CIÊNCIAS EMPRESARIAIS
ESCOLA SUPERIOR
POLITÉCNICO SETÚBAL

RICARDO FILIPE PINTO DO CARMO RODRIGUES

IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (ISO/IEC 27001) NUMA PME

Relatório de projeto do Mestrado em

Gestão de Sistemas de Informação

ORIENTADOR

(Prof. João Assis Barbas)

outubro 2024

AGRADECIMENTOS

Gostaria de expressar a minha profunda gratidão a todos aqueles que contribuíram, direta ou indiretamente, para a realização deste trabalho e deste percurso.

Em primeiro lugar, dirijo os meus agradecimentos ao meu orientador, Prof. João Assis Barbas, pela orientação e pelo incentivo ao longo de cada etapa deste projeto. A sua experiência e disponibilidade foram essenciais para a realização deste trabalho, e é com grande apreço que reconheço a importância do seu apoio.

Não poderia deixar de agradecer ao CEO da Besturban, Nuno Correia, que se disponibilizou a colaborar e permitiu a realização desta pesquisa, fornecendo-me dados e suporte. Aos colaboradores e demais responsáveis da empresa, deixo o meu sincero obrigado pela confiança e pela partilha de conhecimento, elementos fundamentais para que este estudo pudesse avançar.

Aos meus amigos e colegas de curso, pelo companheirismo, troca de ideias e incentivo, deixo também uma palavra de apreço. Foram momentos de partilha e de crescimento conjunto que tornaram este caminho mais leve e significativo.

Agradeço à minha família, com especial destaque para a minha mulher, Carlota. Foi ela quem me impulsionou e motivou a iniciar o mestrado e, ao longo de todo o percurso, esteve ao meu lado como a minha maior fonte de força e inspiração, especialmente nos momentos mais desafiantes. Nos momentos em que surgiram desafios e o certo se tornou incerto, encontrei no seu apoio constante e nas suas palavras de encorajamento o alicerce necessário para prosseguir. Aos meus filhos, que pacientemente compreenderam as minhas ausências e que, com o seu amor, me deram ainda mais razões para persistir, deixo igualmente o meu agradecimento mais profundo.

Por fim, a todos os que, de alguma forma, estiveram presentes ao longo deste percurso, o meu sincero obrigado.

RESUMO

Este trabalho de projeto explora a implementação de um Sistema de Gestão da Segurança da Informação (SGSI) baseado na norma ISO/IEC 27001 na BestUrban, uma Pequena e Média Empresa (PME) portuguesa. O SGSI desempenha um papel crucial na proteção dos ativos de informação da empresa.

O principal objetivo deste estudo é avaliar a eficácia da implementação do SGSI, identificar desafios e oportunidades e analisar o impacto dessa iniciativa na postura geral de segurança da informação da empresa. Para tal, foram avaliadas as práticas de segurança da informação da BestUrban antes da implementação da ISO/IEC 27001, documentado o processo de implementação e destacados os principais marcos e decisões estratégicas.

A implementação do SGSI demonstrou um compromisso sólido com a segurança, evidenciado pelo envolvimento ativo da Administração, pela adoção da metodologia de gestão de riscos da ISO/IEC 27005 e pela aplicação de controlos alinhados com a norma ISO/IEC 27002.

A Administração desempenhou um papel essencial, participando ativamente em auditorias, no processo de gestão de riscos e na promoção de uma cultura organizacional de segurança. A gestão de riscos permitiu identificar vulnerabilidades e ameaças, atenuar potenciais impactos e assegurar a eficácia dos controlos implementados.

Os principais desafios enfrentados durante a implementação do SGSI incluíram a necessidade de formação contínua, a alocação eficiente de recursos financeiros, humanos e tecnológicos, a indução de uma cultura organizacional de segurança e a gestão eficaz do risco. Para superá-los, a BestUrban investiu em capacitação, sensibilização e reforço da governança em segurança da informação, garantindo a adesão de todos os envolvidos.

O estudo também apresenta recomendações práticas para outras PMEs portuguesas interessadas na implementação da norma ISO/IEC 27001. Entre elas, destacam-se a importância de um planeamento detalhado, o envolvimento da gestão de topo e a adaptação das melhores práticas às limitações e especificidades das PMEs.

Palavras-chave: ISO/IEC 27001, Segurança da Informação, Gestão de Riscos, PMEs, Implementação de SGSI.

ABSTRACT

This project work explores the implementation of an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard at BestUrban, a Portuguese Small and Medium Enterprise (SME). ISMS plays a crucial role in protecting the company's information assets.

The main objective of this study is to evaluate the effectiveness of the ISMS implementation, identify challenges and opportunities, and analyse the impact of this initiative on the company's overall information security posture. To this end, BestUrban's information security practices prior to the implementation of ISO/IEC 27001 were evaluated, the implementation process was documented, and the main milestones and strategic decisions were highlighted.

The implementation of the ISMS demonstrated a strong commitment to security, evidenced by the active involvement of Management, the adoption of the ISO/IEC 27005 risk management methodology and the application of controls aligned with the ISO/IEC 27002 standard.

Management played an essential role, actively participating in audits, in the risk management process and in promoting an organizational culture of safety. Risk management has made it possible to identify vulnerabilities and threats, mitigate potential impacts and ensure the effectiveness of the controls implemented.

The main challenges faced during the implementation of the ISMS included the need for continuous training, the efficient allocation of financial, human and technological resources, the induction of an organizational culture of safety and the effective management of risk. To overcome them, BestUrban invested in training, awareness, and reinforcement of information security governance, ensuring the adherence of all those involved.

The study also presents practical recommendations for other Portuguese SMEs interested in implementing the ISO/IEC 27001 standard. Among them, the importance of detailed planning, the involvement of top management and the adaptation of best practices to the limitations and specificities of SMEs stand out.

Keywords: ISO/IEC 27001, Information Security, Risk Management, SMEs, ISMS Implementation.

ÍNDICE

ÍNDICE DE FIGURAS

SIGLAS E ABREVIATURAS

BCMS	*Business Continuity Management System*
CMVM	Comissão de Mercados de Valores Mobiliários
DRP	*Disaster Recovery Plan*
ESG	*Environmental, Social, and Governance*
EUA	Estados Unidos da América
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MFA	*Multi-factor authentication*
NAS	*Network-Attached Storage*
NGF	*Next Generation Firewall*
PCI-DSS	*Payment Card Industry Data Security Standard*
PMEs	Pequenas e Médias Empresas
REV	*Recognized European Valuer*
RICS	*Royal Institution of Chartered Surveyors*
RMM	*Remote Monitoring and Management*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
SGSI	Sistema de Gestão de Segurança da Informação
SoA	*Statement of Applicability*
SI	Sistemas de Informação
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
UPS	*Uninterruptible Power Supply*

1 INTRODUÇÃO

No atual ambiente competitivo, a informação tornou-se um ativo fundamental para as organizações de vários sectores. A transformação digital originou um aumento sem precedentes no volume de dados gerados, armazenados e processados pelas empresas. Este crescimento suscitou benefícios significativos, tais como, a melhoria da tomada de decisões, experiência dos clientes, e eficiência operacional (Pessoa & Estrela, 2021). No entanto, introduziu novos riscos, nomeadamente, no domínio da segurança da informação.

A frequência e a crescente sofisticação das ciberameaças representam um risco substancial para as organizações, tornando a segurança da informação uma preocupação fundamental para empresas de todas as dimensões (Pessoa & Estrela, 2021).

As pequenas e médias empresas (PME), que constituem uma parte significativa da economia mundial, são particularmente vulneráveis a estas ameaças. Em Portugal, as PME representam mais de 99 por cento da população empresarial (Pordata, 2024) e desempenham um papel crucial no desenvolvimento económico do país. Porém, as limitações dos seus recursos implicam, frequentemente, medidas de segurança da informação inadequadas, tornando-as alvos privilegiados de ciberataques (ENISA, 2021). As consequências de tais violações podem ser devastadoras, levando a perdas financeiras, danos reputacionais e, em casos mais graves, à falência da própria empresa. Neste contexto, a implementação de Sistemas de Gestão da Segurança da Informação (SGSI) robustos tornou-se essencial para as PME protegerem os seus ativos de informação críticos.

A ISO/IEC 27001, uma norma internacionalmente reconhecida para a gestão da segurança da informação, oferece um quadro abrangente para “estabelecer, implementar, manter e melhorar continuamente um SGSI”. Foi concebida para ajudar as organizações a gerir a segurança de ativos como informações financeiras, propriedade intelectual, detalhes de funcionários e informações confiadas por terceiros. A sua abordagem baseada no risco garante que as organizações podem identificar e abordar eficazmente potenciais ameaças à segurança, salvaguardando assim os seus ativos de informação (International Organization for Standardization [ISO], 2013).

A implementação da ISO/IEC 27001 no contexto de uma PME apresenta desafios e oportunidades únicos, pela sua menor dimensão e recursos. Isto é particularmente verdade em Portugal, onde muitas PME podem não ter a experiência e os recursos financeiros para adotarem a mesma. No entanto, a obtenção da certificação pode oferecer benefícios substanciais, incluindo maior resiliência contra ciberameaças, maior confiança dos clientes e

conformidade com requisitos legais e regulamentares, como o Regulamento Geral de Proteção de Dados (RGPD) (Bulgurcu et al., 2010).

Este trabalho de projeto explora a implementação da norma ISO/IEC 27001 numa PME portuguesa, cujo SGSI foi implementado até dezembro de 2022. O foco deste estudo é deliberado, dado o papel significativo que estas empresas desempenham na economia nacional e a sua vulnerabilidade aos riscos de segurança da informação.

Ao examinar os desafios e benefícios específicos experimentados durante o processo de implementação, este trabalho de projeto descritivo pretende, ainda, disponibilizar informação para outras PMEs em Portugal que estejam a considerar adotar a norma ISO/IEC 27001 em contexto semelhante.

1.1 Objetivo Geral

O objetivo geral deste trabalho de projeto é analisar e compreender o processo de implementação da norma ISO/IEC 27001 na BESTURBAN, enquanto Pequena e Média Empresa (PME) portuguesa, avaliando a eficácia, identificando desafios e oportunidades, e mensurando o impacto na postura global de segurança da informação da empresa.

1.2 Objetivos específicos

Com base no objetivo geral e nas questões de investigação iniciais, são delineados os seguintes objetivos específicos:

- Avaliar o estado das práticas de segurança da informação na BESTURBAN, antes da implementação da norma ISO/IEC 27001.
- Documentar e analisar o processo da implementação da ISO/IEC 27001 na BESTURBAN, destacando os principais marcos e pontos de decisão.
- Identificar e avaliar os desafios encontrados durante a implementação da ISO/IEC 27001, incluindo limitações de recursos, dificuldades técnicas e resistência organizacional.
- Medir o impacto da implementação da ISO/IEC 27001 na postura de segurança da informação da BESTURBAN, incluindo melhorias na gestão de riscos, proteção de dados e conformidade com os requisitos legais e regulamentares.
- Fornecer recomendações práticas para outras PME portuguesas que estejam a considerar adotar a norma ISO/IEC 27001, com base nos resultados deste estudo de caso.

1.3 Questão Central/Chave

Quais são os fatores críticos que influenciam o sucesso da implementação da ISO/IEC 27001 numa PME portuguesa?

1.4 Questões Derivadas

As questões de investigação que orientaram este estudo, em conformidade com os objetivos específicos, são as seguintes

- Que práticas de segurança da informação estavam em vigor na BESTURBAN antes da implementação da norma ISO/IEC 27001?
- Como é que o processo de implementação da ISO/IEC 27001 foi estruturado na BESTURBAN e quais foram as etapas críticas?
- Quais os desafios específicos que a BESTURBAN enfrentou durante a implementação da ISO/IEC 27001 e como é que esses desafios foram resolvidos?
- Que melhorias na segurança da informação foram observadas após a implementação da ISO/IEC 27001 na BESTURBAN?
- Que lições podem ser retiradas desta implementação para ajudar outras PME portuguesas a adotar a ISO/IEC 27001?

1.5 Estrutura do trabalho

A estrutura deste trabalho de projeto foi concebida para abordar de forma abrangente e sistemática o processo de implementação da norma ISO/IEC 27001 numa Pequena e Média Empresa (PME) portuguesa, com enfoque na gestão da segurança da informação. O trabalho está organizado em seis capítulos principais, cada um abordando diferentes aspetos-chave do estudo.

O Primeiro capítulo introduz o trabalho de investigação, apresentando o seu objetivo geral, objetivos específicos, a questão central e as questões derivadas que orientam a pesquisa,

O segundo capítulo é dedicado ao enquadramento teórico, fundamental para contextualizar os principais elementos conceptuais subjacentes ao trabalho. Nele são abordadas noções fundamentais, quadros legais e normas internacionais. De seguida, o capítulo aborda o enquadramento legal relevante, tanto a nível nacional como europeu, com impacto na segurança da informação em Portugal e na União Europeia. Este capítulo explora também as normas internacionais aplicáveis.

No terceiro capítulo, o trabalho incide sobre a empresa em estudo, descrevendo a sua missão, atividades, visão, organização, papéis e responsabilidades. Para além disso, este capítulo analisa os Sistemas de Tecnologias de Informação (TI) da empresa, bem como as suas práticas de segurança da informação e cibersegurança. A governança da empresa, as políticas internas e a conformidade regulamentar também são discutidas, proporcionando uma melhor compreensão do ambiente organizacional no qual o SGSI foi implementado.

O quarto capítulo centra-se no SGSI da empresa. Este capítulo descreve o sistema existente ou as ações já tomadas e/ou planeadas para a implementação do mesmo nos termos da ISO/IEC 27001. São explorados aspetos como políticas, normas e procedimentos, gestão do risco, controlos e mecanismos de segurança, educação, formação e sensibilização, monitorização e análise, gestão de incidentes e conformidade e certificação. Este capítulo fornece uma visão detalhada das práticas de segurança da informação da empresa e dos esforços para se alinhar com os requisitos da ISO/IEC 27001.

O quinto capítulo analisa a situação atual da segurança da informação. A análise crítica apresentada, identifica desafios, lacunas e áreas de melhoria, fornecendo uma base sólida para as recomendações apresentadas no capítulo final.

O sexto e último capítulo apresenta as conclusões e recomendações resultantes do estudo. As conclusões sintetizam os principais resultados da investigação, enquanto as recomendações visam orientar a empresa na melhoria contínua do seu Sistema de Gestão da Segurança da Informação, promovendo uma maior resiliência contra as ciberameaças e assegurando a continuidade da conformidade com a norma ISO/IEC 27001.

2 ENQUADRAMENTO TEÓRICO

2.1 Noções Fundamentais

Este subcapítulo aborda as noções fundamentais que estão na base deste trabalho subordinado ao tema “Implementação de um Sistema de gestão da Segurança da Informação (ISO/IEC 27001) numa PME” e que são essenciais para compreender o seu contexto.

2.1.1 Ciberespaço

O conceito de ciberespaço, embora amplamente discutido, carece ainda de uma definição consensual e é frequentemente associado à Internet e ao ambiente digital (Mbanaso & Dandaura, 2015). Segundo o Departamento de Defesa dos EUA, o ciberespaço é “um domínio global dentro do ambiente informático, composto por uma rede interdependente de infraestruturas de tecnologias da informação, incluindo a Internet, redes de telecomunicações, sistemas informáticos e processadores e controladores incorporados” (Department of Defense, 2010). Esta visão realça o caráter complexo do ciberespaço, que integra tecnologias de criação, armazenamento e transmissão de dados.

Por seu turno, Choucri (2013) expande esta definição, apresentando o ciberespaço como um “domínio sem fronteiras” de interação social e técnica, composto por camadas físicas e lógicas. Esta visão multifacetada ilustra como o ciberespaço facilita novas formas de interação e organização social (Mbanaso & Dandaura, 2015).

A partir destas definições, o ciberespaço é visto não apenas como um domínio tecnológico, mas como um espaço social e cultural onde surgem novas formas de comunicação e organização (Mbanaso & Dandaura, 2015). No centro da revolução digital, o ciberespaço impulsiona a economia da informação, onde o conhecimento é fonte de valor, e fomenta o crescimento económico global, como exemplificado pela criação da *World Wide Web* e pelo impacto de empresas como a Google (Varian, 2015).

Contudo, o ciberespaço também gera desafios em segurança, como um campo de batalha onde ciberameaças emergem à medida que mais aspetos da vida humana se integram neste domínio, exigindo constante inovação em cibersegurança (Ciot, 2017).

2.1.2 Segurança da Informação

A segurança da informação evoluiu significativamente, alinhando-se com os avanços tecnológicos e a digitalização, tornando-se essencial para proteger informações sensíveis e gerir riscos associados. A segurança da informação é definida como o "processo de proteção da informação e dos sistemas de informação contra o acesso não autorizado, a utilização indevida, a divulgação, a interrupção, a modificação ou a destruição, com o objetivo de preservar a integridade, a confidencialidade e a disponibilidade dos dados" (Belsis et al., 2005, 189).

Este domínio tem suas raízes em sistemas hierárquicos de comando e controlo, particularmente em contextos administrativos e militares, sendo a criptografia uma das primeiras práticas de proteção, datada de 1900 a.C. (Cohen & Kahn, 1997). De acordo com os mesmos autores, a importância da segurança aumentou com a evolução da computação e das redes de computadores, levando ao desenvolvimento de *firewalls* nos anos 90 do século passado, como resposta ao crescimento de vírus e *worms* (Cohen & Kahn, 1997).

Segurança da Informação e cibersegurança são termos frequentemente usados de forma indistinta. A primeira refere-se à proteção de dados/informação, independentemente do seu meio, enquanto a cibersegurança se foca em ativos de informação digitais no ciberespaço.

O objetivo principal da Segurança da Informação é garantir a integridade, confidencialidade e disponibilidade da informação (ISO, 2013). Outros princípios como autenticidade, responsabilidade, não repúdio e fiabilidade são reconhecidos pela norma ISO/IEC 27000, ampliando a robustez da proteção.

2.1.3 Cibersegurança

A cibersegurança, apesar de ser um conceito relativamente recente, tornou-se um dos temas centrais dos debates sobre segurança internacional e defesa nacional no século XXI. No entanto, o seu significado carece de consensualização, com diferentes abordagens teóricas e práticas que moldam a complexidade da sua compreensão. Para efeitos da presente análise, a cibersegurança envolve a identificação, prevenção, controlo e redução de riscos presentes no ambiente digital, abrangendo desde a proteção contra erros humanos até a defesa contra crime organizado, espionagem

industrial e, em casos extremos, ataques que possam afetar as infraestruturas críticas de uma nação (Craigen et al., 2014).

A importância crescente da cibersegurança está intimamente ligada à expansão do ciberespaço como um novo domínio de conflito. Desde o início do século XXI, o estudo da cibersegurança ganhou uma força significativa, refletindo a crescente tomada de consciência de que o ciberespaço pode ser utilizado como uma ferramenta de poder (Gheciu & Wohlforth, 2018). Este reconhecimento levou ao debate pela academia sobre o papel do ciberespaço em operações militares, espionagem, subversão e sabotagem.

Em suma, a literatura sobre cibersegurança é marcada por uma diversidade de opiniões e abordagens. Embora não haja consenso sobre o impacto das capacidades cibernéticas na guerra moderna, existe um entendimento geral de que o ciberespaço se tornou um importante domínio de conflito, com implicações significativas para a segurança nacional e internacional. Os debates sobre a ciberguerra, a utilização de *proxies*, a negação plausível e a dissuasão continuam a moldar o campo da cibersegurança, refletindo a complexidade e a constante evolução deste domínio.

2.1.4 Princípios da Segurança da Informação

Os princípios da segurança da informação constituem a base teórica e prática para proteger dados e sistemas contra acessos, alterações ou destruições não autorizadas. Estes são tradicionalmente agrupados na tríade CIA[1] que significa Confidencialidade, Integridade e Disponibilidade. Estes três pilares, amplamente aceites na segurança da informação, formam o núcleo de um sistema eficaz de gestão (Dronov & Dronova, 2022).

O princípio da confidencialidade, fundamental para a segurança da informação, teve origem em contextos militares, focando-se na proteção de dados sensíveis contra acesso não autorizado. Esse princípio garante que as informações não sejam divulgadas, observadas ou reconhecidas por pessoas, processos ou entidades não autorizadas (ISO, 2005). A confidencialidade envolve medidas que controlam o acesso e a divulgação, indo além da simples restrição, pois visa assegurar proteção completa

[1] Confidentiality, Integrity and Availability

contra a visualização, impressão ou mesmo a perceção de existência de certos dados (Parker, 1998; Dhillon & Backhouse, 2000; Stoneburner et al., 2004).

A integridade assegura a precisão e completude da informação, garantindo que os dados permanecem inalterados durante o armazenamento e transmissão, a não ser que haja uma modificação autorizada. A integridade é essencial para a confiança nos dados e na sua exatidão, protegendo-os contra modificações ou destruições não autorizadas (ISO, 2005; Dhillon & Backhouse, 2000; Pfleeger & Pfleeger, 2003). A literatura divide a integridade em duas vertentes essenciais para os dados e sistemas: uma que se foca na exatidão e outra que visa a proteção contra manipulações. (Whitman & Mattord, 2011; Parker, 1998).

A disponibilidade assegura que informações e sistemas estão acessíveis a entidades autorizadas sempre que necessário, uma função crítica em ambientes onde a interrupção do acesso pode ter consequências graves (ISO, 2005; Whitman & Mattord, 2011). Diferente da confidencialidade e integridade, que focam em restringir o acesso, a disponibilidade prioriza o acesso contínuo, abrangendo a usabilidade para além do simples acesso (Pfleeger & Pfleeger, 2003; Parker, 1998).

Estes três princípios são interdependentes: a violação de qualquer um compromete a segurança do sistema como um todo (Whitman & Mattord, 2011; Stoneburner et al., 2004). Se a confidencialidade for violada, a informação pode ser exposta; se a integridade for comprometida, os dados podem ser alterados; e, se a disponibilidade for afetada, os utilizadores podem perder acesso a informações críticas (Parker, 1998; Dhillon & Backhouse, 2000).

Além da tríade CIA, outros princípios como a autenticidade, não repúdio e fiabilidade são também considerados importantes. A autenticidade verifica as identidades envolvidas numa comunicação; o não repúdio impede a negação da autoria de uma ação; e a fiabilidade assegura que os sistemas operam conforme esperado em várias condições (Whitman & Mattord, 2011).

2.1.5 Sistema de Gestão da Segurança da Informação (SGSI)

Um Sistema de Gestão da Segurança da Informação (SGSI)[2] proporciona uma estrutura contínua e iterativa para proteger dados e mitigar riscos de segurança, o que é crucial para organizações que procuram reduzir a exposição a ameaças. O SGSI oferece um modelo estruturado para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar continuamente a segurança da informação e a cibersegurança nas organizações, alinhadas com os objetivos empresariais (ISO, 2018).

Este processo de melhoria contínua mapeia o ciclo PDCA (Plan, Do, Check, Act), uma metodologia amplamente adotada da gestão de qualidade que promove a eficácia da segurança e a capacidade de resposta às ameaças que evoluem com o tempo (Boehmer, 2008).

2.1.6 Implementação de um SGSI

A primeira fase, planeamento, a organização estabelece a estrutura do SGSI, identifica os ativos de informação que necessitam de proteção e define os limites do sistema. São desenvolvidos documentos-chave, como a Declaração de Aplicabilidade (SoA) e as políticas de segurança da informação, incluindo normas e procedimentos específicos. Esta fase envolve também a avaliação e gestão de risco[3] para identificar vulnerabilidades dos ativos de informação e definir medidas (controlos) preventivas e reativas adequadas.

Na fase de implementação, são aplicadas políticas e os planos[4] definidos anteriormente. A norma ISO/IEC 27002 orienta a aplicação de melhores práticas de segurança, enquanto a ISO/IEC 27003 oferece diretrizes específicas para implementação. Um elemento essencial desta fase é a formação dos colaboradores para que compreendam suas responsabilidades e adotem voluntariamente as políticas estabelecidas.

---

[2] “An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.” (ISO/IEC 27000:2018)

[3] Conforme ISO/IEC 27005, NIST Risk Management Framework, etc.

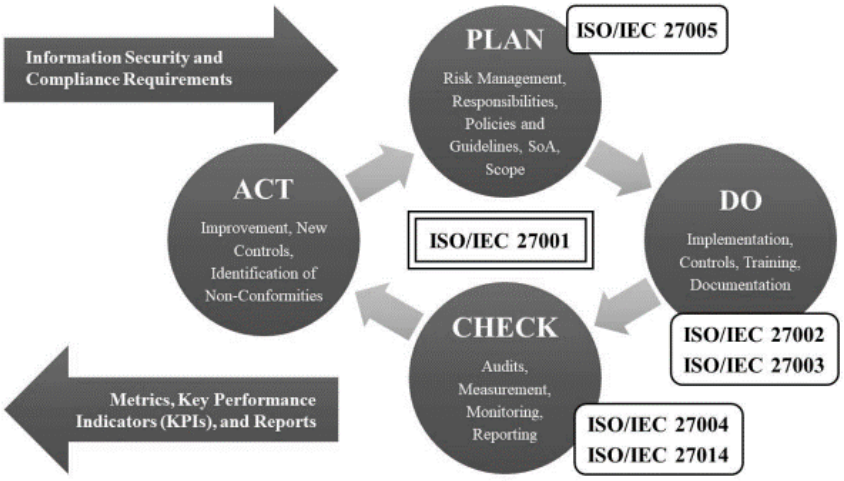
[4] Nomeadamente, identificação, tratamento e comunicação de riscos, continuidade de negócio, recuperação de desastres, melhoria contínua, e resposta a incidentes.

Documentar esta fase é crucial para fornecer evidências de conformidade e eficácia dos controlos de segurança (Boehmer, 2008).

Na fase de monitorização e revisão[5] é continuamente avaliado o desempenho do SGSI para assegurar que ele atende aos requisitos de segurança da organização. Isso inclui a criação de métricas de avaliação, realização de auditorias internas e análise de incidentes de segurança, com o objetivo de verificar a conformidade com os regulamentos e as normas aplicáveis, como a ISO/IEC 27001. Estas auditorias internas ajudam a identificar áreas de melhoria, enquanto normas adicionais, como a ISO/IEC 27004 e a ISO/IEC 27014, orientam a monitorização e a governança da segurança da informação.

Com base nas informações recolhidas durante a monitorização e nas auditorias realizadas são implementadas melhorias na fase subsequente, de ação. A organização aplica medidas corretivas e preventivas para resolver não conformidades e melhorar a eficácia do sistema, assegurando sua adaptação a novas ameaças e ao cenário de segurança em constante evolução. Esta abordagem contínua de adaptação é ilustrada na Figura 1, que representa todo o ciclo de implementação de um SGSI.

Figura 1:Ciclo PDCA aplicado aos sistemas de gestão da segurança da Informação



Fonte:(Adaptado de: Helmke & Uebel, 2013, p. 205)

[5] Review na versão em inglês.

A implementação de um SGSI é uma decisão estratégica e oferece múltiplos benefícios, incluindo a redução de custos associados a falhas de segurança, aumento da conformidade com exigências legais e melhoria da reputação organizacional. Contudo, é essencial reconhecer que nenhum SGSI garante segurança absoluta, exigindo uma gestão constante para manter a eficácia dos controlos e assegurar que eles estejam alinhados aos objetivos organizacionais (ISO, 2013). Essa abordagem realça a importância de vigilância contínua e adaptabilidade, que permitem às organizações protegerem seus ativos críticos num ambiente de ameaças complexas e dinâmicas.

2.1.7 Gestão da Continuidade de Negócio

A integração das Tecnologias de Informação e Comunicação (TIC) nas organizações modernas é crucial para seu funcionamento, tendo transformado profundamente estruturas, processos e interações organizacionais (Laudon & Laudon, 2012). Fritz Machlup foi um dos pioneiros a introduzir o conceito de "Sociedade da Informação", enfatizando a dependência organizacional no conhecimento derivado da informação, que é constantemente influenciado por fatores internos e externos (Laudon & Laudon, 2012). Contudo, essa crescente dependência aumenta a exposição a vulnerabilidades que podem afetar os ativos de informação, gerando riscos que requerem uma gestão cuidadosa para mitigá-los (Dobler, 2005).

A gestão de riscos é fundamental para classificar e avaliar a probabilidade e o impacto potencial de vulnerabilidades e eventuais ameaças, permitindo que as organizações alinhem a mitigação de riscos com os seus objetivos estratégicos, tendo em consideração aspetos legais, socioeconómicos e o interesse dos *stakeholders* (The Institute of Risk Management [IRM], 2002). Esta gestão pode adotar abordagens proativas e reativas para mitigar, transferir, aceitar ou explorar os riscos, fortalecendo a resiliência organizacional e reduzindo a incerteza dos negócios. Neste contexto, a Gestão da Continuidade do Negócio (GCN) torna-se vital.

A GCN é um processo que visa garantir a continuidade das operações durante e após uma interrupção significativa, protegendo ativos, interesses e atendendo a obrigações contratuais e legais (IRM, 2002). Uma componente essencial da GCN é o Plano de Continuidade de negócio (PCN), que fornece um quadro para responder a catástrofes e assegurar a recuperação de atividades críticas. Uma catástrofe é definida como um acontecimento súbito com um impacto significativo que causa perturbações para além

do período tolerável pela organização (IRM, 2002). Este plano foca-se na prevenção de eventos de alto impacto e na minimização de danos à reputação e prejuízos financeiros.

O Plano de Recuperação de Desastres (PRD) destaca-se especialmente por focar na recuperação dos sistemas de informação e TIC após interrupções (Laudon & Laudon, 2012). A atualização constante e a realização de testes frequentes do PCN e do PRD são indispensáveis para manter a eficácia dos planos e alinhá-los às necessidades atuais da organização.

Em síntese, uma gestão de riscos eficaz e um plano de continuidade de negócio sólido são essenciais para a resiliência organizacional em ambientes altamente dependentes das TIC. Organizações que investem em tais áreas estão mais bem preparadas para enfrentar desafios imprevistos e assegurar a continuidade de suas operações.

2.2 Quadro Legal – Nacional

Neste subcapítulo dedicado ao enquadramento legal nacional, será apresentada uma análise sintética dos principais elementos do normativos que moldam a segurança da informação, cibersegurança e proteção de dados em Portugal. Este subcapítulo abordará em primeiro lugar a Lei 109/2009, conhecida como Lei do Cibercrime, que estabelece as bases legais para o combate aos crimes cometidos através de meios digitais. Seguir-se-á a discussão da Lei 58/2019, que adapta o Regulamento Geral de Proteção de Dados (RGPD) ao contexto nacional, destacando as obrigações das organizações no tratamento de dados pessoais.

Será ainda abordada a Lei 46/2018, que define o regime jurídico da segurança no ciberespaço, e a Resolução do Conselho de Ministros 92/2019, que estabelece a Estratégia Nacional de Segurança do Ciberespaço [2.0] para o período de 2019 a 2023. Adicionalmente, será analisado o Regulamento 303/2019, que trata da segurança e integridade das redes e serviços de comunicações eletrónicas e, por fim, o Decreto-Lei 65/2021, que regula o regime jurídico da segurança do ciberespaço.

2.2.1 Lei nº 109/2009, Lei do Cibercrime

A Lei n.º 109/2009, conhecida como Lei do Cibercrime, é essencial na legislação portuguesa para combater crimes através de meios eletrónicos e proteger a integridade dos sistemas informáticos, transpondo para o contexto nacional normas da União

Europeia e da Convenção do Conselho da Europa sobre o Cibercrime (artigo 1.º). Esta lei tipifica como crimes no ciberespaço, a falsidade informática (artigo 3.º), dano de dados (artigo 4.º), sabotagem informática (artigo 5.º), acesso ilegítimo (artigo 6.º) e interceção de comunicações eletrónicas (artigo 7.º), com penas adaptadas à gravidade das infrações.

Para a investigação e punição de cibercrimes, a lei prevê a conservação de dados (artigo 12.º), buscas em sistemas informáticos (artigo 15.º) e apreensão de dados relevantes (artigo 16.º), incluindo a responsabilidade penal de pessoas coletivas por crimes cometidos em seu benefício (artigo 9.º).

A Lei do Cibercrime também destaca a cooperação internacional, facilitando a colaboração entre autoridades portuguesas e estrangeiras em investigações transnacionais, com a Polícia Judiciária como ponto de contacto (artigos 20.º e 21.º). Este quadro legal responde aos desafios do ciberespaço alinhando-se com práticas internacionais contra o cibercrime (artigos 27.º e 28.º).

2.2.2 Lei nº 58/2019, de 8 de agosto | Regulamento Geral de Proteção de Dados (RGPD)

A Lei n.º 58/2019 integra o Regulamento Geral de Proteção de Dados (RGPD) no ordenamento jurídico português, estabelecendo normas adicionais para proteger dados pessoais e assegurar sua livre circulação na União Europeia (artigo 1.º). A aplicação da lei cobre o tratamento de dados em Portugal, assim como realizados fora do país, desde que se relacionem com entidades estabelecidas em território nacional ou impactem indivíduos em Portugal. Exceções são aplicadas para dados mantidos pelo Sistema de Informações da República Portuguesa, através de legislação específica (artigo 2.º).

A Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo nacional, com independência administrativa e financeira, responsável por monitorizar a conformidade com o RGPD e a legislação nacional (artigos 3.º e 4.º). A CNPD protege direitos e garantias relacionados aos dados pessoais e atua como órgão independente (artigo 6.º). É ainda regulado o papel do Encarregado de Proteção de Dados, exigindo que entidades públicas designem esse profissional, enquanto as entidades privadas devem fazê-lo em determinadas situações (artigos 9.º, 12.º e 13.º).

2.2.3 Lei nº 46/2018 de 13 de agosto | Regime jurídico da segurança do ciberespaço

A Lei n.º 46/2018, de 13 de agosto, define o regime jurídico da segurança do ciberespaço em Portugal, alinhando-se com a Diretiva (UE) 2016/1148 (NIS1) para assegurar uma segurança uniforme de redes e informação na União Europeia. Abrange a administração pública, operadores de infraestruturas críticas, serviços essenciais e prestadores de serviços digitais, excluindo as redes de defesa nacional e informação classificada (artigos 1.º e 2.º). A Estratégia Nacional de Segurança do Ciberespaço orienta as ações do Estado nesse campo (artigo 4.º).

O Conselho Superior de Segurança do Ciberespaço atua como órgão consultivo do Primeiro-Ministro, enquanto o Centro Nacional de Cibersegurança, ligado ao Gabinete Nacional de Segurança, supervisiona e implementa as práticas de cibersegurança (artigos 5.º, 6.º e 7.º). A Equipa Nacional de Resposta a Incidentes, CERT.PT, é responsável por coordenar respostas a incidentes de segurança (artigos 8.º e 9.º). Entidades abrangidas devem aplicar medidas de segurança proporcionais aos riscos e reportar incidentes ao Centro Nacional de Cibersegurança (artigos 12.º a 20.º).

O Centro Nacional de Cibersegurança fiscaliza o cumprimento das normas e pode aplicar sanções por infrações graves ou muito graves, punindo também a negligência (artigos 21.º a 28.º). As obrigações para identificação de operadores de serviços essenciais e prestadores de serviços digitais incluem notificação imediata do início das atividades (artigos 29.º e 30.º).

2.2.4 Resolução do Conselho de Ministros (RCM) nº 92/2019, de 5 junho | Estratégia Nacional de Segurança do Ciberespaço 2.0 (2019-2023)

A Resolução do Conselho de Ministros n.º 92/2019 atualiza a Estratégia Nacional de Segurança do Ciberespaço (ENSC) para o período 2019-2023, em resposta ao aumento de ciberameaças e à evolução tecnológica. Esta atualização, coordenada pelo Conselho Superior de Segurança do Ciberespaço, foca-se em três objetivos estratégicos:

- **Maximizar a Resiliência:** Reforçar a resiliência digital nacional para proteger infraestruturas críticas e sistemas essenciais.
- **Promover a Inovação:** Impulsionar a inovação no ciberespaço para o desenvolvimento económico, social e cultural.

- **Gerar e garantir recursos**: Assegurar a atribuição e gestão eficazes dos recursos humanos e técnicos necessários para a segurança do ciberespaço.

A ENSC 2019-2023 divide-se em seis eixos de intervenção principais:

- **Estrutura de Segurança do Ciberespaço**: Consolidação e coordenação nacional na cibersegurança, com papéis centrais atribuídos ao Conselho Superior de Segurança do Ciberespaço e ao Centro Nacional de Cibersegurança.
- **Prevenção, Educação e Sensibilização:** Promoção de uma cultura de cibersegurança com foco em sensibilização pública, formação em cibersegurança e inclusão de temas de cibersegurança nos currículos escolares.
- **Proteção do Ciberespaço e Infraestruturas Críticas:** Propostas para proteger infraestruturas críticas, reforçando a cooperação público-privada e promovendo normas e práticas de segurança nacionais e internacionais.
- **Resposta a Ameaças e Combate ao Cibercrime:** Desenvolvimento de um sistema coordenado para a resposta a incidentes cibernéticos, com adaptação das capacidades das Forças Armadas e de Segurança e revisão da legislação penal em cibercrime.
- **Investigação, Desenvolvimento e Inovação:** Incentivo à investigação e inovação em cibersegurança, integrando o setor público, privado e académico.
- **Cooperação Nacional e Internacional:** Ênfase na participação de Portugal em organismos internacionais e na promoção da ciberdiplomacia para uma governança global do ciberespaço.

A ENSC 2019-2023 é implementada através de um Plano de Ação, elaborado pelo Centro Nacional de Cibersegurança e revisto anualmente.

2.2.5 Regulamento nº 303/2019 de 1 de abril | Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas (SRI/NIS1)

O Regulamento 303/2019, publicado pela Autoridade Nacional de Comunicações (ANACOM) a 1 de abril de 2019, estabelece diretrizes para a segurança e integridade das redes e serviços de comunicações eletrónicas em Portugal. Este regulamento surge da necessidade de garantir a resiliência das infraestruturas de comunicações eletrónicas, vitais para o funcionamento seguro da sociedade moderna.

O regulamento abrange medidas técnicas e organizativas que as empresas de comunicações devem adotar para garantir a segurança das suas infraestruturas, aplicando-se tanto a condições normais quanto a situações extraordinárias, como incidentes de segurança e catástrofes naturais (art. 1.º e art. 3.º). A ANACOM enfatiza a importância da cooperação entre empresas e entre estas e a ANACOM, especialmente em relação à partilha de informações e coordenação na resposta a incidentes (art. 4.º).

As empresas devem implementar medidas adequadas para prevenir, gerir e atenuar riscos à segurança das redes, baseando-se em melhores práticas e normas internacionais, e classificar os seus ativos de acordo com a respetiva criticidade, mantendo um inventário atualizado (art. 6.º, art. 8.º e art. 9.º). O regulamento também exige que as empresas revejam periodicamente suas avaliações de risco, considerando incidentes anteriores e novas ameaças (art. 10.º). Exercícios regulares para testar a eficácia das medidas de segurança são obrigatórios (art. 12.º).

2.2.6 Decreto-Lei nº 65/2021 de 30 de julho | Regulamenta o Regime Jurídico da Segurança do Ciberespaço

O DL 65/2021, publicado a 30 de julho de 2021 pela Presidência do Conselho de Ministros, regulamenta o Regime Jurídico da Segurança do Ciberespaço em Portugal e estabelece as obrigações de certificação de cibersegurança, em conformidade com o Regulamento (UE) 2019/881 do Parlamento Europeu. Este decreto-lei resulta da Lei n.º 46/2018, que transpondo a Diretiva (UE) 2016/1148, reforça a segurança das redes e sistemas de informação.

O principal objetivo do DL 65/2021 é definir os requisitos mínimos de segurança a serem cumpridos pela Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, garantindo assim a segurança das redes e sistemas de informação em Portugal (art. 1.º). O decreto-lei também estabelece as regras para a notificação de incidentes, incluindo os procedimentos e prazos a serem seguidos (art. 2.º).

As entidades abrangidas pelo DL são obrigadas a designar um ponto de contacto permanente para comunicação com o Centro Nacional de Cibersegurança (CNCS) e a nomear um responsável pela segurança que reportará incidentes (art. 4.º e art. 5.º).

Além disso, devem manter um inventário atualizado dos bens essenciais e elaborar um plano de segurança que documente as medidas implementadas (art. 6.º e art. 7.º).

O DL exige a elaboração de um relatório anual sobre as atividades de segurança, que inclui uma análise dos incidentes ocorridos (art. 8.º). As entidades devem realizar análises de risco periódicas e implementar medidas adequadas para assegurar a robustez e a resiliência dos seus ativos (art. 9.º e art. 10.º).

As obrigações de notificação de incidentes são detalhadas, incluindo três tipos de notificação: inicial, de fim de impacto e final, devendo ser enviadas conforme os prazos estabelecidos (art. 11.º a art. 15.º). O CNCS pode emitir regulamentos complementares e normas técnicas para garantir a eficácia das medidas (art. 18.º).

O CNCS é também designado como Autoridade Nacional de Certificação de Cibersegurança, responsável pela supervisão dos sistemas de certificação de cibersegurança (art. 20.º). O regime sancionatório para infrações é definido, prevendo coimas para os incumprimentos (art. 21.º).

Em síntese, o DL 65/2021 estabelece um conjunto robusto de medidas para garantir a segurança do ciberespaço em Portugal, em alinhamento com as normas europeias, reforçando a proteção das redes e sistemas de informação num contexto de crescente digitalização.

2.3 Quadro Legal Europeu

O domínio normativo europeu envolve um conjunto abrangente de regulamentos e diretivas que visam reforçar a cibersegurança e a resiliência das infraestruturas críticas na União Europeia. Este quadro regulamentar, desenvolvido em resposta aos crescentes desafios colocados pelas ameaças digitais, inclui regulamentos específicos como o Regulamento (UE) 2016/679 (também conhecido como RGPD), que estabelece normas rigorosas para a proteção dos dados pessoais, e as Diretivas NIS1.0 e NIS2.0, que definem requisitos para a segurança das redes e dos sistemas de informação. Complementando estas medidas, o *Cybersecurity Act*[6] e o Regulamento de Ciber-

[6]Regulamento Cibersegurança da UE (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881)

resiliência[7] da UE introduzem mecanismos de certificação da cibersegurança e de reforço da ciber-resiliência, enquanto o Regulamento de Ciber-solidariedade[8] da UE e a Diretiva Resiliência das Entidades Críticas visam promover uma maior solidariedade e robustez entre os Estados-Membros face às ciberameaças e assegurar a proteção das entidades críticas. Estes instrumentos legislativos constituem a espinha dorsal da estratégia europeia para garantir um ciberespaço seguro e resiliente.

2.3.1 EU Cybersecurity Strategy "The Digital Decade"[9]

A Estratégia de Cibersegurança da UE para a "The Digital Decade" visa posicionar a Europa como líder em resiliência, segurança e sustentabilidade digitais até 2030. Este plano estabelece metas, alinhadas com a Declaração sobre Direitos e Princípios Digitais, focando-se em inclusão digital, transparência e respeito pelos valores europeus. Análises anuais e consultas com Estados-Membros, indústria e sociedade civil garantem a adaptação das políticas às mudanças digitais e à evolução das ameaças cibernéticas.

A estratégia promove uma abordagem holística, priorizando a capacitação digital, o fortalecimento das infraestruturas, a digitalização empresarial e a segurança dos serviços públicos, áreas que são monitorizadas sistematicamente para fortalecer o ecossistema digital. Através de instrumentos como o Eurobarómetro, a UE avalia a perceção pública sobre privacidade, direitos digitais e acesso, revelando a necessidade de sensibilização e de equidade na proteção dos direitos digitais em todos os Estados-Membros.

A nível regional, a UE incentiva a participação de municípios e regiões na implementação da estratégia, promovendo a inclusão digital e a extensão da cibersegurança para além dos centros urbanos. Em termos globais, a UE busca reforçar a sua posição digital internacional, fomentando parcerias para práticas digitais seguras e sustentáveis.

---

[7] Cyber Resilience Act

[8] Cyber Solidarity Act

[9] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Para sustentar essas metas, a estratégia aloca investimentos significativos do Mecanismo de Recuperação e Resiliência, que impulsiona projetos voltados para a cibersegurança, competências digitais e infraestruturas seguras. Dentre os principais projetos, destacam-se o financiamento de Internet de alta velocidade, o apoio à digitalização de PMEs e o aumento da cibersegurança no setor público. Adicionalmente, ações políticas abrangentes, pós-2020, visam enfrentar novas ameaças à segurança digital.

Em síntese, a "The Digital Decade" proporciona uma estrutura flexível e preparada para evoluir com os riscos digitais e promover um ambiente digital inclusivo, resiliente e seguro para todos os cidadãos europeus, enfatizando a soberania digital e o bem-estar social da região.

2.3.2 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

O Regulamento Geral sobre a Proteção de Dados (RGPD), formalmente designado como Regulamento (UE) 2016/679, visa proteger e regulamentar o tratamento de dados pessoais e a sua circulação livre dentro da União Europeia, conferindo direitos ampliados aos titulares dos dados e controlos rígidos sobre o processamento de informações pessoais. Este regulamento, que entrou em vigor a 25 de maio de 2018, substitui a anterior Diretiva 95/46/CE, introduzindo um quadro robusto de direitos e obrigações para as organizações e as entidades que tratam dados pessoais na União Europeia, com o objetivo de assegurar uma proteção eficaz dos dados pessoais dos cidadãos.

Entre os principais requisitos, o RGPD estabelece que as organizações devem garantir o consentimento explícito dos titulares para o tratamento dos seus dados e notificar prontamente as autoridades competentes em caso de violações de segurança (artigos 1.º a 3.º). Este regulamento define ainda os tipos de tratamento de dados aplicáveis e exceções para atividades de segurança pública e criminal, sublinhando a importância do consentimento informado, que pode ser revogado a qualquer momento pelo titular (artigos 4.º e 7.º).

O RGPD apresenta como princípios fundamentais para o tratamento de dados a transparência, minimização, integridade, confidencialidade e responsabilidade do

responsável pelo tratamento (artigo 5.º). Define ainda bases legais que legitimam o tratamento, incluindo o consentimento explícito, a necessidade contratual e o cumprimento de obrigações legais (artigo 6.º). Adicionalmente, impõe condições específicas para o tratamento de dados de menores e para dados sensíveis, como origem étnica ou informações de saúde, limitando o processamento em contextos restritos e previstos por lei (artigos 8.º e 9.º).

Direitos fundamentais dos titulares, como o direito de acesso, retificação, eliminação ("direito ao esquecimento"), limitação do tratamento e portabilidade dos dados, reforçam a capacidade dos cidadãos para controlar os seus dados pessoais (artigos 12.º a 22.º). Em casos específicos de segurança ou defesa nacional, o regulamento permite restrições proporcionais a esses direitos, desde que fundamentadas em disposições legislativas (artigo 23.º).

Em suma, o RGPD estabelece uma estrutura abrangente de proteção de dados que promove uma abordagem rigorosa e segura ao tratamento de dados pessoais, alinhando-se com os valores de transparência, segurança e respeito pelos direitos individuais na União Europeia.).

2.3.3 Diretivas NIS1.0 e NIS2.0

A Diretiva NIS[10] e a subsequente Diretiva NIS2[11] representam passos significativos da União Europeia na regulamentação da cibersegurança, refletindo uma resposta adaptativa às crescentes ameaças no ciberespaço e à necessidade de reforçar a resiliência do sector na Europa.

Proposta no âmbito da estratégia europeia de cibersegurança, a Diretiva NIS foi adotada em julho de 2016, visando reforçar a cibersegurança a três níveis: a nível europeu, dos estados-membros e das entidades essenciais à segurança do espaço europeu. Foi transposta para o direito português em agosto de 2018, atribuindo ao Centro Nacional de Cibersegurança (CNCS) a responsabilidade de supervisionar a aplicação da diretiva. As entidades competentes foram incumbidas de cumprir os requisitos de segurança da

[10] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[11] http://data.europa.eu/eli/dir/2022/2555/oj

informação e de notificação de incidentes de segurança. Em 2021, o Decreto-Lei n.º 65/2021 (ver 2.2.6) veio detalhar as obrigações destas entidades, como a comunicação de inventários de ativos, a análise de riscos, a elaboração de planos de segurança e a notificação ao CNCS. No entanto, até à data, não há conhecimento de sanções aplicadas no contexto desta diretiva, apesar dos esforços educativos do CNCS e das recentes notificações a cerca de 400 organizações para cumprirem as obrigações (PwC Portugal, 2023).

Publicada em dezembro de 2022, a Diretiva NIS2 substitui a NIS (agora identificada como NIS1), alargando o âmbito de aplicação para incluir novos setores críticos, como a gestão de serviços de TIC, a administração pública e as indústrias alimentar e química, entre outros. A NIS2 reforça e pormenoriza as obrigações das organizações, introduzindo medidas específicas a aplicar, incluindo a análise de risco, a continuidade das atividades, a segurança da cadeia de abastecimento, as práticas de ciber-higiene e a autenticação multifator. A transposição da NIS2 para a legislação nacional tem como prazo limite outubro de 2024, e a aplicação efetiva desta diretiva será crucial para mitigar os riscos crescentes no ciberespaço (PwC Portugal, 2023).

A evolução da NIS1 para a NIS2 reflete uma tentativa de acompanhar a rápida evolução das ciberameaças. No entanto, a eficácia desta legislação depende não só da sua transposição para o direito nacional, mas também do empenhamento das organizações em aplicar as medidas de segurança necessárias. Sem uma atenção rigorosa a estas orientações, o espaço europeu de cibersegurança permanecerá vulnerável, com impactos potencialmente graves tanto em termos de cumprimento da regulamentação como de proteção contra ciberataques.

2.3.4 EU Cyber Security Act

O Regulamento (UE) 2019/881, conhecido como o *EU Cyber Security Act*, visa estabelecer um elevado nível de cibersegurança, resiliência e confiança na União Europeia, conferindo um mandato permanente à Agência da União Europeia para a Cibersegurança (ENISA) para apoiar autoridades e instituições europeias no fortalecimento da cibersegurança. O regulamento também introduz um quadro de certificação à escala da UE para produtos, serviços e processos de TIC, com foco em segurança ao longo de todo o ciclo de vida dos ativos digitais.

A ENISA é central neste regulamento, sendo responsável por promover a aplicação de políticas de cibersegurança, apoiar o desenvolvimento de capacidades e fomentar a cooperação operacional na UE. Além disso, a ENISA contribui para a criação de sistemas de certificação, recolha de dados sobre ameaças e incidentes e sensibilização pública para a cibersegurança (Regulamento (UE) 2019/881). A agência é gerida por representantes de Estados-Membros e pela Comissão Europeia, contando com uma rede de agentes nacionais para intercâmbio de informações e com grupos de peritos para orientação.

O regulamento cria um sistema de certificação que assegura que produtos, serviços e processos TIC atendam a padrões de segurança específicos, inicialmente de adesão voluntária, mas que a Comissão Europeia poderá tornar obrigatória no futuro. Com a entrada em vigor em junho de 2019, a Comissão Europeia adotou o Regulamento de Execução (UE) 2024/482, que estabelece o primeiro sistema de certificação pan-europeu a ser implementado em fevereiro de 2025. O regulamento substitui o anterior Regulamento (UE) n.º 526/2013 e respeita as competências dos Estados-Membros em segurança pública e nacional.

Face ao aumento da relevância dos *Managed Security Services* (MSS), em 2023 a Comissão Europeia propôs incluir esses serviços no *Cyber Security Act*, permitindo a certificação de prestadores de serviços de segurança geridos, o que visa aumentar a qualidade e comparabilidade dos serviços na UE. Um acordo provisório foi alcançado pelo Conselho e Parlamento em março de 2024, e o texto final deverá ser aprovado em breve. Para empresas que atuam com produtos digitais e TIC, o regulamento representa uma oportunidade de aumentar a credibilidade e competitividade no mercado europeu através da certificação em conformidade com os padrões de cibersegurança da UE.

2.3.5 EU Cyber Resilience Act[12]

O *Cyber Resilience Act* é uma regulamentação recente da União Europeia focada na cibersegurança de produtos e *software* com componentes digitais, reforçando a proteção de consumidores e empresas no uso de dispositivos conectados. Esta

[12] (European Commission, 2022)

legislação responde ao aumento de produtos digitais no quotidiano, como monitores de bebé e relógios inteligentes, que frequentemente apresentam lacunas de segurança.

O regulamento aborda duas questões principais: a insuficiência de medidas de cibersegurança em produtos digitais, como atualizações de segurança, e a dificuldade enfrentada por consumidores e empresas em avaliar e configurar dispositivos de forma segura O *Cyber Resilience Act* introduz normas harmonizadas para que a cibersegurança seja considerada desde a conceção até à manutenção de um produto, e obriga os fabricantes a garantir a proteção ao longo do ciclo de vida completo dos dispositivos

Quando implementado, os produtos conectados devem ostentar a marcação CE para indicar a conformidade com os padrões de cibersegurança. Esta marcação visa ajudar consumidores e empresas a identificar dispositivos seguros, promovendo escolhas informadas.

Anunciado na Estratégia de Cibersegurança da UE de 2020 (ver 2.3.1), o *Cyber Resilience Act* complementa normas como a *NIS2*, aplicando-se a produtos conectados, exceto em casos como *software* de código aberto e setores já cobertos por regulamentações específicas (e.g., dispositivos médicos). Prevê-se que entre em vigor no segundo semestre de 2024, com produtos compatíveis obrigatórios no mercado europeu até 2027, e que seja periodicamente revisado pela Comissão Europeia para otimizar a sua aplicação

2.3.6 EU Cyber Solidarity Act[13]

O *Cyber Solidarity Act* visa fortalecer a preparação, deteção e resposta a incidentes de cibersegurança em toda a União Europeia. O regulamento propõe um sistema coordenado de alerta e resposta a emergências cibernéticas, incluindo um Sistema Europeu de Alerta de Cibersegurança composto por Centros de Operações de Segurança (SOC) que utilizam inteligência artificial e análise de dados para monitorizar e partilhar alertas de ameaças entre Estados-Membros. A fase inicial, iniciada em

[13] (European Commission, 2023).

novembro de 2022, já reúne SOC de 17 Estados-Membros e Islândia no âmbito do Programa Europa Digital

O Mecanismo de Emergência Cibernética abrange três frentes principais: apoio a testes de preparação em setores críticos como finanças, energia e saúde; a criação de uma Reserva de Cibersegurança da UE para fornecer serviços de resposta rápida a incidentes; e a promoção de assistência mútua entre Estados-Membros em caso de ataques cibernéticos. A lei também prevê um Mecanismo de Análise de Incidentes de Cibersegurança, coordenado pela ENISA, para avaliar e elaborar relatórios sobre ciber-incidentes de grande escala, com o objetivo de fortalecer a cibersegurança da União.

O financiamento da implementação será garantido pelo Programa Europa Digital, com um orçamento ampliado para 842,8 milhões de euros, podendo chegar a 1,109 mil milhões de euros com a participação dos Estados-Membros. Esses recursos destinam-se ao desenvolvimento dos SOC e à criação da Reserva de Cibersegurança, aumentando a capacidade de resposta coletiva da UE perante ciberameaças.

2.3.7 Critical Entities Resilience Directive

A *Critical Entities Resilience Directive*[14] da União Europeia estabelece um conjunto de obrigações que visam garantir a prestação ininterrupta dos serviços essenciais para a manutenção das funções vitais da sociedade ou das atividades económicas no mercado interno da UE (artigo 1.º, n.º 1, alínea a)). A diretiva exige que os Estados-Membros identifiquem as entidades críticas e prestem apoio para melhorar a sua capacidade de resistência e a continuidade da prestação de serviços essenciais (artigo 1.º, n.º 1, alínea b)). Além disso, define regras para a supervisão das entidades críticas e para a aplicação dessas regras, incluindo a identificação das entidades de importância crucial para a Europa e a organização de missões consultivas para avaliar as medidas adotadas por estas (artigo 1.º, n.º 1, alínea c)).

A diretiva também estabelece procedimentos comuns para a cooperação e para a apresentação de relatórios sobre a aplicação das medidas, com o objetivo de alcançar elevados níveis de resiliência nas entidades críticas, assegurando a prestação contínua

[14] http://data.europa.eu/eli/dir/2022/2557/oj

dos serviços essenciais em toda a União Europeia e o bom funcionamento do mercado interno (artigo 1.º, n.º 1, alínea d)). A sua aplicação não abrange questões que sejam reguladas por outras legislações da União, como a Diretiva (UE) 2022/2555 (NIS2), e garante a aplicação coordenada dessas normas, tendo em conta a relação entre a segurança física e a cibersegurança das entidades críticas (artigo 1.º, n.º 2). A diretiva também assegura que as obrigações impostas não envolvam a divulgação de informações que possam prejudicar a segurança nacional dos Estados-Membros, mantendo a confidencialidade necessária para o intercâmbio de dados (artigo 1.º, n.º 4).

Por fim, a *Critical Entities Resilience Directive* reforça a responsabilidade dos Estados-Membros pela segurança e defesa nacionais, bem como por outras funções essenciais do Estado (artigo 1.º, n.º 5). A diretiva contribui para a maior resiliência e segurança da União Europeia, permitindo que as entidades críticas se preparem, respondam, resistam, atenuem e se recuperem de incidentes que possam comprometer a continuidade dos serviços essenciais (artigo 2.º, n.º 2).

2.3.8 EU Artificial Intelligence (AI) Act[15]

A Lei da Inteligência Artificial (AI) da União Europeia (UE) (Regulamento (UE) 2024/1689), conhecida como Lei da IA, marca a introdução de um quadro jurídico inovador destinado aos desafios e riscos específicos da inteligência artificial, promovendo simultaneamente um ambiente de inovação seguro e fiável na Europa. Este regulamento visa normalizar os requisitos para os criadores e implementadores de IA, especialmente em sectores de alto risco, e reduzir os encargos administrativos e financeiros para as empresas, com especial incidência nas pequenas e médias empresas (PME). Combinada com o Pacote de Inovação em IA e o Plano Coordenado de IA, a legislação visa não só a segurança e o respeito pelos direitos fundamentais, mas também incentiva a adoção e os investimentos em IA em toda a UE.

O regulamento adota uma abordagem baseada no nível de risco, estabelecendo quatro categorias distintas: risco inaceitável, risco elevado, risco limitado e risco mínimo ou

[15] European Commission (2024).

inexistente. As aplicações de IA consideradas de risco inaceitável, como a pontuação social pelos governos, são proibidas. Os sistemas de alto risco, incluindo as tecnologias utilizadas em infraestruturas críticas, processos educativos, produtos de segurança e justiça, devem cumprir requisitos de conformidade rigorosos antes de serem lançados no mercado, incluindo avaliações pormenorizadas, rastreabilidade e supervisão humana.

O *AI Act* também aborda a necessidade de transparência para utilizações de risco limitado, como os *chat-bots* e os conteúdos gerados por IA, exigindo que os utilizadores sejam informados sobre a interação com uma máquina (Comissão Europeia, 2024). Por fim, sistemas com risco mínimo, como videojogos e filtros de spam, são de uso livre na UE, abrangendo a maior parte das tecnologias de IA atualmente em operação no bloco (Comissão Europeia, 2024). A aplicação dessas regulamentações visa garantir que a IA desenvolvida e utilizada na Europa seja confiável, ética e respeite os valores e direitos fundamentais dos cidadãos europeus.

2.4 Normas Internacionais

2.4.1 ISO/IEC 27001:2022[16]

A norma ISO/IEC 27001:2022 é a principal referência para a gestão da segurança da informação, fornecendo uma abordagem abrangente para garantir a proteção da informação nas organizações. Esta edição revista em 2022, desenvolvida pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC), representa uma atualização importante das edições anteriores e reflete a natureza mutável das novas ameaças do seu impacto na cibersegurança (ISO, 2022).

A ISO/IEC 27001:2022 faz parte da família de normas ISO/IEC 27000 que oferece uma estrutura para a Gestão da Segurança da Informação. Esta norma destina-se a ajudar as organizações a estabelecer um Sistema de Gestão da Segurança da Informação (SGSI) com o objetivo de identificar, avaliar e gerir os riscos associados à segurança da informação (Robayo Jácome et al., 2023).

[16] Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Todas as alterações incluídas na versão atualizada da ISO/IEC 27001:2022 refletem a importância da gestão do risco. A norma orienta as organizações para a realização de uma avaliação exaustiva dos riscos, na qual é suposto identificarem os riscos potenciais que podem ameaçar a segurança da informação (Von Solms & Van Niekerk, 2013). Decorrente desta, as organizações devem garantir a aplicação de controlos adequados que possam contribuir para a minimização dos riscos. A norma pode ser integrada com outras normas, como a ISO/IEC 9001, relativa ao sistema de gestão da qualidade, e a ISO/IEC 14001, relativa ao sistema de gestão ambiental, facilitando a implementação e articulação dos vários subsistemas (Disterer, 2013).

A adoção da norma ISO/IEC 27001:2022 pode trazer inúmeros benefícios, nomeadamente, na promoção uma abordagem estruturada da gestão da segurança da informação, minimizando a probabilidade de incidentes e protegendo a reputação da organização. Em sectores críticos como das finanças, saúde e tecnologias, a conformidade com esta norma pode representar uma vantagem competitiva, reforçando a confiança dos clientes e parceiros na proteção de dados sensíveis (Robayo Jácome et al., 2023). A certificação ISO/IEC 27001, apoiada por controlos identificados na norma ISO/IEC 27002, pode também melhorar a imagem da organização e reduzir o risco de exposição à perda de informação confidencial.

A atualização dá ênfase a uma abordagem baseada na gestão do risco, em que a norma sugere que as organizações identifiquem potenciais ameaças e vulnerabilidades e estabeleçam uma gestão da segurança da informação que apoie os seus objetivos estratégicos, o que contribui para a criação de planos de segurança específicos e adaptáveis ao contexto de cada organização (Iqbal et al., 2009).

No entanto, a implementação do SGSI com base na norma ISO/IEC 27001:2022 envolve desafios. A adaptação aos requisitos da norma exige investimentos significativos de tempo, recursos financeiros e formação do pessoal. Além disso, o processo de certificação é rigoroso e exige auditorias regulares para garantir que o SGSI se mantém atualizado e em conformidade com a norma. A manutenção da certificação implica uma revisão e melhoria contínuas dos processos, o que exige um forte empenho organizacional (Disterer, 2013).

2.4.2 ISO/IEC 27002:2022

A ISO/IEC 27002:2022 é a mais recente atualização da norma que orienta a gestão da segurança da informação, atuando como um recurso fundamental na família de normas ISO/IEC 27000. Com um foco central nos controlos, esta versão foi revista para se alinhar com as mudanças tecnológicas e as novas ciberameaças, oferecendo um quadro detalhado para a implementação e manutenção de práticas de segurança da informação (Disterer, 2013).

A ISO/IEC 27002:2022 introduz novos controlos, como a segurança em ambientes de nuvem, a proteção do trabalho remoto e a ciber-resiliência. Estes controlos refletem a transformação digital acelerada pela pandemia da COVID-19, que incentivou a utilização de soluções em nuvem e de ferramentas de trabalho remoto, ampliando os riscos e exigindo um reforço dos mecanismos de segurança (ISO, 2022).

A ISO/IEC 27002:2022 introduz uma abordagem atualizada e detalhada para estabelecer controlos de segurança da informação, refletindo a evolução das ameaças e dos avanços tecnológicos. Esta norma complementa a ISO/IEC 27001, que estabelece os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI). Assim, enquanto a ISO/IEC 27001 é a norma de referência para a certificação, a ISO/IEC 27002 fornece as orientações práticas para a implementação de cada um dos controlos. Os requisitos para o cumprimento da norma, assim como os controlos presentes no Anexo A da mesma.

Uma das principais alterações introduzidas na ISO/IEC 27002:2022 é a reestruturação dos controlos, que passam a ser categorizados em quatro grandes temas: recursos organizacionais, humanos, físicos e tecnológicos. Esta nova organização permite uma melhor adequação aos sistemas de gestão da segurança, abrangendo todos os domínios, desde as políticas e procedimentos organizacionais até aos controlos de segurança físicos e tecnológicos específicos, abordando de forma abrangente as áreas críticas com impacto na segurança da informação (Iqbal et al., 2009). Tal dá às organizações a flexibilidade de escolher os controlos adequados ao seu contexto, sempre em linha com os requisitos da ISO/IEC 27001.

Estas adaptações à estrutura e ao enfoque da ISO/IEC 27002 reforçam o seu papel como recurso vital para as organizações desenvolverem e manterem controlos sólidos e eficazes, acompanhando as melhores práticas de proteção da informação.

2.4.3 ISO/IEC 27005:2022

A norma ISO/IEC 27005:2022 centra-se na gestão dos riscos de segurança da informação, fornecendo orientação para desenvolver um programa de gestão dos riscos, essencial para um SGSI. Esta norma ajuda as organizações a identificarem, avaliarem e mitigarem os riscos que podem comprometer a segurança dos seus dados e sistemas (Klipper, 2015).

A atualização de 2022 da norma reflete práticas modernas e adapta-se ao sofisticado ambiente digital, utilizando abordagens progressivas e mais eficientes para a avaliação e gestão dos riscos. Estas práticas incluem metodologias avançadas que têm em conta a rápida evolução das ciberameaças e as exigências de respostas ágeis e precisas. A norma destaca a importância de um processo de monitorização cíclico e contínuo, que permite às organizações monitorizar e responder a mudanças rápidas nos riscos de segurança, promovendo uma postura de segurança proactiva e adaptativa.

A ISO/IEC 27005:2022 estrutura o seu processo de gestão de riscos em várias fases que começam com a identificação detalhada de ativos críticos, vulnerabilidades e ameaças. A norma recomenda que as organizações analisem esses riscos considerando tanto o impacto potencial como a probabilidade de ocorrência, permitindo uma avaliação abrangente e completa. A norma orienta as organizações para estabelecerem controlos específicos e ações de mitigação que se alinhem com os seus objetivos de segurança e com a proteção dos ativos mais vulneráveis.

Ao adotar uma abordagem iterativa, a norma permite que as organizações revejam continuamente as suas práticas e ajustem os controlos e medidas de segurança conforme necessário. Esta metodologia de melhoria contínua garante que o programa de gestão de riscos não só acompanha as mudanças no ambiente digital, como também reforça a capacidade da organização para se adaptar a novas ameaças. A ISO/IEC 27005:2022 também oferece recomendações para garantir que o processo de gestão de riscos seja claramente documentado, facilitando o alinhamento com os requisitos regulamentares e as auditorias internas e externas.

A norma propõe ainda que as organizações integrem as suas práticas de gestão do risco com outros sistemas de gestão e segurança, criando um sistema mais coeso e abrangente. Desta forma, a ISO/IEC 27005:2022 contribui para a segurança da informação de uma forma holística, garantindo que todas as partes interessadas compreendem as ameaças e as medidas de proteção adotadas.

2.4.4 NIST SP 800-53

A publicação especial 800-53 do NIST ou NIST SP 800-53 é uma das diretrizes normalizadas utilizadas no domínio da cibersegurança, especialmente nos Estados Unidos. Esta publicação do *National Institute of Standards and Technology* (NIST) fornece um catálogo detalhado de controlos de segurança e privacidade que se destinam a proteger as operações das organizações, os seus ativos, pessoas e outras partes interessadas de uma vasta gama de ameaças (National Institute of Standards and Technology, 2009). A importância do NIST SP 800-53 reside na forma sistemática como aborda a segurança com um conjunto de controlos agrupados em categorias como o controlo do acesso, a resposta a incidentes e a proteção do sistema e das comunicações (Amiruddin et al., 2021).

A versão atual do quadro, lançada em 2020 (Revisão 5), representa uma melhoria significativa em relação às versões anteriores da publicação, uma vez que capta a natureza dinâmica da cibersegurança. Esta revisão alargou o seu enfoque aos controlos de segurança e privacidade, uma vez que estas áreas estão cada vez mais inter-relacionadas. Esta abordagem centra-se na incorporação de controlos de segurança e privacidade em todo o ciclo de vida de desenvolvimento do sistema, em vez de se limitar a adotar a segurança e a privacidade como duas abordagens diferentes ou relacionadas (Möller, 2023).

A flexibilidade do NIST SP 800-53 pode ser vista especialmente no que diz respeito à integração de novas tecnologias que incluem a computação em nuvem. Apesar do facto de os controlos do NIST SP 800-53 terem sido desenvolvidos para sistemas locais, são transferíveis para soluções de nuvem, que exigem medidas de segurança flexíveis e escaláveis. Isto é importante porque cada vez mais organizações estão a mudar as suas operações para serviços de nuvem, que têm uma arquitetura de segurança muito forte, mas facilmente alterável (Möller, 2023).

A abordagem baseada em riscos descrita no NIST SP 800-53 é especialmente útil no caso das PMEs, pois essas organizações provavelmente têm recursos limitados. Isto significa que estas organizações são capazes de implementar eficazmente os controlos mais importantes, sendo as prioridades determinadas pela gestão do risco (National Institute of Standards and Technology, 2009).

2.4.5 COBIT 19

O COBIT 2019 é um quadro de governação e gestão das TI lançado pela *Information Systems Audit and Control Association* (ISACA), Este, oferece às organizações um quadro através do qual podem integrar as estratégias de TI com as estratégias empresariais, a fim de obter valor e, ao mesmo tempo, gerir os riscos e os recursos. Este quadro baseia-se nas versões anteriores do COBIT, como o COBIT 5, mas o quadro atual introduziu muitas alterações que merecem ser incorporadas devido à atual transformação digital e à crescente complexidade dos ambientes de TI (Steuperaert, 2019).

Outra vantagem do COBIT 2019 é a sua flexibilidade para assimilar outras normas e boas práticas de governação das TI e a sua adaptabilidade aos requisitos de qualquer organização. Baseia-se em 40 princípios de governação e gestão que estão relacionados com elementos-chave da organização, nomeadamente: processos, estruturas, informação e cultura. Este modelo abrangente permite que as organizações revejam sistematicamente e melhorem as suas estruturas de governação (Steuperaert, 2019).

Um aspeto único do quadro revisto é a enfâse no desenvolvimento de um sistema de governação de TI específico da empresa, que esteja alinhado com os objetivos da entidade, o apetite pelo risco e o ambiente atual de TI. Esta flexibilidade é especialmente benéfica no ambiente atual, em que as organizações empresariais têm de responder às tecnologias emergentes, à evolução dos quadros jurídicos e à mudança das preferências dos consumidores no mais curto espaço de tempo possível (Wattimury & Faza, 2023). O COBIT 2019 é suficientemente flexível para permitir que as organizações passem pelo processo de transformação digital e, ao mesmo tempo, tenham uma governação e um controlo sólidos dos recursos de TI.

Para além disso, o COBIT 2019 define “áreas de foco” que se destinam a determinados domínios de preocupação, como a cibersegurança, DevOps e computação em nuvem. Esta caraterística pode ajudar as organizações a destacar e desenvolver os aspetos mais críticos para a sua estratégia. Estas áreas de foco estão incluídas no quadro, o que mostra que este é sensível às tendências e desafios atuais do sector das TI (Steuperaert, 2019). Isto significa que o COBIT 2019 é muito útil para dar resposta às novas tecnologias e aos novos riscos.

A COBIT 2019 integra também a medição do desempenho através de modelos de maturidade, através dos quais as organizações podem determinar a sua prática atual de governação e as potenciais necessidades de desenvolvimento. Este processo de melhoria contínua é importante para garantir que a estrutura se mantenha relevante e eficaz nos anos seguintes. Tal como sugerido por Lobo et al. (2022), as ferramentas de gestão do desempenho do COBIT 2019 são capazes de oferecer medidas e informações essenciais que ajudam a melhorar a governação das TI numa base contínua.

2.4.6 PCI-DSS (Payment Card Industry Data Security Standard)

A norma de segurança de dados da indústria de cartões de pagamento (PCI-DSS) é um quadro crucial concebido para salvaguardar as informações dos titulares de cartões e melhorar a segurança das transações financeiras a nível mundial. Criado *pelo Payment Card Industry Security Standards Council* (PCI SSC), o PCI-DSS oferece um conjunto sólido de requisitos e diretrizes de segurança com o objetivo de garantir que todas as organizações envolvidas no manuseamento de cartões de pagamento mantêm padrões rigorosos de proteção de dados. O regulamento engloba vários requisitos, como a segurança da rede, a encriptação, o controlo de acesso e a monitorização e teste periódicos dos sistemas (Bonner et al., 2011).

O PCI-DSS baseia-se num conjunto de princípios essenciais destinados a proteger as informações sensíveis dos cartões de pagamento. O quadro está organizado em doze requisitos-chave, que são categorizados em seis objetivos principais: Estabelecer e sustentar uma rede segura, salvaguardar as informações do titular do cartão, gerir proactivamente as vulnerabilidades, aplicar medidas rigorosas de controlo de acesso, realizar monitorização e testes periódicos da rede e adotar uma política de segurança da informação (Ukidve et al., 2017).

Cada requisito contém orientações detalhadas e melhores práticas concebidas para lidar com vários aspetos da segurança da informação, desde a proteção da arquitetura da rede até à adoção de métodos avançados de encriptação de dados (Bonner et al., 2011).

2.4.7 ITIL (*Information Technology Infrastructure Library*)

A ITIL é uma estrutura para a gestão de serviços de TI que é atualmente popular entre muitas organizações e que visa apoiar os objetivos empresariais através de uma gestão adequada dos serviços de TI. Iniciando o seu percurso na década de 1980 na *Central Computer and Telecommunications Agency* (CCTA) no Reino Unido, a ITIL transformou-se numa estrutura completa que visa melhorar a qualidade da prestação de serviços de TI. A ITIL é um quadro que define as melhores práticas para a gestão dos serviços informáticos, a fim de satisfazer as necessidades dos clientes, centrando-se simultaneamente na melhoria dos serviços.

A estrutura ITIL está organizada em vários componentes-chave, incluindo o ciclo de vida do serviço ITIL, que consiste em cinco fases: estratégia do serviço, conceção do serviço, transição do serviço, operação do serviço e melhoria contínua do serviço (González, 2015). Cada fase contém processos e práticas que visam o controlo e a melhoria dos serviços de TI em todas as fases da sua existência. A estrutura centra-se na necessidade de reunir conhecimentos sobre as necessidades do cliente, monitorizar e controlar a qualidade do serviço e garantir que os serviços de TI contribuem para a realização dos objetivos empresariais.

As novas alterações feitas à ITIL, especialmente à ITIL 4, proporcionaram melhorias valiosas para enfrentar os desafios atuais da gestão de serviços de TI. Uma das principais mudanças na ITIL 4 é que é dada mais atenção à forma como a gestão de serviços de TI se deve alinhar com outros sistemas de gestão e melhores práticas, incluindo Agile, DevOps e Lean. Esta integração mostra que existe uma necessidade crescente de flexibilidade e cooperação nos atuais ambientes de TI (González, 2015).

2.4.8 ISO/IEC 22301

A norma ISO/IEC 22301 foi revista em outubro de 2019 para fornecer a segunda edição da norma BCM que define os requisitos para a conceção e implementação do BCMS. Esta norma oferece um quadro através do qual as organizações podem estar

preparadas para gerir e manter as suas operações durante e após uma perturbação, garantindo assim a segurança e a resiliência organizacional (ISO, 2019).

A norma é genérica e pode ser utilizada por qualquer organização, independentemente da sua natureza, dimensão ou indústria, e o seu objetivo é facilitar a continuidade das atividades comerciais, mesmo em caso de incidentes perturbadores. A ISO/IEC 22301 também exige que as organizações adotem uma abordagem metódica para identificar riscos e ameaças, a sua suscetibilidade, bem como para desenvolver e aplicar medidas para os minimizar e assegurar a continuidade das atividades e a recuperação de incidentes (ISO, 2019).

O núcleo da norma é a aplicação do ciclo Plan-Do-Check-Act (PDCA), que estrutura o processo de gestão em quatro fases principais: As diferentes fases são o planeamento, a implementação, a verificação e a ação. A fase de planeamento consiste na definição do contexto e dos objetivos da continuidade das atividades, na identificação dos riscos e das oportunidades, bem como na formulação de políticas e objetivos adequados. A implementação e a operação estão relacionadas com o desenvolvimento do sistema e dos seus controlos para garantir a continuidade da atividade, enquanto a verificação é o ato de observar o sistema e avaliar a sua eficácia. A ação, por outro lado, centra-se nos aspetos contínuos, como a melhoria, as retificações de não conformidades e o reforço dos sistemas de gestão (ISO, 2019).

Os principais elementos da norma consistem em descrever as fronteiras do sistema de gestão da continuidade, estabelecer as políticas de continuidade, identificar os requisitos legais e regulamentares e desenvolver planos e procedimentos para a gestão de crises e a recuperação das operações. Também fornece o foco principal no envolvimento da liderança, recursos, comunicação e documentação no apoio à implementação e avaliação do sistema (ISO, 2019).

Ao mesmo tempo, a norma prescreve a análise do impacto nas empresas e a avaliação dos riscos, o planeamento da continuidade e as soluções de planeamento, o programa de exercícios e as revisões contínuas. A ISO/IEC 22301 também sublinha que a conformidade com a norma pode ser comprovada através de autoavaliação, feedback das partes interessadas ou certificação por uma parte externa, o que significa que as organizações têm a possibilidade de escolher a forma como irão comprovar a sua conformidade (ISO, 2019).

3 A EMPRESA

3.1 Missão | Atividades | Visão

A Besturban é uma consultora imobiliária nacional especializada em serviços imobiliários integrados. Com mais de uma década de experiência no mercado português, a empresa tem trabalhado tanto no sector público como no privado, afirmando-se como um pilar de fiabilidade e competência. A sua equipa é constituída por profissionais altamente qualificados e experientes, empenhados em acompanhar os clientes ao longo de todo o processo imobiliário, garantindo assim um serviço de qualidade superior.

Desde a sua fundação, a Besturban tem-se dedicado a servir um vasto leque de clientes, incluindo investidores institucionais, promotores imobiliários e instituições financeiras. A empresa reconhece que uma decisão de investimento bem-sucedida requer um conhecimento profundo do mercado e uma análise meticulosa. Por esta razão, a Besturban acompanha os seus clientes em todas as fases, desde a análise inicial até à promoção e gestão de projetos e empreendimentos, assegurando que cada decisão é baseada em informação rigorosa e relevante.

De acordo com o website da empresa[17], a *missão* da Besturban é prestar serviços imobiliários de excelência, baseados na transparência, integridade e responsabilidade. A empresa está empenhada na melhoria contínua dos seus serviços, procurando a satisfação total dos seus clientes. A abordagem da Besturban é pautada por um profundo conhecimento do mercado e rigorosas práticas de avaliação, visando auxiliar investidores, e instituições financeiras a atingirem seus objetivos com sucesso.

Os *valores* da Besturban - credibilidade, experiência e responsabilidade - são fundamentais para o compromisso da empresa com o sucesso dos seus clientes. A empresa acredita que a estreita colaboração com os seus clientes é crucial para os ajudar a atingir os seus objetivos. Com registo na Comissão do Mercado de Valores Mobiliários (CMVM) e seguro de responsabilidade civil reforça o seu compromisso de excelência e confiança no sector imobiliário.

[17] https://www.Besturban.pt/

A Besturban oferece uma gama completa de *serviços* de consultoria e avaliação imobiliária, com enfoque nas seguintes áreas:

- Avaliação de imóveis: Realiza avaliações imobiliárias precisas e fiáveis em todo o território nacional, incluindo imóveis residenciais, comerciais e industriais. A empresa está certificada pela NP EN ISO/IEC 9001:2015 e é membro da ASAVAL, garantindo a qualidade e independência dos seus serviços.
- Avaliação de Ativos Geradores de Rendimento: Especializada na avaliação de imóveis geradores de rendimento, tais como hotéis, centros comerciais e edifícios de escritórios. Utiliza análises de cash-flows e cenários para determinar o valor dos ativos.
- Avaliação de Máquinas e Equipamentos: Realiza avaliações técnicas detalhadas de máquinas e equipamentos, considerando aspetos como segurança, manutenção, eficiência energética e obsolescência.
- Consultoria e Gestão de Projetos Imobiliários: Apoia os clientes em todas as fases dos projetos imobiliários, desde a análise inicial e promoção até à gestão e execução do projeto.
- Avaliação de Imóveis e Outros Serviços: Oferece avaliações para compra e venda, crédito à habitação, participações sociais, seguros e contabilidade.

Com uma equipa de profissionais altamente qualificados e uma rede de colaboradores experientes em todo o país, a Besturban distingue-se pela capacidade de prestar serviços de elevada qualidade e soluções adaptadas às necessidades específicas de cada cliente.

3.2 Organização, papeis e responsabilidades

A Besturban, conta com cerca de 40 colaboradores internos e uma rede de peritos avaliadores externos, distribuídos por diferentes áreas de especialização. A estrutura organizacional foi desenhada para garantir a máxima eficiência e qualidade nos serviços prestados, desde avaliações imobiliárias até consultoria e gestão de projetos. A equipa é composta por profissionais qualificados, cuja atuação integrada permite à empresa manter os elevados padrões de excelência que a caracterizam.

A empresa possui uma hierarquia funcional (Figura 2), com papéis e responsabilidades bem definidos, de modo a assegurar que todas as atividades são realizadas de acordo

com as exigências do mercado e os requisitos normativos, incluindo a recente certificação ISO/IEC 27001, que confirma o seu compromisso com a segurança da informação.

Figura 2: Hierarquia funcional da Besturban

Fonte: Documento interno Besturban

O Conselho de Administração (CA) é o órgão que supervisiona a estratégia global da Besturban, assegurando o alinhamento com os seus valores e missão. É responsável por tomar decisões cruciais relacionadas à expansão, inovação e alinhamento com os valores e normas regulamentares. O CA também assegura o cumprimento das certificações ISO/IEC 9001 e ISO/IEC 27001[18], gerindo os riscos e oportunidades de melhoria contínua da empresa.

O Departamento Comercial (Vendas e Marketing) está encarregue de gerir o relacionamento com os clientes, oferecendo serviços personalizados que atendem às suas necessidades. Este departamento tem um papel fundamental na negociação de

[18] Após a implementação do SGSI documentado neste trabalho de projeto.

contratos e na assessoria técnica, garantindo que os projetos imobiliários sejam viáveis e que a satisfação do cliente seja sempre uma prioridade.

A equipa de avaliação imobiliária é responsável por realizar avaliações rigorosas e independentes de ativos, como imóveis residenciais, comerciais e industriais. A Besturban é membro da ASAVAL, o que assegura que todas as avaliações seguem padrões rigorosos de qualidade e imparcialidade. Este departamento também realiza a avaliação de máquinas e equipamentos, utilizando metodologias detalhadas para garantir a precisão dos relatórios.

A infraestrutura de IT da Besturban é gerida por uma empresa externa contratada para este fim. Esta parceria estratégica permite à Besturban focar-se no seu core business, enquanto garante um suporte especializado em todas as questões tecnológicas. A empresa externa é responsável pela:

- Manutenção da infraestrutura tecnológica.
- Implementação e atualização de sistemas de *software* e *hardware*.
- Garantir a segurança cibernética, incluindo a proteção de dados sensíveis e a conformidade com a legislação aplicável, como o Regulamento Geral sobre a Proteção de Dados (RGPD).
- Assistência técnica ao pessoal da Besturban, assegurando que as operações do dia-a-dia correm de forma eficiente.
- Segurança da informação, assegurando conformidade com a certificação ISO/IEC 27001[18].
- Proteção de dados sensíveis, de acordo com os requisitos da ISO/IEC 27001[18] e do RGPD.

A subcontratação dos serviços de IT garante apoio especializado, reduz a necessidade de recursos humanos internos dedicados e permite beneficiar de tecnologias de ponta e práticas de segurança avançadas.

A comunicação interna na Besturban é essencial para o alinhamento de todos os departamentos e colaboradores. Reuniões periódicas garantem que as atividades estão alinhadas com os objetivos estratégicos da empresa e que qualquer desafio ou questão pode ser rapidamente resolvido. A cooperação entre a empresa externa responsável

pelo IT e os departamentos internos é fundamental para assegurar que a segurança da informação e a gestão tecnológica são tratadas de forma eficiente.

A Besturban tem o compromisso de garantir a qualidade em todos os seus processos, tal como evidenciado pelas certificações ISO/IEC 9001 e ISO/IEC 27001[18]. A ISO/IEC 27001, em particular, reflete o empenho da empresa em proteger a confidencialidade, integridade e disponibilidade da informação, um ativo crítico no setor imobiliário, onde a segurança de dados financeiros e pessoais é primordial.

A melhoria contínua é uma prioridade para a Besturban, que investe regularmente em formação para os seus colaboradores, garantindo que as práticas de segurança e qualidade são sempre mantidas em níveis elevados.

3.3 Sistemas e Tecnologias de Informação

A Besturban possui uma infraestrutura de Tecnologias da Informação e Comunicação (TIC) robusta e moderna, concebida para suportar as suas operações comerciais, tanto na área da consultoria imobiliária como na construção. A infraestrutura de rede da empresa é composta por uma rede local (LAN), constituída por ativos de rede de gama empresarial que asseguram uma conectividade rápida, estável e segura entre os vários departamentos.

Além disso, a empresa adotou medidas de proteção avançadas contra falhas e interrupções, reforçadas pela aquisição de novo *hardware* durante o projeto de implementação do SGSI, incluindo fontes de alimentação ininterrupta (UPS) e sistemas de backup para os principais servidores e dispositivos de armazenamento, permitindo a continuidade operacional em caso de avarias ou falhas de energia. Estas soluções são complementadas por *backups* automáticos e redundantes, realizados diariamente e armazenados em localizações geograficamente dispersas, garantindo uma rápida recuperação de dados em situações críticas.

A Besturban dispõe de um Sistema de Informação (SI) abrangente que integra plataformas e *software* especializados para apoiar as atividades dos seus diversos departamentos. O sistema foi concebido para garantir a segurança, integridade e eficiência dos dados, fatores críticos para o sucesso da empresa no setor imobiliário. A infraestrutura de servidores combina soluções locais e na nuvem, proporcionando flexibilidade, escalabilidade e alta disponibilidade dos dados e serviços.

As principais áreas de operação da Besturban são suportadas por diferentes sistemas de informação. Para a gestão de projetos, a empresa utiliza plataformas que permitem o acompanhamento em tempo real dos recursos alocados, do progresso das tarefas e da gestão de prazos, otimizando a eficiência operacional. No departamento financeiro, a Besturban adota um sistema ERP (*Enterprise Resource Planning*) que agiliza os processos contabilísticos, financeiros e de compras, assegurando o cumprimento das normativas regulamentares e facilitando a tomada de decisões estratégicas.

3.4 Colaboração e Produtividade

Para apoiar a colaboração interna e a comunicação entre os colaboradores, a Besturban adotou ferramentas de produtividade baseadas na nuvem, como o Microsoft 365, que inclui soluções de correio eletrónico empresarial, videoconferência e armazenamento seguro de documentos. Estas ferramentas facilitam a comunicação e o trabalho colaborativo, permitindo que as equipas operem de forma eficaz, quer estejam no escritório ou em trabalho remoto.

A utilização dessas plataformas garante que todos os dados estão protegidos com os mais altos níveis de segurança e que os colaboradores podem aceder a informações e colaborar em tempo real, independentemente da sua localização geográfica. Esta abordagem não só aumenta a eficiência interna, mas também reforça a capacidade da Besturban de se adaptar rapidamente às necessidades em constante evolução do mercado.

3.5 Suporte a Clientes e CRM

No que diz respeito à gestão de relações com os clientes, a Besturban utiliza um sistema de CRM (*Customer Relationship Management*) para acompanhar todas as interações com os clientes e parceiros. Este sistema permite uma gestão personalizada de cada projeto e das oportunidades de negócio, assegurando um acompanhamento eficaz e uma comunicação clara ao longo de todo o ciclo de vida dos projetos imobiliários.

O CRM contribui para a melhoria contínua dos serviços prestados, permitindo à Besturban responder de forma eficiente às expectativas dos seus clientes, promovendo a sua satisfação e fidelização.

3.6 Gestão de IT e Monitorização Remota

A gestão das tecnologias de informação da Besturban é assegurada por uma equipa externa especializada, que utiliza *software* de *Remote Monitoring and Management* (RMM) para supervisionar de forma proativa os sistemas e dispositivos da empresa. Este *software* permite a monitorização contínua da infraestrutura tecnológica, identificando possíveis falhas ou vulnerabilidades antes que possam causar interrupções significativas nas operações.

Graças ao RMM, a equipa de IT consegue garantir a máxima disponibilidade dos sistemas, resolver incidentes de forma rápida e aplicar atualizações ou correções de segurança sem afetar o fluxo normal de trabalho. Este tipo de gestão proativa é essencial para manter a integridade e a eficiência dos sistemas de informação, garantindo que os dados da Besturban permanecem protegidos e que as operações comerciais correm de forma contínua e estável.

3.7 Resiliência e Recuperação de Desastres

A Besturban tem uma estratégia de resiliência bem definida, com soluções de backup e recuperação de desastres robustas. Os *backups* automáticos são realizados diariamente, com cópias dos dados críticos armazenadas em locais geograficamente redundantes, o que minimiza o tempo de inatividade em caso de falhas catastróficas. A infraestrutura de monitorização contínua também permite que a equipa de IT identifique e responda prontamente a quaisquer incidentes ou anomalias na rede, reduzindo o impacto potencial nas operações.

Em suma, o sistema de Tecnologias de Informação da Besturban foi projetado para suportar a sua missão de prestar serviços no setor imobiliário, garantindo a segurança dos dados, a continuidade operacional e a eficiência dos processos.

4 O SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

4.1 Introdução

4.1.1 Motivações para a Certificação ISO/IEC 27001

A certificação ISO/IEC 27001 reflete o compromisso da Besturban com a segurança da informação, ao passo que a combinação de infraestruturas locais e na nuvem permite que a empresa inove e se adapte às necessidades em constante mudança dos seus clientes e do mercado.

A decisão da empresa de procurar a certificação ISO/IEC 27001 foi motivada pela necessidade crescente de proteger a informação confidencial gerida pela empresa, especialmente no contexto das suas operações com o setor bancário e outras entidades financeiras. De acordo com o CEO, a natureza sensível dos dados exige um sistema robusto que possa garantir a sua segurança, integridade e confidencialidade.

A certificação foi uma escolha estratégica para reforçar a confiança dos clientes e parceiros e demonstrar o compromisso da empresa com os mais elevados padrões de segurança da informação. Detalhes sobre essa motivação podem ser encontrados na entrevista ao CEO que consta no Anexo A. Nela, o CEO destacou que, "uma vez que na nossa atividade trabalhamos com informação confidencial, temos de ter o máximo de cuidado em conservá-la em nossa posse, sem perigo de ser tornada pública." Essa preocupação com a segurança da informação foi um fator crucial na decisão de prosseguir com a certificação.

Outra motivação importante decorreu do objetivo de melhoria continua dos processos internos. A Besturban já havia implementado outras normas, como a ISO/IEC 9001, pelo que a ISO/IEC 27001 veio complementar essa estratégia de conformidade com padrões internacionais, consolidando a imagem da empresa como líder em qualidade e segurança. Além disso, ser das primeiras empresas no setor de avaliação imobiliária em Portugal a obter a certificação ISO/IEC 27001 proporcionou uma potencial vantagem competitiva, reforçando a sua posição no mercado nacional.

4.1.2 Objetivos da Certificação ISO/IEC 27001

O principal objetivo da Besturban com a certificação ISO/IEC 27001 foi garantir que todos os processos e sistemas relacionados com a gestão da informação estivessem em conformidade com normas nacionais e internacionais de segurança. A empresa

procurou estabelecer um **Sistema de Gestão de Segurança da Informação (SGSI)** que não só protegesse os dados sensíveis, mas também aumentasse a confiança dos seus *stakeholders*.

Além disso, a certificação visava:

- **Mitigar riscos** associados à perda, roubo ou divulgação não autorizada de dados.
- **Padronizar processos de segurança** da informação para garantir consistência e eficiência operacional.
- **Automatizar** o máximo de processos possível antes da auditoria externa, permitindo uma gestão mais eficiente e reduzindo a intervenção manual.
- **Aumentar a confiança** dos clientes e parceiros no compromisso da Besturban com a segurança e conformidade regulamentar, especialmente no setor financeiro.

4.1.3 Programação e Cronograma de Implementação

O processo de certificação foi planeado em várias fases, envolvendo uma preparação minuciosa antes da auditoria externa. Esta fase preparatória estendeu-se ao longo de vários meses, durante os quais foram implementadas alterações significativas tanto a nível tecnológico como ao nível dos comportamentos dos colaboradores.

Uma das alterações tecnológicas mais relevantes foi a aquisição de um novo servidor e a deslocalização de um disco de rede para um local remoto, garantindo redundância e maior proteção contra falhas físicas e eventuais intrusões. Esta medida assegurou que os dados da Besturban estariam protegidos mesmo em caso de incidentes localizados.

Ao mesmo tempo, foi necessário automatizar o maior número possível de processos e garantir que as práticas de segurança da informação estivessem alinhadas com os padrões da ISO/IEC 27001. A empresa também investiu em fontes de alimentação ininterrupta (UPS) e em soluções de backup geograficamente redundantes, assegurando a continuidade do negócio em caso de falhas ou interrupções.

O cronograma da certificação foi fortemente condicionado pela preparação da infraestrutura tecnológica e pela sensibilização dos colaboradores para os novos processos de segurança.

4.1.4 Metodologia Adotada

A metodologia adotada pela Besturban na implementação do SGSI baseado na norma ISO/IEC 27001 foi composta por várias etapas chave, todas alinhadas com o ciclo PDCA[19] (Plan-Do-Check-Act). Esta abordagem permitiu uma implementação estruturada, com uma forte ênfase na identificação de riscos, definição de controlos e auditorias internas e externas.

4.1.5 Fase de Planeamento (Plan)

A fase de planeamento incluiu uma avaliação inicial dos sistemas e processos existentes, seguida de uma análise de lacunas face aos requisitos da norma ISO/IEC 27001. A empresa identificou áreas críticas que precisavam de melhorias, especialmente na gestão da infraestrutura de TI, segurança de dados e nas práticas dos colaboradores. O CEO mencionou que a Besturban teve o apoio de consultores externos, nomeadamente, o consultor responsável pela implementação do Sistema de Gestão de Segurança da Informação (SGSI) e o consultor responsável pela infraestrutura de TI. Este último esteve presente em todas as reuniões, proporcionando uma ajuda valiosa na definição de estratégias e na identificação de áreas críticas que precisavam de melhorias.

4.1.6 Fase de Implementação (Do)

Na fase de implementação, foram introduzidas mudanças tecnológicas e comportamentais. Do ponto de vista tecnológico, a empresa adotou novas soluções de monitorização de sistemas através de *software Remote Monitoring and Management* (RMM), que permitiu o controlo centralizado das operações de TI. Foram também implementadas políticas de criptografia em todos os dispositivos dos colaboradores, assegurando a proteção de dados em caso de perda ou roubo de equipamentos.

Paralelamente, a Besturban investiu na formação e sensibilização dos seus colaboradores para garantir que todos compreendessem os novos procedimentos de segurança. O CEO sublinhou a importância de criar uma cultura de segurança da

[19] Ver 2.1.6

informação, onde cada colaborador tem um papel ativo na proteção dos dados da empresa.

4.1.7 Fase de Verificação (Check)

A fase de verificação incluiu a **auditoria interna** dos processos implementados, com o apoio de uma nova empresa de consultoria. A auditoria serviu para identificar não conformidades e ajustar o sistema antes da auditoria externa, assegurando que todos os requisitos da ISO/IEC 27001 estavam a ser cumpridos.

4.1.8 Fase de Melhoria Contínua (Act)

A Besturban continua a manter um ciclo de melhoria contínua, adaptando os seus processos e tecnologias à medida que surgem novas ameaças e desafios no campo da segurança da informação. A sensibilização dos novos colaboradores para as normas de segurança e o investimento constante em soluções de backup e recuperação de desastres são exemplos práticos do compromisso da empresa com a manutenção da certificação.

A implementação da ISO/IEC 27001 pela Besturban foi um processo desafiante, mas fundamental para garantir a proteção da informação sensível com que a empresa lida diariamente. A certificação trouxe vantagens competitivas e fortaleceu a posição da empresa no mercado nacional, mostrando aos clientes e parceiros que a segurança da informação é tratada com o mais alto nível de seriedade e profissionalismo. O sucesso do processo reflete-se na capacidade da Besturban de melhorar continuamente os seus sistemas e de se adaptar às exigências tecnológicas e regulamentares do setor.

4.2 Segurança da Informação e Conformidade com a ISO/IEC 27001

A segurança da informação é uma prioridade absoluta para a Besturban, que obteve a certificação ISO/IEC 27001, reforçando o seu compromisso com a proteção da confidencialidade, integridade e disponibilidade dos dados. A empresa implementou uma combinação de medidas técnicas e organizacionais para mitigar os riscos de segurança e garantir a conformidade com as melhores práticas de cibersegurança.

Entre os controlos utilizados para proteger a infraestrutura de TIC, destacam-se as firewalls NGF (*Next Generation Firewall*), sistemas de deteção e prevenção de intrusões

(IDS/IPS) e políticas de gestão de acesso. Para fortalecer ainda mais a segurança, a Besturban passou a utilizar autenticação multifator (MFA) para todos os seus colaboradores, e todos os computadores da empresa são protegidos por criptografia de disco, garantindo que os dados armazenados estão inacessíveis em caso de perda ou roubo de dispositivos. Essas práticas asseguram que apenas utilizadores autorizados acedem aos sistemas críticos, protegendo informações confidenciais contra ameaças externas e internas.

Adicionalmente, a empresa centralizou a gestão de dados sensíveis em servidores NAS (*Network-Attached Storage*), e os dispositivos de backup, como discos externos USB, são armazenados em locais seguros para proteção extra contra falhas e ataques. Estas medidas asseguram que as operações da Besturban continuam de forma estável e protegida, mesmo em situações adversas.

4.3 Governança

A governança na Besturban é essencial para garantir que a empresa atinja seus objetivos de forma eficaz e ética, especialmente no contexto da certificação ISO/IEC 27001. A estrutura de governança da Besturban inclui um Conselho de Administração que define a visão e a estratégia da empresa, aprova políticas e supervisiona a conformidade com normas, incluindo a ISO/IEC 27001. Além disso, a empresa possui comités de governança. Esses comités são formados por membros da equipa de gestão e consultores externos, que se reúnem regularmente para discutir questões críticas, avaliar o desempenho e propor melhorias.

A Besturban implementou uma política robusta de segurança da informação que orienta a proteção de informações confidenciais, assegurando que todos os colaboradores conheçam suas responsabilidades. A equipa de TI, composta por profissionais e consultores externos, assegura a infraestrutura tecnológica e implementa soluções de segurança.

A empresa adota uma abordagem sistemática para identificar e mitigar riscos relacionados com a segurança da informação, garantindo a implementação de controlos adequados. Programas de formação contínua são oferecidos para sensibilizar os colaboradores sobre suas responsabilidades e melhores práticas em segurança da

informação. Para avaliar a conformidade com a ISO/IEC 27001 e a eficácia do SGSI, a Besturban realiza auditorias internas e externas, identificando áreas de melhoria.

A revisão e atualização regulares das políticas e práticas de segurança são prioridades na Besturban, que procura constantemente inovações que fortaleçam sua postura de segurança e agreguem valor aos serviços. A governança eficaz na Besturban, com responsabilidades bem definidas e foco na melhoria contínua, é fundamental para o sucesso da implementação da ISO/IEC 27001 e para a sua posição de liderança no setor imobiliário.

4.3.1 Política(s), Normas e Procedimentos

A Besturban implementou um Sistema de Gestão da Segurança da Informação (SGSI) com uma política geral e várias políticas pormenorizadas (setoriais), cada uma das quais aborda aspetos específicos da segurança.

A *Política Geral de Segurança da Informação* da Besturban estabelece os princípios fundamentais do SGSI, salientando a importância da disponibilidade, integridade e confidencialidade da informação. A empresa compromete-se a proteger os ativos de informação contra o acesso não autorizado, a minimizar os riscos para evitar incidentes e, caso estes ocorram, a comunicá-los e investigá-los adequadamente. A gestão do risco é efetuada de forma periódica e sistemática e a Besturban assegura o cumprimento dos requisitos legais, regulamentares e contratuais. A segurança da informação é incorporada na cultura organizacional, sendo os colaboradores formados para atuar na prevenção e minimização dos riscos.

A *Política de Classificação da Informação* da Besturban define categorias específicas para a classificação da informação com base nos níveis de segurança, comunicação e reprodução. As informações são classificadas em quatro níveis de segurança: Confidencial, Restrito, Corporativo e Público. O nível de comunicação determina quem pode aceder à informação, enquanto o nível de reprodução define as permissões para reproduzir ou alterar documentos. O manuseamento da informação deve seguir as regras estabelecidas para cada classificação, e a eliminação deve garantir que a informação não pode ser recuperada.

A *Política de Controlo de Acessos Físico e Digital* pressupõe um ambiente de *open space* com acesso físico controlado por chaves (físicas) atribuídas aos colaboradores.

Os computadores são protegidos por senhas e a documentação sensível é guardada em armários fechados à chave, acessíveis apenas ao Diretor e ao Coordenador Geral. O acesso digital é regulado através de contas de acesso pessoais e intransmissíveis, e a autorização de acesso a bens e serviços baseia-se em perfis de privilégio definidos.

A *Política de Salvaguarda da Informação, Proteção contra Ameaças e Códigos Maliciosos* inclui processos de backup diários efetuados num servidor NAS fora das instalações da Besturban e testes mensais para garantir a integridade dos dados.

A empresa utiliza ferramentas para proteger os seus ativos contra vírus, *trojans*, *worms* e outros códigos maliciosos, mas os utilizadores devem também adotar comportamentos seguros para minimizar a probabilidade de infeção. Estas precauções estão descritas na *Política de Utilização de Dispositivos Móveis*.

A *Política de Uso de Dispositivos Móveis* detalha os cuidados que os utilizadores devem ter com os dispositivos disponibilizados pela Besturban, como garantir a integridade física do equipamento, manter o ambiente de trabalho limpo e assegurar que as informações estejam no servidor para backup diário. É importante também que os dispositivos móveis estejam atualizados e protegidos por ferramentas de segurança, e que os usuários não instalem *softwares* não autorizados ou acedam redes Wi-Fi públicas sem as devidas precauções.

A política de palavras-passe (Autenticação) estabelece orientações para a utilização de palavras-passe fortes, alterando-as regularmente e não as partilhando com outras pessoas. As palavras-passe devem ter pelo menos 10 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais, e uma sugestão para criar palavras-passe fortes é utilizar frases e as suas iniciais.

A *Política de Acesso Remoto* restringe o acesso remoto aos ativos de informação e serviços da Besturban apenas aos utilizadores que dele necessitem para a sua atividade profissional, incluindo terceiros ou prestadores de serviços quando necessário. Todas as informações acedidas, transmitidas, recebidas ou produzidas via acesso remoto estão sujeitas a controlo.

A *Política de Resposta a Incidentes de Segurança da Informação* define que qualquer ocorrência que afete a confidencialidade, integridade ou disponibilidade dos ativos de informação deve ser tratada para minimizar o impacto e restaurar a segurança. Os

incidentes devem ser imediatamente comunicados ao responsável pela segurança da informação, que, se necessário, contactará o gestor de TI e, em casos graves, informará as organizações externas relevantes.

A *Política De Utilização Aceitável Dos Ativos De Informação* abrange a utilização de equipamento, componentes amovíveis e equipamento de impressão. A utilização de dispositivos USB e discos rígidos deve ser cuidadosa para evitar a contaminação por *malware*.

A *Política de Utilização do Correio Eletrónico e do Acesso à Internet* permite que os serviços de correio eletrónico e de Internet sejam utilizados exclusivamente para atividades profissionais, com monitorização para proteger a organização e garantir o cumprimento das regras de segurança da informação.

A *Política de Proteção de Dados Pessoais* assegura a confidencialidade da informação recebida para a prestação de serviços, com a celebração de acordos de confidencialidade. Embora a empresa não seja obrigada a ter um responsável pela proteção de dados, foi nomeado um responsável pela proteção de dados.

A formação e a sensibilização exigem que os funcionários e terceiros recebam formação para utilizar os recursos de informação e aplicar conceitos de segurança para garantir a proteção da informação. Qualquer violação das políticas pode levar a ações disciplinares.

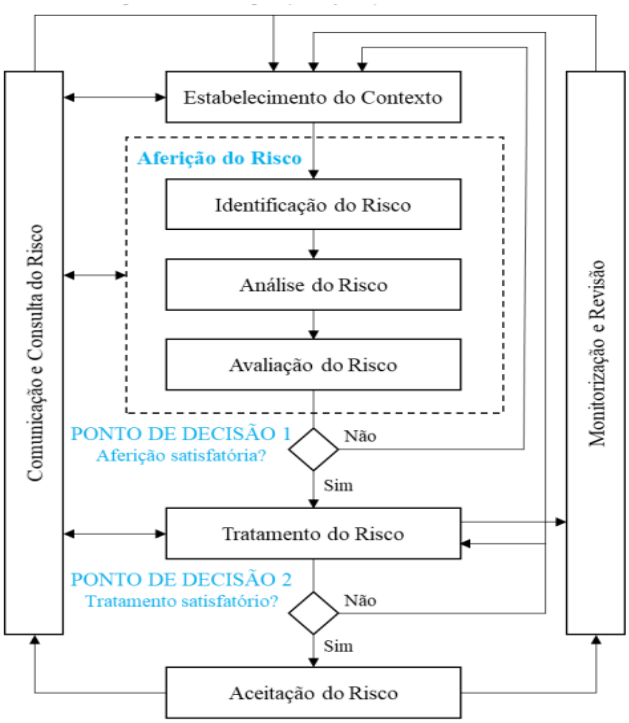
Por fim, a Besturban incentiva sugestões e relatos de irregularidades observadas, com comunicação imediata ao responsável pela Segurança da Informação para que sejam tomadas as medidas necessárias e implementadas melhorias contínuas na segurança da informação.

4.4 Gestão de Risco

A metodologia de avaliação de riscos tem como objetivo identificar e tratar os riscos relacionados com a segurança da informação num sistema organizacional, garantindo a proteção dos ativos de informação. Este processo está estruturado para avaliar o impacto e a probabilidade dos riscos, ajudando a definir ações adequadas para mitigar esses riscos.

O processo de gestão do risco adotado pela Besturban teve como base a norma ISO/IEC 27005 (Figura 3).

Figura 3 : Processo de gestão do risco da segurança da informação.



Fonte: Adaptado de ISO/IEC 27005

Nos termos da norma ISO/IEC 27005:2022, o primeiro passo da metodologia (ver 2.4.3) foi a análise do contexto da organização, incluindo, nomeadamente, a identificação dos ativos de informação e o perfil de risco da organização. Estes ativos podem incluir dados críticos, sistemas, *hardware* e qualquer outro elemento essencial para as operações da organização.

Uma vez identificados, o passo seguinte foi determinar as ameaças e vulnerabilidades associadas a cada ativo. As ameaças podem incluir ciberataques, erros humanos ou falhas de sistema, enquanto as vulnerabilidades podem ser fraquezas nos sistemas de segurança ou práticas inadequadas de tratamento de dados.

Depois de identificar as ameaças e as vulnerabilidades, o foco passou a ser a avaliação dos impactos. Cada ativo foi avaliado em termos do seu potencial impacto nos três princípios da segurança da informação: confidencialidade, integridade e disponibilidade (ver 2.1.4).

Para quantificar o impacto, foi utilizada uma escala qualitativa que atribuiu valores ao impacto de uma violação da confidencialidade, integridade e disponibilidade. A tabela de impacto está dividida em cinco níveis, que vão de “Muito baixo” a “Muito alto”, com uma descrição correspondente dos efeitos adversos nas operações, ativos ou pessoas da organização. Por exemplo, no caso da confidencialidade, um impacto “muito baixo” ocorre quando o acesso não autorizado à informação tem um efeito adverso limitado, enquanto um impacto “muito elevado” seria catastrófico para a organização.

Posteriormente, foi avaliada a probabilidade de ocorrência de cada cenário de risco. A probabilidade foi categorizada qualitativamente numa escala semelhante. A combinação do nível de impacto e da probabilidade fornece uma base para o cálculo do nível de risco, que é determinado pela fórmula: Nível de risco = Impacto x Probabilidade. Este cálculo fornece uma medida quantitativa que ajuda a estabelecer prioridades para os riscos.

Figura 4 - Tabela Cálculo nível de risco

Nome do ativo	Ameaças	Vulnerabilidade	Impacto			Prob.	Nível de risco
			C	D	I		
servidor de portal e ficheiros	acesso `informação externos	acesso indevido a informação	4			3	12
		roubo	4			2	8
		destruição	4			2	8
				4		2	8
					4	2	8
Disco USB backups diarios	ausencia parcial da redundancia	Avaria		3		2	6
		roubo	2			1	4
				2		1	4
					2	1	4
		destruição	2			2	4
				2		2	4
					2	2	4
UPS	Perda de proteção e operacional	Avaria		2		2	4
		destruição		2		2	4
workstation nas instalações da	Perda de posto de trabalho	Avaria		3		2	6
		roubo	2			1	2
				2		1	2
					2	1	2
		destruição		2		1	2

Fonte: Documento interno Besturban

Os níveis de risco obtidos foram então comparados com um limiar de aceitação do risco (RA). Para a Besturban, o risco foi considerado aceitável se o nível fosse inferior a 12. Quando o nível de risco excede este valor, são definidas ações de tratamento para mitigar o risco para um nível aceitável. Estas ações podem incluir melhorias de segurança, formação do pessoal ou a implementação de controlos adicionais.

Para além de avaliar o impacto direto na segurança da informação, a metodologia também considera outros elementos relevantes que podem afetar a organização. Estes são classificados em aumentos de custos, perda de rendimentos, imagem e credibilidade, recursos humanos e aspetos jurídicos. Cada um destes potenciais impactos é avaliado qualitativamente numa escala de "Muito baixo" a "Muito alto", com descrições específicas para diferentes intervalos de valores. Por exemplo, considera-se um impacto financeiro "Muito Baixo" quando o aumento de custos ou a perda de receitas é inferior a 0,5 mil euros, enquanto um impacto "Muito Elevado" pode ultrapassar os 10 mil euros. A **Figura 4** e a **Figura 5** apresentam os quadros de referência utilizados na avaliação de risco.

Figura 5 - Tabela de Impacto

Impacto	Qualitativo	Aumento do Custo	Perda de Rendimentos	Imagem/Credibilidade	RH	Legal
1	Muito Baixo	< 0,5k	< 0,5k	Sem Impacto	Sem Impacto	Sem Impacto
2	Baixo	€ [0,5k 1k]	€ [0,5k 1k]	Impacto interno (nos colaboradores)	Desconforto momentaneo	Processo interno
3	Médio	€ [1k 5k]	€ [1k 5k]	Impacto em alguns clientes e fornecedores	Diminuição da motivação	Acção judicial e/ou multa ligeira
4	Alto	€ [5k 10k]	€ [5k 10k]	Impacto em todos os clientes e fornecedore	Falta de motivação com possível saíd	Acção judicial e/ou multa elevada
5	Muito Alto	> 10k	> 10k	Impacto em todos os clientes e fornecedores e media	Risco de demissão ou para a saúde	Acção judicial e/ou multa elevada e/ou responsabilidade criminal

Fonte: Documento interno Besturban

Em resumo, a metodologia de avaliação de risco da Besturban fornece um quadro estruturado para identificar, avaliar e tratar os riscos relacionados com a segurança da informação. Ao combinar a avaliação do impacto e da probabilidade com um processo sistemático de tratamento do risco, a metodologia ajuda a garantir a proteção adequada dos ativos de informação e a continuidade das operações organizacionais.

4.5 Controlos | Mecanismos de Segurança

Os controlos e mecanismos de segurança são fundamentais para proteger os bens vitais da empresa e garantir a continuidade das operações. No que respeita à informação, a proteção contra o roubo e destruição é gerida principalmente através de controlos de

acesso. Estes controlos visam atenuar o elevado impacto destes riscos, com um risco residual classificado como 4. A responsabilidade recai sobre o Diretor e o Responsável pela Segurança da Informação, que estão encarregues de reforçar as medidas de controlo e monitorização. Para fazer face a ciberataques e falhas de *software*, como vírus e *malware*, são utilizadas ferramentas de proteção e antivírus. As medidas adicionais incluem a formação contínua dos funcionários, embora as ações planeadas para mitigar o risco, com um impacto crítico avaliado em 12, tenham sido parcialmente implementadas até dezembro de 2022. A negligência é abordada através da sensibilização para a segurança da informação, também parcialmente implementada até ao final de 2022.

No que diz respeito aos recursos humanos, a falta de pessoal para tarefas críticas foi abordada através do planeamento dos recursos humanos e do desenvolvimento profissional. As ações incluem o desenvolvimento de tarefas difíceis e a formação contínua, com implementação parcial até dezembro de 2022.

A utilização não autorizada ou inadequada dos recursos é abordada através da formação e do desenvolvimento de políticas de teletrabalho. Embora as ações tenham sido parcialmente implementadas até dezembro de 2022, o risco é moderado, com um nível de risco residual de 8. Os procedimentos e políticas para a utilização de recursos são continuamente atualizados, com um risco moderado de 6 e implementação prevista até dezembro de 2022. No que diz respeito aos procedimentos disciplinares, a formalização de acordos de confidencialidade e a definição de sanções são essenciais para gerir o risco de 8, com ações previstas para serem concluídas até ao final de 2022. Para prevenir a sabotagem e o vandalismo, o controlo do acesso às instalações é crucial, com um risco crítico de 5 e ações implementadas até dezembro de 2022.

No que respeita a terceiros, a divulgação não autorizada de informações é tratada através de acordos de confidencialidade com clientes e fornecedores. O risco associado a esta questão é baixo, com um nível de risco residual de 2 para os clientes e variando de baixo a moderado para os fornecedores de comunicações e serviços. A falta de redundância nos fornecedores de comunicações e o risco de ciberataques são tratados com um risco moderado de 4. No caso dos fornecedores de serviços, como consultores e serviços de segurança, são utilizados acordos de confidencialidade e controlo de acesso para minimizar os riscos relacionados com a divulgação não autorizada e a sabotagem, com riscos que variam entre baixo e moderado (2-5).

Em termos de instalações, a proteção contra o acesso indevido e atos deliberados de sabotagem e vandalismo é assegurada através de controlos de acesso, com um risco moderado classificado em 4. A proteção contra incêndios e inundações é gerida por sistemas de proteção e redundância, como a implementação de NAS externos, que demonstrou eficácia com um nível de risco residual de 5. A utilização indevida do espaço é monitorizada e controlada continuamente, com medidas implementadas para gerir riscos moderados a críticos, classificados entre 4 e 5.

Estes controlos e mecanismos de segurança são essenciais para uma gestão eficaz dos riscos e para garantir uma proteção adequada dos ativos e das operações da empresa. A implementação e a avaliação contínuas das medidas são cruciais para manter a integridade e a segurança da organização.

4.6 Sistema de Gestão de Continuidade de Negócio

O Plano de Continuidade de negócio da BESTURBAN, tendo como base a ISO/IEC 22301 (ver 2.4.8) é uma parte fundamental do Sistema de Gestão de Continuidade de Negócios da empresa. Este plano foi desenvolvido com base em três componentes essenciais: Simulação de Incidentes, Projeção de Necessidades de Capacidade Futura e Simulacros. Cada um destes elementos desempenha um papel crucial para garantir a resiliência e a continuidade das operações da empresa face a eventuais incidentes de segurança da informação.

A *Simulação de Incidentes*, é uma atividade fundamental para avaliar e preparar a resposta da BESTURBAN a diferentes cenários de incidentes. Para cada cenário simulado, são estimados dois parâmetros críticos: o *Recovery Time Objective* (RTO) e o *Recovery Point Objective* (RPO). O RTO é o período máximo aceitável que o sistema pode levar para voltar à operação normal após um incidente. Este parâmetro é essencial para garantir que a empresa possa retomar as suas atividades num prazo que minimize o impacto operacional e financeiro. O RPO, por sua vez, refere-se à quantidade máxima de dados que a organização está disposta a perder em caso de incidente. A definição do RPO é fundamental para garantir que os procedimentos de backup e recuperação de dados são adequados para proteger a integridade e a continuidade das informações essenciais ao funcionamento da empresa.

A Projeção de Necessidades de Capacidade Futura aborda a necessidade de antecipar e projetar a capacidade necessária para apoiar a continuidade das operações e a segurança da informação à medida que a empresa evolui. A projeção deve ter em conta o crescimento esperado, as alterações tecnológicas e as novas ameaças emergentes, assegurando que o plano de continuidade está sempre alinhado com as necessidades futuras da Besturban.

Os simulacros são a terceira parte fundamental do plano de continuidade. Estes exercícios práticos são realizados anualmente e têm como objetivo testar e validar a eficácia das estratégias e procedimentos estabelecidos no Simulacro de Incidente e na Projeção de Necessidades de Capacidade Futura. Os simulacros são descritos em documentos específicos, organizados de acordo com o ano em que foram realizados. Estes documentos permitem um registo detalhado dos exercícios e dos resultados obtidos, permitindo à empresa avaliar a sua capacidade de resposta e identificar áreas de melhoria.

No que respeita ao Simulacro de Incidentes, a Besturban optou por centralizar a documentação dos simulacros num único documento abrangente, que engloba os simulacros realizados em diferentes anos. Este catálogo de simulacros serve de base de referência para os simulacros anuais, facilitando a atualização e adaptação contínua dos procedimentos de resposta a incidentes. Ao adotar esta abordagem, a Besturban garante que os simulacros de incidentes são abrangentes e que a preparação para lidar com possíveis cenários de segurança da informação é sistemática e bem fundamentada.

Em suma, o Plano de Continuidade de Segurança da Informação da Besturban é um sistema robusto e dinâmico que integra a Simulação de Incidentes, a Projeção de Necessidades de Capacidade Futura e os *Drills*. Através da definição clara de RTO e RPO, da antecipação de necessidades futuras e da realização de simulacros anuais, a empresa garante que está preparada para enfrentar e ultrapassar qualquer incidente de segurança da informação, mantendo a continuidade e integridade das suas operações e dados essenciais.

4.7 Formação, Treino e Sensibilização

A formação, o treino e a sensibilização dos colaboradores são pilares fundamentais na estratégia de segurança da informação da Besturban, especialmente no contexto da certificação ISO/IEC 27001. A empresa reconhece que a proteção de dados não é apenas uma responsabilidade do departamento de TI, mas uma missão coletiva que envolve todos os colaboradores.

A formação tem como principal objetivo garantir que todos os colaboradores compreendam as políticas de segurança da informação, as suas responsabilidades e a importância de preservar a confidencialidade dos dados. Para a Besturban, cultivar uma cultura de segurança é crucial, e isso traduz-se num ambiente onde todos os membros da equipa se sentem responsabilizados pela segurança da informação que manipulam.

O programa de formação da Besturban é estruturado em diferentes níveis e planeado em conjunto com o departamento de TI externo. Para novos colaboradores, é oferecida uma formação inicial que abrange as políticas de segurança da informação e os procedimentos operacionais modelo. Além disso, a empresa organiza sessões de atualização periódicas e workshops focados em temas específicos, como cibersegurança e prevenção de fraudes. Uma parte significativa dos *workshops* e ações de formação é ministrada pela empresa externa que gere o departamento de TI, garantindo uma abordagem especializada e alinhada com as melhores práticas do setor. As metodologias de ensino adotadas variam entre sessões presenciais e online (*webinars*) e utilização de materiais de apoio, como manuais e vídeos, permitindo que todos os colaboradores se adaptem ao seu estilo de aprendizagem.

O feedback dos colaboradores é também considerado para aprimorar continuamente os programas de formação, assegurando que as informações se mantenham relevantes e atualizadas. Além disso, a Besturban utiliza conteúdos disponibilizados pelo Centro Nacional de Cibersegurança, que complementam os programas de formação e garantem que os colaboradores estejam cientes das ameaças mais recentes e das melhores práticas em segurança.

Para além da formação formal, a Besturban implementa campanhas de sensibilização que ocorrem ao longo do ano. Estas iniciativas incluem o "Dia da Cibersegurança", onde os colaboradores são incentivados a participar em atividades interativas que reforçam

comportamentos seguros, como a utilização de senhas robustas e a identificação de e-mails de *phishing*. A empresa também envia newsletters informativas com dicas de segurança e alertas sobre ameaças emergentes, promovendo assim uma mentalidade proativa em relação à segurança da informação.

Os resultados das iniciativas de formação e sensibilização têm sido positivos, com uma redução visível nos incidentes de segurança e um aumento na conformidade com as políticas internas. O feedback dos colaboradores tem sido encorajador, indicando que as medidas adotadas foram bem recebidas e que a cultura de segurança está a solidificar-se na organização.

A Besturban procura continuamente formas de expandir e aprimorar o seu programa de formação e sensibilização. À medida que novas ameaças e tecnologias emergem, a empresa planeia integrar conteúdos atualizados e relevantes, assegurando que a sua equipa esteja sempre bem preparada para enfrentar desafios futuros.

4.8 Monitorização e Revisão

A monitorização e revisão contínuas dos sistemas e práticas de segurança da informação da Besturban são fundamentais para garantir a conformidade com a ISO/IEC 27001 e para manter a segurança e resiliência dos dados confidenciais da empresa. Estes processos permitem identificar de forma proativa potenciais vulnerabilidades e assegurar que os controlos implementados continuam a ser eficazes, mesmo diante de novas ameaças e desafios.

- Monitorização Contínua de Sistemas e Redes

A Besturban utiliza um *software* de *Remote Monitoring and Management* (RMM) fornecido pelo seu parceiro externo de TI, o que permite monitorizar em tempo real o desempenho e a segurança dos sistemas. Esta ferramenta de RMM verifica constantemente a rede e os dispositivos, gerando alertas automáticos para qualquer atividade suspeita ou incomum, como tentativas de acesso não autorizadas, falhas de sistema ou aumento repentino de tráfego.

Além disso, a empresa adotou *firewalls* de última geração, sistemas de deteção e prevenção de intrusões (IDS/IPS) e políticas de autenticação multifatorial, que são monitorizadas para assegurar que as camadas de proteção estão a funcionar

corretamente. A monitorização contínua contribui para uma resposta rápida e eficiente a incidentes de segurança, reduzindo o tempo de reação e permitindo a mitigação de riscos antes que afetem a operação.

- Revisão Regular dos Controlos de Segurança

Para garantir que todos os controlos de segurança da informação são adequados e atualizados, a Besturban realiza revisões periódicas em conjunto com o seu parceiro de TI. Essas revisões incluem auditorias internas de segurança, verificações de conformidade com a ISO/IEC 27001 e avaliações dos procedimentos implementados. Sempre que necessário, os processos e políticas são ajustados para incorporar melhorias e atender a requisitos adicionais de segurança.

A revisão regular permite que a empresa se adapte a novas ameaças de cibersegurança e garanta a conformidade com as melhores práticas. Além das auditorias internas, a Besturban colabora com a empresa externa de TI para avaliar a eficácia dos *backups* e dos planos de *disaster recovery*, assegurando que estes estão prontos para ser acionados em caso de falha grave.

- Avaliação Pós-Incidente e Melhoria Contínua

Após qualquer incidente de segurança, a Besturban realiza uma avaliação detalhada das causas e dos impactos do evento. Este processo de revisão pós-incidente é crucial para aprender com as falhas e ajustar os controlos e procedimentos de segurança, reduzindo a probabilidade de ocorrência de problemas semelhantes no futuro.

A Besturban adota uma abordagem de melhoria contínua, incorporando feedback obtido através das auditorias e dos workshops de sensibilização. Sempre que necessário, os colaboradores recebem formações adicionais para garantir que estão preparados para lidar com novos desafios de segurança. A parceria com o departamento de TI externo contribui para trazer uma perspetiva atualizada e técnica sobre o que deve ser ajustado ou reforçado na estratégia de monitorização e revisão da empresa.

- Relatórios e Comunicação com a Gestão de topo

A monitorização e revisão dos controlos de segurança são atividades acompanhadas pela direção da Besturban, que recebe relatórios regulares sobre o desempenho do

Sistema de Gestão de Segurança da Informação (SGSI). Estes relatórios incluem métricas de segurança, estatísticas sobre incidentes e análises de conformidade, oferecendo uma visão clara do estado de segurança da informação. Dessa forma, a alta direção pode tomar decisões informadas sobre investimentos em segurança e melhorias no SGSI.

A Besturban também consulta os conteúdos e recomendações do Centro Nacional de Cibersegurança para complementar as suas práticas de segurança e manter a equipa atualizada sobre as ameaças emergentes. Este acesso a recursos de cibersegurança fortalece a monitorização e a revisão contínua dos sistemas, ajudando a empresa a manter uma postura de segurança robusta e alinhada aos padrões internacionais da ISO/IEC 27001.

4.9 Gestão de Incidentes

A gestão de incidentes é um processo essencial no contexto da segurança da informação da Besturban, apoiando a sua capacidade de identificar, responder e mitigar rapidamente ameaças e falhas de segurança. Com a certificação ISO/IEC 27001, a Besturban está comprometida com padrões de segurança que garantem a continuidade das operações e a proteção de dados contra acessos não autorizados, perdas ou danos. Além disso, a empresa adota práticas alinhadas com a ISO/IEC 27035[20], norma específica para a gestão de incidentes de segurança da informação, que fornece diretrizes para um processo estruturado de resposta, deteção e comunicação de incidentes.

A estrutura e planeamento de gestão de incidentes da Besturban, em colaboração com o seu provedor externo de TI, incluem um plano de ação robusto, com protocolos definidos para responder a vários tipos de incidentes de segurança. Este plano é desenvolvido com base nos requisitos da ISO/IEC 27001 e nas diretrizes da ISO/IEC 27035, que ajudam a empresa a organizar-se para uma resposta eficaz. A ISO/IEC 27035 especifica etapas importantes, como a categorização dos incidentes por

[20] ISO/IEC 27035-2:2023(en), Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

gravidade e impacto, o que a Besturban adota para definir ações apropriadas para cada cenário.

Para assegurar que todos os colaboradores compreendem as suas responsabilidades na gestão de incidentes, a Besturban promoveu ações de formação regulares que incluem simulações e exercícios práticos, alinhados com as melhores práticas da ISO/IEC 27035. Estas sessões visam sensibilizar a equipa sobre os sinais de alerta, como tentativas de *phishing* e atividades suspeitas, garantindo que todos seguem os procedimentos de resposta a incidentes. O departamento de TI externo desempenha um papel essencial, fornecendo orientação e treinamento contínuos para fortalecer essa capacidade de resposta.

Na identificação e notificação de incidentes, a Besturban utiliza um *software* de *Remote Monitoring and Management* (RMM) para monitorar e relatar atividades anómalas em tempo real, o que facilita uma resposta rápida e permite a deteção precoce de problemas. Esta prática está em consonância com a ISO/IEC 27035, que recomenda a implementação de mecanismos de monitorização contínua e de sistemas de alerta que ajudem na identificação rápida de incidentes. Os colaboradores também são incentivados a reportar atividades suspeitas e têm instruções claras de como notificar os responsáveis pela segurança da informação e o departamento de TI.

A resposta e mitigação de incidentes na Besturban é um processo estruturado que envolve uma contenção inicial do incidente, investigação da causa raiz e execução de ações corretivas, em conformidade com as recomendações da ISO/IEC 27035. Os responsáveis pelo TI externo têm um papel importante na coordenação das medidas de recuperação, assegurando que os sistemas são restaurados com segurança. Parte da resposta envolve a utilização de *backups* e planos de *disaster recovery*, com *backups* automáticos que permitem uma rápida recuperação e minimizam o tempo de inatividade. Além disso, políticas de *multi-factor authentication* (MFA) e criptografia reforçam a segurança em dispositivos críticos, conforme recomendado pela ISO/IEC 27035.

Após cada incidente, a Besturban realiza uma revisão pós-incidente com o objetivo de identificar falhas nos procedimentos e oportunidades de melhoria, reforçando a sua conformidade com a ISO/IEC 27035. Esta fase de análise e aprendizagem é essencial para aumentar a resiliência contra futuros incidentes e integra-se no processo de melhoria contínua previsto pela ISO/IEC 27035. Os relatórios gerados são discutidos

com a direção e com o parceiro de TI externo para assegurar que as lições aprendidas são aplicadas, resultando em processos mais robustos. A colaboração com o departamento de TI externo permite ainda à Besturban adaptar o seu plano de gestão de incidentes com base em novas ameaças identificadas no setor.

Assim, a gestão de incidentes da Besturban reflete uma abordagem pró-ativa e bem estruturada, onde as normas ISO/IEC 27001 e ISO/IEC 27035 são cruciais para garantir uma resposta eficaz e uma melhoria contínua das práticas de segurança. A empresa também beneficia dos conteúdos de segurança do Centro Nacional de Cibersegurança, reforçando a capacitação interna para a prevenção de incidentes e alinhando-se com as melhores práticas internacionais de segurança.

4.10 Conformidade e Certificação

A análise da conformidade e certificação da Besturban, descrita no relatório de auditoria n.º. SI – 0104 que pode ser consultado no Anexo B, fornece uma visão abrangente da conformidade da empresa com os requisitos da norma NP ISO/IEC 27001:2013. Este processo é fundamental para garantir que o Sistema de Gestão de Segurança da Informação (SGSI) da empresa está alinhado com as normas internacionais e continua a satisfazer as necessidades e expectativas das suas partes interessadas.

A auditoria foi realizada como uma avaliação de acompanhamento após a renovação da certificação do Sistema de Gestão da Qualidade e Segurança da Informação da Besturban. A empresa é membro da ASAVAL, que assegura que os seus membros mantêm sistemas de controlo interno robustos para garantir a qualidade e independência das avaliações, evitando conflitos de interesse que possam pôr em causa a integridade dos processos de avaliação.

Durante a auditoria, foram identificadas algumas mudanças significativas na empresa, como a aquisição de novos clientes, o impacto da inflação e o aumento das taxas de juro, que resultaram numa redução prevista de cerca de 20% do volume de negócios para 2023. A empresa também sofreu alterações de pessoal, incluindo uma mudança de coordenador técnico, e está a funcionar com um modelo híbrido de trabalho presencial e remoto, além de estar em processo de atualização do seu portal de gestão operacional.

A auditoria não incluiu uma avaliação física no local, uma vez que não havia serviços em curso no momento da auditoria. Em vez disso, foram analisados os processos e requisitos aplicáveis do Sistema de Gestão através de uma análise documental. Os processos de avaliação de clientes auditados incluíram a avaliação de equipamentos e imóveis, que foram analisados através de documentação relevante.

A participação da organização na auditoria foi evidenciada pela colaboração e envolvimento ativo de todos os colaboradores, incluindo a gestão de topo, nas reuniões de abertura e encerramento. A direção demonstrou um empenho na melhoria contínua do SGSI, com uma participação efetiva na auditoria.

O nível de confiança no processo de auditoria interna e na análise da gestão foi positivo, com provas da realização de uma auditoria interna e de uma análise abrangente da gestão. A empresa conseguiu prestar serviços que satisfazem os requisitos aplicáveis e cumprem os objetivos definidos. No entanto, foi registada uma não-conformidade que exige medidas corretivas e cinco oportunidades de melhoria, que a gestão da Besturban deve avaliar e implementar conforme necessário. Estas oportunidades de melhoria incluem a avaliação da separação dos indicadores de incidentes críticos e não críticos, a implementação de um sistema de dupla autenticação para acesso à VPN e a inclusão da aceitação formal das condições de prestação do serviço na Declaração de Aceitação do Perito Avaliador.

Para além disso, foram analisadas as reclamações dos clientes, tendo sido recebidas e tratadas adequadamente cinco reclamações. Não foram identificadas inspeções de entidades reguladoras durante os anos de 2022 e 2023. A análise das não conformidades e das oportunidades de melhoria revelou a necessidade de uma revisão mais detalhada das ações para fazer face aos riscos e oportunidades, bem como da eficácia das ações de melhoria definidas.

Os pontos fortes do sistema incluem o envolvimento dos funcionários e a utilização de uma plataforma de apoio à avaliação de imóveis que incorpora inteligência artificial. No entanto, a auditoria também apontou áreas de melhoria, como a análise mais detalhada dos indicadores de segurança da informação e a definição de uma periodicidade para a análise dos resultados relacionados com as ações de melhoria.

O Certificado de Conformidade número SI - 0104, emitido pela EIC - Empresa Internacional de Certificação, S.A., atesta que o Sistema de Gestão da Segurança da Informação da BESTURBAN - Avaliação e Gestão de Patrimónios Imobiliários, Lda. cumpre os requisitos estabelecidos pela norma NP ISO/IEC 27001:2013.

O certificado, que abrange a atividade de Avaliação de Imóveis e Máquinas e Equipamentos, foi emitido na sequência de uma auditoria de concessão realizada em 20 de dezembro de 2022. A Declaração de Aplicabilidade relevante para este certificado é a Edição 2, datada de 09 de dezembro de 2022.

A validade do certificado estende-se até 31 de outubro de 2025, substituindo o certificado anteriormente emitido com o número SI - 0090. O certificado foi emitido oficialmente em Lisboa a 14 de abril de 2023 e assinado por Manuel Vidigal, Presidente do Conselho de Administração da EIC.

Em resumo, a análise de conformidade e certificação da Besturban indica que a empresa está bem posicionada para manter a conformidade com as normas de segurança da informação, com áreas específicas que precisam de atenção para garantir a eficácia contínua do sistema de gestão.

5 ANÁLISE DA SITUAÇÃO E MELHORES PRÁTICAS

Enquanto PME, a Besturban tem demonstrado um sólido compromisso com a segurança da informação, sustentado por um robusto Sistema de Gestão de Segurança da Informação (SGSI). Este sistema integra práticas e políticas abrangentes que visam assegurar a proteção dos ativos de informação da empresa, em linha com os princípios da norma ISO/IEC 27001:2013. A análise das práticas de segurança adotadas pela Besturban revela a aplicação consistente de medidas para garantir a confidencialidade, integridade e disponibilidade da informação.

5.1 Práticas anteriores de Segurança da Informação

Antes da implementação da ISO/IEC 27001, a Besturban já possuía algumas práticas de segurança da informação, embora de forma menos estruturada e sem um sistema formal de gestão. Estas práticas visavam sobretudo a proteção de dados e a garantia da continuidade das operações. As principais práticas de segurança adotadas pela empresa antes do processo de certificação eram:

- *Backup* de Dados:

  A Besturban realizava *backups* diários de forma automatizada. Os *backups* eram armazenados localmente, utilizando dispositivos como discos USB e servidores *NAS* (*Network Attached Storage*) sem redundância geográfica, o que representava um risco significativo em caso de falhas nos sistemas ou desastres. Além disso, não eram realizados testes frequentes para verificar a integridade dos *backups* e assegurar a capacidade de recuperação dos dados. Embora eficazes em alguma medida, esses procedimentos eram dependentes de intervenção manual e estavam sujeitos a riscos de erro humano e de inconsistências no processo de recuperação.

- Controlos de Acesso Simples:

  Os controlos de acesso existentes eram implementados recorrendo ao uso de senhas para proteger sistemas e documentos sensíveis. No entanto, esses controlos não se enquadravam numa política formal de autenticação e autorização, o que fazia com que o processo de gestão de acessos se tornasse mais vulnerável a inconsistências. Além disso, não se encontrava implementado um sistema de

autenticação multifator, o que representava um risco adicional para a segurança da informação.

- Proteção Física:

  As medidas de proteção física incluíam o uso de chaves para garantir o acesso restrito a determinadas áreas, onde se encontravam localizados os documentos sensíveis e servidores. Essa proteção física visava limitar o acesso a pessoas não autorizadas, mas não existia um controlo mais rigoroso de quem acedia a estes locais, o que tornava o sistema mais suscetível a falhas.

- Antivirus e *Firewall*

  Por forma a proteger os sistemas contra ameaças digitais, a Besturban utilizava programas antivirus e *firewalls* de rede. Estas ferramentas garantiam que seria possível mitigar os riscos de vírus e *malware*, mas a configuração não era acompanhada de monitorização contínua ou de uma resposta estruturada a eventuais incidentes, o que deixava lacunas na segurança geral da rede.

- Política de Utilização dos Dispositivos

  Antes da implementação da ISO/IEC 27001 já existia uma política básica de utilização dos dispositivos da empresa. Nessa mesma política constava a recomendação para que os colaboradores evitarem o uso de dispositivos pessoais para fins profissionais e não procederem à instalação de *software* não autorizado nos computadores da empresa. No entanto, a aplicação desta política decorria de forma informal, sem fiscalização regular ou regras formalizadas que assegurassem o seu cumprimento.

Apesar das práticas de segurança adotadas pela Besturban antes da implementação da ISO/IEC 27001, existiam limitações importantes. A ausência de uma estrutura formal para a gestão da segurança da informação, a dependência de processos manuais, e a falta de políticas formalizadas potenciavam a exposição a riscos significativos. A implementação da ISO/IEC 27001 conduziu a uma abordagem mais sistemática, com processos padronizados e maior robustez na proteção dos ativos de informação.

5.2 Processo de implementação

A gestão de risco é uma componente central do SGSI da Besturban. A empresa utilizou uma abordagem sistemática para identificar ativos críticos, avaliar ameaças e vulnerabilidades e quantificar impactos e probabilidades. Este processo permitiu à empresa definir ações de tratamento adequadas, conforme indicado na norma ISO/IEC 27002:2022, e implementar medidas de controlo proporcionais ao nível de risco aceitável. A metodologia de avaliação, combinando abordagens qualitativas e quantitativas, foi um dos fatores críticos que contribuíram para a eficácia do SGSI.

Desde o início do processo de implementação da norma, foram identificadas etapas críticas para estruturar o SGSI, incluindo a avaliação da posição inicial da empresa em relação aos requisitos da ISO/IEC 27001, a definição de políticas específicas para a proteção de dados, e a formação dos colaboradores para garantir que todos compreendessem as suas responsabilidades no contexto do SGSI. Uma fase inicial importante foi a definição clara das políticas de segurança da informação, como a Política Geral de Segurança da Informação, pilar fundamental na implementação do SGSI e que estabeleceu um compromisso claro com a proteção contra acessos não autorizados, minimizando os riscos associados. Esta política reflete um esforço de integração da segurança da informação na cultura organizacional, assegurando que todos os colaboradores estão conscientes das suas responsabilidades e formados para lidar com eventuais incidentes.

Uma das boas práticas implementadas pela Besturban é a Política de Classificação da Informação, que categoriza os dados em diferentes níveis de sensibilidade, como Confidencial, Restrito, Corporativo e Público. Esta prática já existia parcialmente antes da implementação da ISO/IEC 27001, mas foi fortalecida para atender aos requisitos da norma, regulando com rigor o acesso e a reprodução da informação e estabelecendo procedimentos para a eliminação segura de dados sensíveis. Para controlar o acesso a esses dados, a gestão de acessos foi melhorada com controlos físicos e digitais. O uso de chaves para o acesso físico e de senhas complexas para os sistemas digitais, juntamente com a proteção de documentação sensível em áreas restritas, demonstra a aplicação de controlos eficazes que cumprem os critérios da norma ISO/IEC 27001.

A proteção contra ameaças digitais, que inclui *backups* diários e testes mensais para garantir a integridade dos dados, foi uma área significativa de melhoria após a

implementação da ISO/IEC 27001. Além disso, a empresa adotou ferramentas de defesa contra vírus e *malware* e promoveu a orientação dos utilizadores para comportamentos seguros, com rigor na utilização de dispositivos móveis e na gestão de palavras-passe. Este reforço nas práticas de segurança foi uma resposta direta à análise de riscos realizada, que identificou vulnerabilidades específicas e medidas de mitigação adequadas.

5.3 Desafios

O processo de implementação enfrentou desafios específicos, principalmente ligados a limitações de recursos e ao desafio de alinhar todos os colaboradores com as novas práticas de segurança.

Um dos maiores desafios para a Besturban foi lidar com a limitação de recursos financeiros e humanos. Tratando-se de uma PME, a empresa não tinha a possibilidade de alocar um orçamento suficientemente robusto ou dedicar uma equipa exclusiva para a implementação da ISO/IEC 27001. Em face dessas dificuldades, em muitas situações, os colaboradores acumularam funções, tendo de gerir em simultâneo as suas atividades diárias e as associadas ao desenvolvimento do Sistema de Gestão de Segurança da Informação (SGSI).

A mudança para uma mentalidade de segurança da informação exigiu um esforço significativo na formação e sensibilização dos colaboradores. Muitos dos membros da equipa não tinham experiência prévia em temas relacionados com a segurança da informação, o que implicou um investimento em formação contínua e workshops.

Outro desafio encontrado foi a resistência à mudança por parte dos colaboradores. A implementação da ISO/IEC 27001 levou à implementação novas políticas, procedimentos e controlos, que exigiram alterações nos hábitos de trabalho. O processo não foi simples, e houve resistência inicial devido à perceção de que as novas regras e controlos iriam acrescentar uma maior carga burocrática às atividades do dia a dia. Por forma a superar essa mesma resistência, a Besturban investiu em comunicação constante e na demonstração dos benefícios da certificação para a segurança e credibilidade da empresa.

Embora a Besturban tenha promovido melhorias na sua infraestrutura tecnológica, como a aquisição de novos servidores e a implementação de novos modelos de *backups*, o

processo de adaptação à ISO/IEC 27001 evidenciou algumas deficiências. A necessidade de deslocalização de discos de rede para locais mais seguros e a implementação de sistemas de autenticação multifator, por exemplo, acrescentaram dificuldades devido aos custos associados e à complexidade de integração com os sistemas existentes.

Outro desafio relevante foi a falta de experiência da consultora externa contratada para a implementação do SGSI. Segundo o CEO da Besturban, a consultora não demonstrou experiência ou a solidez de conhecimentos necessários em relação à ISO/IEC 27001 e ao seu processo de implementação. Essa lacuna acabou por levar a que o processo de preparação se tivesse prolongando e gerado incertezas na sua execução.

Os desafios enfrentados pela Besturban durante a implementação da ISO/IEC 27001 foram diversos e compreendem tanto questões técnicas quanto culturais. Apesar das dificuldades, a empresa conseguiu superar os desafios através de um forte compromisso com a melhoria contínua e o apoio de parceiros estratégicos.

5.4 Impacto da implementação

Desde a certificação, observam-se melhorias concretas na segurança da informação, incluindo maior consistência nos procedimentos de backup, maior rigor no controlo de acessos e uma resposta mais eficiente a incidentes. A auditoria interna e a auditoria de acompanhamento destacaram uma melhoria na prontidão para responder a ameaças e na clareza dos processos de segurança. Em termos de boas práticas, a Besturban demonstra uma postura proativa e estruturada na proteção de seus ativos de informação, o que reflete a integração dos princípios da ISO/IEC 27001 na cultura organizacional.

5.5 Lições e Melhores práticas

A experiência da Besturban com a ISO/IEC 27001 também oferece lições valiosas para outras PME em Portugal. Destacam-se, especialmente, a importância de formar continuamente os colaboradores, a necessidade de colaboração com parceiros especializados em IT para auxiliar na gestão de segurança e a relevância de uma liderança comprometida.

A adesão da administração e o envolvimento dos colaboradores foram essenciais para superar os desafios encontrados na implementação do SGSI, pois a governança e sensibilização da gestão de topo e a formação contínua ajudaram a alinhar todos os membros da equipa com os objetivos de segurança.

Um outro fator crítico para o sucesso foi o apoio contínuo do parceiro de IT externo, que não apenas ajudou na implementação dos requisitos técnicos, mas também participou das reuniões de planeamento, oferecendo orientações valiosas.

Em suma, a análise da situação atual da Besturban no âmbito da segurança da informação demonstra uma aplicação efetiva dos princípios da norma ISO/IEC 27001, com a empresa a adotar práticas detalhadas e rigorosas de proteção dos seus ativos de informação. A relação entre as práticas adotadas e os requisitos da norma evidenciam o alinhamento da Besturban com as melhores práticas internacionais, salientando a importância da implementação da ISO/IEC 27001 como uma base de proteção e melhoria contínua para uma PME portuguesa.

Estes fatores ajudaram a Besturban a fortalecer sua resiliência e a desenvolver uma postura sólida contra ciberameaças. Como resultado, a empresa está agora mais bem posicionada para manter a conformidade e proteger seus ativos informacionais no ambiente dinâmico e desafiador de hoje.

6 CONCLUSÕES E RECOMENDAÇÕES

O principal objetivo deste trabalho de projeto foi explorar e analisar o processo de implementação do Sistema de Gestão de Segurança da Informação (SGSI) da Besturban alinhado com a norma ISO/IEC 27001, focando as práticas, políticas e controlos implementados para garantir a proteção dos ativos de informação da empresa. A análise detalhada revelou que a Besturban tem um sólido compromisso com a segurança da informação, refletido na implementação de práticas e políticas, que incluem uma rigorosa classificação de dados, controlo de acessos, proteção contra ameaças digitais e uma gestão eficaz do risco.

Um dos pontos fortes identificados no projeto foi a implementação de uma Política de Classificação da Informação. Esta política organiza os dados de acordo com o seu nível de sensibilidade e define procedimentos claros para aceder, utilizar e eliminar a informação. Esta abordagem não só protege os dados contra o acesso não autorizado, como também facilita a gestão e o cumprimento da regulamentação aplicável, em conformidade com os requisitos da norma ISO/IEC 27001. A adoção de controlos físicos e digitais robustos, como chaves para áreas sensíveis e *passwords* complexas para sistemas informáticos, demonstra um cuidado meticuloso na proteção dos recursos da empresa.

Outro aspeto positivo é a abordagem sistemática da Besturban na gestão de riscos. A empresa segue uma metodologia detalhada de identificação, avaliação e tratamento de riscos, permitindo a definição de ações adequadas para mitigar potenciais ameaças. A utilização de um quadro de impacto e a combinação de avaliações qualitativas e quantitativas garantem que as medidas de controlo são eficazes e ajustadas ao nível de risco aceitável para a organização. Para além disso, a forte aposta da empresa na formação contínua dos seus colaboradores e na aplicação de medidas preventivas contra ciberataques evidencia a sua dedicação à segurança da informação.

No entanto, o trabalho de projeto também revelou algumas limitações que devem ser abordadas para uma compreensão mais profunda e abrangente do SGSI da Besturban. Um aspeto importante, não suficientemente explorado, foi a realização de entrevistas com os responsáveis pela implementação do SGSI na empresa. A inclusão de tais entrevistas permitiria uma visão mais pormenorizada das práticas diárias, dos desafios enfrentados e das perceções das pessoas envolvidas no processo de gestão da

segurança da informação. Esta abordagem qualitativa poderia fornecer informações valiosas sobre áreas a melhorar e necessidades específicas da empresa que não são totalmente captadas através da análise de documentos e auditorias.

Além disso, seria vantajoso efetuar um estudo mais aprofundado da eficácia das medidas de segurança aplicadas e da sua adequação ao contexto específico da Besturban. A análise das experiências e práticas dos responsáveis pela segurança poderia ajudar a identificar lacunas e oportunidades de melhoria, promovendo um SGSI ainda mais robusto e alinhado com as melhores práticas do sector.

Para investigação futura, recomenda-se a inclusão de metodologias qualitativas, como *focus groups*, para complementar a análise documental e as auditorias. A interação direta com os profissionais envolvidos na gestão da segurança da informação permitiria uma compreensão mais rica e contextualizada dos processos e desafios enfrentados pela empresa. Além disso, a análise de casos de sucesso e insucesso em organizações similares poderia fornecer uma visão mais ampla da eficácia das práticas adotadas e das tendências emergentes na área da segurança da informação.

Em conclusão, o trabalho de projeto forneceu uma visão detalhada das práticas e políticas de segurança da informação da Besturban, destacando o empenho da empresa na proteção dos seus ativos de informação.

Para uma avaliação mais completa e aprofundada deste caso, é fundamental considerar a inclusão de entrevistas com os responsáveis pela segurança e a exploração de metodologias qualitativas que possam oferecer uma perspetiva mais rica sobre a gestão da segurança da informação. Esta abordagem alargada contribuirá para a construção de um SGSI ainda mais eficaz e alinhado com as necessidades e desafios específicos da empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

A., Horie, D., Goto, Y., & Cheng, J. (2009). A Database System for Effective Utilization of ISO/IEC 27002. In *2009 Fourth International Conference on Frontier of Computer Science and Technology (FCST)*. IEEE. https://doi.org/10.1109/fcst.2009.88

Amiruddin, A., Afiansyah, H. G., & Nugroho, H. A. (2021). Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. In *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE. https://doi.org/10.1109/icimcis53775.2021.9699337

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security*, *13*(3), 189–202. https://doi.org/10.1108/09685220510602013

Boehmer, W. (2008): Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO/IEC 27001. *Second International Conference on Emerging Security Information, Systems and Technologies*, pp. 224–231, Cap Esterel, France, IEEE, August 25–31, 2008.

Bonner, E., O' Raw, J., & Curran, K. (2011). Implementing the Payment Card Industry (PCI) Data Security Standard (DSS). *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *9*(2), 365. https://doi.org/10.12928/telkomnika.v9i2.709

Bulgurcu, Cavusoglu & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

Choucri, N. (2013) *Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences,* World Social Science Forum (WSSF) 2013 Montreal, Canada. t.ly/lQk0N

Ciot, M.-G. (2017). Cyberspace and the New World Order. *Studia Universitatis Babeș-Bolyai Studia Europaea*, *62*(2), 5–15. https://doi.org/10.24193/subbeuropaea.2017.2.01

Cohen, E. A., & Kahn, D. (1997). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. *Foreign Affairs*, *76*(3), 129. https://doi.org/10.2307/20048054

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Department of Defense (DoD), (2010). Dictionary of Military and Associated Terms http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Dhillon G, Backhouse J (2000) Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125–128.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Dobler, M. (2005). National and International Developments in Risk Reporting: May the German Accounting Standard 5 Lead the Way Internationally? German Law Journal, 6(8), 1191–1200. https://doi.org/10.1017/s207183220001422

Dronov, V. Y., & Dronova, G. A. (2022). Principles of information security management system. *Journal of Physics: Conference Series*, *2182*(1), 012092. https://doi.org/10.1088/1742-6596/2182/1/012092

ENISA. (2021). *Cybersecurity for SMEs - Challenges and Recommendations.* European Union Agency for Cybersecurity.

European Commission (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

European Commission (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing

Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1735381999426

European Commission (2019). Regulation (EU) 2019/881 of the European parliament and of the council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Commission (2020). Joint communication to the European parliament and the council the EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Commission (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1735385258459

European Commission (2022). Regulation of the European parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

European Commission (2023). Regulation of the European parliament and of the council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act

European Commission (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence

and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1735385703635

Gheciu, A., & Wohlforth, W. C. (Eds.). (2018). The Future of Security Studies. *The Oxford Handbook of International Security*. Oxford University Press.

González, F. M. d. l. P. (2015). *ITIL (Information Technology Infrastructure Library) Descripción, Funcionamiento y Aplicaciones* [Tesis de Licenciatura, Universidad Autónoma del Estado de México]. RI UAEMex. http://hdl.handle.net/20.500.11799/99997

International Organization for Standardization. (2005). *Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2005). https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en

International Organization for Standardization. (2013). *Information technology — Security techniques — Information security management systems — Requirements.* (ISO/IEC Standard No. 27001:2013). https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabular.* (ISO Standard No. 27000:2018). https://www.iso.org/standard/73906.html

International Organization for Standardization. (2019). *Security and resilience — Business continuity management systems — Requirements.* (ISO Standard No. 22301:2019). https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. (ISO Standard No. 27001:2022). https://www.iso.org/standard/27001

Klipper, S. (2015). ISO/IEC 27005. In *Information Security Risk Management* (pp. 59–96). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-08774-6_3

Laudon, K. C., & Laudon, J. P. (2012). Management Information Systems (12th ed.). Pearson.

Lobo, M. N. B., Perez, T. V., & Rico-Bautista, D. (2022). Systematic Mapping of Literature: Governance and IT Management Practices in organizations, under the COBIT 2019 reference framework. In *2022 11th International Conference On Software Process Improvement (CIMPS)*. IEEE. https://doi.org/10.1109/cimps57786.2022.10035692

Mbanaso, U., & Dandaura, E. (2015). Cyberspace: Redefining A New World. *OSR Journal of Computer Engineering (IOSR-JCE)*, *17*(3), 2278–661. https://www.researchgate.net/publication/280101879_The_Cyberspace_Redefining_A_New_World

Möller, D. P. F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In *Advances in Information Security* (pp. 231–271). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-26845-8_5

National Institute of Standards and Technology. (2009). *NIST SP 800-41 Guidelines on Firewalls and Firewall Policy: NiST SP 800-41*. Createspace Independent Publishing Platform.

Parker DB (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. J. Wiley.

Pessoa, C. R. M., & Estrela, S. (2021). A gestão da informação nas PME desafios e oportunidades. *Prisma.com*, *46*, 80–96. https://doi.org/10.21747/16463153/46a5

Pfleeger CP & Pfleeger SL (2003) *Security in Computing. Pearson Education*. Upper Saddle River

Pordata (2024). *Pequenas e médias empresas em % do total de empresas: total e por dimensão*. Lisboa: PORDATA. Disponível em outubro, 27, 2024 em https://www.pordata.pt/sites/default/files/202406/Portugal_Pequenas_e_medias_empresas__total_e_por_dimensao.xlsx

PwC Portugal (2023). *De NIS a NIS2 – a evolução da legislação europeia de cibersegurança.* https://www.pwc.pt/pt/sala-imprensa/artigos-opiniao/2023/legislacao-ciberseguranca-nis2.html

Robayo Jácome, D. J., Aguilar-Molina, P., & Chiliquinga Véjar, L. d. C. (2023). Information Security through the ISO/IEC 27001:2013 Standard. *Medwave*, *23*(S1), Artigo eUTA275. https://doi.org/10.5867/medwave.2023.s1.uta275

Steuperaert, D. (2019). COBIT 2019: A SIGNIFICANT UPDATE. *EDPACS*, *59*(1), 14–18. https://doi.org/10.1080/07366981.2019.1578474

Stoneburner G, Hayden C, & Feringa A (2004) *NIST SP 800-27 Rev A – Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.* NIST Special Publication.

The Institute of Risk Management. (2002). A Risk Management Standard. https://www.theirm.org/media/4709/arms_2002_irm.pdf

Ukidve, A., SMantha, D. S., & Tadvalka, M. (2017). Analysis of Payment Card Industry Data Security Standard [PCI DSS] Compliance by Confluence of COBIT 5 Framework. *International Journal of Engineering Research and Applications*, *07*(01), 42–48. https://doi.org/10.9790/9622-0701014248

Varian, H.R. (2015) *The Information Economy: How much will two bits be worth in the digital marketplace. https://cooperative-individualism.org/varian-hal_the-information-economy-1995-sep.pdf*

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

Wattimury, G., & Faza, A. (2023). COBIT 2019 Implementation for Enhancing IT Governance in Educational Institutions. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *8*(3), 210–221. https://doi.org/10.14421/jiska.2023.8.3.210-221

Whitman ME &N Mattord HJ (2011) *Principles of Information Security*. Cengage Learning

Legislação

Lei nº 109/2009, Lei do Cibercrime. Diário da República n.º 179/2009, Série I de 2009-09-15, páginas 6319 – 6325. https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693

Lei nº 46/2018. Regime Jurídico da Segurança do Ciberespaço. Diário da República n.º 155/2018, Série I de 2018-08-13, 4031 – 4037. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384

RCM 92/2019. Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Diário da República n.º 108/2019, Série I de 2019-06-05, 2888 – 2895. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962

Lei nº 58/2019. Regulamento Geral de Proteção de Dados. Diário da República n.º 151/2019, Série I de 2019-08-08, 3 – 40. https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Regulamento n.º 303/2019 da Autoridade Nacional de Comunicações. Diário da República n.º 64/2019, Série II de 2019-04-01, páginas 10214 – 10231. https://diariodarepublica.pt/dr/detalhe/regulamento/303-2019-121784730

Decreto-Lei n.º 65/2021. Diário da República n.º 147/2021, Série I de 2021-07-30, páginas 8 – 21. https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988

ANEXOS

ANEXO A - Entrevista com o CEO da Besturban

1. **O que motivou a sua empresa a procurar a certificação ISO/IEC 27001?**

R: Uma vez que na nossa atividade, trabalhamos com informação confidencial, a qual temos de ter o máximo de cuidado em conservá-la em nossa posse, sem perigo de ser tornada pública. A certificação ISO/IEC 27001, foi uma decisão estratégica muito importante para aumentarmos e termos padronizados a segurança do nosso sistema. E sermos vistos pelos nossos clientes que nos preocupamos e procuramos elevar os nossos serviços a um patamar superior.

Infelizmente fomos a primeira e ainda somos a única empresa de avaliação imobiliária, com esta certificação.

2. **Quais foram os principais fatores que influenciaram a decisão de avançar com esta certificação?**

R: Um dos nossos objetivos diários é a melhoria contínua, pelo que esta certificação vem nesse sentido, sermos melhores, cumprir padrões internacionais em variados campos (ISO/IEC 9001 – qualidade, ISO/IEC 27001 – Segurança da Informação, inscrição na CMVM – cumprir as normativas de avaliação em Portugal, ter membros REV (Recognised European Valuer) normas europeias de avaliação, sermos regulados pelo RICS (Royal Institution of Chartered Surveyors) – normas internacionais de avaliação.

4. **Como foi o processo de preparação para a certificação?**
    - Houve necessidade de alterar ou melhorar processos já existentes?

R: Sim, o processo de preparação até à auditoria externa para obtenção da certificação foi um longo processo de vários meses. Existiram algumas mudanças tanto na parte informática da empresa, como ao nível de comportamentos que cada um tem que ter para que o conjunto consiga cumprir os standards da norma.

Em termos informáticos a alteração mais significativa foi a aquisição de um novo servidor e a deslocalização de um disco de rede, que se encontra fora do escritório, num distrito diferente e com ligação à rede de um operador diferente.

5. **Quais foram os maiores desafios que a empresa enfrentou ao longo deste processo?**
    - Foram necessários investimentos significativos em tecnologias, formações ou recursos humanos?

R: O maior desafio foi conseguir ter tudo em automatizado antes da auditoria externa. A preparação e implementação do sistema foi demorada, porque foi começar quase do zero. A nossa consultora externa foi a primeira vez que participou a conceção e estava muito “verde” e pouco à vontade com todas as incidências da norma. Por isso este terá sido o maior desafio. No entanto foi “compensado” com o nosso parceiro de negócio de informática e redes. Sem ele teria sido ainda muito mais difícil.

6. **Como foi envolvida a equipa e como foi a aceitação interna desta mudança?**

R: Tenho a sorte de ter uma equipa de colaboradores fantástica, todos eles assumem e aceitam os desafios que lhe proponho. E sabem que quando a mudança é benéfica para a equipa, também o será para o individuo.

7. **A empresa recorreu a consultores externos ou foi um processo maioritariamente interno?**

R: Recorremos a consultores externos, os mesmos que já nos acompanhavam no âmbito da ISO/IEC 9001.

No entanto este ano deixámos de colaborar com a empresa de consultoria externa e estamos internamente a fazer o processo, estamos uma empresa de consultoria apenas para nos fazer a auditoria interna. Estamos esperançados que essa nova empresa auditora, nos traga outras visões e melhorias a introduzir no sistema integrado.

8. **Que benefícios concretos a empresa obteve com a certificação?**
    - Houve melhoria na eficiência operacional, confiança dos clientes ou segurança de dados?

R: Esse feedback, mais direto nunca existiu, mas acredito que os clientes sejam sensíveis a esta certificação. E dado que trabalhamos maioritariamente com a Banca e há sempre a necessidade de cumprimento do sigilo bancário, o fato de termos uma camada de proteção adicional, será melhor.

9. **A certificação ISO/IEC 27001 trouxe vantagens competitivas no mercado, tanto a nível nacional como internacional?**

R: Nós trabalhamos só o mercado nacional, a vantagem competitiva em relação à concorrência é que fomos pioneiros nesta certificação e ainda os únicos no nosso sector de atividade.

10. **Que impacto teve na relação com os seus clientes, fornecedores e parceiros? Notou um aumento de confiança ou oportunidades de negócio?**

R: Como respondido anteriormente, nunca tivemos um feedback direto, mas julgo que nos veem como uma empresa dinâmica e que aposta muito na melhoria continua dos nossos serviços e das pessoas.

11. **Como asseguram a continuidade e manutenção dos padrões exigidos pela ISO/IEC 27001 no dia a dia da empresa?**

R: Sempre que entra um colaborador novo é sensibilizado sobre as normas em que somos certificados, há sempre uma preocupação pela sensibilização dos mais novos.

Em termos informáticos (*hardware*/*software*/redes) os computadores de cada utilizador estão monitorizados, bloqueados a instalarem programas não autorizados.

12. **A empresa planeia obter outras certificações ou continuar a investir em melhorias contínuas em segurança da informação?**

R: Dentro em breve teremos de nos debruçar e melhorar a nossa estratégia de ESG - *Environmental, Social and Corporate Governance*.

13. **Que conselhos daria a outras PME que estão a considerar a certificação ISO/IEC 27001?**

R: Todo o investimento que se faça na melhoria dos nossos serviços e recursos, é sempre uma mais-valia, independente de se ter um retorno direto ou mais indireto. No mínimo somos mais respeitados e admirados pelos nossos pares e clientes.

14. **Olhando para o futuro, quais são os próximos objetivos em termos de segurança da informação e desenvolvimento da empresa?**

R: Manter o sistema funcional, com os elevados padrões de segurança.

ANEXO B – Certificado de conformidade

Certificado de Conformidade

IPAC acreditação
A0008
ISO/IEC 17021-1
Sistemas de Gestão

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF

N.º: SI - 0104

A EIC - Empresa Internacional de Certificação, S.A.

Certifica que
Hereby certifies that

O Sistema de Gestão da Segurança da Informação implementado pela
The Information Security Management System implemented by

BESTURBAN - Avaliação e Gestão de Patrimónios Imobiliários, Lda.

Avenida Coronel Eduardo Galhardo, 30 C - Galeria Esquerda
1170-105 LISBOA

cumpre os requisitos especificados na norma
fulfills the requirements of the Standard

NP ISO/IEC 27001: 2013

para a atividade de
to the following activity

Avaliação Imobiliária e de Máquinas e Equipamentos de acordo com a Declaração de Aplicabilidade - Edição 2, de 09/12/2022.

Este Certificado é válido até
This Certificate is valid until

31-10-2025

tendo a Auditoria de Concessão ocorrido em
having the First Audit occurred at

20-12-2022

Este Certificado substitui o anteriormente emitido nº SI - 0090
Lisboa, 14 de abril de 2023

Manuel Vidigal
Presidente C.A.

Para confirmar a validade deste certificado, queira p.f. contactar a eiC através de geral@eic.pt ou 214 220 640

eiC
empresa internacional de certificação