P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

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

1. Introdução

A segurança da informação representa um dos pilares fundamentais para a sustentabilidade e competitividade das organizações tecnológicas. No caso da **FelgTech**, empresa dedicada ao desenvolvimento de software, consultoria digital e soluções IoT, a proteção dos ativos de informação é essencial para garantir confiança, disponibilidade dos serviços, conformidade legal e continuidade do negócio.

Este segundo trabalho prático tem como objetivo aprofundar a implementação do Sistema de Gestão de Segurança da Informação (SGSI), com foco específico na **gestão de riscos**, conforme os requisitos definidos na ISO/IEC 27001:2022, nomeadamente o Requisito 6 - Planeamento.

Neste relatório serão apresentados:

- a metodologia de avaliação de riscos adotada pela organização,
- o inventário de ativos,
- a identificação, análise, avaliação e priorização dos riscos,
- as opções de tratamento dos riscos,
- e a Declaração de Aplicabilidade (DA), alinhada com o Anexo A da norma.

Este trabalho complementa o primeiro projeto desenvolvido na UC, permitindo que a FelgTech avance para um SGSI mais robusto, estruturado e alinhado com as melhores práticas internacionais.

2. Revisão Bibliográfica

A Segurança da Informação tem-se afirmado como um domínio crítico para as organizações modernas, especialmente num contexto de crescente digitalização, globalização dos serviços e sofisticação das ameaças cibernéticas. Diversos autores e entidades normativas destacam que a proteção da informação deve ser tratada como um processo sistemático, contínuo e alinhado com a estratégia organizacional (Whitman & Mattord, 2021; ISO/IEC, 2022).

2.1. Conceito de Segurança da Informação e SGSI

A Segurança da Informação é tradicionalmente compreendida através dos seus três princípios fundamentais - **Confidencialidade, Integridade e Disponibilidade (CIA)**, que asseguram que a informação permanece acessível apenas por entidades autorizadas, mantém-se completa e exata, e está disponível sempre que necessário (ISO/IEC 27000).

Um **Sistema de Gestão de Segurança da Informação (SGSI)**, segundo a ISO/IEC 27001:2022, é definido como um conjunto de políticas, processos, procedimentos, recursos e tecnologias interligados com o objetivo de gerir, controlar e melhorar continuamente a segurança da informação. O SGSI não é apenas um conjunto de medidas técnicas, mas um **mecanismo de governação**, articulado com a missão, visão e objetivos estratégicos da organização. A norma ISO destaca que o SGSI deve enquadrar a gestão da segurança como um **processo racional**, baseado em risco e integrado na gestão corporativa.

2.2 Abordagem Baseada no Risco

A ISO/IEC 27001 estrutura-se sobre uma filosofia essencial: a **gestão de risco** como base da tomada de decisão. De acordo com a ISO 31000 (gestão de risco), os riscos são definidos como o “efeito da incerteza sobre os objetivos”. No contexto da segurança da informação, os riscos emergem da possibilidade de **ameaças explorarem vulnerabilidades**, causando impacto negativo na organização.

O processo de gestão de riscos para um SGSI segue tipicamente as etapas:

1. **Identificação de ativos, ameaças, vulnerabilidades e cenários de risco**
2. **Análise de risco**, considerando probabilidade e impacto
3. **Avaliação de risco**, comparando com critérios de aceitabilidade
4. **Tratamento de risco**, selecionando medidas de controlo adequadas
5. **Monitorização e melhoria continua**

A norma ISO/IEC 27005 (gestão de risco em SI) reforça a necessidade de um método estruturado que assegure consistência, repetibilidade e rastreabilidade, permitindo comparar resultados ao longo do tempo.

2.3 Importância dos Ativos de Informação

Um dos pilares fundamentais da gestão de riscos é o **inventário de ativos**. Para autores como Von Solms & Van Niekerk (2013), os ativos de informação devem ser entendidos não apenas como elementos tecnológicos, mas como uma hierarquia que abrange:

- Informação (dados, relatórios, bases de dados)
- Software (aplicações, código-fonte, sistemas internos)
- Hardware (servidores, estações de trabalho, IoT)
- Pessoas (colaboradores, utilizadores, fornecedores)
- Processos (procedimentos, fluxos críticos)
- Instalações (salas, datacenters, edifícios)

A ISO 27001 reforça que cada ativo deve ter um **proprietário**, responsável pela sua proteção e conformidade.

2.4 Ameaças, Vulnerabilidades e Cenários de Risco

A identificação de riscos exige compreender três vetores fundamentais:

- **Ameaças**: eventos potencialmente prejudiciais (ex.: ransomware, acesso não autorizado, erro humano)
- **Vulnerabilidades**: fragilidades que podem ser exploradas (ex.: falta de MFA, servidores desatualizados, políticas inexistentes)
- **Cenários de risco**: a forma como a ameaça pode explorar a vulnerabilidade e causar impacto

Esta abordagem é apoiada por métodos como OCTAVE, NIST RMF e EBIOS, todos reconhecidos internacionalmente.

A literatura aponta que o erro humano é responsável por mais de 80% dos incidentes de cibersegurança, reforçando a importância dos controlos organizacionais e comportamentais, não apenas tecnológicos.

2.5 Matriz de Probabilidade e Impacto

A avaliação de riscos requer a atribuição de uma probabilidade de ocorrência (NP) e um impacto associado (NI). Modelos como o NIST SP 800-30 sugerem escalas de 3, 4 ou 5 níveis. A combinação destes fatores gera o **nível de risco**, frequentemente calculado como:

Risco = NP × NI

A matriz de risco permite:

- Identificar prioridades

- Apoiar decisões de gestão
- Definir riscos aceitáveis e não aceitáveis

2.6 Tratamento de Riscos e Controlo

A ISO 27001 define quatro estratégias padrão:

- **Mitigar**: reduzir o risco através de controlos (Ex.: firewall, MFA, encriptação)
- **Transferir**: passar parte do risco para terceiros (Ex.: seguros, outsourcing)
- **Aceitar**: admitir o risco quando está dentro do nível aceitável
- **Evitar**: eliminar a atividade que gera o risco

O conjunto de controlos encontra-se no **Anexo A – 93 controlos**, reorganizados em 2022 pelas categorias:

- Organizacionais
- Pessoas
- Físicos
- Tecnológicos

A literatura sublinha que o tratamento deve ser proporcional, eficiente e economicamente racional (Sonnenreich, 2006).

2.7 Importância da Declaração de Aplicabilidade (SoA)

A Declaração de Aplicabilidade (DA) é um documento nuclear do SGSI, pois estabelece:

- Que controlos ISO 27001 são aplicáveis
- Quais são implementados ou não
- Justificação para inclusões e exclusões
- Evidências associadas

2.8 Importância Estratégica para Organizações Tecnológicas

Para organizações como a FelgTech, com foco em IoT e desenvolvimento de software, a segurança da informação não é apenas um requisito operacional, mas um **elemento diferenciador de competitividade**, influenciando:

- confiança dos clientes
- conformidade com RGPD
- resiliência operacional
- reputação
- continuidade do negócio

A literatura é clara: empresas que adotam SGSI estruturados reduzem significativamente o impacto de incidentes, aumentam a maturidade e competem de forma mais sustentável.

3. Metodologia

Para a implementação do SGSI na FelgTech, foi adotada uma abordagem estruturada e alinhada com as recomendações da ISO/IEC 27001:2022 e ISO/IEC 27005 (gestão de riscos). A metodologia utilizada segue as seguintes fases:

1. **Definição da Metodologia de Avaliação de Risco:** Estabelecimento de critérios de probabilidade, impacto e aceitabilidade, com escalas de 1 a 4, alinhadas com a realidade operacional da organização.
2. **Inventário de Ativos**: Identificação e catalogação de todos os ativos críticos, incluindo hardware, software, pessoas, informação, processos e infraestruturas físicas.
3. **Identificação de Riscos**: Análise de ameaças, vulnerabilidades e cenários de risco associados a cada ativo, considerando contexto interno e externo.
4. **Análise e Avaliação de Riscos:** Cálculo do nível de risco através da fórmula Risco = Probabilidade × Impacto, considerando os três pilares da segurança (Confidencialidade, Integridade e Disponibilidade).
5. **Priorização e Tratamento**: Definição de opções de tratamento (mitigar, aceitar, transferir, evitar) com base na criticidade dos riscos identificados.
6. **Construção da Declaração de Aplicabilidade**: Mapeamento dos controlos do Anexo A da ISO 27001 aplicáveis à organização, com justificação para inclusões e exclusões.

Esta abordagem garante que a gestão de riscos seja sistemática, documentada e continuamente melhorada, permitindo decisões informadas e alinhadas com os objetivos estratégicos da FelgTech.

4. Resultados

Os resultados deste trabalho incluem a documentação estruturada de todos os elementos essenciais para um SGSI robusto e conforme com a ISO/IEC 27001:2022. Os principais entregáveis são:

4.1. Inventário de Ativos

Foi criado um inventário completo com 10 ativos críticos, categorizados por tipo (software, hardware, pessoas, informação, infraestrutura e serviços subcontratados). Cada ativo foi caracterizado e atribuído a um responsável específico, garantindo accountability.

4.2. Análise de Riscos

Foram identificados e analisados múltiplos cenários de risco para cada ativo, considerando ameaças como malware, acessos não autorizados, falhas de hardware, erro humano e vulnerabilidades técnicas. A análise incluiu:

1. Cálculo do nível de probabilidade (escala 1-4)
2. Avaliação do impacto em Confidencialidade, Integridade e Disponibilidade (escala 1- 4)
3. Determinação do nível de risco global (NP × NI)
4. Classificação da aceitabilidade (Aceitável, Admissível, Inadmissível, Crítico)

4.3. Tratamento de Riscos

Para cada risco identificado, foram selecionados controlos específicos do Anexo A da ISO 27001, incluindo medidas organizacionais (consciencialização, gestão de acessos), técnicas (antivírus, encriptação, backup) e físicas (proteção de instalações). A estratégia de tratamento privilegia a mitigação através de controlos proporcionais e eficazes.

4.4. Declaração de Aplicabilidade

Foi construída a Declaração de Aplicabilidade (Statement of Applicability - SoA), documentando todos os controlos do Anexo A aplicáveis à FelgTech. Para cada controlo foi indicado:

1. Se está implementado ou não
2. Justificação para inclusão
3. Evidências documentadas associadas

Esta SoA serve como base para auditorias futuras e demonstra o compromisso da organização com a segurança da informação.

5. Conclusão

Este trabalho permitiu consolidar a implementação do Sistema de Gestão de Segurança da Informação (SGSI) da FelgTech, com particular enfoque na gestão de riscos conforme o Requisito 6 da ISO/IEC 27001:2022. Através de uma abordagem estruturada e baseada em boas práticas internacionais, foi possível:

- Identificar e catalogar os ativos críticos da organização, garantindo visibilidade e responsabilização sobre os recursos que suportam o negócio.
- Implementar uma metodologia de avaliação de riscos clara, replicável e alinhada com a realidade operacional da FelgTech, permitindo decisões informadas e proporcionais.
- Analisar sistematicamente ameaças, vulnerabilidades e cenários de risco, priorizando intervenções através de critérios objetivos de probabilidade e impacto.
- Definir estratégias de tratamento de risco adequadas, selecionando controlos do Anexo A da ISO 27001 que equilibram segurança, custo e operacionalidade.
- Construir a Declaração de Aplicabilidade, estabelecendo um mapa completo dos controlos implementados e justificando decisões de segurança para stakeholders e auditores.

Os resultados obtidos demonstram que a FelgTech está a evoluir para um nível de maturidade superior em segurança da informação, com processos documentados, riscos identificados e controlos implementados de forma racional. Este trabalho não só reforça a conformidade com a ISO 27001, como também contribui para:

1. Redução da exposição a incidentes de segurança
2. Aumento da confiança de clientes e parceiros
3. Conformidade com requisitos legais e contratuais (RGPD, SLAs)
4. Melhoria contínua da postura de segurança organizacional

No entanto, é fundamental reconhecer que a segurança da informação é um processo contínuo. Recomenda-se que a FelgTech:

1. Realize revisões periódicas do inventário de ativos e da análise de riscos, adaptando-se a novas ameaças e mudanças no contexto organizacional.
2. Implemente programas de formação e consciencialização contínua para colaboradores, dado que o erro humano continua a ser uma das principais causas de incidentes.
3. Monitorize continuamente a eficácia dos controlos implementados, ajustando estratégias conforme necessário.
4. Prepare-se para auditorias internas e externas, mantendo evidências atualizadas e rastreáveis.

Em conclusão, este projeto representa um marco significativo na jornada da FelgTech para um SGSI robusto e resiliente. A metodologia adotada, os processos implementados e a documentação produzida constituem uma base sólida para a certificação ISO 27001 e para a proteção sustentável dos ativos de informação da organização.

6. Referências Bibliográficas

ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. International Organization for Standardization.

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization.

ISO 31000:2018. Risk management — Guidelines. International Organization for Standardization.

NIST SP 800-30 Rev. 1 (2012). Guide for Conducting Risk Assessments. National Institute of Standards and Technology. Disponível em: https://csrc.nist.gov/pubs/sp/800/30/r1/final

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment (ROSI): A Practical Quantitative Model. Journal of Research and Practice in Information Technology, 38(1).

Verizon. (2024). Data Breach Investigations Report. Verizon Business.

World Economic Forum. (2024). Global Cybersecurity Outlook. Disponível em: https://www.weforum.org

SC World. (2024). Human error contributes to nearly all cyber incidents, study finds. Disponível em: https://www.scworld.com/news/human-error-contributes-to-nearly-all-cyber-incidents-study-finds

ENISA. (2024). Threat Landscape Report. European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu