança da informação.

A nível **externo**, sobressaem a **oportunidade de certificação ISO 27001** e a **ameaça crescente de ataques cibernéticos**.

De forma geral, a FelgTech apresenta uma **base sólida**, mas deve reforçar a **gestão da segurança e resiliência organizacional**.

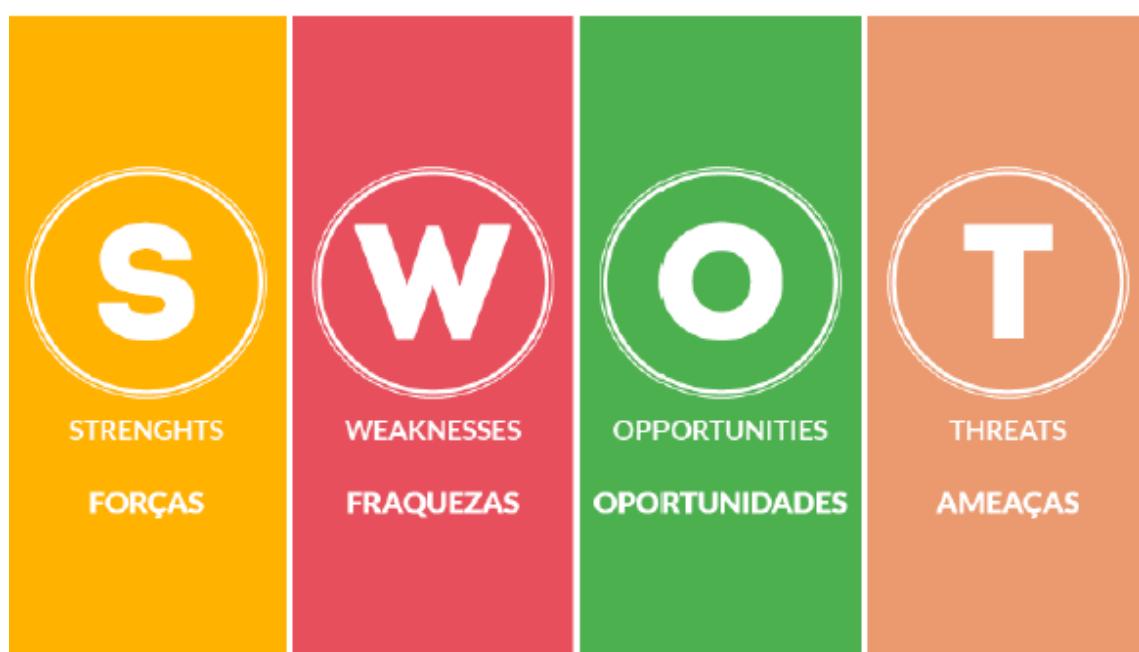


Figura 2 - Análise SWOT

# FelgTech

## *Internas*

### Forças

1. Equipa técnica com elevada qualificação e formação especializada em **segurança informática e da informação**, capaz de conceber e implementar soluções resilientes.
2. **Infraestrutura tecnológica moderna**, com plataformas e ferramentas que suportam desenvolvimento ágil, integração IoT e operações contínuas.
3. Cultura interna orientada para a inovação e melhoria contínua, com capacidade para customizar soluções para clientes empresariais e particulares.

### Fraquezas

1. Ausência de **processos formalizados de gestão de incidentes**, o que limita a resposta coordenada a eventos de segurança.
2. **Dependência significativa de fornecedores e serviços externos**, vulnerabilizando prazos e controlo operacional.
3. Baixo nível de **sensibilização e formação contínua dos colaboradores** em práticas de segurança da informação e higiene digital.

## *Externas*

### Oportunidades

1. Interesse e oportunidade estratégica em obter **certificação ISO/IEC 27001**, que pode diferenciar a empresa no mercado e abrir portas a contratos com clientes com requisitos de compliance.
2. Crescente procura por soluções IoT seguras por parte de setores industriais e serviços, criando linhas de receita para produtos com foco em cibersegurança.

### Ameaças

1. **Aumento contínuo da sofisticação e frequência de ataques cibernéticos**, incluindo ransomware e compromissos de cadeia de fornecimento.
2. Riscos reputacionais e comerciais associados a incumprimentos de segurança ou falhas na proteção de dados de clientes.
3. **Evolução constante das exigências legais e normativas** em matéria de proteção de dados e segurança da informação, podendo gerar **custos acrescidos de conformidade** e necessidade de **adaptação contínua dos sistemas e processos internos**.

## Análise Interna e Externa da Empresa

Com a análise SWOT, torna-se mais simples realizar uma avaliação interna e externa da empresa.

Na análise interna, é possível compreender e controlar melhor o que acontece dentro da organização, identificando os pontos fortes e fracos em aspectos como a tecnologia utilizada, a localização, a estrutura organizacional, os acessos e os recursos humanos (colaboradores).

### Análise Interna

Área	Questão	Aspecto da Segurança da Informação (SI)
Tecnologia	A infraestrutura tecnológica da empresa é moderna e suporta operações ágeis e contínuas.	A tecnologia atual permite elevada disponibilidade e redundância, reforçando a continuidade do negócio e a resiliência dos sistemas. Contudo, deve ser mantida e atualizada para prevenir vulnerabilidades emergentes.
Colaboradores	A equipa técnica é altamente qualificada, mas há falta de sensibilização geral sobre segurança da informação.	A existência de uma equipa especializada é uma vantagem competitiva; porém, é necessário reforçar a formação e consciencialização contínua em cibersegurança, promovendo uma cultura organizacional segura.
Estrutura Organizacional	Estrutura bem definida, mas ausência de processos formais de gestão de incidentes.	A empresa apresenta uma estrutura sólida que facilita a comunicação entre departamentos, mas deve implementar procedimentos de resposta a incidentes e planos de contingência documentados.
Acessos e Controlo Interno	Falta de uniformização de políticas de acesso e gestão de credenciais.	É essencial aplicar o princípio do menor privilégio, com controlo de acessos baseado em funções (RBAC), registos de auditoria e autenticação multifator (MFA), garantindo a integridade e confidencialidade da informação.
Localização e Infraestrutura Física	Sede única em Felgueiras, o que centraliza recursos tecnológicos e humanos.	A localização física permite uma gestão centralizada de recursos, mas requer políticas de segurança física, controlo de visitantes e monitorização de ambientes críticos (como servidores).
Parcerias e Dependências	Dependência significativa de serviços externos e fornecedores de cloud.	Embora permita escalabilidade e eficiência, esta dependência aumenta o risco de exposição de dados e falhas de terceiros; é necessário definir contratos com cláusulas de segurança e SLA rigorosos.

<b>Cultura Organizacional</b>	Foco na inovação e na melhoria contínua.	Uma cultura orientada para a inovação facilita a adoção de boas práticas de segurança, promovendo o <b>equilíbrio entre criatividade e conformidade</b> , com políticas claras e comunicadas a todos os níveis.
-------------------------------	--	---

Tabela 1 - Análise Interna

### Análise Externa

Área	Questão	Aspecto da Segurança da Informação (SI)
<b>Fornecedores</b>	Dependência de múltiplos serviços externos de cloud e software.	É fundamental avaliar <b>riscos na cadeia de fornecimento</b> , assegurando que parceiros cumprem requisitos de <b>segurança, confidencialidade e continuidade de serviço</b> , reduzindo vulnerabilidades externas.
<b>Mercado e Clientes</b>	Crescente procura por soluções seguras e certificadas (ex.: ISO 27001).	A certificação e o cumprimento de normas internacionais fortalecem a <b>credibilidade e competitividade</b> da empresa, gerando novas oportunidades e fidelizando clientes.
<b>Leis e Regulamentações</b>	Exigências legais em constante evolução (ex.: RGPD, ISO/IEC 27001).	É necessário manter <b>conformidade legal e normativa</b> , atualizando políticas e controlos internos. O incumprimento pode gerar <b>multas, sanções e danos reputacionais</b> .
<b>Tendências Tecnológicas</b>	Expansão das soluções IoT e aumento dos riscos associados.	A crescente digitalização cria oportunidades de inovação, mas também expõe a empresa a <b>novas vulnerabilidades</b> . É essencial investir em <b>segurança de IoT, encriptação e monitorização ativa</b> .
<b>Ameaças Cibernéticas</b>	Aumento da sofisticação e frequência de ataques (ransomware, phishing, supply chain).	Requer implementação de <b>mecanismos avançados de deteção e resposta (EDR, SOC, SIEM)</b> , testes de intrusão regulares e <b>planos de recuperação</b> para garantir continuidade operacional.
<b>Reputação e Imagem</b>	Riscos de danos reputacionais associados a falhas de segurança.	A confiança dos clientes depende da <b>transparência e da robustez das medidas de segurança</b> . Um incidente pode afetar gravemente a imagem da empresa, tornando crucial um <b>plano de comunicação de crise</b> .

Tabela 2 - Análise Externa

## Necessidades e Expectativas das Partes Interessadas Relevantes em SI

A identificação das **necessidades e expectativas das partes interessadas** é fundamental para a eficácia da **Segurança da Informação** na FelgTech. Este processo permite compreender os requisitos e preocupações de **colaboradores, clientes, fornecedores, utilizadores finais e parcerias**, assegurando que a empresa responde de forma adequada às suas exigências.

A FelgTech avalia a sua **capacidade organizacional** para atender a essas necessidades e define **ações específicas** a implementar, com **responsabilidades atribuídas** aos diferentes departamentos, garantindo a **proteção da informação** e a **conformidade com as boas práticas e normas de segurança**.

Partes Interessadas	Necessidades	Expectativas	Capacidade da Organização	Ação a Implementar	Responsável
Colaboradores	Formação contínua em segurança da informação e boas práticas digitais.	Ter acesso a recursos atualizados, políticas claras e um ambiente de trabalho seguro e colaborativo.	Sim	Implementar programas regulares de <b>formação e sensibilização em cibersegurança</b> , comunicação interna de políticas e incentivos à melhoria contínua.	DRH / DSG
Clientes	Soluções tecnológicas seguras, fiáveis e adaptadas às suas necessidades.	Garantia de <b>proteção dos dados</b> , cumprimento de <b>prazos e transparência nos serviços</b> prestados.	Sim	Reforçar contratos de <b>níveis de serviço (SLA)</b> , auditorias regulares e certificações (ex.: <b>ISO/IEC 27001</b> ).	DV / DSG
Fornecedores	Processos claros de contratação e comunicação eficiente.	Relação de <b>confiança, cumprimento de prazos de pagamento e partilha de requisitos de segurança</b> .	Não totalmente	Implementar uma <b>política de gestão de fornecedores</b> , avaliando o cumprimento de normas de segurança e definindo <b>acordos de confidencialidade (NDA)</b> .	DF / DSG
Utilizadores Finais	Acesso a produtos e serviços intuitivos, funcionais e seguros.	Experiência de utilização fluida, <b>suporte técnico eficaz e proteção dos dados pessoais</b> .	Sim	Melhorar os <b>testes de segurança e usabilidade</b> antes do lançamento dos produtos; reforçar canais de <b>suporte técnico</b> .	DD / SI

<b>Parcerias</b>	Cooperação estratégica e troca de conhecimento técnico.	<b>Transparência, inovação conjunta e benefícios mútuos em projetos tecnológicos.</b>	Sim	Formalizar acordos de colaboração tecnológica, definir requisitos mínimos de segurança e reuniões de alinhamento regulares.	<b>DG / DSG</b>
------------------	---	---	-----	---	-----------------

*Tabela 3 – Necessidades e Expectativas das partes interessadas*

#### **Legenda das Siglas de Responsáveis**

- **DG** – Direção Geral / Gestão de Topo
- **DF** – Departamento Financeiro
- **DRH** – Departamento de Recursos Humanos
- **DV** – Departamento de Vendas
- **DD** – Departamento de Desenvolvimento
- **DSG** – Departamento de Segurança e Gestão
- **SI** – Setor Informático

## **Definição do Âmbito do SGSI**

**Sistema de Gestão da Segurança da Informação (SGSI)** da FelgTech abrange todos os **processos, sistemas, ativos e recursos** relacionados com o **desenvolvimento, implementação e gestão de software, consultoria tecnológica e soluções de Internet das Coisas (IoT)**.

Este sistema tem como propósito assegurar que todas as **informações processadas, armazenadas ou transmitidas** pela organização são devidamente **protegidas quanto à sua confidencialidade, integridade e disponibilidade**.

O SGSI aplica-se a **todas as áreas organizacionais**, incluindo **infraestruturas tecnológicas, plataformas de software, recursos humanos, parceiros, fornecedores e clientes**, que participam direta ou indiretamente nas operações da FelgTech. Engloba também os **ambientes físicos e digitais, os sistemas de suporte, as redes internas e externas**, bem como os **serviços em cloud** utilizados pela empresa.

O principal objetivo deste âmbito é **garantir a continuidade do negócio, minimizar riscos associados a incidentes de segurança** e assegurar o **cumprimento das normas, requisitos legais e contratuais aplicáveis**, nomeadamente os definidos na **ISO/IEC 27001** e no **Regulamento Geral de Proteção de Dados (RGPD)**.

Através deste sistema, a FelgTech reforça o seu compromisso com a **proteção da informação, a melhoria contínua dos controlos de segurança e a confiança dos seus clientes e parceiros**, sustentando a sua posição como **referência em inovação e segurança tecnológica**.

## FelgTech – ISO 27001

### Benefícios do SGSI



Figura 3 - Benefícios do SGSI

## Política de Segurança da Informação

### 1. Objetivo

A presente Política de Segurança da Informação tem como objetivo expressar o compromisso da FelgTech com a proteção da informação, garantindo a sua confidencialidade, integridade e disponibilidade, bem como o cumprimento das normas legais, regulamentares e contratuais aplicáveis.

### 2. Âmbito

Esta política aplica-se a todos os colaboradores, prestadores de serviços, parceiros, fornecedores e terceiros que tenham acesso à informação, sistemas ou infraestruturas tecnológicas da FelgTech.

### **3. Compromissos da FelgTech em matéria de Segurança da Informação**

A FelgTech compromete-se a:

- Proteger a informação contra o acesso, uso, modificação, divulgação ou destruição não autorizados, assegurando que apenas é acedida por pessoas e sistemas devidamente credenciados.
- Garantir a conformidade legal e normativa, cumprindo integralmente o Regulamento Geral de Proteção de Dados (RGPD), a norma ISO/IEC 27001 e outras legislações e requisitos contratuais aplicáveis.
- Gerir riscos e incidentes de forma proativa, assegurando a identificação, avaliação e mitigação contínua de ameaças, bem como uma resposta rápida e eficaz sempre que ocorra um incidente de segurança.
- Promover uma cultura de segurança, sensibilizando e formando todos os colaboradores e parceiros sobre boas práticas e responsabilidades no uso da informação e dos sistemas.
- Assegurar o desenvolvimento e operação seguros dos sistemas e aplicações, aplicando princípios de Security by Design e Secure Coding desde as fases iniciais dos projetos.
- Garantir a melhoria contínua do Sistema de Gestão da Segurança da Informação (SGSI), através da revisão periódica de políticas, procedimentos e controlos, assegurando a sua adequação às mudanças tecnológicas, organizacionais e legais.
- Disponibilizar os recursos necessários para a implementação eficaz desta política e para a manutenção dos níveis de segurança definidos.

### **4. Responsabilidades**

- Gestão de Topo: aprova, patrocina e garante os recursos necessários à implementação e melhoria do SGSI.
- Departamento de Segurança e Gestão (DSG): coordena a execução, monitorização e revisão desta política.
- Colaboradores, parceiros e fornecedores: devem cumprir todas as normas, procedimentos e orientações de segurança da informação definidas pela FelgTech.
- Encarregado de Proteção de Dados (DPO): assegura o cumprimento do RGPD e supervisiona o tratamento de dados pessoais.

### **5. Revisão e Divulgação**

Esta política é revista anualmente ou sempre que ocorram alterações relevantes no contexto tecnológico, organizacional ou legal.

A versão atualizada é aprovada pela Gestão de Topo, assinada digitalmente e divulgada através dos canais internos de comunicação, garantindo que todos os colaboradores têm conhecimento e acesso à mesma.

## **Política de Inteligência Artificial (IA)**

- Qualquer sistema de IA deve ser **avaliado quanto a riscos de segurança, privacidade e viés algorítmico**.
- A tomada de decisão automatizada deve ser **auditável e supervisionada por um humano responsável**.
- É proibida a utilização de IA que envolva **dados pessoais sensíveis sem consentimento explícito**.
- Os projetos de IA devem seguir os princípios de **transparência, ética e proteção de dados**.

## **Objetivos Estratégicos de Segurança da Informação e Metas a Atingir**

A FelgTech define os seguintes **objetivos estratégicos de Segurança da Informação**, alinhados com a sua missão, visão e os requisitos da norma **ISO/IEC 27001**, garantindo a proteção contínua dos seus ativos de informação e a melhoria permanente do **SGSI**.

### **1. Reforçar a Resiliência e a Continuidade Operacional**

A empresa compromete-se a implementar **controlos preventivos e planos de recuperação** que assegurem a continuidade do negócio e minimizem o impacto de incidentes.  
As metas associadas incluem garantir que **100% dos sistemas críticos** possuem **planos de backup e recuperação testados trimestralmente** e **reduzir o tempo médio de recuperação (RTO) em 20% no prazo de um ano**.

### **2. Aumentar a Consciencialização e Formação em Segurança**

A FelgTech promove uma **cultura de segurança sólida** em toda a organização, envolvendo colaboradores e parceiros.  
Como metas, pretende **realizar duas formações anuais obrigatórias** em cibersegurança e alcançar **uma taxa mínima de 90% de participação** dos colaboradores.

### **3. Garantir a Conformidade Legal e Normativa**

A empresa assegura o **cumprimento rigoroso** da **ISO/IEC 27001**, do **RGPD** e de outros requisitos legais e contratuais aplicáveis.  
Os objetivos passam por **eliminar não conformidades críticas** nas auditorias internas e **alcançar a certificação ISO/IEC 27001** até ao final do ciclo de implementação.

### **4. Integrar Segurança desde a Concepção (Security by Design)**

A FelgTech compromete-se a integrar princípios de segurança no **ciclo de vida de todos os projetos de software e IoT**, garantindo a proteção desde a fase inicial de desenvolvimento.  
As metas incluem assegurar que **100% dos novos projetos** passam por **revisão de segurança antes da implementação** e **reduzir em 30% as vulnerabilidades identificadas** nos testes de penetração.

## Campanhas de Sensibilização em Segurança da Informação

Com o objetivo de **reforçar a consciencialização** dos colaboradores relativamente aos riscos cibernéticos, a FelgTech implementou **campanhas de sensibilização em segurança da informação**. Estas iniciativas visam **promover boas práticas**, incentivar **mudanças comportamentais** e destacar a **importância das ações individuais na prevenção de incidentes de segurança**.



Figura 4 - Flayer de sensibilização



Figura 5 - Outro flayer de sensibilização

## **Política de Classificação da Informação**

A **Política de Classificação da Informação** da FelgTech estabelece as diretrizes para **identificar, classificar, proteger e gerir** a informação produzida, recebida ou armazenada pela organização, garantindo a **confidencialidade, integridade e disponibilidade** dos dados ao longo de todo o seu ciclo de vida.

Esta política aplica-se a **todos os colaboradores, prestadores de serviços, parceiros e fornecedores** com acesso à informação da FelgTech, abrangendo **todos os ambientes tecnológicos, físicos e digitais**, incluindo **infraestruturas locais, serviços em cloud e dispositivos IoT**.

A **Gestão de Topo** aprova e supervisiona a política, enquanto o **Departamento de Segurança e Gestão (DSG)** assegura a sua execução, monitorização e auditoria. O **Encarregado de Proteção de Dados (DPO)** garante a conformidade com o **RGPD** no tratamento de dados pessoais.

A informação é classificada em **quatro níveis de sensibilidade**, que determinam o grau de proteção e os controlos aplicáveis:

- **Informação Pública:** aplicável a conteúdos destinados ao público externo (ex.: website, materiais institucionais). Pode ser divulgada livremente.
- **Informação Interna:** aplicável a processos e comunicações de uso interno (ex.: políticas, procedimentos). Acesso restrito a colaboradores.
- **Informação Confidencial:** aplicável a dados empresariais e de clientes (ex.: contratos, relatórios técnicos, dados financeiros). Acesso limitado a equipas autorizadas, com encriptação e controlo de acesso.
- **Informação Restrita:** aplicável a dados altamente sensíveis (ex.: dados pessoais, credenciais, código-fonte, chaves de encriptação). Acesso exclusivo a responsáveis designados; armazenamento em sistemas segregados e encriptados.

Todos os utilizadores devem **etiquetar, armazenar e transmitir a informação** de acordo com o nível de classificação atribuído, respeitando o princípio do “**necessário saber**” e utilizando apenas **canais de comunicação e armazenamento seguros**.

Esta política é **revista anualmente** ou sempre que haja alterações tecnológicas, legais ou operacionais, e está **integrada com as políticas de Segurança da Informação, Proteção de Dados, Utilização de Ativos e Inteligência Artificial**, reforçando o compromisso da FelgTech com a **segurança, conformidade e responsabilidade digital**.

## **Política de Utilização Aceitável de Ativos**

A **Política de Utilização Aceitável de Ativos (PUAA)** da **FelgTech** define as regras para o **uso responsável e seguro dos ativos de informação**, assegurando a conformidade com a **Política de Segurança da Informação**, a **Política de Classificação da Informação** e a norma **ISO/IEC 27001:2022**. Esta política aplica-se a **todos os colaboradores, prestadores de serviços, parceiros e fornecedores** com acesso a recursos da empresa, incluindo **equipamentos, sistemas, redes, aplicações, dados e infraestruturas tecnológicas**.

O seu **objetivo** é garantir que os ativos são utilizados de forma **ética, controlada e alinhada com as boas práticas de segurança**, prevenindo incidentes, perdas de informação e uso indevido.

A **Gestão de Topo** aprova e supervisiona esta política, enquanto o **Departamento de Segurança e Gestão (DSG)** assegura a sua aplicação, monitorização e auditoria. Todos os utilizadores são responsáveis por seguir as normas internas e **reportar imediatamente incidentes de segurança**.

A política abrange a utilização de **ativos físicos e digitais**, definindo as seguintes regras gerais:

- Os recursos devem ser usados **exclusivamente para fins profissionais**.
- O **acesso à informação** deve respeitar o **nível de classificação atribuído** (Pública, Interna, Confidencial ou Restrita).
- É obrigatória a utilização de **credenciais individuais e autenticação multifator (MFA)** para acesso a sistemas críticos.
- Dados **Confidenciais e Restritos** devem ser **criptados e armazenados em ambientes protegidos**.
- É proibido o uso de **software não autorizado** ou de **aplicações externas sem validação de segurança**.
- Qualquer perda, roubo ou dano de dispositivos deve ser **comunicado imediatamente ao DSG**.

O **não cumprimento** das regras desta política pode resultar em **ações disciplinares, suspensão de acessos ou medidas legais**, sendo todas as ocorrências registadas no **Sistema de Gestão de Incidentes (SGI)**.

A política é **revista anualmente** ou sempre que ocorram alterações significativas nos sistemas, processos ou contexto tecnológico, e está diretamente relacionada com as políticas de **Segurança da Informação, Classificação da Informação, Proteção de Dados, Gestão de Incidentes e Inteligência Artificial**, reforçando o compromisso da **FelgTech** com a **cibersegurança e a integridade dos seus ativos digitais**.

## **Conclusões**

A implementação do SGSI na FelgTech representa um passo estratégico essencial para reforçar a proteção dos ativos de informação e a confiança dos seus clientes e parceiros.

Através da adoção das normas ISO/IEC 27001:2022 e da definição de políticas claras, a empresa consolidou práticas de segurança, mitigou riscos e melhorou a sua capacidade de resposta a incidentes.

O envolvimento dos colaboradores, a formação contínua e o compromisso da Gestão de Topo são fatores críticos para o sucesso e sustentabilidade do sistema.

Assim, a FelgTech posiciona-se como uma organização tecnologicamente segura, inovadora e preparada para enfrentar os desafios da cibersegurança.

## Bibliografia

- ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.*
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.
- Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
- European Union (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho -RGPD.*