COIMBRA BUSINESS SCHOOL

iscac Politécnico de Coimbra

100 ANOS | since 1921

Gestão de Riscos em Sistemas de Informação: Estudo aplicado ao HUC

Mariana Oliveira Santos

ISCAC | 2025

COIMBRA
BUSINESS
SCHOOL

iscac 100 ANOS
Politécnico de Coimbra

Mariana Oliveira Santos

Gestão de Riscos em Sistemas de Informação: Estudo aplicado ao HUC

Coimbra, outubro de 2025

Mariana Oliveira Santos

Gestão de Riscos em Sistemas de Informação: Estudo aplicado ao HUC

Relatório de estágio submetido ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Sistemas de Informação de Gestão**, realizado sob a orientação do Professor Doutor Fernando Paulo dos Santos Rodrigues Belfo, coorientação da Eng.ª Elisabete Mateus dos Reis e supervisão de Eng.º Rui Jorge M.M. Correia Gomes.

Coimbra, outubro de 2025

TERMO DE RESPONSABILIDADE

Declaro ser a autora deste relatório de estágio, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação do presente relatório de estágio.

PENSAMENTO

"Every great dream begins with a dreamer." – Harriet Tubman

DEDICATÓRIA

Dedico este trabalho aos meus pais e à minha avó por me incentivarem, desde sempre, a ser a melhor versão de mim mesma.

AGRADECIMENTOS

Com o encerramento desta etapa, não posso deixar de agradecer a todos os que ajudaram a tornar isto possível.

Em primeiro, aos meus pais, por tudo o que me têm ensinado, desde aprender a caminhar, até à introdução constante do que há de melhor no cinema, na música e na vida. Obrigada por nunca deixarem de acreditar em mim, apoiarem-me desde sempre e tornarem-me em alguém que tenho orgulho em ser.

À minha avó Dina, mulher com M grande, a minha segunda mãe e a minha inspiração constante em ser bondosa, resiliente, ter um coração gigante e fazer de tudo, por todos os que amamos.

Aos meus outros avós, onde quer que estejam, sei que me estão a apoiar incondicionalmente.

Aos de sempre, Francisca C., Francisca R., Marco, Mariana C., Marta, Nené, Verónica e Zé, por estarem sempre presentes em todas as fases, por crescerem comigo e me ensinarem que a vida não é nada sem amizades verdadeiras.

Aos que entraram na minha vida mais tarde, mas na altura certa, Bia, João, Jonicas e Mariana F., que me fazem sentir que os conheço desde sempre. Obrigada por me darem o prazer de fazer parte da vossa vida.

Aos restantes familiares e amigos que, de algum modo, contribuíram, muito obrigada.

Aos meus orientadores, Professor Fernando Belfo e Professora Elisabete Reis, pela orientação prestável e estarem disponíveis sempre que necessário.

À ULS de Coimbra, em especial ao meu supervisor, Sr. Eng.º Rui Gomes, pela oportunidade concedida e por me orientar durante todo o processo.

RESUMO

O presente relatório de estágio descreve um estudo no âmbito da Unidade Local de Saúde de Coimbra, com o objetivo de avaliar a gestão dos riscos tecnológicos e operacionais associados aos principais sistemas de informação dessa unidade hospitalar. O estudo foi realizado no âmbito do Mestrado em Sistemas de Informação de Gestão da Coimbra *Business School* | ISCAC, em parceria com o Departamento de Tecnologias e Sistemas de Informação da ULS de Coimbra.

O estudo utilizou a metodologia de Investigação-Ação delineada por Baskerville, de acordo com uma sequência iterativa de diagnóstico, planeamento, implementação, avaliação e especificação do conhecimento. Foram selecionadas e avaliadas dez aplicações hospitalares, de forma a criar uma matriz de risco estruturada, desenvolvida em conformidade com as normas internacionais ISO 31000:2018 e ISO/IEC 27005:2022. A recolha de dados foi realizada utilizando um questionário distribuído maioritariamente a responsáveis na área do o referido departamento, com o intuito de avaliar fatores de vulnerabilidade e impacto e, consequentemente, o cálculo do risco, de cada aplicação.

Um dos principais resultados deste estudo foi o desenvolvimento de uma matriz de risco semi-quantitativa 5x5, que ilustra visualmente o posicionamento das aplicações nessa matriz, de acordo com os seus níveis de vulnerabilidade e de impacto, e ainda, o seu nível de risco. Esta análise permitiu aumentar o entendimento quanto aos níveis de risco de cada aplicação e auxiliar a tomada de decisões futuras relacionadas com a manutenção, elaboração de planos de contingência e a gestão da segurança da informação destas aplicações. Os resultados sublinham a necessidade de incorporar a gestão de riscos no governo de um portefólio de sistemas de informação de uma unidade hospitalar de grande dimensão e enfatizam a importância de definir estratégias que permitam reforçar aspetos, tas como, resiliência técnica, proteção de dados e segurança do paciente.

Palavras-chave: gestão de riscos, sistemas de informação, matriz de risco, setor hospitalar, ULS de Coimbra, ISO 31000:2018, ISO/IEC 27005:2022

ABSTRACT

This internship report describes a study on Risk Management in Information Systems, implemented at the LHU of Coimbra, with the aim of assessing the management of technological and operational risks associated with the main hospital information systems. The study was conducted as part of the Master's Degree in Management Information Systems at Coimbra Business School | ISCAC, in partnership with the Department of Information Technology and Systems at ULS Coimbra.

The study used the Action-Research methodology outlined by Baskerville, following an iterative sequence of diagnosis, planning, implementation, evaluation, and knowledge specification. Ten hospital applications were selected and evaluated in order to create a structured risk matrix, developed in accordance with international standards ISO 31000:2018 and ISO/IEC 27005:2022. Data collection was carried out using a questionnaire distributed mainly to those responsible for the Department, with the aim of assessing vulnerability and impact factors and, consequently, calculating the risk of each application.

One of the main results of this study was the development of a 5x5 semi-quantitative risk matrix, which visually illustrates the positioning of applications within this matrix according to their vulnerability and impact levels, as well as their risk level. This analysis allowed for a greater understanding of the risk levels of each application and assisted in future decision-making related to maintenance, contingency planning, and information security management of these applications. The results underscore the need to incorporate risk management into the governance of a portfolio of information systems in a large hospital unit and emphasize the importance of defining strategies that strengthen aspects such as technical resilience, data protection, and patient safety.

Keywords: risk management, information systems, risk matrix, hospital sector, LHU of Coimbra, ISO 31000:2018, ISO/IEC 27005:2022

ÍNDICE GERAL

ÍNDICE DE TABELAS

ÍNDICE DE EQUAÇÕES

ÍNDICE DE FIGURAS

Lista de abreviaturas

CDM	*Cyber Defense Matrix*
CHIS	*Cloud based Hospital Information Systems*
CNCS	Centro Nacional de Cibersegurança
COBIT	*Control Objectives for Information and Related Technologies*
CRM	*Clinical Risk Management*
CVSS	*Common Vulnerability Scoring System*
DTID	Departamento de Transformação e Inovação Digital
DTSI	Departamento de Tecnologias e Sistemas de Informação
EHRs	*Electronic Health Records*
ePHI	*Electronic Protected Health Information*
FAIR	*Factor Analysis of Information Risk*
GRC	Governança, Risco e Conformidade
HIPAA	*Health Insurance Portability and Accountability Act*
HL7	*Health Level 7*
IEC	*International Electrotechnical Commission*
IRMIS	*Integrated Risk Management Information System*
ISACA	*Information Systems Audit and Control Association*
ISCAC	Instituto Superior de Contabilidade e Administração de Coimbra
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
KPIs	*Key Performance Indicators*
LEF	*Loss Event Frequency*
LF	Logística e Farmácia
MFA	*Multifactor Authentication*
NIST	*National Institute of Standards and Technology*

OCR	*Office for Civil Rights*
OCTAVE	*Operationally Critical Threat, Asset, and Vulnerability Evaluation*
OWASP	*Open Worldwide Application Security Project*
PACS	*Picture Archiving and Communication System*
PEM	Prescrição Eletrónica Médica
PLM	*Probable Loss Magnitude*
RGPD	Regulamento Geral sobre a Proteção de Dados
RMIS	*Risk Management Information Systems*
RSE	Registo de Saúde Eletrónico
SAPE	Sistema de Apoio à Prática de Enfermagem
SAS	*Statistical Analysis System*
SGICM	Sistema de Gestão Integrado do Circuito do Medicamento
SI	Sistema(s) de Informação
SNS	Serviço Nacional de Saúde
SPMS	Serviços Partilhados do Ministério da Saúde
SPSS	*Statistical Package for the Social Sciences*
STSI	Serviço de Tecnologias e Sistemas de Informação
SWOT	*Strengths*, *Weaknesses*, *Opportunities and Threats*
TEF	*Threat Event Frequency*
TI	Tecnologias de Informação
ULS	Unidade Local de Saúde

1 INTRODUÇÃO

A revolução digital no setor da saúde resultou em mudanças significativas na forma como os hospitais armazenam informações, prestam cuidados e garantem a continuidade dos serviços.

Os Sistemas de Informação (SI) tornaram-se essenciais para o funcionamento das organizações de saúde, integrando procedimentos clínicos, administrativos e logísticos, tal como possibilitando escolhas baseadas em dados. No entanto, à medida que a tecnologia avança, surgem preocupações operacionais e de segurança mais complexas, que devem ser geridas estrategicamente (Argaw et al., 2020; CNCS, 2025).

A gestão de riscos surge como um processo crítico para identificar, avaliar e mitigar os riscos que ameaçam a segurança dos dados, a integridade operacional e a confiança institucional. Em contextos clínicos, a falha dos SI pode ter um impacto direto na segurança do paciente, exigindo uma estratégia metódica e preventiva.

Frameworks como a *International Organization for Standardization* 31000:2018 (ISO 31000:2018) e a ISO/*International Electrotechnical Commission* 27005:2022 (ISO/IEC 27005:2022) fornecem conceitos estruturados e recomendações para incorporar a gestão de riscos na governança corporativa, incentivando a resiliência e o desenvolvimento contínuo (ISO, 2018; ISO/IEC, 2022).

A gestão de riscos é especialmente crucial em hospitais, dada a sua dependência com SI interoperáveis. Os autores Cagliano et al. (2011) e Briner et al. (2010) relatam que a integração de abordagens de gestão de riscos minimiza incidentes, melhora recursos e apoia uma cultura de segurança. A *Clinical Risk Management* (CRM) que se concentra na deteção e diminuição de riscos clínicos, é agora reconhecida como um pilar da qualidade e da segurança do paciente (Farokhzadian et al., 2015).

Outras *frameworks*, como a *Control Objectives for Information and Related Technologies* 2019 (COBIT 2019) e a *National Institute of Standards and Technology Cybersecurity Framework* 2.0 (NIST CSF 2.0) fornecem diretrizes específicas para gerenciar e monitorizar riscos de Tecnologias da Informação (TI) e garantem o alinhamento entre os

objetivos estratégicos das instituições e as práticas de segurança da informação governança, avaliação contínua, resposta a incidentes e resiliência operacional que são, adicionalmente, apoiadas por legislações como o Regulamento Geral sobre a Proteção de Dados (RGPD) e a *Health Insurance Portability and Accountability Act* (HIPAA) (Johnson, 2004; Tucker, 2022).

Em Portugal, o Centro Nacional de Cibersegurança (CNCS) e os Serviços Partilhados do Ministério da Saúde (SPMS) têm trabalhado no desenvolvimento de políticas e programas nacionais sobre risco e segurança da informação no ecossistema do Serviço Nacional de Saúde (SNS), conforme documentação interna facultada pela instituição.

Estas iniciativas destacam a importância de utilizar metodologias consistentes de gestão de riscos, apoiadas por métricas, auditorias e planos de contingência, como o implementado na Unidade Local de Saúde de Coimbra (ULS de Coimbra) e apresentado na documentação interna facultada para fins do estágio, o qual define procedimentos específicos para falhas do sistema e recuperação de informações clínicas.

Neste contexto, este estudo descreve o trabalho realizado no âmbito do programa de Mestrado em Sistemas de Informação de Gestão da Coimbra *Business School* | Instituto Superior de Contabilidade e Administração de Coimbra (ISCAC), em conjunto com o Departamento de Tecnologias e Sistemas de Informação (DTSI) da ULS de Coimbra.

O relatório tem como objetivo avaliar e classificar os riscos operacionais e tecnológicos dos principais SI hospitalares, de modo a criar uma matriz de risco.

A metodologia utilizada foi o modelo de Investigação-Ação estabelecido por Baskerville (1999), que inclui um ciclo iterativo de diagnóstico, planeamento, implementação, avaliação e especificação do conhecimento. Esta estratégia permitiu articular a teoria e a prática, de forma a identificar os riscos das aplicações hospitalares.

Por fim, a pesquisa visa demonstrar que a integração organizada da gestão de riscos dos SI em hospitais, não é apenas uma necessidade legislativa, mas também um pré-requisito necessário para manter a continuidade do tratamento, a segurança do paciente e a maturidade digital nas organizações de saúde.

O relatório está organizado em 6 capítulos, cujo primeiro capítulo é a introdução para este trabalho, com foco nas motivações e justificações para realizar o mesmo; o segundo capítulo é a revisão da literatura, onde apresenta o quadro teórico da gestão de riscos em SI, com foco na gestão de riscos em geral, no contexto hospitalar, nas principais ferramentas de avaliação e matriz de riscos, bem como nas normas e quadros de referência; o terceiro capítulo, metodologia, descreve a abordagem de Investigação-Ação de Baskerville (1999) e a sua relevância para o trabalho; o quarto capítulo, entidade acolhedora, descreve a ULS de Coimbra e os principais SI selecionados e analisados; o quinto capítulo, etapas da Investigação-Ação, descreve os processos de diagnóstico, planeamento, execução, avaliação e especificação do conhecimento; o sexto capítulo, conclusão, apresenta as principais conclusões e recomendações e por último, as referências bibliográficas e apêndices.

2 REVISÃO DE LITERATURA

A revisão da literatura é uma componente essencial para qualquer estudo académico, pois permite identificar as principais contribuições científicas existentes e estabelecer um enquadramento teórico sólido.

No contexto da gestão de riscos e segurança da informação, esta torna-se ainda mais relevante, uma vez que os avanços tecnológicos e o aumento das ameaças cibernéticas exigem uma atualização contínua de metodologias e *frameworks*. No setor da saúde, onde a proteção dos dados dos pacientes e a continuidade dos serviços são fatores críticos, a gestão de riscos de segurança da informação desempenha um papel crucial.

O objetivo principal é analisar, sintetizar e avaliar criticamente as principais contribuições no domínio da gestão de riscos de SI, com foco nas organizações de saúde. Denney & Tewksbury (2013) afirmam que uma revisão bibliográfica abrangente não deve apenas resumir pesquisas anteriores, mas também identificar deficiências conceituais, contradições e requisitos crescentes de pesquisa, fornecendo assim uma justificação para a investigação atual. Embora existam diversos estudos internacionais sobre a aplicação da gestão de riscos em SI hospitalares (Cagliano et al., 2011; Farokhzadian et al., 2015; Manser et al., 2016), observa-se uma escassez de investigações empíricas em instituições portuguesas, limitadas sobretudo a iniciativas internas do CNCS e SPMS (CNCS, 2025), o que reforça a relevância e o caráter prático do presente estudo.

Esta revisão emprega uma metodologia narrativa e crítica, conforme recomendado por Arshed & Danson (2015), ao integrar aspetos de uma revisão convencional, com o rigor de uma estratégia de pesquisa sistemática. O procedimento envolveu a localização de artigos de revistas académicas, normas e relatórios institucionais que abordam a gestão de riscos, estruturas de segurança da informação e governança dentro dos SI hospitalares. A ênfase foi dada a estudos revistos por parte da última década, complementados por *frameworks* de referência, incluindo ISO 31000:2018, ISO/IEC 27005:2022, COBIT 2019 e a estrutura de cibersegurança do NIST que são, globalmente, reconhecidas por orientar a segurança da informação e a governança de riscos.

A revisão foi conduzida através de bases de dados académicas, incluindo a ScienceDirect[1] e IEEE Xplore[2], complementadas por publicações oficiais de organizações de saúde e normas internacionais. Os critérios de inclusão incluíram estudos focados em metodologias de gestão de risco em SI, estratégias de aprendizagem organizacional, estratégias baseadas no conhecimento e relacionadas com os riscos, a implementação de estruturas de governança em ambientes de saúde e padrões e modelos pertinentes ao sistema público de saúde português.

Esta abordagem sistemática e analítica à revisão da literatura, não só estabelece a base académica para o estudo, como também clarifica o quadro teórico para a investigação empírica subsequente, assegurando o alinhamento entre os objetivos da investigação e a conceção metodológica.

2.1 Gestão de Riscos

A gestão de riscos é um processo sistemático e contínuo feito para identificar, avaliar, mitigar e monitorizar os riscos que podem comprometer a consecução dos objetivos estratégicos de uma organização. De acordo com o CNCS, a gestão de riscos envolve, fundamentalmente, a gestão da incerteza, identificando e executando as atividades necessárias para mitigá-la, dado que uma gestão de riscos eficiente permite às empresas tomarem decisões informadas e priorizadas sobre a aplicação de recursos e a execução de ações preventivas, de acordo com normas internacionais como a ISO 31000:2018 e a ISO/IEC 27005:2022 (CNCS, 2025).

Estas normas definem a gestão de riscos como um processo cíclico e dinâmico que consiste em seis etapas principais: estabelecer o contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos e monitorização e comunicação, mencionando ainda conceitos como ameaça, vulnerabilidade, impacto e risco (CNCS, 2025; ISO, 2018; ISO/IEC, 2022).

[1] https://www.sciencedirect.com/
[2] https://ieeexplore.ieee.org/Xplore/home.jsp

Em ambientes de saúde, uma abordagem baseada no risco recomenda mapear ativos críticos, gerir *trade-offs* entre riscos e benefícios, reforçar a gestão de vulnerabilidades, restringir privilégios administrativos e preparar planos de resposta a incidentes e de continuidade, com ênfase na formação de utilizadores e na partilha de informação (Argaw et al., 2020).

A governação eficaz envolve a clarificação de papéis e responsabilidades, critérios de aceitabilidade, mecanismos de revisão periódica, alinhando a gestão de riscos com políticas e processos. Combinam-se métodos qualitativos e semi-quantitativos com registos de responsáveis, prazos e critérios de decisão (CNCS, 2025).

Para além da componente técnica, a perceção de risco das diferentes partes interessadas desempenha um papel crucial na definição dos critérios de aceitabilidade e na ponderação entre objetivos institucionais. A gestão de risco em SI deve articular a análise técnica com a compreensão das expectativas e preocupações de *stakeholders*, de forma a garantir que as decisões refletem um equilíbrio entre segurança, eficiência e continuidade operacional. A integração de evidência técnica com a participação informada contribui para aumentar a legitimidade e robustez das decisões (Renn, 1998).

Ainda sobre a gestão dinâmica do risco, existem artigos que demonstram que restrições financeiras condicionam a mitigação: quando o capital interno é escasso, as organizações tendem a canalizá-lo para a operação/investimento, reduzindo a cobertura de risco, pelo que a priorização deve considerar custos de oportunidade e capacidade de execução (Rampini et al., 2014).

Nas organizações hospitalares, a ligação entre análise de risco, continuidade e resposta a incidentes, torna-se crítica. De acordo com a documentação técnica interna disponibilizada pela ULS de Coimbra relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI, existem procedimentos que envolvem critérios de ativação, fluxos de comunicação, responsabilidades e medidas de contingência em papel, garantindo a prestação segura de cuidados e a recuperação da informação clínica.

Neste contexto, é essencial apresentar alguns princípios fundamentais pertinentes à gestão de riscos como a ameaça, a qual se trata de uma possível origem de um evento indesejável que pode causar danos a um sistema, indivíduo ou organização; a vulnerabilidade, que é uma deficiência num ativo ou controlo que pode ser aproveitada por uma ou mais ameaças; o impacto, que é um efeito de um incidente de segurança específico num ou mais recursos resultando, normalmente, em repercussões diretas ou indiretas para estes e o risco, que é uma situação ou ocorrência que pode afetar, negativamente, a segurança das redes e dos SI (CNCS, 2025).

A gestão de riscos, orientada para a melhoria contínua, permite que as empresas definam, quantifiquem e priorizem critérios e objetivos de aceitação de riscos pertinentes à organização. A gestão dos riscos de uma organização envolve a administração da incerteza e a identificação das atividades necessárias para reduzi-la a níveis considerados aceitáveis pela empresa (CNCS, 2025).

O processo de identificação de riscos deve ser contínuo e baseado no conhecimento ao longo de toda a vida útil do projeto, em vez de um evento único. A abordagem envolve a identificação de ativos em risco, as operações comerciais que estes sustentam, ameaças potenciais e vulnerabilidades relacionadas. Os autores defendem a utilização de equipas interdisciplinares e multifuncionais, incluindo abordagens como *brainstorming*, metodologias Delphi, entrevistas, análise de *Strengths*, *Weaknesses*, *Opportunities and Threats* (SWOT) e diagramas de causa e efeito para identificar riscos explícitos e latentes. Esta metodologia colaborativa e iterativa garante que os riscos não sejam negligenciados, nem tratados isoladamente (Barati & Mohammadi, 2008).

Barati & Mohammadi (2008) afirmam que a identificação de riscos é a fase mais crucial do processo de gestão de riscos uma vez que, quaisquer riscos negligenciados nesta fase, não podem ser avaliados, monitorizados ou mitigados posteriormente. Torna-se essencial criar um registo de riscos completo que registe os perigos identificados, as suas fontes e as ações possíveis. Este serve como fonte principal para a monitorização contínua dos riscos e promove uma cultura de responsabilização, colaboração e melhoria contínua.

A gestão de riscos deve ser entendida, não apenas como uma obrigação normativa, mas como um instrumento estratégico que sustenta a continuidade e a qualidade dos serviços. Esta perspetiva é bastante relevante para as instituições de saúde, cuja fiabilidade dos SI e a gestão eficaz de incidentes são determinantes para a segurança dos doentes, tema aprofundado na secção seguinte.

2.2 Gestão de risco hospitalar

Depois de serem explicados os princípios gerais da gestão de riscos, é importante compreender a sua aplicação nas instituições de saúde. A gestão de riscos em hospitais é essencial para garantir que as operações clínicas e administrativas sejam conduzidas com o mínimo de interrupções e com a máxima segurança, dado que SI geridos eficientemente, podem ajudar, substancialmente, a identificar vulnerabilidades, antecipar potenciais falhas e facilitar uma resposta rápida e eficaz. Isto permite aumentar a segurança dos pacientes, assegurar a conformidade regulamentar e maximizar os recursos, possibilitando aos hospitais um funcionamento mais eficiente e resiliente (Singh & Ghatala, 2012).

Uma gestão de riscos inadequada pode resultar em ineficiências, despesas operacionais elevadas e incidentes dispendiosos, como violação de dados, avarias de equipamentos ou erros médicos, que poderiam ter sido evitados com um quadro de gestão de riscos eficiente (Singh & Ghatala, 2012).

Alam (2016) afirma que os ambientes de saúde são suscetíveis a resultados adversos devido à sua complexidade, elevada demanda e sistemas interdependentes logo, os hospitais devem usar estratégias proativas e orientadas para o sistema, em vez de intervenções reativas.

O processo de gestão de riscos na área da saúde compreende cinco etapas essenciais: definir o contexto, identificar riscos, avaliar e analisar riscos, aplicar estratégias de mitigação e monitorizar continuamente os resultados. Cada fase depende da divulgação precisa de informações e do envolvimento colaborativo entre os departamentos (Alam, 2016).

A gestão dos riscos hospitalares é necessária devido à prevalência de erros médicos e doenças adquiridas em hospitais que contribuem, significativamente, para a mortalidade. Alam (2016) destaca que, em alguns países desenvolvidos, aproximadamente um em cada dez pacientes sofre algum tipo de lesão durante a hospitalização, onde os principais fatores que contribuem para estes acidentes, incluem falhas de comunicação, divulgação inadequada de informações, treinamento insuficiente do pessoal e deficiências sistémicas nos protocolos clínicos e tecnológicos. Mitigar estas vulnerabilidades requer uma transição de uma cultura reativa, centrada na atribuição de culpa, para uma cultura de segurança proativa, baseada em análises de dados rigorosas, colaboração interdepartamental e melhorias contínuas.

A complexidade dos SI hospitalares exige a adoção de metodologias integradas para a identificação e mitigação de riscos. Cagliano et al. (2011) propõem uma metodologia sistémica baseada na teoria das falhas de Reason para a gestão de riscos, no setor da saúde, cuja abordagem não considera apenas os fatores diretos que afetam os pacientes, mas também os elementos organizacionais e humanos que contribuem para estas falhas.

Dückers et al. (2009) destacam que os hospitais devem adotar intervenções de gestão de risco baseadas em setores de alto risco, como a aviação e a indústria. A implementação de sistemas de reporte de incidentes e auditorias regulares são elementos-chave para garantir a segurança dos pacientes. No entanto, os autores alertam também para a necessidade de um compromisso institucional contínuo para garantir a eficácia destas estratégias.

Adicionalmente, o *Clinical Risk Management* (CRM) é considerado um aspeto fundamental da governança clínica, abrangendo as estruturas, procedimentos e instrumentos destinados a identificar, analisar, mitigar e monitorizar os riscos diretamente relacionados com a prestação de tratamento (Manser et al., 2016). O objetivo é diminuir a probabilidade de eventos adversos e, quando estes ocorrem, suavizar os efeitos nos pacientes, profissionais e instituições de saúde (Farokhzadian et al., 2015).

Briner et al. (2010) sustentam a ideia de que o CRM é um tipo de gestão de riscos que se concentra em procedimentos clínicos que estão direta e indiretamente associados ao

paciente, possuindo a estrutura abrangente, os procedimentos, as ferramentas e as atividades que capacitam o pessoal hospitalar a detetar, analisar, mitigar e gerir riscos durante a prestação de tratamento clínico e cuidados ao paciente.

De acordo com estes autores, o CRM baseia-se em quatro pilares fundamentais: a identificação do risco clínico, que envolve a documentação de incidentes, eventos adversos, auditorias clínicas, revisões da literatura e referências mundiais; a análise e avaliação, que inclui técnicas como *Root Cause Analysis* (RCA) e *Failure Modes and Effects Analysis* (FMEA), frequentemente utilizadas para identificar as causas fundamentais das falhas e priorizar áreas essenciais; tratamento e a mitigação que envolvem a introdução de barreiras de segurança, procedimentos clínicos, listas de verificação e tecnologia de apoio à decisão clínica, incluindo a prescrição eletrónica e monitorização e a aprendizagem, que é uma cultura de segurança que não seja punitiva, mecanismos de comunicação, aprendizagem organizacional e formação contínua da equipa (Briner et al., 2010; Farokhzadian et al., 2015).

Da mesma forma, Briner et al. (2010), desenvolveram um instrumento de monitorização para avaliar a implementação do CRM nos hospitais. O instrumento inclui formação contínua da equipa, *feedback* eficiente sobre ocorrências e um maior envolvimento de todos os níveis hierárquicos no reconhecimento e mitigação de riscos, além de que fornece aos hospitais um quadro estruturado para o desenvolvimento do CRM, permitindo a definição de estratégias de melhoria, a priorização de intervenções e a otimização da atribuição de recursos.

Pesquisas nacionais, como um inquérito a hospitais alemães feito por Manser et al. (2016), indicam que a maioria, cerca de 72%, possuía uma estratégia formal de CRM, com estruturas centralizadas em dois terços dos casos. No entanto, apenas 38% incorporam consistentemente o CRM nas reuniões executivas, o que sugere a necessidade de uma maior dedicação estratégica.

De acordo com Singh & Ghatala (2012), o programa de gestão de riscos de um hospital necessita de alguns passos fundamentais para manter os doentes em segurança e reduzir ao mínimo as perdas financeiras. Em primeiro lugar, é necessário contratar um gestor de

riscos, sendo necessário o conselho de administração, o diretor executivo, a equipa médica e outras pessoas importantes do hospital concordarem com esta contratação. Este gestor é responsável em garantir que os planos de gestão de riscos são seguidos e que as regras do hospital são cumpridas (Singh & Ghatala, 2012).

Seguidamente, o gestor de riscos deve fazer rondas regulares e reunir-se com os chefes de área, dando-lhes a conhecer as suas obrigações relacionadas com a matéria de gestão de riscos e assegurar que todas as partes do hospital estão cientes dos possíveis riscos e trabalham em conjunto para os reduzir (Singh & Ghatala, 2012).

Embora muitos hospitais adotem medidas de gestão de risco, há uma grande variação a nível de implementação entre as instituições. Esta heterogeneidade indica que, para ser eficaz, a gestão de riscos hospitalar deve ser continuamente monitorizada e ajustada às necessidades específicas de cada organização.

2.2.1 Instrumentos

Tendo como base a tarefa de análise de riscos com suporte numa matriz feita numa folha de cálculo do Microsoft Excel, presente no Apêndice 2, na Tabela 6 e Tabela 7, procedeu-se à avaliação crítica dos principais instrumentos de avaliação de risco referenciados na literatura e normativos internacionais.

A análise teve como objetivo determinar a adequação de cada instrumento à realidade da ULS de Coimbra, tendo em conta os objetivos institucionais, os recursos disponíveis e o enquadramento regulatório, nomeadamente o RGPD, a ISO 31000:2018 e a ISO/IEC 27005:2022.

A matriz de risco (avaliação qualitativa ou semi-quantitativa) é um instrumento recomendado pelas normas ISO 31000:2018 e ISO/IEC 27005:2022, sendo amplamente utilizado para avaliar e comunicar riscos com base na probabilidade e impacto. A sua abordagem visual, como uma matriz 5x5, facilita a priorização de riscos e a comunicação com os decisores, sendo altamente adequada ao contexto hospitalar e operacional da ULS de Coimbra.

O instrumento *Factor Analysis of Information Risk* (FAIR) é suportado pelo FAIR *Institute* e pelo NIST SP 800-30, proporcionando uma abordagem quantitativa para a análise de risco, baseada na frequência e magnitude do impacto (Stoneburner et al., 2002). É um paradigma de análise de risco que salienta os determinantes do risco, examinando informações de risco e identificando ativos, ameaças e vulnerabilidades que, normalmente, envolve princípios quantitativos e uma abordagem inovadora e pragmática para analisar o risco com base na recolha direta de factos.

O NIST *Special Publication* 800-30 (NIST SP 800-30) é um documento padronizado lançado pelo NIST, que serve como uma estrutura para avaliar as técnicas de gestão de risco (Putra Eryawan et al., 2021).

O NIST SP 800-30 contém três fases principais, em que a primeira é a avaliação de riscos, que se centra à volta do processo de avaliação de riscos e os processos realizados abrangem a caraterização do sistema, a identificação da ameaça, a avaliação da vulnerabilidade, a análise do controlo, a determinação da probabilidade, a análise do impacto, a avaliação do risco e as recomendações de controlo. Seguidamente, a mitigação do risco que inclui, nomeadamente, as fases envolvidas na formulação da estratégia de execução dos controlos de segurança, como a prioridade da ação, recomendações de opções de controlo, análise de custos/benefícios, seleção de controlos, atribuição de responsabilidades. Por fim, a avaliação do risco, que é o resultado de uma estratégia de risco e da sua gestão (Putra Eryawan et al., 2021).

O *Open Worldwide Application Security Project* (OWASP**)** avalia o risco associado a uma vulnerabilidade com base na sua gravidade, sendo esta avaliada de acordo com a probabilidade e consequências das vulnerabilidades. No caso de Søhoel & Gilje Jaatun (2018), as vulnerabilidades são classificadas como altas, médias ou baixas e, visto que a metodologia de classificação de risco do OWASP serve como uma ferramenta de avaliação, é imperativo avaliar a exatidão da avaliação.

O *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) é uma estrutura utilizada para identificar e avaliar questões de segurança da informação. A utilização do OCTAVE tem como objetivo ajudar a empresa a formular critérios

qualitativos de avaliação de risco, tolerância ao risco operacional da organização, determinar os ativos críticos para a missão da empresa, identificar vulnerabilidades e ameaças aos ativos e avaliar e analisar os potenciais resultados para a empresa no caso de surgirem ameaças (Suroso & Fakhrozi, 2018).

O *Common Vulnerability Scoring System* (CVSS) é um quadro técnico utilizado, principalmente, para avaliar vulnerabilidades em *software*. Atribui uma pontuação numérica (0-10) com base em fatores de explorabilidade (por exemplo, vetor de acesso, complexidade, autenticação) e considerações de impacto (por exemplo, confidencialidade, integridade, disponibilidade). O objetivo é facilitar a definição de prioridades na gestão de *patches* e na correção de vulnerabilidades em sistemas de TI (Ugur et al. 2017).

2.2.2 Matriz de Risco

A matriz de risco é um instrumento prevalecente na gestão do risco, particularmente eficaz em contextos complexos como os SI hospitalares. Trata-se de uma ferramenta de apoio à decisão que avalia os riscos de acordo com duas dimensões principais: a probabilidade de ocorrência de um evento e o efeito das suas consequências nos objetivos da organização (Alarfaj & Rahman, 2024; Al-Zuheri et al., 2019).

As organizações podem selecionar entre metodologias quantitativas, qualitativas e semi-quantitativas. O método quantitativo calcula valores numéricos associados a cada elemento resultante da avaliação do risco, onde o efeito do risco, a probabilidade do risco e o nível de risco são quantificados através de números. Como exemplo, os níveis de risco de lesão de um doente devido a um procedimento médico específico, podem ser determinados através da avaliação da probabilidade com base na frequência histórica ou nos dados estatísticos disponíveis, juntamente com valores numéricos que representam o impacto potencial, que vai desde lesões ligeiras, a traumatismos graves que podem resultar em morte (Pascarella et al., 2021).

Ao contrário dos procedimentos quantitativos, os métodos qualitativos não quantificam a probabilidade ou as consequências com valores numéricos. Os níveis de probabilidade e de impacto de um evento específico são quantificados através de uma escala de

classificação pré-determinada, o que normalmente indica uma avaliação incorreta do risco e é aplicável nos casos em que a quantificação dos valores de risco é difícil ou inviável (Pascarella et al., 2021).

A matriz é geralmente representada como uma grelha com escala de, por exemplo, 5x5 ou 3x3, com cada célula a indicar uma combinação particular de probabilidade e impacto. Esta representação visual permite uma categorização qualitativa ou semi-quantitativa dos níveis de risco em classificações como "baixo", "moderado", "elevado" ou "crítico", auxiliando assim na priorização das estratégias de mitigação (Dumbravă & Iacob, 2013; T & Ganeshan, 2021).

Uma matriz qualitativa utiliza categorias descritivas, enquanto as matrizes semi-quantitativas atribuem valores numéricos (por exemplo, 1-5) a cada grau de probabilidade e impacto. O cálculo final do risco é calculado através da multiplicação destes dois fatores (T & Ganeshan, 2021):

$$Risco = Probabilidade \times Impacto$$

Equação 1 - Cálculo standard *do risco*

Além destes fatores, podem ser apresentados outros, como a frequência e severidade, presentas na Figura 1.

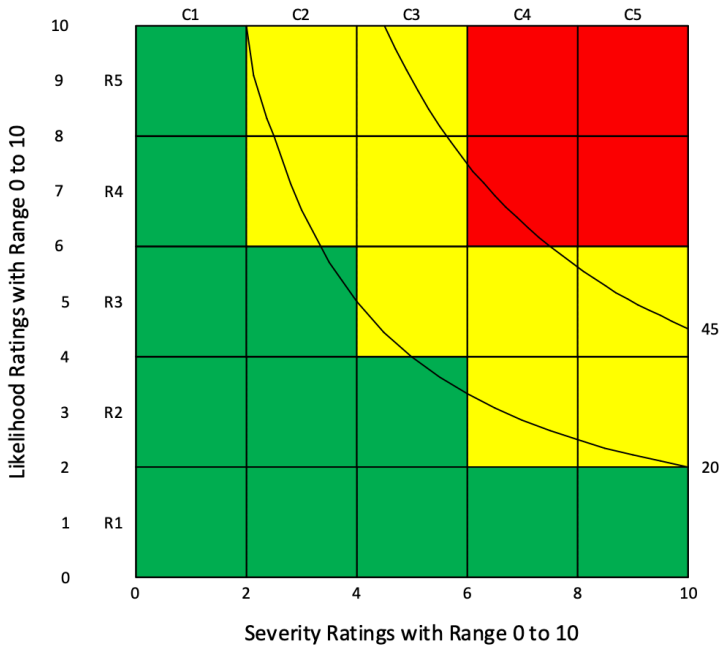


Figura 1 - Matriz de Risco (exemplo 1)
Fonte: Jensen et al. (2022)

Ou também probabilidade e consequência, presentes na Figura 2.

Likelihood	Consequence				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Rare (1)	LOW	LOW	MODERATE	HIGH	HIGH
Unlikely (2)	LOW	LOW	MODERATE	HIGH	EXTREME
Possible (3)	LOW	MODERATE	HIGH	EXTREME	EXTREME
Likely (4)	MODERATE	MODERATE	HIGH	EXTREME	EXTREME
Almost Certain (5)	MODERATE	HIGH	EXTREME	EXTREME	EXTREME

Figura 2 - Matriz de Risco (exemplo 2)
Fonte: Elmontsri, (2014)

A matriz de risco emergiu como uma ferramenta de apoio à decisão nos setores público e privado, incluindo organizações de cuidados de saúde, devido à sua capacidade de normalizar o processo de classificação do risco. A matriz presente na Figura 2 ilustra, tanto a probabilidade de ocorrência de um evento, como os seus potenciais efeitos,

oferecendo uma visão direta da forma como estes elementos contribuem para o risco global, o que auxilia nas discussões entre as partes interessadas relativamente aos riscos identificados (Pascarella et al., 2021).

Este instrumento é definido como um mecanismo para caracterizar e classificar os riscos do processo, normalmente identificados através de revisões multifuncionais, tais como análises de perigos do processo, auditorias ou investigações de incidentes. Também é descrita como uma tabela que apresenta várias categorias de "probabilidade" ou "frequência" nas suas linhas (ou colunas) e várias categorias de "gravidade", "impacto" ou "consequências" nas suas colunas (ou linhas, respetivamente) (Elmontsri, 2014).

Uma matriz de riscos ajuda o gestor de riscos, o conselho de administração e todos os proprietários de riscos a determinar o nível de prioridade das ações corretivas ou controlos necessários no departamento, unidade ou instalação, com base na pontuação obtida. Além disto, facilita a avaliação e a documentação de alterações no risco antes e depois da implementação de medidas de controlo (Pascarella et al., 2021).

Já no contexto específico dos SI em saúde, o documento da SPMS facultado pela instituição, para fins de estágio, destaca que os cenários de risco devem ser avaliados com base na probabilidade e impacto, devendo esta análise servir de base à tomada de decisão sobre mitigação e resposta a incidentes.

Considerando as principais categorias de risco para o SI do hospital, foram identificadas, através deste documento, as diretamente associadas à sua segurança: perda de dados, roubo, acesso não autorizado, *malware* e ataques lógicos. Esta orientação está alinhada com a norma ISO/IEC 27799, que reforça a importância da avaliação estruturada e ponderada dos riscos para a segurança da informação.

Importa referir que a atribuição de pesos aos fatores de impacto e vulnerabilidade é essencial para contextualizar os riscos face às prioridades e características da instituição. Em ambientes complexos como os hospitais, onde diferentes áreas têm graus distintos de criticidade, a utilização de pesos permite ajustar a análise à realidade local, como demonstrado no artigo de Acebes et al. (2024), que propõe uma abordagem quantitativa

para a priorização de riscos, substituindo a matriz clássica por uma análise baseada em simulações de Monte Carlo.

O eixo da frequência de uma matriz normalmente está ligado a valores numéricos que abrangem várias ordens de magnitude. O eixo das consequências é frequentemente baseado numa escala qualitativa, onde estas são determinadas por um julgamento subjetivo, no entanto, a escala de consequências possui, geralmente, valores numéricos implícitos, que podem ou não ser reconhecidos (Elmontsri, 2014).

As áreas de risco são designadas de forma arbitrária ou com base na simetria, em que uma categorização incorreta dos blocos da matriz de risco pode levar a conclusões erradas relativamente ao risco associado a incidentes. Três categorias de matrizes de risco são, frequentemente, utilizadas para a priorização de riscos, onde uma matriz puramente qualitativa define os seus blocos através de uma terminologia descritiva ou qualitativa (Elmontsri, 2014).

Complementarmente, no artigo de Hapon et al. (2021), é evidenciada a aplicação da *Decision Matrix Risk Assessment* (DMRA), uma técnica que permite quantificar o risco de forma semi-quantitativa, atribuindo valores numéricos, tanto à probabilidade, como ao impacto. A combinação destes valores numa grelha de 5x5 possibilita a determinação objetiva do nível de risco e a comparação entre diferentes cenários, como apresentado na Figura 3.

		IMPACT/CONSEQUENCE LEVELS				
		SLIGHT / NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
LIKELIHOOD DESCRIPTORS		Injuries requiring no treatment or first aid	Minor injury, first aid only required	Injury requiring medical treatment and some lost time	Serious injury, hospital treatment required	Death or permanent disability
RARE / REMOTE	May happen only in exceptional circumstances	VERY LOW	VERY LOW	LOW	LOW	MODERATE
UNLIKELY	Could happen some time	VERY LOW	LOW	MODERATE	MODERATE	MODERATE
POSSIBLE / OCCASIONALLY	Might occur occasionally	LOW	MODERATE	MODERATE	MODERATE	HIGH
LIKELY	Will probably occur in most circumstances	LOW	MODERATE	MODERATE	HIGH	VERY HIGH
ALMOST CERTAIN	Expected to occur in most circumstances	MODERATE	MODERATE	HIGH	VERY HIGH	VERY HIGH

RISK EXAMPLE	LIKELIHOOD	IMPACT	RISK GRADING
PATIENT INJURY	UNLIKELY	MAJOR	MODERATE

RISK GRADING COLORS				
VERY LOW RISK	LOW RISK	MODERATE RISK	HIGH RISK	VERY HIGH RISK

Figura 3 - Matriz de Risco 5x5 (Exemplo 3)
Fonte: Pascarella et al. (2021)

Nos cuidados de saúde, em particular nos sistemas de saúde digital e de *Electronic Health Records* (EHRs), a matriz de risco facilita a avaliação das ameaças à cibersegurança, das violações de dados e das falhas do sistema. Os riscos caracterizados por uma elevada probabilidade e um impacto significativo são classificados como "críticos", exigindo uma ação imediata, ao passo que os riscos com baixa probabilidade e impacto mínimo podem ser tolerados ou observados (Alarfaj & Rahman, 2024).

Normas internacionais, como a ISO 31000:2018 (gestão de riscos), a ISO/IEC 27005:2022 (gestão de riscos de segurança da informação) e *frameworks* como o COBIT 2019, defendem a utilização da matriz de risco na tomada de decisões, especialmente na avaliação de riscos tecnológicos e operacionais nos sistemas de saúde (ISO, 2018; ISO/IEC, 2022; Steuperaert, 2019).

A utilização de uma matriz de risco melhora a comunicação entre o pessoal técnico e os gestores de risco, convertendo as avaliações de risco técnico numa representação visualmente compreensível e estratégica da vulnerabilidade organizacional (Bianco et al., 2022; Dumbravă & Iacob, 2013).

2.3 COBIT 2019

Para além das ferramentas operacionais, importa também considerar as *frameworks* que suportam a gestão de risco nos SI hospitalares. O COBIT 2019 constitui uma melhoria substancial do COBIT 5, desenvolvido pela *Information Systems Audit and Control Association* (ISACA) ao incorporar caraterísticas mais flexíveis, especialmente pertinentes para as organizações de saúde. A área da saúde, progressivamente dependente da transformação digital e da governação de TI, pode implementar o COBIT 2019 para melhorar a gestão dos seus SI e diminuir os riscos associados com a cibersegurança (Steuperaert, 2019).

A principal vantagem do COBIT 2019 está na sua flexibilidade e adaptabilidade, permitindo que as instituições personalizem procedimentos, estruturas e mecanismos de controlo de governança para se alinharem com a sua realidade operacional, o que se torna pertinente em hospitais e instituições de saúde, em que a conformidade regulatória, a proteção de dados e a continuidade clínica devem coexistir dentro de infraestruturas digitais complexas.

O estudo de Antariksa et al. (2025) afirma que o COBIT 2019 promove a criação de valor através de uma estratégia abrangente e integrada que engloba todas as funções organizacionais e alinha a gestão de riscos de TI, com o desempenho dos negócios.

Os hospitais que dependem, significativamente, das aplicações de cuidados de saúde para gerir os registos médicos dos utentes, informações sensíveis dos mesmos e operações de cuidados de saúde, obtêm vantagens de uma estrutura como o COBIT 2019, uma vez que esta ajuda a garantir o cumprimento de requisitos (Dhimas Azizah et al., 2021).

O COBIT 2019 dá prioridade à avaliação de riscos, oferecendo aos hospitais uma estrutura sistemática para melhorar a qualidade e a segurança dos sistemas de TI do setor da saúde, tal como uma garantia de que a qualidade do *software* cumpre as rigorosas expectativas estabelecidas pela regulamentação dos cuidados de saúde. As organizações devem identificar, avaliar e mitigar os riscos relacionados com o não cumprimento destes requerimentos (Dhimas Azizah et al., 2021; Gebremedhin Kassa, 2017).

A implementação do COBIT 2019 no setor da saúde pode desempenhar um papel fundamental na conformidade com regulamentos internacionais, especialmente no que diz respeito à segurança da informação e proteção de dados. O estudo de Dhimas Azizah et al. (2021) baseia-se na análise da *Halodoc*, uma plataforma digital de telemedicina e demonstra que o COBIT 2019, na estruturação dos processos de TI, contribuiu para a identificação e mitigação de riscos relacionados à segurança da informação, a monitorização contínua da conformidade, utilizando um modelo estruturado de governança, e o alinhamento dos processos de TI com os requisitos regulatórios, o que garante que a plataforma cumpra com os padrões de proteção de dados sensíveis dos pacientes.

Este autor afirma ainda que a integração do COBIT 2019, no ciclo de desenvolvimento de *software* para aplicações médicas, melhora a capacidade das organizações de cumprir normas como a HIPAA, Regulamento Geral sobre a Proteção de Dados (RGPD) e ISO/IEC 27001 (Dhimas Azizah et al., 2021).

Estes resultados sugerem que o COBIT 2019 pode ser amplamente utilizado no setor hospitalar para assegurar a conformidade com normas de segurança e privacidade, especialmente num contexto onde a adoção de registos eletrónicos de saúde e plataformas digitais está em crescimento.

2.4 ISO 31000:2018

Nota: A designação ISO/IEC aplica-se a normas publicadas em conjunto pelas ISO e IEC, geralmente em domínios tecnológicos ou de segurança da informação. Por este motivo, a ISO/IEC 27005:2022 é emitida por ambas as entidades, enquanto a ISO 31000:2018 é, exclusivamente, uma norma ISO, de âmbito mais geral e aplicável a qualquer tipo de organização (EVS, 2023).

A ISO 31000:2018 fornece recomendações abrangentes de gestão de risco, incluindo um quadro definido e um conjunto de princípios que podem aplicar-se a qualquer tipo de empresa, independentemente da sua dimensão ou setor (ISO, 2018). Esta norma é bastante importante em ambientes hospitalares, como a ULS de Coimbra, em que a gestão do risco é fundamental para garantir a segurança dos doentes, dados e a estabilidade operacional.

Esta norma estabelece um conjunto de princípios fundamentais para garantir que a gestão do risco gera e preserva valor, facilita a tomada de decisões e incentiva a melhoria contínua (ISO, 2018).

Os princípios incluem a integração, o que significa que a gestão do risco deve ser incorporada em todas as atividades organizacionais e ter uma abordagem estruturada e abrangente; uma adaptação ao contexto e objetivos específicos da organização; a inclusão, ao encorajar a participação de todas as partes interessadas; dinamismo, reconhecendo que os riscos evoluem ao longo do tempo; a melhor informação ao dispor da organização; a consideração dos fatores humanos e culturais e um compromisso com a melhoria contínua (ISO, 2018).

A estrutura da ISO 31000:2018 relata a importância da liderança de alto nível e a dedicação à gestão de riscos, garantindo que esta seja incorporada à estrutura de governança e à cultura da empresa, o que inclui a disponibilização de recursos suficientes, a definição clara de funções e deveres e a implementação de processos abertos de comunicação e consulta com as partes interessadas (ISO, 2018).

A norma define o processo de gestão do risco como comunicação e consulta, estabelecimento do âmbito, contexto e critérios de risco, avaliação do risco (ou seja, identificação, análise e avaliação), tratamento do risco, monitorização e revisão, registo e comunicação, presente na Figura 4 (ISO, 2018). Esta abordagem foi utilizada na ULS de Coimbra, de modo a rever SI hospitalares importantes.

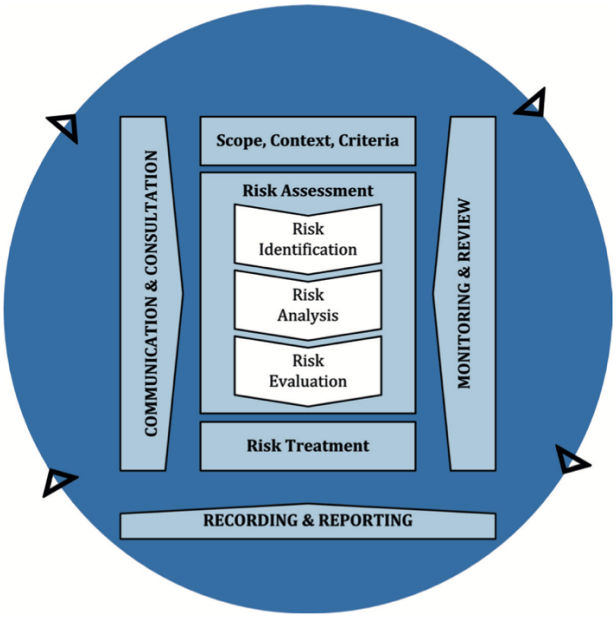


Figura 4 – Processo de gestão de risco
Fonte: ISO (2018)

A identificação de riscos serve para destacar os potenciais perigos para a continuidade dos doentes e para a segurança da informação. A análise de risco avalia a possibilidade e o impacto destes perigos, enquanto a avaliação de risco tem o papel de relacionar os resultados com os critérios de risco do hospital para ajudar a dar prioridade às ações. O tratamento do risco implica a criação e implementação de métodos para reduzir, transferir, aceitar ou evitar os perigos, apoiados por planos documentados e avaliações regulares para verificar a sua eficácia (Ahmet & Vladi, 2017).

Enquanto a ISO 31000:2018 se foca nos princípios gerais de gestão de risco aplicáveis a qualquer organização, a ISO/IEC 27005:2022 traduz estes princípios para o domínio específico da segurança da informação, sendo complementar na gestão de riscos tecnológicos e de cibersegurança na ULS de Coimbra (ISO, 2018; ISO/IEC, 2022; WeSecure, 2024).

2.5 ISO/IEC 27005:2022

A norma ISO/IEC 27005:2022 é uma diretriz internacional que oferece princípios e orientações para a gestão de riscos em segurança da informação, alinhada com a norma ISO/IEC 27001 (ISO/IEC, 2022).

Consiste numa *framework* para a identificação, avaliação, tratamento, monitorização e comunicação de riscos de segurança da informação (Forêt, 2023) sendo, particularmente, relevante para a gestão de risco em organizações de saúde, onde a proteção de dados sensíveis dos pacientes e a garantia da continuidade dos serviços são essenciais (Bonnie & Leung, 2023).

A classificação da informação é um dos aspetos críticos na aplicação da ISO/IEC 27005:2022, especialmente, em ambientes hospitalares, em que os dados clínicos, administrativos e financeiros precisam de níveis diferenciados de proteção.

Agrawal (2017) propõe um modelo de classificação de informação baseado na ISO/IEC 27005:2022, permitindo que as organizações identifiquem, classifiquem e protejam ativos críticos. No setor da saúde, a aplicação deste modelo implica a identificação de dados sensíveis, incluindo registos digitais, exames clínicos, a definição de níveis de proteção, estabelecendo controlos de segurança para cada tipo de informação e a garantia da confidencialidade e integridade, evitando acessos não autorizados e modificações indevidas nos dados. Ao utilizar esta abordagem, os hospitais podem melhorar a governança de segurança da informação, garantindo conformidade com normas como a HIPAA e RGPD.

A ISO/IEC 27005:2022 é pertinente em ambientes de saúde, como a ULS de Coimbra, onde a salvaguarda da confidencialidade, integridade e disponibilidade da informação dos doentes é essencial para proteger dados sensíveis e garantir a continuidade operacional (ISO/IEC, 2022).

Durante o estágio na ULS de Coimbra, foram utilizados os conceitos da norma ISO/IEC 27005:2022 para analisar e avaliar as aplicações do hospital, alinhando a estratégia de gestão do risco com os objetivos institucionais e os mandatos regulamentares que foram fornecidos para o âmbito deste estágio.

De acordo com a norma em questão, o processo de gestão do risco é iterativo e inicia-se com o estabelecimento do contexto, o que implica a análise do ambiente interno e externo, a compreensão dos objetivos estratégicos do hospital, a identificação das expectativas das partes interessadas e a consideração das obrigações legais e regulamentares relevantes,

incluindo as leis de proteção de dados, como o RGPD. Esta fase essencial garante que as atividades de avaliação dos riscos são congruentes com a missão e os objetivos operacionais do hospital. A última fase, a avaliação do risco, consiste em três atividades principais: identificação do risco, análise do risco e avaliação do risco (ISO/IEC, 2022).

No âmbito da ULS de Coimbra, a identificação do risco concentrou-se em detetar os riscos potenciais que poderiam afetar os sistemas clínicos escolhidos, através das suas vulnerabilidades e impacto.

A análise do risco avaliou, subsequentemente, o possível impacto e a vulnerabilidade causada pela manifestação destes perigos, utilizando instrumentos adequados, tais como matrizes de risco qualitativas, ou semi-quantitativas, e o tratamento do risco incluiu a seleção e recomendação de métodos adequados para mitigar, evitar, transferir ou aceitar os riscos identificados. (ISO/IEC, 2022)

A monitorização e avaliação contínuas constituem um aspeto fundamental desta norma, o que permite aos hospitais ajustarem os seus protocolos de segurança e manter a eficácia ao longo do tempo em reação a ameaças emergentes, ou alterações no sistema.

2.6 NIST *Cybersecurity Framework* 2.0

A NIST CSF 2.0 do NIST, publicada em 2024, representa um avanço significativo nas metodologias de governança e gestão de riscos de cibersegurança (Wu et al., 2024). É concebida como uma estrutura versátil e expansível, permitindo que as empresas de vários setores, incluindo infraestruturas essenciais como a saúde, giram os riscos de cibersegurança de acordo com os seus objetivos estratégicos e requisitos regulamentares.

Em contraste com as normas orientadas, exclusivamente, para a conformidade, o NIST CSF 2.0 adota uma metodologia baseada no risco que incorpora a cibersegurança na estrutura global de governança e operacional das empresas, destacando a monitorização contínua, a responsabilidade e a resiliência (Melo Gomes & Macedo, 2024; Wu et al., 2024). Embora seja uma iniciativa dos EUA, o CSF é amplamente adotado internacionalmente devido à sua abordagem abrangente e flexível.

Uma característica notável do NIST CSF 2.0 é a sua adaptabilidade e compatibilidade com outras estruturas reconhecidas. Wu et al. (2024) afirmam que a integração do NIST CSF 2.0 com a ISO/IEC 27001:2022 e a *Cyber Defense Matrix* (CDM) estabelece uma estrutura de governança em vários níveis que combina supervisão estratégica com controlos operacionais.

Enquanto que a ISO/IEC 27001 delineia controlos de segurança específicos para a implementação e manutenção de um *Information Security Management System* (ISMS), o NIST CSF 2.0 oferece uma estrutura estratégica para a gestão de riscos, e a CDM serve como uma ferramenta de visualização para mapeamento de capacidades, identificação de lacunas e priorização de recursos. Coletivamente, estas estruturas fornecem uma metodologia global do ciclo de vida para a gestão da cibersegurança que abrange a identificação, prevenção, deteção e melhoria contínua dos riscos (Wu et al., 2024).

A progressão contínua das ameaças digitais, juntamente com a crescente complexidade dos ataques à cibersegurança, destacou a necessidade de adaptação do CSF. O lançamento do NIST CSF 2.0 foi uma reação a estas dificuldades, integrando contribuições das partes interessadas da área da saúde, de forma a garantir a relevância e a resiliência da estrutura em relação à tecnologia contemporânea e aos riscos emergentes (John Lynch & Associates, 2024).

As funções fundamentais do CSF, identificar, proteger, detetar, responder e recuperar, oferecem uma perspetiva estratégica sobre o ciclo de vida da gestão de riscos de cibersegurança em ambientes de saúde. Esta metodologia sistemática permite que as empresas compreendam e atenuem os riscos para sistemas, ativos, dados e capacidades, enquanto cumprem as exigências da HIPAA para a proteção das informações dos pacientes (John Lynch & Associates, 2024).

A implementação do NIST CSF 2.0 no setor de saúde é essencial devido à sensibilidade dos dados médicos e à dependência de sistemas interconectados, incluindo os EHRs, plataformas de diagnóstico e infraestruturas de telemedicina. O NIST CSF 2.0 facilita a interoperabilidade com normas regulatórias, como a HIPAA e o RGPD, fornecendo orientações sistemáticas para proteger as informações dos pacientes por meio de

avaliações de risco contínuas, controlos de segurança e protocolos de resposta a incidentes (John Lynch & Associates, 2024; Melo Gomes & Macedo, 2024).

O uso combinado do NIST CSF 2.0 e do CDM provou ser benéfico em vários setores, reforçando a resiliência organizacional, facilitando a comunicação entre equipas técnicas e executivas e gerando resultados quantificáveis para o desempenho da cibersegurança (Wu et al., 2024). Em instituições de saúde como a ULS de Coimbra, esta integração pode facilitar a monitorização proativa de vulnerabilidades, minimizar o tempo de inatividade do sistema e garantir o alinhamento das práticas de cibersegurança com as normas nacionais e europeias de proteção de dados.

O NIST CSF 2.0 cria uma estrutura de governança coesa e flexível que melhora a interação entre cibersegurança, gestão de riscos e resiliência organizacional. Ao integrar-se com *frameworks* complementares, como a ISO/IEC 27001 e a CDM, oferece às organizações de saúde uma base sólida para salvaguardar a confidencialidade dos dados, garantir a disponibilidade do sistema e alcançar a conformidade regulamentar num ambiente progressivamente digital e repleto de ameaças (John Lynch & Associates, 2024; Wu et al., 2024).

2.7 HIPAA

A HIPAA é um estatuto federal nos EUA que regula a salvaguarda das informações de saúde, com ênfase específica na confidencialidade, integridade e acessibilidade das *electronic Protected Health Information* (ePHI). Esta norma de segurança exige que as empresas abrangidas estabeleçam proteções administrativas, técnicas e físicas para reduzir os riscos e manter a proteção contínua dos dados dos doentes (Johnson, 2004).

A Especificação de Implementação da Análise de Risco (§164.308) é uma especificação exigida pelo Processo de Gestão de Segurança, que exige uma "avaliação abrangente e meticulosa dos potenciais riscos e vulnerabilidades à confidencialidade, integridade e disponibilidade das informações de saúde eletrónicas protegidas mantidas pela entidade abrangida". Esta avaliação deve ser registada e revista de forma consistente, especialmente quando há alterações nas tecnologias ou nos procedimentos operacionais (Johnson, 2004).

O processo de análise de risco, em conformidade com a HIPAA, engloba atividades como análises de vulnerabilidade, avaliações de rede e de perímetro, entrevistas a pessoal, auditorias e avaliações de políticas, todas ideadas para detetar e mitigar riscos de forma proactiva. Sublinha a melhoria e o registo contínuos, garantindo que, quaisquer medidas de segurança instituídas, mantêm a sua eficácia e relevância ao longo do tempo (Johnson, 2004).

Do ponto de vista da gestão de riscos hospitalares, a HIPAA salienta a necessidade de estratégias sistemáticas e proativas. O *Office for Civil Rights* (OCR) tem enfatizado, consistentemente, que a cibersegurança começa com uma avaliação de risco completa, seguida por estratégias contínuas de monitorização e reparação. Incidentes em ambientes de saúde, incluindo divulgações não autorizadas e ataques de *ransomware*, têm aumentado a necessidade de integrar processos clínicos e administrativos com os regulamentos da HIPAA (Vanderpool, 2019).

Os hospitais são obrigados a manter um inventário atualizado dos sistemas e ativos que armazenam ou processam ePHI, identificar ameaças e vulnerabilidades, desenvolver planos de ação corretiva e implementar programas contínuos de formação e sensibilização. Estas medidas estão alinhadas com as recomendações do OCR, que afirma que uma análise de risco precisa e abrangente deve ser contínua e atualizada, periodicamente, para manter a conformidade e a resiliência (Tucker, 2022).

Apesar de ser uma lei dos EUA, os princípios da HIPAA são aplicáveis em instituições de saúde de todo o mundo, incluindo hospitais na Europa. A ênfase na segurança baseada no risco, monitorização contínua e responsabilização está em conformidade com normas internacionais como a ISO/IEC 27005:2022 e o RGPD, salvaguardando informações confidenciais dos pacientes e garantindo a continuidade dos serviços de saúde (Tucker, 2022).

3 METODOLOGIA

Para este relatório, foi utilizada a metodologia de Baskerville (1999) que afirma que a técnica de Investigação-Ação segue, frequentemente, uma abordagem cíclica de cinco fases, pertinente para a investigação em SI. Na Figura 5, encontra-se uma sinopse de cada uma das cinco fases desta metodologia.

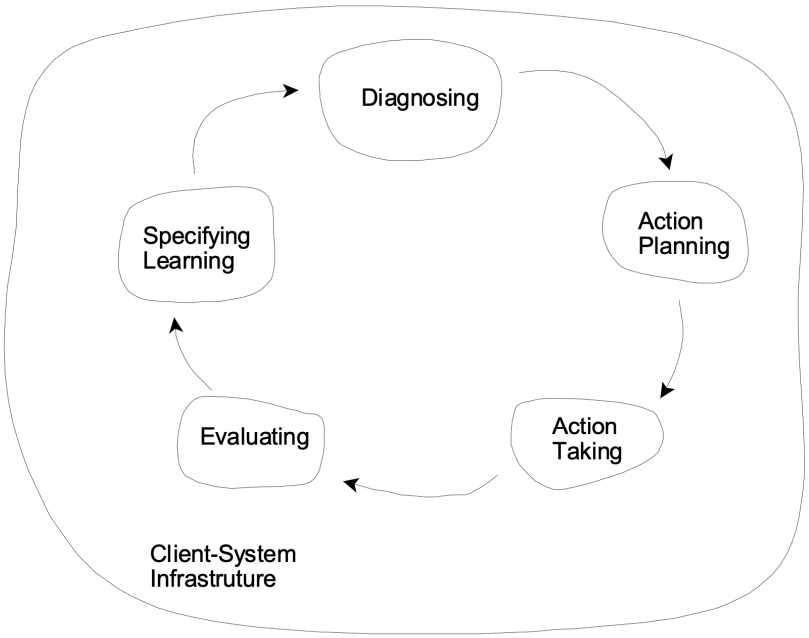


Figura 5 – Ciclo da Metodologia Investigação-Ação

Fonte: (Baskerville, 1999)

3.1 Diagnóstico

A fase do diagnóstico dá ênfase à compreensão do quadro organizacional existente e à identificação dos problemas fundamentais. A técnica é colaborativa, ou seja, os investigadores colaboram com os membros da organização para avaliar a situação.

O objetivo é encapsular a complexidade do sistema organizacional, em vez de reduzir o problema a variáveis discretas, onde o resultado desta etapa é o desenvolvimento de pressupostos teóricos preliminares, ou hipóteses de trabalho sobre a natureza do problema (Baskerville, 1999).

Nesta fase, foram avaliadas várias aplicações hospitalares, com foco na identificação de riscos e questões de integração cruciais para um funcionamento sustentado. Posteriormente, foram delineadas ações para melhorar a integração entre os sistemas, com base na interoperabilidade.

As entrevistas planeadas com o pessoal selecionado podiam ser realizadas com o objetivo de detetar quais os problemas operacionais, incluindo uma integração insuficiente dos SI e a relutância dos especialistas em adotar novas tecnologias. Subsequentemente, foram avaliadas as questões através da análise da infraestrutura e dos processos atuais, com destaque para as deficiências na comunicação interna e a capacidade de resposta inadequada a situações importantes.

3.2 Planeamento da ação

Na sequência dos resultados do diagnóstico, os investigadores e os profissionais formulam, de forma conjunta, um plano estratégico, que tem por objetivo resolver os problemas identificados, sugerindo intervenções ou modificações organizacionais. O processo é teoricamente fundamentado, o que indica que as ações pretendidas não são arbitrárias, mas antes fundamentadas num quadro concetual ou científico (Baskerville, 1999).

A análise dos aspetos críticos revelados nas entrevistas, foi integrada nesta fase e estabelecido um plano para criar uma matriz de risco mais sistemática e garantir a monitorização contínua dos riscos, em conformidade com as melhores práticas de *frameworks*, como a ISO/IEC 27005:2022.

Planeou-se estabelecer uma metodologia sistemática para avaliar os sistemas escolhidos, através de uma matriz de risco 5x5 semi-quantitativa (segundo a dimensão "impacto" e a dimensão "vulnerabilidade", onde cada uma é constituída por 5 fatores distintos), adaptada ao contexto operacional do hospital. Esta matriz integrou normas internacionais, incluindo a ISO/IEC 27005:2022, a ISO 31000:2018 e a COBIT 2019, estando em conformidade com os mandatos institucionais de proteção de dados e resiliência de serviços, bem como a formulação de fatores de impacto e de vulnerabilidade, de modo a criar o questionário para avaliação.

3.3 Execução da ação

A execução da ação implementou o plano elaborado, em que os investigadores e profissionais se envolveram, ativamente, na organização do estudo, resultando na implementação de melhorias específicas. Podem ser empregues diversas estratégias de intervenção, e a intervenção pode ser diretiva, em que o estudo orienta explicitamente a mudança, ou não diretiva em que a mudança é procurada de forma indireta (Baskerville, 1999).

As intervenções concebidas nesta fase foram executadas no contexto organizacional atual e os investigadores e os profissionais, pertencentes ao Departamento de Tecnologias de Informação e Sistemas (DTSI), colaboraram para identificar e, posteriormente, se for possível, implementar as modificações. Esta fase encerrou o princípio fundamental da Investigação-Ação: a aquisição de conhecimentos através da prática (Baskerville, 1999).

A implementação sugeriu medidas para melhorar os recursos atuais, incluindo a negociação de contratos de manutenção adequados e a utilização eficaz de recursos para garantir a continuidade operacional.

Esta fase consistiu na utilização das 10 aplicações na matriz de risco, recolhendo e analisando indicações como a integração do sistema, o nível de manutenção e o envolvimento dos utilizadores, onde a participação dos profissionais internos garantiu que o processo se mantivesse enraizado na viabilidade operacional, com o objetivo de compreender melhor em que estado se encontram as aplicações selecionadas.

3.4 Avaliação

Baskerville (1999) afirma que a fase de avaliação constitui um período de exame crítico e ponderado, com o objetivo de avaliar a eficácia das medidas implementadas e compreender os fatores que contribuem para o sucesso ou fracasso das intervenções. Esta avaliação deve basear-se em factos verídicos, observações diretas e comparações com as hipóteses teóricas estabelecidas durante a fase de diagnóstico, garantindo assim a validade das conclusões e evitando interpretações superficiais.

Além disto, a avaliação facilita a aprendizagem organizacional (*double-loop learning*) ao converter as lições aprendidas em conhecimento prático, o que pode resultar na reinterpretação das normas, práticas e políticas institucionais (Baskerville, 1999).

A avaliação vai além da mera verificação de resultados, servindo como um processo reflexivo colaborativo que fortalece a conexão entre a teoria e a prática e que facilita a evolução do modelo de gestão de riscos e o estabelecimento de uma cultura de melhoria organizacional. Nesta fase, os resultados foram discutidos com as partes interessadas, para se verificar a adequação do modelo de pontuação e o significado prático das categorias de risco indicadas, onde o *feedback* obtido facilitou o refinamento do modelo e a validação da interoperabilidade (Baskerville, 1999).

3.5 Especificação do conhecimento

A fase de especificação do conhecimento é a última etapa do ciclo de Investigação-Ação, onde o objetivo é tornar o conhecimento adquirido, durante o processo, mais formal e concreto. De acordo com Baskerville (1999), esta etapa tem dois objetivos: ajudar a organização a progredir e fazer contribuições científicas que possam ser utilizadas noutras situações.

Do ponto de vista organizacional, esta fase baseia-se em tornar a experiência prática em conhecimento utilizável, permitindo que a instituição de saúde considere integrar os conhecimentos adquiridos nas suas políticas, processos e práticas de gestão de riscos (Baskerville, 1999).

As informações recolhidas podem ser utilizadas para melhorar os processos ao longo do tempo, o que fortalece a cultura de segurança e a maturidade da gestão de riscos nos SI hospitalares. Além disto, garante benefícios mútuos, tanto para a organização, como para a comunidade académica (Baskerville, 1999).

Numa perspetiva académica, a delineação do conhecimento garante que os resultados adquiridos sejam registados de forma meticulosa e teórica, permitindo assim a sua contribuição para a literatura científica sobre SI e gestão de riscos. Para o setor de saúde, a estruturação das evidências, o pensamento crítico sobre o processo e a ligação entre a

teoria e a prática podem tornar o estudo válido e útil para outras instituições com características semelhantes.

4 ENTIDADE ACOLHEDORA

4.1 História

A ULS de Coimbra é a maior unidade de saúde em Portugal, criada pela consolidação de várias unidades de saúde, nos termos do Decreto-Lei n.º 102/2023, de 7 de novembro (Presidência do Conselho de Ministros, 2023). Esta empresa pública, integrada no SNS, visa melhorar a prestação de cuidados de saúde especializados, apoiar a formação académica e fomentar a investigação e a inovação. A necessidade de melhorar a prestação de cuidados de saúde através da consolidação de recursos e competências, foi um dos fatores que motivou a criação da ULS de Coimbra (SPMS, 2025d).

A ULS de Coimbra inclui várias unidades hospitalares essenciais, entre elas os hospitais da Universidade de Coimbra, o Geral, o Sobral Cid, especializado em cuidados psiquiátricos, o Arcebispo João Crisóstomo (Cantanhede), o Pediátrico, o Centro de Medicina de Reabilitação da Região Centro - Rovisco Pais (Tocha) e as maternidades Bissaya Barreto e Daniel de Matos (SPMS, 2025d).

As unidades estão localizadas em Coimbra e prestam serviços à população local, funcionando também como centros de referência para a região centro de Portugal e, em certas áreas especializadas, para todo o país (SPMS, 2025d).

A missão da ULS de Coimbra engloba a prestação de cuidados de saúde diferenciados e de elevada qualidade, a promoção do ensino académico e clínico, a realização de investigação avançada e a procura permanente de inovação. O objetivo é estabelecer uma rede de cuidados de saúde aberta e integrada que garanta cuidados de saúde humanos, eficientes e de qualidade (SPMS, 2025d).

4.1.1 Departamento de Tecnologias e Sistemas de Informação

O DTSI da ULS de Coimbra é uma unidade integral que presta apoio crítico às operações hospitalares e é oficialmente reconhecida no âmbito administrativo da instituição. As principais tarefas são a gestão de infraestruturas, redes e comunicações, o apoio a sistemas clínicos e administrativos, a interoperabilidade, a segurança da informação e a assistência técnica/*helpdesk*, com base na documentação técnica interna elaborada no âmbito da

Estratégia Nacional para o Ecossistema de Informação de Saúde (ENESIS), disponibilizada no âmbito do estágio.

A nível estratégico, o DTSI passou por um processo de reestruturação que integrou vários departamentos de SI para garantir uma gestão consolidada dos serviços de TI, aderindo às melhores práticas como, *Information Technology Infrastructure Library* (ITIL) e melhorando áreas de operações, qualidade de *software*, interoperabilidade, gestão de serviços e suporte, sistemas clínicos e inteligência empresarial.

Ao nível operacional, é responsável pela ativação e coordenação de planos de contingência em caso de falha do SI, bem como pela comunicação e coordenação com os prestadores de cuidados de saúde para garantir a continuidade dos cuidados, conforme documentação técnica interna elaborada no âmbito da ENESIS, disponibilizada no âmbito do estágio.

Apesar da sua importância estratégica, a documentação interna destaca a deficiência da DTSI em termos de autonomia sobre a centralização do SPMS como uma vulnerabilidade, sublinhando a necessidade de consolidação local da sua governação e autoridade de tomada de decisões.

4.1.2 Descrição das atividades realizadas durante o estágio

O estágio foi realizado na ULS de Coimbra, no DTSI, fazendo parte da componente não letiva do Mestrado em Sistemas de Informação de Gestão da Coimbra *Business School* | ISCAC.

O objetivo principal era avaliar a gestão de riscos nos SI hospitalares, concentrando-se, especificamente, na avaliação das vulnerabilidades e impactos das aplicações essenciais utilizadas pela instituição, ajudando assim na formulação de uma matriz de riscos institucional em conformidade com normas internacionais como ISO 31000:2018, ISO/IEC 27005:2022 e COBIT 2019.

As atividades foram realizadas em colaboração com representantes técnicos e clínicos de cada serviço, em conformidade com os documentos estratégicos do hospital, disponibilizados para fins do estágio, documentação técnica interna disponibilizada pela

ULS de Coimbra relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI e a análise técnica da plataforma de interoperabilidade, presente na documentação interna sobre a integração de sistemas clínicos em utilização na instituição.

As principais tarefas consistiram na avaliação e caracterização dos SI hospitalares, recolha de dados técnicos e funcionais acerca de aplicações essenciais em funcionamento (por exemplo, SClínico, Registo de Saúde Eletrónico (RSE), Clinidata XXI, Sonho V2), entrevistas informais com o pessoal da DTSI e os principais utilizadores de diversas unidades hospitalares. Foram presenciadas algumas reuniões com o supervisor do estágio e outros elementos do DTSI, relativas a problemas e/ou a criação de soluções para a ULS de Coimbra, especificamente no departamento mencionado.

Houve também a análise de documentos sobre normas, políticas e planos institucionais relativos à gestão de riscos e segurança da informação, incluindo o Plano de Gestão de Riscos da ULS de Coimbra, documentação técnica interna disponibilizada pela ULS de Coimbra relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI e o documento que relata sobre a plataforma de integração dos SI clínicos em utilização na instituição.

Realizou-se o processamento quantitativo e análise dos resultados, empregando uma metodologia de avaliação semi-quantitativa com o objetivo de calcular médias ponderadas para características dos fatores de vulnerabilidade e impacto, onde os resultados agregados foram utilizados para colocar cada aplicação numa matriz de risco 5x5, que forneceu uma base para priorizar estratégias de mitigação e estabelecer níveis de risco institucional.

A identificação e categorização de vulnerabilidades significativas também foi feita, como a falta de contratos de manutenção ativos, desafios de interoperabilidade, *softwares* antigos, dependência de infraestruturas essenciais e deficiências nos protocolos de acesso e segurança.

A criação de uma ferramenta de diagnóstico, na forma de um questionário *online*, teve como intuito reunir as opiniões de especialistas em saúde sobre a vulnerabilidade, impacto

e os aspetos que influenciam as aplicações hospitalares, abordando variáveis como o número de utilizadores, disponibilidade do sistema, importância clínica, interoperabilidade, frequência de atualização, manutenção, segurança de acesso e sensibilidade dos dados.

Todas estas tarefas auxiliaram e permitiram o desenvolvimento deste relatório de estágio, de forma a poder contribuir, de alguma maneira, para a melhoria dos SI hospitalares da ULS de Coimbra.

4.2 Sistemas de Informação

Os SI têm a capacidade de resolver várias questões relacionadas com a prestação de cuidados de saúde, a segurança dos doentes e a prática clínica, o que é possível se os SI puderem ser efetivamente aplicados no local de prestação de cuidados.

Os SI são definidos por duas caraterísticas principais: a integração de subsistemas e a capacidade de fornecer informações essenciais de uma forma utilizável, o que garante que a informação seja precisa, atual e fiável para a tomada de decisões, resultando numa melhor prestação de serviços. Podem ser caracterizados como um sistema digital destinado a supervisionar as operações clínicas e administrativas quotidianas, a facilitar os serviços de saúde e a gerir os procedimentos de tratamento e de seguro (Sayyadi Tooranloo & Saghafi, 2021).

No entanto, os profissionais de saúde têm grandes apreensões relativamente à utilização dos SI e às suas implicações para as suas funções, dado que as questões relacionadas com a aceitação e a satisfação dos profissionais de saúde são, atualmente, consideradas um dos maiores obstáculos à implementação de SI nestes ambientes (Cohen et al., 2016).

A análise das necessidades dos profissionais de saúde e a compreensão das características dos SI que influenciam a sua satisfação e produtividade, tornaram-se aspetos essenciais na avaliação e investigação destes sistemas. A avaliação que um utilizador de SI faz das caraterísticas do sistema pode ter impacto na sua felicidade emocional, afetando assim os seus comportamentos de utilização. Uma maior satisfação do utilizador está correlacionada com um maior envolvimento no funcionamento de um sistema, o que é

crucial para a obtenção de benefícios avançados das instalações dos mesmos (Cohen et al., 2016).

Os SI hospitalares são essenciais para manter registos médicos completos dos doentes e dados associados, bem como supervisionar os serviços médicos, incluindo o diagnóstico, o tratamento, a investigação, os relatórios de acompanhamento e as decisões clínicas vitais. Estes sistemas melhoram os cuidados prestados aos doentes, aumentando os conhecimentos dos utilizadores, diminuindo a ambiguidade e facilitando a tomada de decisões através de informações integradas e, os dados armazenados, são utilizados para fornecer informações acessíveis aos utilizadores do sistema (Sayyadi Tooranloo & Saghafi, 2021).

O SI hospitalar, enquanto subsistema sociotécnico, engloba todos os sistemas de processamento de informação pertinentes e facilita vários objetivos, incluindo a utilização dos recursos e a melhoria do desempenho, cumprindo um papel fundamental na facilitação das operações hospitalares através da utilização de TI adequadas (Sayyadi Tooranloo & Saghafi, 2021).

Além disto, os SI aumentam a eficiência operacional, reduzem os riscos e controlam os custos enquanto fornecem um quadro tecnológico que garante serviços de alta qualidade e atempados de uma forma financeiramente sustentável, bem como uma solução global para os prestadores de cuidados de saúde que procuram manter a competitividade no panorama atual dos cuidados de saúde. Um SI estruturado facilita serviços rápidos e eficientes, aumenta o controlo sobre a prestação de serviços, diminui os encargos administrativos e aumenta a produção a todos os níveis (Sayyadi Tooranloo & Saghafi, 2021).

Os SI hospitalares são infraestruturas essenciais para o funcionamento eficiente das instituições de saúde, facilitando a integração das atividades clínicas, administrativas e financeiras. Sutejo et al. (2021) afirmam que os hospitais são instituições intensivas em mão de obra, tecnologia e risco que dependem de tecnologias digitais para orquestrar processos complexos, garantir a segurança dos pacientes e mitigar os riscos operacionais.

Neste contexto, o SI hospitalar e o *Risk Management Information System* (RMIS) desempenham funções complementares: o primeiro facilita as operações diárias de saúde, enquanto o segundo identifica, avalia e mitiga, sistematicamente, os riscos relacionados com dados, sistemas e segurança dos pacientes (Sutejo et al., 2021).

A incorporação da TI em ambientes hospitalares revolucionou a tomada de decisões, oferecendo acesso imediato a dados clínicos e administrativos, dado que um SI de saúde executado de forma eficaz, permite aos profissionais de saúde a recolha, processo e divulgação de informações dos pacientes de forma eficiente, minimizando erros e melhorando a continuidade do tratamento. Sutejo et al. (2021) afirmam que a eficácia da gestão de riscos hospitalares depende cada vez mais da interoperabilidade e funcionalidade destes sistemas.

Existe a necessidade de um *Integrated Risk Management Information System* (IRMIS), que combine os princípios de gestão de riscos com a arquitetura de informação hospitalar, onde esta integração garante a monitorização constante dos dados relativos a ocorrências clínicas, vulnerabilidades do sistema e questões de conformidade que são, consequentemente, incorporados nos processos de tomada de decisões estratégicas (Sutejo et al., 2021).

Além da gestão de riscos, os SI hospitalares servem como instrumentos vitais de apoio à tomada de decisões, visto que aumentam a capacidade dos gestores e médicos de tomar decisões baseadas em evidências, ao analisarem dados extensos sobre os resultados dos pacientes, a utilização de recursos e a eficácia do sistema (Low & Hsueh Chen, 2012).

De acordo com Low & Hsueh Chen (2012), a implementação de *Cloud-based Hospital Information Systems* (CHIS) aprimorou estas capacidades, aumentando a escalabilidade, a acessibilidade dos dados e a eficiência de custos.

Os CHIS permitem o acesso universal aos registos médicos, permitindo que médicos, enfermeiros e administradores obtenham informações de qualquer local, promovendo assim a colaboração entre hospitais e a continuidade do tratamento. Esta transição tecnológica originou novas preocupações com relação à segurança dos dados e

privacidade, obrigando os hospitais a implementar estruturas de avaliação e governança mais avançadas para os seus SI (Low & Hsueh Chen, 2012).

O processo de gestão de riscos de segurança da informação, apresentado na Figura 6 e conforme definido pela norma ISO/IEC 27005:2022 e pelas instruções do CNCS, oferece uma metodologia sistemática e contínua para a proteção dos SI. O processo envolve a definição do ambiente corporativo e dos parâmetros de risco, a identificação e análise de riscos, vulnerabilidades e ativos, e a avaliação do seu possível impacto e probabilidade (CNCS, 2025; ISO/IEC, 2022).

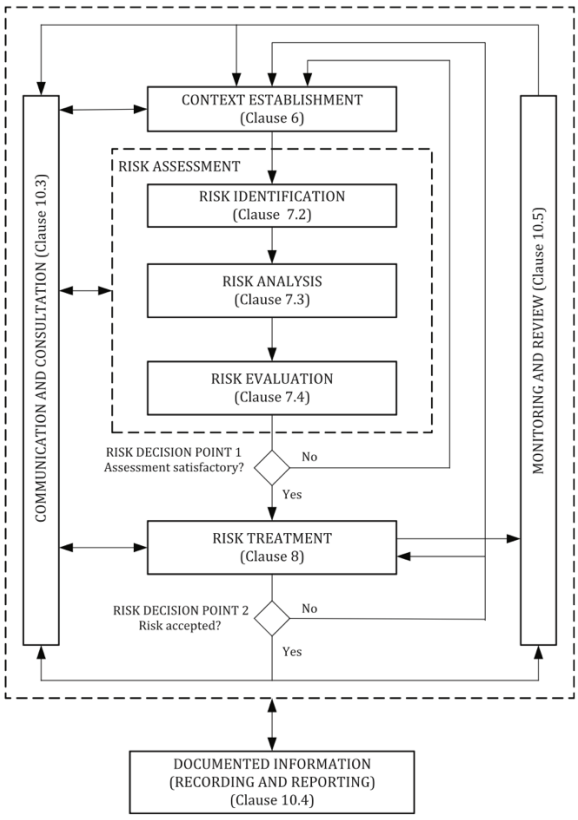


Figura 6 - Processo de gestão de riscos de segurança da informação
Fonte: (ISO/IEC, 2022)

4.3 Descrição das aplicações

A partir de uma Folha de Cálculo Microsoft Excel[3], foi estruturada uma tabela com o intuito de organizar informação sobre os SI da ULS de Coimbra escolhidos para este trabalho, facilitando a avaliação da influência de cada aplicação nas operações diárias e na segurança geral.

Esta tabela permite uma avaliação sistemática das variáveis de risco críticas para cada aplicação, incluindo frequência de utilização, níveis de atualização e disponibilidade de assistência técnica. Através desta, foi possível estabelecer uma base robusta para identificar áreas cruciais, tais como SI com manutenção inadequada ou integração restrita, que poderiam comprometer a continuidade de serviços importantes.

Ao reunir ideias de especialistas na saúde sobre a sensibilidade dos dados, a importância das aplicações de cuidados aos pacientes e as consequências potenciais de falhas, é possível mapear prioridades operacionais e de segurança dentro da ULS de Coimbra.

Neste sentido, o desenvolvimento desta tabela, demonstrada no Apêndice 1, foi essencial para melhorar a compreensão das aplicações e formular um diagnóstico mais preciso, facilitando a tomada de decisões sobre a gestão de riscos e a melhoria dos SI hospitalares.

Entre as 10 aplicações avaliadas, encontra-se a CardioBase que é um SI de cardiologia desenvolvido para gerir o processo clínico dos pacientes, desde a admissão até à alta no serviço de cardiologia. O sistema guarda os dados demográficos dos pacientes, assim como os seus perfis de risco correspondentes, cujos dados podem ser adquiridos automaticamente através de um SI hospitalar (por exemplo, Sonho V2). O registo de cada paciente fornece acesso ao seu histórico médico, incluindo exames, hospitalizações e consultas (Cardiobase, 2025).

Juntamente com uma coleção de listas fundamentais, todos os dados introduzidos podem ser examinados e integrados de forma rápida e fácil, facilitando a aquisição de informações para investigação clínica ou métricas de desempenho. Estes dados podem

[3] https://www.microsoft.com/pt-pt/microsoft-365/excel?market=pt

ser exportados para o Microsoft Excel ou outros aplicativos de análise estatística, como *Statistical Package for the Social Sciences* (SPSS) ou *Statistical Analysis System* (SAS) (Cardiobase, 2025).

O Clinidata XXI é um *software* que ajuda a gerir laboratórios ao receber, processar e disponibilizar resultados de análises clínicas. Encontra-se conectado à SClínico e à RSE, o que permite visualizar os resultados nos processos clínicos eletrónicos. No entanto, uma falha nesta aplicação afetaria a prestação de cuidados, atrasando diagnósticos e terapias (Maxdata Software, 2025).

O OphthalSuite é um *software* dedicado à área da oftalmologia, utilizado para registo clínico, imagens diagnósticas e relatórios associados a consultas e cirurgias oftalmológicas. Por lidar com dados altamente sensíveis e exames visuais, a sua disponibilidade é crucial para o apoio à decisão clínica (BlueWorks, 2025).

A *Picture Archiving and Communication System*, designada como PACS, é fundamental para radiologia, cardiologia e outras especialidades que utilizam meios complementares de diagnóstico por imagem, em que a integração com sistemas como este, permite aos médicos aceder rapidamente às imagens para apoiar diagnósticos. De acordo com documentação técnica interna elaborada no âmbito da ENESIS, disponibilizada no âmbito do estágio, é um dos sistemas mais críticos do hospital, devido ao seu impacto direto no tratamento de emergência e internamento.

A SClínico é um SI desenvolvido pela SPMS, que resultou da fusão de dois sistemas utilizados por milhares de médicos, enfermeiros e outros profissionais de saúde: o Sistema de Apoio Médico (SAM) e o Sistema de Apoio à Prática de Enfermagem (SAPE). Cresceu até se tornar uma única aplicação, comum a todos os prestadores de cuidados de saúde e centrada no paciente, estando presente em mais de 50 hospitais, instituições de caridade e institutos, contando com cerca de 60 000 profissionais registados (SPMS, 2025a).

O SClínico faz parte da estratégia definida pelo Ministério da Saúde para a informatização clínica do SNS, que prevê a padronização dos procedimentos de registo clínico, a fim de garantir a normalização da informação. Em conformidade com a documentação técnica interna elaborada no âmbito da ENESIS, disponibilizada no âmbito do estágio, o acesso

a uma variedade de informações clínicas sobre o utilizador, a utilização e partilha de dados com profissionais de saúde de diferentes áreas e a sistematização destes dados permitem organizar as práticas e as informações recolhidas a nível nacional, tornando o trabalho dos profissionais de saúde mais eficaz, com um desempenho mais adequado à sua função na equipa multidisciplinar e, deste modo, um melhor apoio, cuidados e acompanhamento ao utilizador.

A PEM é a aplicação de Prescrição Eletrónica de Medicamentos utilizada, tanto nas organizações hospitalares, como em cuidados primários. A sua integração com o SClínico e os sistemas de farmácia garante segurança e rastreabilidade das prescrições, em que uma falha comprometeria a medicação dos doentes (SPMS, 2025b).

A RSE funciona como repositório central de informação clínica dos utentes, consolidando dados provenientes de diferentes instituições do SNS. É fundamental para a interoperabilidade, permitindo que os profissionais tenham acesso a um histórico clínico unificado e a sua criticidade relaciona-se com a continuidade de cuidados interinstitucionais e a confidencialidade dos dados pessoais de saúde (SPMS, 2025c).

O Sistema de Gestão Integrado do Circuito do Medicamento (SGICM) apoia o circuito do medicamento no hospital, desde a prescrição até à administração ao doente. Garante rastreabilidade e segurança no processo do medicamento, reduzindo erros e assegurando conformidade legal, em que a sua integração com a PEM e SClínico é crítica para garantir a consistência da informação (MediaWiki, 2016).

A SGICM-LF trata-se de uma vertente específica do SGICM, orientada para Logística e Farmácia (LF), responsável pela gestão de *stocks*, armazenamento e distribuição de medicamentos e produtos farmacêuticos. É essencial para assegurar a disponibilidade contínua de terapêuticas e consumíveis hospitalares (MediaWiki, 2016).

Por fim, o Sonho V2 é o sistema de gestão hospitalar administrativa e financeira, abrangendo módulos de gestão de doentes, faturação, recursos humanos e logística, e responsável pela articulação administrativa com o SNS e gestão financeira da instituição. Embora não diretamente clínico, a sua falha teria impacto reputacional e organizacional,

afetando a sustentabilidade do hospital, de acordo com documentação técnica interna elaborada no âmbito da ENESIS, disponibilizada no âmbito do estágio (SPMS, 2025e).

Através da análise minuciosa das diversas características técnicas e funcionais de cada sistema, organizadas na tabela do Microsoft Excel, inserida no Apêndice 1, foi possível identificar e compreender as características distintas de cada aplicação que afetam diretamente o perfil de risco e a capacidade de resposta a instâncias de falha, ou vulnerabilidade. Isto permitiu a identificação de potenciais vulnerabilidades e o estabelecimento de prioridades para ações futuras.

A secção seguinte fornece uma justificação para a importância de cada campo, destacando os elementos técnicos, funcionais e estratégicos essenciais para delinear com precisão o risco associado a cada aplicação. Esta análise fornece uma perspetiva abrangente e completa, crucial para uma melhor tomada de decisão e o estabelecimento de estratégias de mitigação e monitorização adequadas.

Em primeiro, o campo **"**fabricante**"** é essencial para identificar riscos associados à origem dos ativos e fornecedores, os quais são considerados fontes externas de risco, devendo ser analisados no processo de identificação e avaliação de risco, o que inclui riscos relacionados com suporte, atualização e fiabilidade do sistema (ISO, 2018; ISO/IEC, 2022).

A determinação do fabricante permite a avaliação da confiança externa e da fiabilidade do sistema, o que é crucial em ambientes críticos como os hospitais (ISO, 2018; ISO/IEC, 2022). A ausência de assistência técnica ou de atualizações pode agravar os riscos operacionais, tal como descrito nos planos de gestão de riscos da ULS de Coimbra e os de contingência presentes na documentação técnica interna, disponibilizada pela instituição, que definem procedimentos operacionais em caso de falência dos SI.

As "interfaces" entre sistemas são pontos críticos de vulnerabilidade. A ISO/IEC 27005:2022 reconhece que a comunicação entre sistemas deve ser segura, sendo esta uma área de risco potencial e a ISO 31000:2018 reforça que o contexto interno e externo da organização, incluindo ligações entre sistemas, deve ser considerado no processo de gestão de risco. Isto deve-se ao facto de a gestão de risco ocorrer no contexto dos objetivos

e operações da organização, dos elementos organizacionais poderem constituir uma fonte de risco e a finalidade e o âmbito do risco estarem relacionados com os objetivos gerais da organização (ISO, 2018; ISO/IEC, 2022).

A natureza da interface afeta diretamente a interoperabilidade e as potenciais áreas de falha no fluxo de dados entre aplicações, onde o exame técnico do sistema em utilização, mencionado na documentação técnica interna disponibilizada pela ULS de Coimbra, sublinha a complexidade das interligações e a importância de regras de encaminhamento precisas.

A "integração real" das aplicações envolve risco tecnológico e organizacional, pois a má integração pode comprometer a interoperabilidade e a segurança dos dados. Tanto a ISO 27005:2022, como a ISO 31000:2018 enfatizam a importância da avaliação de riscos associados a sistemas interligados (ISO, 2018; ISO/IEC, 2022).

A documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a uma plataforma de integração de sistemas clínicos em utilização, ilustra a função fulcral da desta plataforma na gestão da informação clínica, cujo funcionamento contínuo e eficaz das integrações delineadas neste documento permite a identificação de problemas de comunicação com impacto nas operações clínicas.

A presença de um "contrato de manutenção ativo" reduz o risco operacional e garante respostas rápidas a falhas. A ISO/IEC 27005:2022 relata a importância da manutenção como controlo de risco, bem como as consequências de falhas em contratos. Por outro lado, a ISO 31000:2018 discute a necessidade de seleção de estratégias de tratamento do risco que incluem recursos externos como contratos, tendo em conta que a organização deve considerar os valores e o conhecimento das partes interessadas (ISO, 2018; ISO/IEC, 2022).

Com base na documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI, a presença de um contrato de manutenção diminui os riscos de interrupções prolongadas em caso de falha, sendo uma medida preventiva essencial no

plano de contingência institucional, o que define prazos para uma execução em situações de colapso de sistemas.

Os "interlocutores internos" e "interlocutores externos" são críticos para garantir uma comunicação eficaz na gestão de riscos, conforme recomendado pela ISO 31000:2018 e também pela ISO/IEC 27005:2022 no contexto da gestão interna e funções organizacionais associadas ao risco (ISO, 2018; ISO/IEC, 2022).

A presença de contactos internos e externos é um procedimento previsto na documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a planos de contingência desta, que definem procedimentos operacionais em caso de falência dos SI, fundamental para facilitar a coordenação da resposta a incidentes durante as falhas planeadas e não planeadas.

A "interoperabilidade das bases de dados" é um elemento crítico para a integridade e disponibilidade da informação e a ISO 31000:2018 reconhece a necessidade de compreender interdependências técnicas, visto que a gestão dos riscos se insere no âmbito dos objetivos e das ações da organização (ISO, 2018).

Este aspeto diz respeito à integridade e às informações trocadas entre os sistemas. A análise da documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a uma plataforma de integração de sistemas clínicos em utilização, demonstra as interações entre sistemas essenciais, incluindo o SGICM e Cardiobase.

O "número de utilizadores" tem impacto direto relativamente ao risco, dado que um número elevado de utilizadores exige controlos robustos de acesso, sendo esta uma prática recomendada na ISO/IEC 27005:2022 e na avaliação de contexto da ISO 31000:2018 (ISO, 2018; ISO/IEC, 2022). Este campo reflete o grau de exposição do sistema, em que aplicações com mais utilizadores implicam maior risco de erro ou falha, o que obriga a uma vigilância e controlo de acessos proporcionais. Isto está alinhado com as práticas de segurança da SPMS, presentes na documentação interna para fins de estágio, facultada pela instituição.

Os “grupos profissionais” são cruciais para entender quais os utilizadores principais das aplicações e de que modo são afetados com a falha ou o sucesso destes.

A "data da última atualização" está associada à gestão de vulnerabilidades. A ISO 31000:2018 identifica o acompanhamento contínuo como parte do ciclo de melhoria, onde o objetivo do acompanhamento e da revisão é garantir e melhorar a qualidade, bem como a eficácia da conceção, execução e resultados do processo. A supervisão contínua e a avaliação regular do processo e dos resultados devem ser uma componente integral para a gestão do risco. Os resultados da monitorização e da revisão devem ser incluídos nos processos de gestão, medição e comunicação do desempenho da organização (ISO, 2018).

A "localização dos servidores" influencia a exposição a riscos físicos e ambientais. A ISO/IEC 27005:2022 relata a importância do ambiente físico na segurança da informação, e a ISO 31000:2018 recomenda considerar fatores físicos e geográficos no entendimento do contexto organizacional (ISO, 2018; ISO/IEC, 2022). A literatura sobre o SPMS, na documentação interna facultada para fins de estágio, sublinha a necessidade de garantir a redundância e a segurança física e lógica no ambiente do SNS.

Relativamente às "infraestruturas dos centros de dados", a ISO 31000:2018 reforça que a infraestrutura faz parte do contexto do processo de gestão do risco que deve ser determinado através da compreensão dos ambientes externo e interno em que a organização funciona, devendo corresponder ao ambiente específico relevante para a atividade a que o processo de gestão do risco se destina (ISO, 2018).

O suporte físico à operação dos sistemas é fundamental na continuidade dos serviços, como evidenciado na solução de contingência proposta à ULS de Coimbra, mencionada numa documentação técnica para efeitos de estágio, que oferece redundância e monitorização contínua.

A "proteção física e lógica do acesso" é um dos pilares da segurança da informação, em que ambas as normas reconhecem a importância de implementar controlos adequados de acesso (ISO, 2018; ISO/IEC, 2022). A segurança do acesso é abordada na documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a planos de contingência, que define regras específicas para acesso a dados e registos em papel em caso de falência dos SI, onde o mesmo plano distingue responsabilidades por perfil profissional.

O campo **"**quem pode extrair estas informações**?"** está relacionado com o controlo de acessos e a confidencialidade dos dados. A ISO/IEC 27005:2022 recomenda a definição clara de responsabilidades, e a ISO 31000:2018 sublinha a importância da delimitação do acesso no contexto organizacional (ISO, 2018; ISO/IEC, 2022). Este campo está envolvido com a rastreabilidade e a proteção de dados sensíveis, uma preocupação transversal a todos os planos de contingência, segurança e melhoria da SPMS, com base na documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI.

A **"**licença de *software***"** é um fator legal e de segurança, cuja utilização de um *software* não licenciado pode expor a organização a riscos técnicos e jurídicos. A ISO/IEC 27005:2022 trata da gestão de *software* e licenças como parte da segurança dos ativos, enquanto a ISO 31000:2018 enquadra este controlo dentro da seleção de medidas de tratamento de risco (ISO, 2018; ISO/IEC, 2022).

A legalidade e atualidade das licenças utilizadas afetam a conformidade com as políticas internas do hospital e os requisitos contratuais, como referido no plano de contingência presente na documentação técnica interna disponibilizada pela ULS de Coimbra.

5 ETAPAS DA INVESTIGAÇÃO-AÇÃO

Nesta secção, é delineada a metodologia utilizada durante o estágio, assente no modelo de Investigação-Ação proposto por Baskerville (1999), considerado o mais adequado devido às suas características iterativas e colaborativas, o que facilita a intervenção prática no contexto real da organização e, simultaneamente, gera conhecimento pertinente.

5.1 Diagnóstico

Durante esta fase preliminar, procedeu-se a uma avaliação detalhada de várias aplicações informáticas utilizadas na ULS de Coimbra, essenciais ao funcionamento clínico e administrativo. Esta fase envolveu a análise da documentação institucional, entrevistas informais aos responsáveis informáticos e recolha de dados, seguindo orientações pelas normas internacionais como a ISO/IEC 27005:2022 e a ISO 31000:2018.

A instituição possui protocolos de contingência estabelecidos para falhas previstas e imprevistas dos SI, delineando funções específicas e tempos de resposta, o que realça a importância do assunto e a necessidade de preparação operacional e documental para garantir a continuidade dos cuidados, bem como a recuperação dos dados clínicos em cenários de contingência.

Contudo, o diagnóstico revelou uma forte dependência dos sistemas clínicos e administrativos, tornando a sua resiliência e continuidade operacionais críticas para a prestação de cuidados e segurança dos doentes. O mau funcionamento destes sistemas afeta diretamente a prestação de cuidados, a segurança dos doentes e as operações dos serviços, com base na documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI.

Identificou-se que a plataforma de integração referida na documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a uma plataforma de integração de sistemas clínicos em utilização, gere vários padrões *Health Level* 7 (HL7) e regras de encaminhamento que ligam aplicações essenciais (por exemplo, Sonho V2, PACS, RSE), o que apresenta riscos de interoperabilidade, concentração de integrações numa única

produção e falta de ambientes de teste/qualidade que aumentam a criticidade operacional e agravam o impacto em cascata dos incidentes.

O HL7 é um protocolo da camada de aplicação para a troca de dados em ambientes de cuidados de saúde que unifica os esforços de prestadores de cuidados de saúde, fornecedores e consultores. A organização internacional de padrões HL7 defende e implementa a padronização das informações eletrónicas de cuidados de saúde para melhorar a partilha, administração, qualidade, eficiência e eficácia da prestação de cuidados de saúde e da troca de informações médicas. Os responsáveis pelas aplicações em cuidados de saúde deviam integrar o HL7 em cada sistema para facilitar a troca e partilha de dados com sistemas internos e externos (Cheng et al., 2004; Munnelly & Clarke, 2009).

Esta fase de diagnóstico permitiu delimitar um conjunto de vulnerabilidades relacionadas com a integração tecnológica, manutenção e a gestão documental. Diagnosticou-se que a resiliência tecnológica da ULS Coimbra depende de uma melhor coordenação entre infraestruturas, planos de contingência e práticas de monitorização contínua, dado que a ausência de mecanismos sistemáticos de avaliação e atualização dos sistemas reforça a necessidade de uma abordagem estruturada de gestão de riscos.

As constatações obtidas orientaram os acontecimentos das próximas etapas, centradas na avaliação dos riscos das aplicações críticas através da construção de uma matriz de risco 5x5, sustentada em fatores de impacto e vulnerabilidade, combinando dados técnicos e perceções dos profissionais.

5.2 Planeamento da ação

A fase de planeamento da ação é considerada uma etapa essencial na conversão do diagnóstico para um plano de ação sistemático e com base científica. As intervenções sugeridas são consistentes com *frameworks* estabelecidas, incluindo ISO 31000:2018 (ISO, 2018), ISO/IEC 27005:2022 (ISO/IEC, 2022), COBIT 2019 (Gebremedhin Kassa, 2017) e NIST *Cybersecurity Framework* 2.0 (Stoneburner et al., 2012), garantindo assim precisão metodológica e comparabilidade global.

Esta fase teve como objetivo o planeamento da avaliação dos riscos das aplicações críticas selecionadas e o desenvolvimento de uma matriz de risco semi-quantitativa 5x5, projetada especificamente para ambientes de saúde, integrando fatores de impacto e vulnerabilidade e para facilitar a priorização contínua e transparente dos riscos (Dumbravă & Iacob, 2013; Pascarella et al., 2021).

Seguindo a metodologia de Investigação-Ação de Baskerville (1999), o plano frisa o envolvimento colaborativo das partes interessadas, incluindo pessoal de TI, profissionais de saúde e líderes administrativos, garantindo assim a integridade técnica e a legitimidade organizacional. Foram definidos critérios de avaliação, sustentados por *Key Performance Indicator* (KPI), como apresentado na Tabela 6 e Tabela 7 do Apêndice 2 (CNCS, 2025; Gebremedhin Kassa, 2017).

A partir deste método sistemático, planeou-se detetar e avaliar as vulnerabilidades, pontos de integração, ausência de contratos de manutenção e outros fatores de risco que colocassem em causa a segurança, a disponibilidade e a integridade dos SI, bem como realizar uma avaliação do nível de risco associado às aplicações informáticas utilizadas no contexto da ULS de Coimbra.

Foi planeada a definição de uma fórmula específica de avaliação de risco, onde o cálculo do risco teve em consideração diversos fatores, de modo a poder ser calculado, posteriormente.

5.2.1 Descrição dos modelos adequados

Foi essencial reconhecer que nem todos os modelos são igualmente eficazes no ambiente hospitalar. Cada um apresenta benefícios e limitações que dependem do contexto organizacional, da disponibilidade de recursos e das estipulações regulatórias e a fase de planeamento requer uma avaliação crítica para diferenciar técnicas adequadas de inadequadas, no contexto de uma instituição de saúde complexa.

A matriz de risco (avaliação qualitativa ou semi-quantitativa) é um instrumento recomendado pelas normas ISO 31000:2018 e ISO/IEC 27005:2022, sendo amplamente utilizado para avaliar e comunicar riscos, com base na probabilidade e impacto. A sua abordagem visual (ex.: matriz 5x5) facilita a priorização de riscos e a comunicação com

os decisores, sendo altamente adequada ao contexto hospitalar e operacional da ULS de Coimbra (Kaya et al., 2019; Pascarella et al., 2021).

Além disto, este modelo implementa a premissa fundamental de que o risco é uma função dependente da probabilidade e do impacto, tal como se apresenta na Equação 2, permitindo a colocação de cada aplicação numa grelha 5×5 com vários níveis de criticidade (baixo a crítico).

$$Risco = Probabilidade \times Impacto$$

Equação 2 - Cálculo do risco

Este método semi-quantitativo atribui pontuações que variam de 1 a 5 a cada fator e, quando aplicável, inclui pesos, antes de traduzir os resultados nos eixos da matriz (Kaya et al., 2019).

O modelo FAIR permite que as organizações transmitam as suas informações de risco, alinhando-se assim com os objetivos organizacionais por meio do estudo de cenários de risco e avaliações, calculando a frequência e a magnitude das perdas (Traoré & Yamamoto, 2018).

Este modelo oferece uma estrutura definitiva para avaliar o risco como uma função da *Loss Event Frequency* (LEF) e da *Probable Loss Magnitude* (PLM), com base em cenários delineados por ativo, ameaça e vulnerabilidade. O guia introdutório de Nair (2021) descreve os componentes e procedimentos operacionais do FAIR: identificar a comunidade de ativos e ameaças; estimar a *Threat Event Frequency* (TEF), a capacidade de ameaça e a força de controlo para determinar a vulnerabilidade; integrar a TEF e a vulnerabilidade para calcular a LEF e a PLM, facilitando o alinhamento de fatores de avaliação práticos com uma taxonomia coerente.

Além disto, Nair (2021) ilustra que os resultados podem ser representados qualitativamente numa matriz, melhorando assim a priorização e a comunicação com os decisores quando a quantificação financeira não é necessária, tornando-o num bom candidato para a realização deste trabalho.

O NIST SP 800-30 é um documento lançado pelo NIST, que serve como uma estrutura para avaliar as técnicas de gestão de risco (Putra Eryawan et al., 2021). Embora mais

complexo, pode ser considerado uma ferramenta de evolução para a ULS de Coimbra, à medida que se desenvolve uma maturidade organizacional em risco cibernético.

Este modelo distingue-se pela sua abordagem iterativa e adaptável, que promove uma avaliação contínua e quantitativa dos riscos, sustentada por métricas de desempenho e indicadores de ameaça. Além de quantificar a exposição e a probabilidade, o NIST SP 800-30 integra-se também com *frameworks* complementares, como o *Risk* IT da ISACA e o NIST CSF 2.0**,** reforçando a governança e o alinhamento estratégico das práticas de segurança com os objetivos institucionais (ISACA, 2017; Olaes, 2025).

5.2.2 Descrição dos modelos inadequados

O OWASP é particularmente relevante para o desenvolvimento de *software* e segurança de aplicações, algo que não constitui o principal objetivo do estágio.

A ULS de Coimbra dá prioridade à proteção de dados clínicos, à garantia de disponibilidade operacional e à adesão a regras de dados de saúde (por exemplo, o RGPD). O OWASP não engloba estes requisitos institucionais mais amplos, nem o modelo de matriz semi-quantitativa utilizado nesta investigação, tornando-se irrelevante para os SI como o Sonho V2, SClínico, ou para os processos intersistemas avaliados nesta investigação (Søhoel, 2018).

Embora o OCTAVE seja um modelo extenso, exige muitos recursos e pressupõe um grau de maturidade que pode não existir em todos os departamentos da ULS de Coimbra. Requer o envolvimento sincronizado de várias unidades e um tempo considerável para a sua execução e, tendo em conta a duração e a extensão limitadas do estágio realizado para este trabalho, seria excessivo e inviável (Suroso & Fakhrozi, 2018).

O CVSS é um instrumento técnico fundamental concebido para avaliar defeitos e vulnerabilidades de *software*, ignorando o contexto empresarial, os mandatos específicos dos cuidados de saúde e as *frameworks* de risco institucionais, como a ISO/IEC 27005:2022 ou a NIST SP 800-30. Não inclui dimensões estratégicas (por exemplo, conformidade legal, privacidade, procedimentos clínicos) essenciais para a gestão do risco hospitalar.

O estágio na ULS de Coimbra centra-se na avaliação do risco aplicacional nas organizações hospitalares, destacando a continuidade operacional, a segurança dos doentes e as implicações organizacionais. Este trabalho, utilizando uma matriz de risco baseada em Excel e uma avaliação semi-quantitativa, é mais congruente com as técnicas recomendadas pela ISO/IEC.

5.2.3 Seleção do modelo adotado para avaliação de risco

O uso de matrizes de risco baseadas em probabilidade e impacto é comum na literatura e na prática hospitalar, dado que são ferramentas visuais e analíticas que facilitam a identificação, categorização e priorização de riscos.

Segundo Lemmens et al. (2022), o uso da matriz de risco permite combinar de forma clara os níveis de probabilidade (de "raro" a "muito provável") e impacto (de "mínimo" a "catastrófico"), atribuindo um valor total ao risco com base na multiplicação entre estas variáveis, presente na Figura 7.

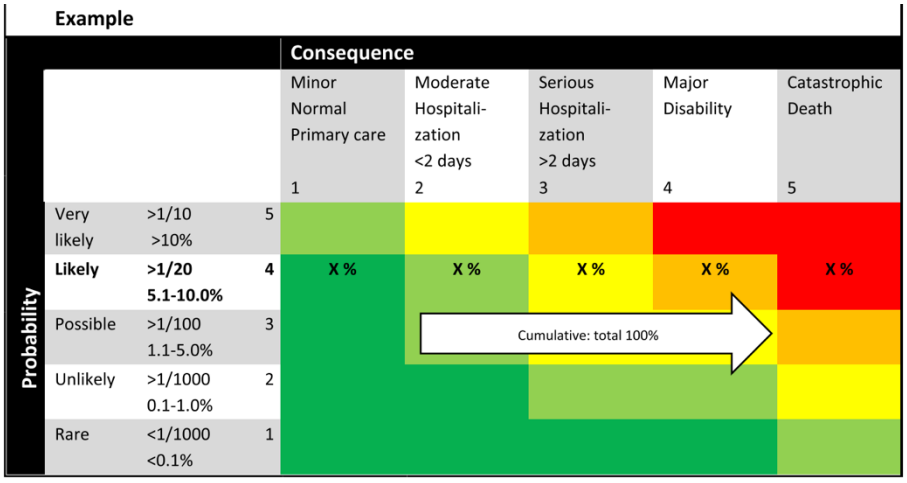


Fig. 1 Example of a risk matrix

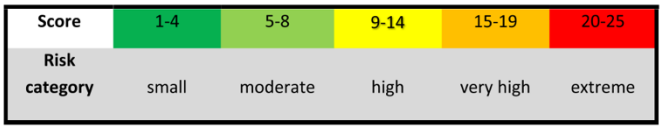


Fig. 2 Risk categories with corresponding scores and colors

Figura 7 – Exemplo 1 de Matriz de Risco 5x5
Fonte: (Lemmens et al., 2022)

A opção pela utilização de uma matriz de risco revelou-se a mais adequada ao contexto hospitalar da ULS de Coimbra. Este instrumento, recomendado pelas normas ISO 31000:2018 e ISO/IEC 27005:2022, permitiu uma avaliação visual e sistemática da vulnerabilidade e do impacto de cada risco, facilitando a priorização e a comunicação (ISO, 2018; ISO/IEC, 2022).

Em comparação com metodologias quantitativas, como o FAIR ou o NIST SP 800-30, que exigem dados numéricos extensos e uma maturidade organizacional mais elevada (Putra Eryawan et al., 2021; Stoneburner et al., 2002), a matriz semi-quantitativa 5x5 apresenta um equilíbrio entre rigor analítico e aplicabilidade prática. Esta abordagem é reconhecida na literatura como particularmente eficaz em contextos hospitalares complexos, onde coexistem múltiplos sistemas interdependentes e é necessário assegurar decisões rápidas e colaborativas sobre vulnerabilidades e impactos (Alarfaj & Rahman, 2024; Dumbravă & Iacob, 2013; Pascarella et al., 2021).

5.2.4 Planeamento do questionário

Foi planeada a elaboração de um questionário concebido especificamente para apoiar a avaliação e gestão de riscos associados aos SI utilizados na ULS de Coimbra. A utilização de um questionário, como instrumento central para avaliação de risco associado às aplicações críticas da ULS de Coimbra, justifica-se tanto por razões práticas, como teóricas.

Os SI hospitalares operam num contexto organizacional complexo, interdependente e altamente sensível à falha, sendo necessário compreender o risco, não apenas a partir de análises técnicas, mas também através da perceção dos seus utilizadores.

De acordo com Kubra Kaya et al. (2016), os profissionais de saúde nem sempre partilham uma compreensão uniforme do conceito de risco, o que influencia significativamente a forma como lidam com ameaças tecnológicas ou operacionais. O estudo revela que muitos profissionais associam "risco" a danos clínicos diretos, negligenciando, frequentemente, riscos organizacionais ou informáticos, o que sustenta a conveniência de um instrumento que promova a importância destes domínios.

Por sua vez, Sayyadi Tooranloo & Saghafi (2021) destacam a elevada taxa de insucesso na implementação de SI hospitalares e apontam como fatores críticos a ausência de compromisso dos utilizadores, a má adaptação à cultura organizacional e a falta de planeamento e manutenção.

Estes elementos são, em grande medida, identificados da melhor forma através da recolha de perceções diretas, nomeadamente por via de questionários estruturados, como o pretendido para este relatório. A avaliação de risco nos SI deve incluir componentes organizacionais e não apenas tecnológicas (Motevali Haghighi & Torabi, 2020).

Desta forma, planeou-se que o questionário demonstrasse uma abordagem participativa e distribuída, ao recolher várias perceções de diferentes serviços e perfis de utilizadores, algo fundamental numa organização da dimensão da ULS de Coimbra. Tal como refere o trabalho de Kubra Kaya et al. (2016), os profissionais tendem a valorizar mais os riscos que conhecem diretamente e a subestimar aqueles que não compreendem, o que justifica a necessidade de envolver estes profissionais em processos formais de avaliação.

Adicionalmente, a utilização de questionários permite recolher dados estruturados sobre dimensões subjetivas, mas fundamentais, como a perceção da disponibilidade e fiabilidade dos sistemas, o grau de confiança nos mecanismos de recuperação de dados, a sensibilidade dos dados tratados e a integração entre aplicações e o risco associado à fragmentação da informação (Pickering & Taylor, 2025).

O questionário desenvolvido está apresentado no Apêndice 1. Um questionário deste tipo permitiu fornecer uma visão multidimensional do risco, alinhada com a ISO/IEC 27005:2022 e a ISO 31000:2018, que defende a inclusão da perspetiva humana no processo de avaliação, bem como orientações específicas do setor da saúde, o que permitiu que o questionário abrangesse fatores críticos relevantes para o contexto hospitalar, desde técnicos a organizacionais (ISO, 2018; ISO/IEC, 2022).

Após a administração do questionário, planeou-se uma fase específica para a recolha de dados que permitisse caracterizar os riscos associados às aplicações críticas. Esta etapa tornou-se crucial para suportar os objetivos centrais do trabalho, ou seja, avaliar a

maturidade dos SI, identificar vulnerabilidades e propor medidas para reforço da resiliência e continuidade dos serviços.

Pretendeu-se avaliar, não apenas a importância clínica e operacional de cada aplicação, mas também a robustez dos mecanismos que garantem a sua continuidade**.** Os resultados esperados podiam ou não diferir da perceção inicial dos profissionais, sendo precisamente esta comparação uma das mais-valias desta análise.

Para este efeito, planeou-se a elaboração do questionário na plataforma *Google Forms*[4], tendo como objetivo classificar as aplicações críticas numa escala de 1 a 5, considerando duas grandes dimensões, respetivamente fatores de impacto e de vulnerabilidade.

Previa-se que as perceções recolhidas pudessem revelar fragilidades associadas, como a falta de atualizações, a inexistência de redundância, a fraca interoperabilidade e a indefinição de procedimentos de recuperação, uma vez que são especialmente importantes quando afetam aplicações críticas como registos clínicos, imagiologia ou prescrição eletrónica (Motevali Haghighi & Torabi, 2020). Esta combinação de indicadores foi criada de forma a permitir a recolha de dados objetivos e a perceção dos utilizadores relativamente às práticas de segurança e gestão de incidentes, utilizando uma abordagem semi-quantitativa com escalas de avaliação previamente definidas, facilitando assim uma análise integrada e a priorização dos riscos identificados.

Com base na gravidade do impacto e na vulnerabilidade percebida, provenientes dos resultados do questionário preenchido pelos respondentes, o plano seguinte foi o tratamento dos dados e a construção da matriz de risco 5x5, adaptada ao contexto da ULS de Coimbra, permitindo classificar as aplicações em função do seu nível de risco, identificar áreas críticas onde se verifica falta de manutenção, ausência de redundância ou integração deficiente e suportar recomendações práticas para a melhoria da segurança, integração e resiliência dos SI da ULS de Coimbra. Esta abordagem está em linha com os modelos propostos por Motevali Haghighi & Torabi (2020), ainda que adaptada à realidade nacional e à estrutura organizacional da ULS de Coimbra.

[4] https://docs.google.com/forms/u/0/

O próprio processo de resposta ao questionário funcionou como catalisador de sensibilização, promovendo entre os profissionais maior consciência sobre a dependência dos sistemas e a importância de garantir a sua continuidade e segurança. Esta perspetiva é também suportada por Kubra Kaya et al. (2016), que identificam a cultura organizacional como fator determinante para o sucesso da gestão de risco hospitalar.

Planeou-se, com base nos dados recolhidos, elaborar recomendações informadas no relatório de estágio, alinhadas com a realidade observada e com as prioridades identificadas pelos próprios utilizadores. Desta forma, as propostas de melhoria deixam de ser apenas teóricas e passam a estar sustentadas por evidência recolhida diretamente "no terreno".

Após a recolha das respostas do questionário distribuído aos especialistas da ULS de Coimbra, planeou-se iniciar o desenvolvimento da matriz de risco. As respostas permitiam avaliar e contestar os graus de suscetibilidade e impacto associados a cada aplicação, fornecendo uma base empírica para o desenvolvimento da matriz.

Esta metodologia integra a visão de especialistas com as estruturas propostas pela ISO 31000:2018 e ISO/IEC 27005:2022, proporcionando assim uma descrição precisa do risco operacional e clínico, baseada nas experiências de utilizadores e técnicos (Cagliano et al., 2011; Farokhzadian et al., 2015; ISO, 2018; ISO/IEC, 2022).

A incorporação dos resultados obtidos a partir do questionário foi reconhecida como um método eficaz para aumentar a confiabilidade da análise de risco e fortalecer o processo de tomada de decisão em ambientes hospitalares (Dumbravă & Iacob, 2013; Manser et al., 2016).

5.3 Execução da ação

Tendo em conta todos os fatores mencionados na etapa anterior, foi selecionada para este estudo, uma matriz de risco com avaliação semi-quantitativa que serve de intermediária entre as avaliações qualitativas textuais e as avaliações quantitativas numéricas, avaliando os perigos com base num sistema de pontuação específico, facilitando assim o processamento de informações quantitativas. Avaliando os méritos e os inconvenientes

das metodologias quantitativas e qualitativas, a integração destas duas abordagens pôde constituir uma solução no domínio dos cuidados de saúde (Pascarella et al., 2021).

O método semi-quantitativo reuniu as vantagens distintas de cada abordagem, diminuindo as suas desvantagens e elucidando a sua disseminação na organização de cuidados de saúde em questão, tal como recomendado pelas diretrizes governamentais e pelas melhores práticas não-governamentais, apesar da sua capacidade limitada de replicar com precisão as avaliações de risco apresentadas pelos modelos quantitativos (Pascarella et al., 2021).

Antes da elaboração do questionário e de modo a adquirir um conhecimento aprofundado do funcionamento, manutenção e integração dos SI hospitalares da ULS de Coimbra, foram realizadas várias entrevistas informais e discussões técnicas com os profissionais do Departamento de SI e representantes de empresas externas envolvidas na manutenção de aplicações essenciais.

Estas interações tiveram como objetivo proporcionar uma compreensão mais abrangente do contexto operacional dos sistemas, a identificação de vulnerabilidades e a caracterização dos processos de gestão de riscos e contingências tecnológicas. A Tabela 1 apresenta a lista dos entrevistados que auxiliaram de alguma forma na elaboração do estudo.

Cargo/Função	Área de atuação e aplicações associadas	Contributo principal para o estudo
Especialista de informática	Gestão e supervisão de sistemas clínicos (SER, PEM, Sonho V2, Clinidata XXI)	Forneceu uma visão global das aplicações críticas, estrutura de suporte e indicações para obtenção de outros contactos técnicos
Especialista de informática	Administração e integração de aplicações clínicas	Responsável pela extração dos dados e suporte técnico para levantamento e caracterização dos sistemas
Técnico da Glintt	Suporte e manutenção do SGCIM/SGICM-LF	Forneceu informação técnica sobre o SGICM, integrações e a versão instalada
Especialista de informática	Controlo físico e alojamento dos servidores	Esclareceu sobre a localização física dos servidores, controlo de acessos e redundâncias
Diretor do departamento de Sistemas de Informação	Diretor do departamento de Sistemas de Informação	Envolvido em todo o processo ao longo do relatório

Tabela 1 - Entrevistados para auxílio na elaboração do relatório

Este processo visou, não só identificar os níveis de risco, como também a percecionar as áreas que necessitavam de melhorias em termos de segurança e gestão de riscos, promovendo assim a recomendação de práticas que ajudassem na continuidade operacional e na proteção das informações sensíveis do hospital.

5.3.1 Administração do questionário

A administração do questionário foi, cuidadosamente planeada, para garantir a recolha de dados fiáveis e representativos das práticas e perceções dos utilizadores relativamente à gestão de riscos nos SI da ULS de Coimbra.

O questionário, apresentado em detalhe no Apêndice 1, foi feito a um conjunto selecionado de profissionais, incluindo responsáveis pelas áreas de SI, utilizadores finais, e gestores que desempenham funções relevantes na operação e segurança das aplicações hospitalares, angariando um total de 28 respostas. O início da sua aplicação foi o dia 30 de julho de 2025 e o fecho do mesmo ocorreu no final de agosto.

A partir dos resultados do questionário, elaborou-se a matriz de risco semi-quantitativa 5x5 para facilitar uma avaliação clara e sistemática dos níveis de risco, considerando as dimensões de impacto e vulnerabilidade. Esta preparação seguiu as normas internacionais, nomeadamente a ISO/IEC 27005:2022, a ISO 31000:2018 e o COBIT 2019 e o alinhamento com os objetivos estratégicos de continuidade e segurança da informação da ULS de Coimbra.

A escala utilizada nos fatores referentes à vulnerabilidade encontra-se na Tabela 2.

Valor	Descrição
1	Muito baixa
2	Baixa
3	Moderada
4	Alta
5	Muito alta

Tabela 2 - Escala de Vulnerabilidade

A escala utilizada nos fatores referentes ao impacto encontra-se na Tabela 3.

Valor	Descrição
1	Mínimo
2	Moderado
3	Significativo
4	Elevado
5	Catastrófico

Tabela 3 - Escala de Impacto

Os dados recolhidos foram, posteriormente, organizados e preparados para análise, garantindo a integridade das respostas que serviram de base para a avaliação quantitativa e qualitativa dos riscos e vulnerabilidades associados aos SI na ULS de Coimbra. Esta fase foi fundamental para assegurar que as conclusões do estudo refletiam a realidade operacional e as necessidades dos diferentes intervenientes.

Através dos campos mencionados na fase anterior e para realizar uma análise de risco adequada, foram consideradas tanto as variáveis de impacto, como as de vulnerabilidade, associadas a cada aplicação.

A lista apresentada quanto aos impactos, é a seguinte:

- Número de utilizadores
- Criticidade para os doentes
- Disponibilidade da aplicação
- Interoperabilidade
- Impacto reputacional

A lista apresentada quanto às vulnerabilidades, é a seguinte:

- Grau de atualização
- Nível de manutenção e assistência
- Proteção física e lógica do acesso
- Nível de redundância
- Sensibilidade e importância dos dados

5.3.2 Formulação para o cálculo do risco

A fórmula proposta para a avaliação do impacto da aplicação "a" é a seguinte:

$$Impacto_a = \sum_{i=1}^{I} \left(impacto_{i,a} \times peso_i \right)$$

Equação 3 - Fórmula para o impacto da aplicação "a"

A fórmula proposta para a avaliação da vulnerabilidade da aplicação "a" é a seguinte:

$$Vulnerabilidade_a = \sum_{v=1}^{V} \left(vulnerabilidade_{v,a} \times peso_v \right)$$

Equação 4 - Fórmula para a vulnerabilidade da aplicação "a"

A fórmula proposta para a avaliação do risco é a seguinte:

$$Risco_a = \frac{(Impacto_a \times Vulnerabilidade_a)}{5}$$

Equação 5 - Fórmula para o cálculo do risco da aplicação "a"

Onde:

a = aplicação

i = fator de impacto

I = 5 fatores de impacto

v = fator de vulnerabilidade

V = 5 fatores de vulnerabilidade

$impacto_{i,a}$ = valor do fator de impacto i relativo à aplicação a

$vulnerabilidade_{v,a}$ = valor do fator de vulnerabilidade v relativo à aplicação a

$peso_i$ = peso associado a cada fator de impacto

$peso_v$ = peso associado a cada fator de vulnerabilidade

A fórmula é suportada por diversos estudos e práticas consolidadas em gestão de risco, particularmente no contexto da saúde e dos SI. Esta abordagem parte do princípio de que o risco resulta da combinação entre a vulnerabilidade de cada aplicação e o seu impacto, sendo ponderados por fatores de peso que refletem a sua criticidade no contexto específico da ULS de Coimbra (A et al., 2019).

Por conseguinte, o impacto e a vulnerabilidade são considerados, não como quantidades singulares e definitivas, mas como agregados de vários aspetos. Os fatores de impacto indicam as potenciais repercussões de uma ocorrência e os de vulnerabilidade avaliam a extensão da exposição ao risco.

Para este estudo, cada fator foi avaliado com uma pontuação que varia de 1 a 5, em que 1 indica uma vulnerabilidade ou impacto negligenciável e 5 significa vulnerabilidade ou impacto extremamente elevado. No entanto, reconhecendo que nem todos os elementos

têm a mesma importância em contextos institucionais, esta metodologia, como mencionado anteriormente, permitiu a atribuição de pesos a cada um destes fatores.

Após a criação das fórmulas acima mencionadas, tornou-se essencial avaliar a importância relativa de cada elemento que contribui para o impacto e a vulnerabilidade.

Consequentemente, foram atribuídos pesos variáveis a cada componente para representar a avaliação dos profissionais quanto à sua importância no contexto dos sistemas de informação da ULS Coimbra.

Os pesos foram estabelecidos com base nas respostas do questionário institucional, presente no Apêndice 1, onde os participantes avaliaram cada aplicação a partir de dez fatores de risco, cinco relacionadas com o impacto e cinco com a vulnerabilidade.

Estes números, presentes na Tabela 4, apresentam a ponderação empírica de cada elemento, permitindo que os mais significativos, como a sensibilidade dos dados e a interoperabilidade, exerçam um impacto maior na avaliação final do risco. Esta ponderação não modifica as conclusões obtidas na matriz de risco, apenas fornece uma justificativa teórica e empírica para o modelo utilizado.

Dimensão	Fator	Peso relativo
Impacto	Número de utilizadores	0,214
	Disponibilidade da aplicação	0,189
	Impacto reputacional	0,181
	Criticidade para os doentes	0,199
	Sensibilidade e importância dos dados	0,218
Vulnerabilidade	Interoperabilidade	0,303
	Grau de atualização da aplicação	0,185
	Nível de manutenção e assistência	0,153
	Proteção de acesso (física e lógica)	0,188
	Nível de redundância	0,170

Tabela 4 - Peso dos fatores

Os pesos foram calculados a partir das médias das respostas do questionário aplicado aos profissionais da ULS Coimbra, posteriormente normalizados, ou seja, ajustados proporcionalmente de modo que a soma total dos pesos de cada dimensão correspondesse a 1, o que equivale a 100% da importância total atribuída aos fatores deste grupo.

A metodologia utilizada está em conformidade com as normas ISO 31000:2018 e ISO/IEC 27005:2022, que defendem métodos semi-quantitativos baseados em perspetivas institucionais e na importância prática dos fatores de risco.

Após a interpretação das respostas e dos gráficos do questionário, foi criada a matriz de risco 5x5, utilizando o modelo da Figura 8, com o objetivo de avaliar sistematicamente os níveis de risco das aplicações hospitalares em análise, integrando os resultados das dimensões de vulnerabilidade e impacto.

O primeiro passo foi o cálculo dos valores médios para cada variável, onde a pontuação média para cada fator (por exemplo, nível de manutenção e assistência) foi calculada a partir de todos os inquiridos, o que resultou num valor médio para cada fator de vulnerabilidade e de impacto por aplicação.

De seguida, as pontuações médias das variáveis de vulnerabilidade foram agregadas e posteriormente calculadas em média, resultando num índice de vulnerabilidade para cada aplicação, sendo a mesma técnica utilizada para os fatores de impacto, o que resultou num índice de impacto.

Finalmente, os índices conclusivos de vulnerabilidade e impacto foram representados numa matriz de risco 5x5, do género da que se apresenta na Figura 8, onde a convergência dos dois eixos estabeleceu o nível de risco abrangente de cada aplicação, categorizando-as como muito baixo, baixo, médio, alto ou crítico.

O risco global foi avaliado multiplicando estes resultados de ambos os fatores, que representam a correlação entre a gravidade do impacto e a vulnerabilidade das aplicações, e dividindo o nível de risco de cada aplicação por 5, de forma aos resultados se apresentarem numa escala idêntica à do impacto e da vulnerabilidade. Esta metodologia garante uniformidade e imparcialidade no estudo, convertendo as perceções das respostas dos especialistas em métricas quantificáveis e comparando-as com as melhores práticas globais para a gestão de riscos em SI hospitalares (Alam, 2016; Bianco et al., 2022; Dumbravă & Iacob, 2013).

PROBABILIDADE	IMPACTO				
	Mínimo	Moderado	Significativo	Elevado	Catastrófico
Muito baixa	MÉDIO	MÉDIO	ALTO	CRÍTICO	CRÍTICO
Baixa	BAIXO	MÉDIO	MÉDIO	ALTO	CRÍTICO
Moderada	BAIXO	MÉDIO	MÉDIO	MÉDIO	ALTO
Alta	MUITO BAIXO	BAIXO	MÉDIO	MÉDIO	MÉDIO
Muito alta	MUITO BAIXO	MUITO BAIXO	BAIXO	BAIXO	MÉDIO

Figura 8 - Modelo de Matriz de Risco

(Modelo baseado no de TemplateLab (2023))

A matriz resultante não só destacou as aplicações com maior risco operacional e clínico, como também forneceu uma representação visual que melhorou a comunicação com os restantes profissionais envolvidos, permitindo que as intervenções nos SI venham a ser priorizadas com base no seu impacto e na sua vulnerabilidade.

Esta abordagem está alinhada com o estudo de Kaya, Ward & Clarkson (2018), que reconhece as matrizes de risco como ferramentas bastante utilizadas em contexto hospitalar pela sua clareza visual e capacidade de suporte à decisão, embora com limitações quanto à precisão quantitativa. Também é sustentada pelo trabalho de Cohen et al. (2016), que prioriza modificações nos SI que apoiam diretamente a tomada de decisões clínicas, melhorando, desta forma, a segurança do paciente e os resultados dos cuidados de saúde.

5.4 Avaliação

O questionário recolheu 28 respostas de profissionais das diversas áreas de TI e SI da ULS de Coimbra. Foram avaliadas dez dimensões essenciais de risco nas aplicações clínicas e de apoio à prestação de cuidados, estruturando os resultados para a matriz de risco.

Os inquiridos incluíram membros do Departamento de TIC, do DTSI, do Departamento de Transformação e Inovação Digital (DTID), das equipas de assistência técnica (tanto hospitalares como de cuidados primários), bem como profissionais das unidades de infraestruturas e SI clínica. Esta seleção foi intencional, uma vez que estes profissionais são os principais utilizadores, gestores ou técnicos de suporte das aplicações críticas em avaliação e garantem uma visão abrangente e clara dos riscos.

Esta escolha metodológica é apoiada por vários autores que destacam a importância de adotar uma abordagem multidisciplinar na gestão de riscos hospitalares. Cagliano et al. (2011) argumentam que a avaliação de riscos na área da saúde deve integrar, não apenas as dimensões técnicas, como também as humanas e organizacionais, uma vez que as vulnerabilidades, geralmente, surgem na interseção destes domínios. Da mesma forma, Cohen et al. (2016) destacam que o envolvimento de especialistas técnicos e de pessoal clínico proporciona uma avaliação mais integral e fiável dos SI hospitalares.

Cada dimensão foi avaliada com base na escala de Likert de cinco pontos, com o significado de cada valor a diferir de acordo com o elemento a ser analisado (Jebb et al., 2021; Joshi et al., 2015).

Para a primeira questão (Figura 29, no Apêndice 1) que se tratava do número de utilizadores de cada aplicação, em que quanto maior o número, maior o impacto potencial em caso de falha, ou incidente de segurança, várias aplicações, incluindo a SClínico, PEM e RSE, possuem mais de 500 em simultâneo.

Devido a isto, atribuiu-se que uma pontuação de 1, indicava menos de 10 utilizadores, 2 representava entre 10 e 50 utilizadores, 3 entre 51 e 200 utilizadores, 4 entre 201 e 500 utilizadores e 5 referia-se a mais de 500 utilizadores regulares da aplicação. Devido ao seu grande volume de utilização, estas aplicações são especialmente sensíveis, uma vez que qualquer falha teria efeito rápido e de longo alcance em toda a empresa.

De acordo com a Figura 9, *softwares* mais especializados, como o Cardiobase ou o OphthalSuite, revelaram ter menos utilizadores, demonstrando o seu âmbito clínico restrito, o que se demonstra consistente com o estudo de Portela et al. (2023), que descobriram que as falhas nos SI hospitalares podem causar perturbações organizacionais significativas, especialmente com um número elevado de utilizadores (Heeks, 2006).

Por outro lado, observando a Figura 10, aplicações como a SClínico, PEM e RSE são proeminentes, cada uma abrangendo mais de 500 especialistas simultaneamente, onde o seu alcance transversal, tanto em hospitais como em cuidados primários, torna-as significativamente vulneráveis em caso de falha.

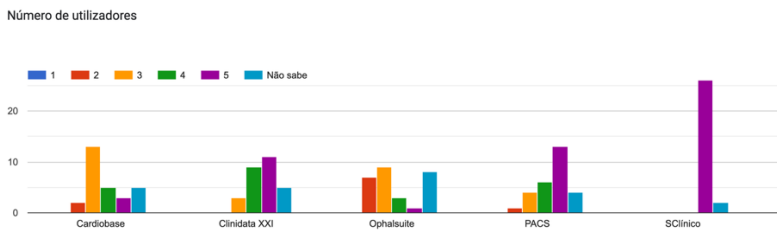


Figura 9 - Número de utilizadores das aplicações

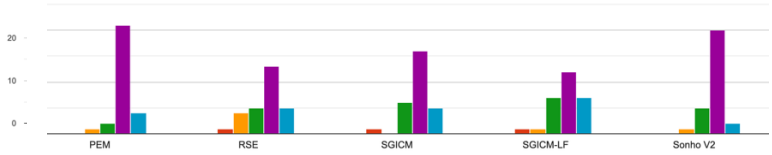


Figura 10 - Número de utilizadores das aplicações

Na disponibilidade da aplicação (Figura 30, no Apêndice 1), as aplicações críticas para as operações hospitalares necessitam de elevados níveis de disponibilidade, pois a sua falha pode comprometer processos essenciais.

De forma a avaliar este fator, uma classificação de 1 denotava baixa disponibilidade, caracterizada por falhas frequentes e tempo de inatividade prolongado, 2 disponibilidade moderada, marcada por interrupções mensais notáveis, 3 boa disponibilidade, com interrupções pouco frequentes e breves, 4 disponibilidade muito boa, em que as falhas eram incomuns e rapidamente resolvidas e 5 excelente disponibilidade, em que o sistema estava sempre operacional, com interrupções insignificantes.

A grande maioria dos participantes classificou a disponibilidade das aplicações como boa ou muito boa, o que significa que os sistemas estudados raramente ficam indisponíveis e as interrupções são breves e pouco frequentes.

Com base na Figura 11, a PACS e Cardiobase foram consideradas excecionalmente estáveis, apresentando baixo tempo de inatividade devido à sua infraestrutura resiliente, e a SClínico e a PEM demonstraram disponibilidade louvável, no entanto, a sua complexidade e integração extensa podem introduzir pontos fracos.

Em contrapartida, e apresentado na Figura 12, o Sonho V2 foi associado a uma estabilidade reduzida e a uma maior probabilidade de interrupção, indicando que nem todos os sistemas oferecem o mesmo nível de estabilidade operacional, de acordo com documentação técnica da ULS de Coimbra, sobre uma solução de contingência hospitalar.

Larsen et al. (2019) corroboram estas impressões, constatando que mesmo pequenas interrupções nos EHRs, podem causar atrasos na prestação de cuidados e diminuir a eficiência.

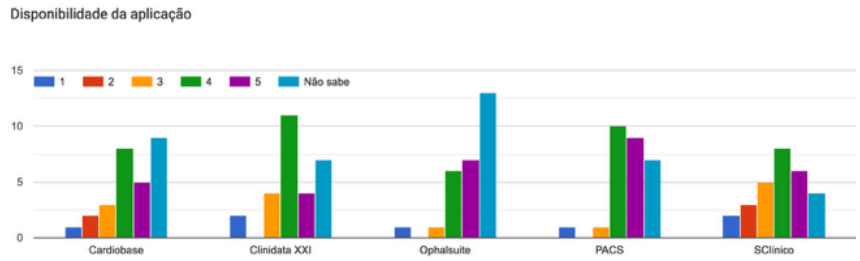


Figura 11 - Disponibilidade das aplicações

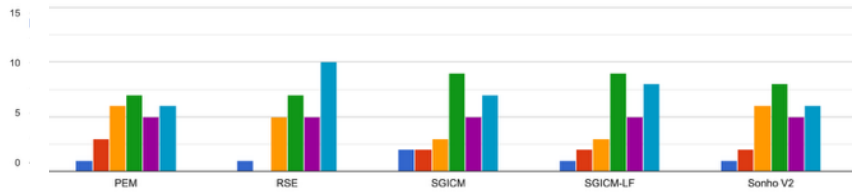


Figura 12 - Disponibilidade das aplicações

Em relação à questão do impacto reputacional (Figura 31, no Apêndice 1), onde a falha ou violação de segurança em sistemas pode causar danos significativos à imagem institucional, afetando a confiança dos utentes e *stakeholders*, uma pontuação de 1 significa que não há repercussões externas em caso de falha, 2 impacto interno sem visibilidade externa, 3 efeitos potenciais na confiança interna, 4 uma possível perda de confiança pública e 5 o cenário mais crítico, caracterizado por exposição negativa na média e danos à credibilidade institucional.

Os participantes afirmaram que falhas prolongadas em sistemas essenciais podem prejudicar, significativamente, a reputação da instituição, alterando, potencialmente, a confiança dos pacientes e resultando em cobertura negativa por parte da *media*.

Observando a Figura 13 e Figura 14, aplicações como a SClínico, PEM e Sonho V2 foram consideradas as mais cruciais, pois influenciam diretamente os EHRs, as práticas de

prescrição e o intercâmbio de informações entre instituições. Estes mecanismos são observados de forma proeminente, tanto por profissionais como por pacientes, indicando que falhas prolongadas podem resultar em repercussões significativas para a reputação. Sistemas especializados como OphthalSuite ou Cardiobase exerceriam um impacto reputacional mais restrito, principalmente nos seus respetivos departamentos.

Seh et al. (2020) salientam que violações de dados e falhas de sistema na área da saúde prejudicam a confiança do público e a credibilidade institucional.

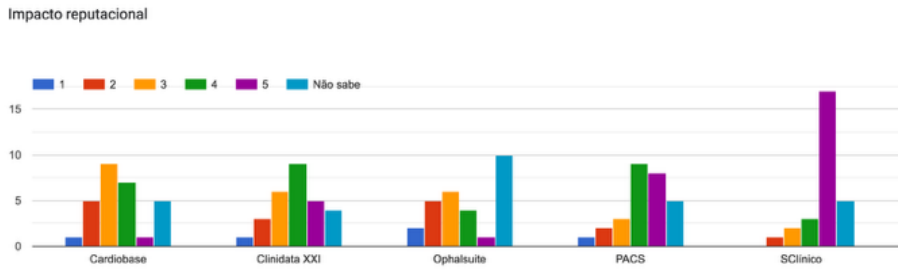


Figura 13 - Impacto Reputacional

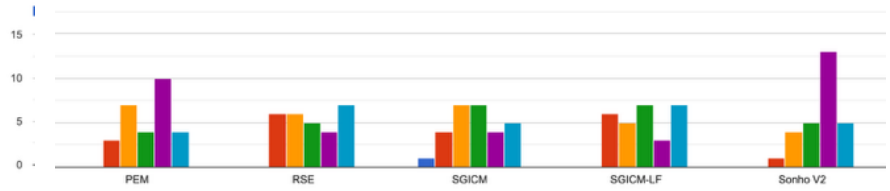


Figura 14 - Impacto Reputacional

Na criticidade para os doentes (Figura 32, no Apêndice 1), é avaliado o impacto direto da aplicação na prestação de cuidados aos utentes dado que, quanto mais crítica for a aplicação para o diagnóstico, terapêutica, monitorização ou emergência, maior a criticidade.

Visto isto, 1 significava nenhum impacto no atendimento ao paciente, 2 impacto mínimo com assistência para tarefas não essenciais, 3 importância moderada em procedimentos clínicos sem ser vital, 4 alta importância para atividades clínicas cruciais, como monitoramento e prescrição, e 5 uma função crítica, em que a falha comprometeria

diretamente a segurança do paciente em cenários de diagnóstico, ou tratamento de emergência.

Observando a Figura 15, foram selecionadas aplicações como SClínico, PEM e PACS, vitais para o tratamento clínico, dado o seu papel no apoio a diagnósticos, prescrições e imagens médicas. Uma avaria nestes sistemas resultaria, provavelmente, em repercussões imediatas para a segurança do paciente, incluindo atrasos no tratamento e possíveis erros na medicação.

Em contrapartida, na Figura 16, a SGICM-LF e a OphthalSuite foram consideradas moderadamente críticas, uma vez que apoiam, principalmente, contextos clínicos específicos.

Lyon et al. (2023) corroboram esta afirmação, demonstrando que as deficiências nos SI clínicos têm consequências diretas para a segurança do paciente e podem adiar ações críticas.

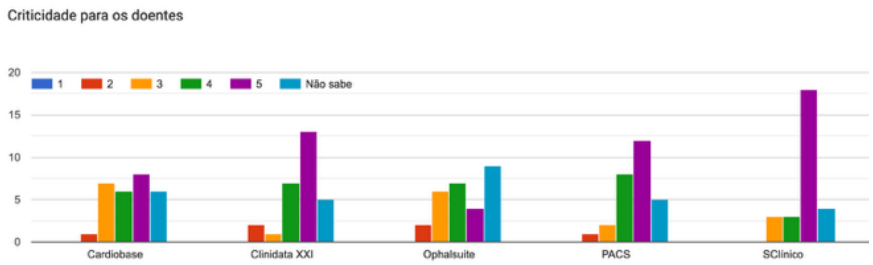


Figura 15 - Criticidade para os doentes

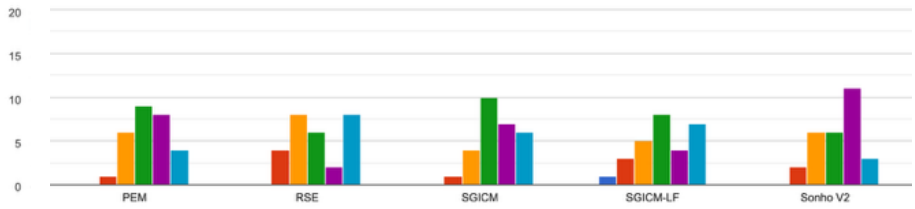


Figura 16 - Criticidade para os doentes

Na interoperabilidade (Figura 33, no Apêndice 1), quanto maior a dependência de integração com outros sistemas ou aplicações, maior o risco de vulnerabilidades externas, já que a exposição aumenta com as ligações a múltiplos sistemas

Este fator tornou-se um aspeto vital, em que 1 representa uma aplicação isolada sem integrações, 2 uma integração singular com um sistema, 3 uma integração moderada com dois ou três sistemas, 4 uma integração extensa com vários sistemas e 5 um nível crítico ou dependente de integração em tempo real com vários sistemas centrais.

Com base na Figura 17 e Figura 18, a SClínico, a RSE e a PACS apresentam o mais alto nível de interoperabilidade, permitindo a troca de dados em tempo real com outros sistemas, em que esta integração melhora os fluxos de trabalho da área da saúde e aumenta a eficiência embora, ao mesmo tempo, aumente o risco sistémico, pois o mau funcionamento de um sistema pode provocar falhas em outros.

Através da Figura 17, confirma-se que a Clinidata XXI e Cardiobase dependem de uma interoperabilidade elevada para facilitar a integração dos dados laboratoriais e cardiológicos nos registos dos pacientes. Em contrapartida, a OphthalSuite apresentou níveis de integração reduzidos, funcionando com maior autonomia em relação ao ecossistema hospitalar central, conforme documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a uma plataforma de integração de sistemas clínicos em utilização.

O trabalho de He et al. (2021) enfatiza isto, afirmando que, em ambientes de saúde altamente interoperáveis, as falhas técnicas ou de segurança tendem a disseminar-se mais rapidamente e exercer uma influência institucional mais significativa.

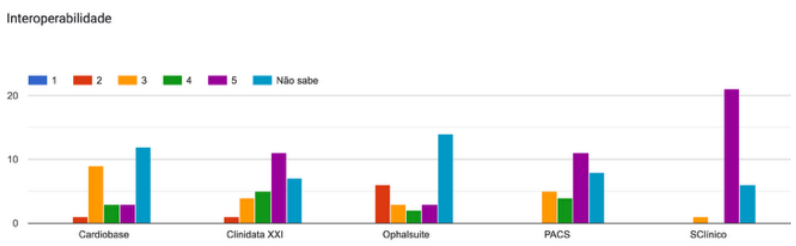


Figura 17 - Interoperabilidade

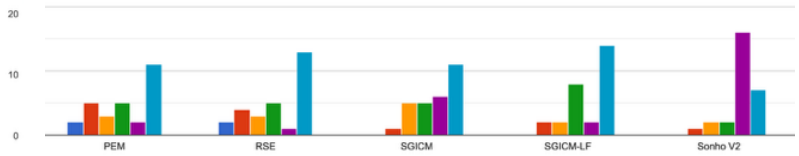


Figura 18 - Interoperabilidade

Relativamente ao grau de atualização da aplicação (Figura 34, no Apêndice 1), em que, quanto mais antiga a versão, maior a vulnerabilidade e, as aplicações desatualizadas, podem ter falhas de segurança que não foram corrigidas, uma pontuação de 1 significava atualizações muito recentes nos últimos doze meses, 2 atualizações recentes nos últimos um a dois anos, 3 frequência moderada de atualizações, com a última atualização entre dois e quatro anos, 4 sistemas antigos sem atualizações há mais de quatro anos e 5 sistemas obsoletos sem suporte do fornecedor e com vulnerabilidade elevada.

Com base na Figura 19, a frequência das atualizações foi considerada inconsistente: certos sistemas foram considerados atuais e frequentemente atualizados, como a Cardiobase e a PACS, enquanto outros, como a Clinidata XXI e o Sonho V2, foram caracterizados como obsoletos e, portanto, mais suscetíveis.

Esta questão está em conformidade com estudos que indicam que os sistemas obsoletos são uma fonte primária de vulnerabilidades na área da saúde, uma vez que a falta de atualizações frequentes aumenta a suscetibilidade a falhas técnicas e ataques à cibersegurança (He et al., 2021).

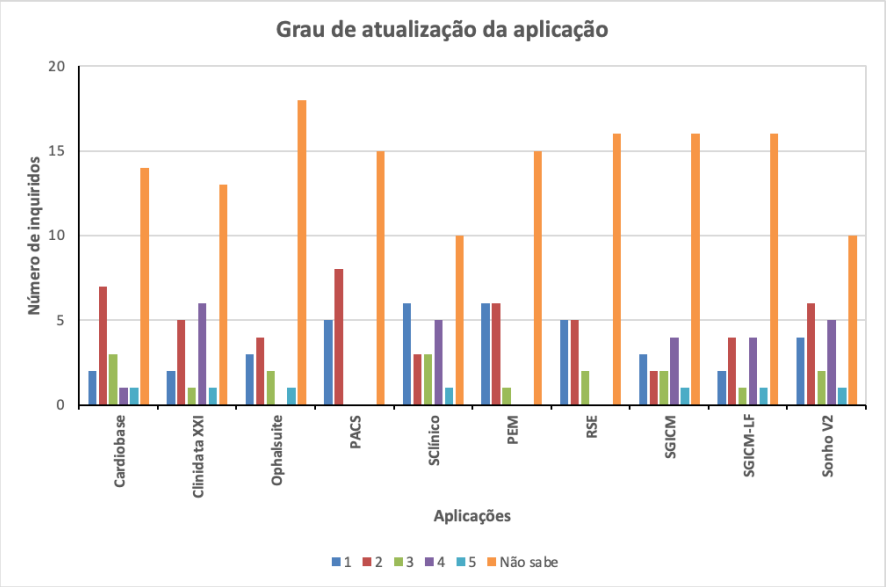


Figura 19 - Grau de atualização da aplicação

A nível de manutenção e assistência (Figura 35, no Apêndice 1) são avaliadas a qualidade e disponibilidade do suporte técnico e da manutenção da aplicação, em que 1 exemplificava suporte excecional, com um contrato de manutenção abrangente, cobertura 24 horas por dia, tempos de resposta garantidos e atualizações regulares, 2 suporte louvável durante o horário comercial, acompanhado de atualizações periódicas, 3 suporte satisfatório, mas limitado, com manutenção inconsistente, 4 suporte insuficiente caracterizado por tempos de resposta prolongados, e 5 a ausência de contratos de suporte ou manutenção.

Como é possível observar na Figura 20, embora várias aplicações como a PACS e SClínico, recebam assistência técnica abrangente 24 horas por dia, 7 dias por semana, devido à sua importância para o diagnóstico e o registo clínico, outras continuam a apresentar atrasos nos tempos de resposta e manutenção inconsistente.

Esta vulnerabilidade pode comprometer a resiliência organizacional durante crises, e Reeder et al. (2010) enfatizam a necessidade de manutenção contínua e planeamento de contingência para garantir a continuidade do serviço em ambientes clínicos.

Por outro lado, a Sonho V2 e PEM, por exemplo, apresentaram manutenção inferior ou irregular, resultando em maior suscetibilidade a ocorrências, em que esta disparidade

ilustra as apreensões institucionais em relação à gestão de riscos, nas quais os contratos de manutenção são claramente reconhecidos como um mecanismo de controlo crucial, com base na documentação internada disponibilizada, sobre um plano de prevenção de riscos de gestão na ULS de Coimbra.

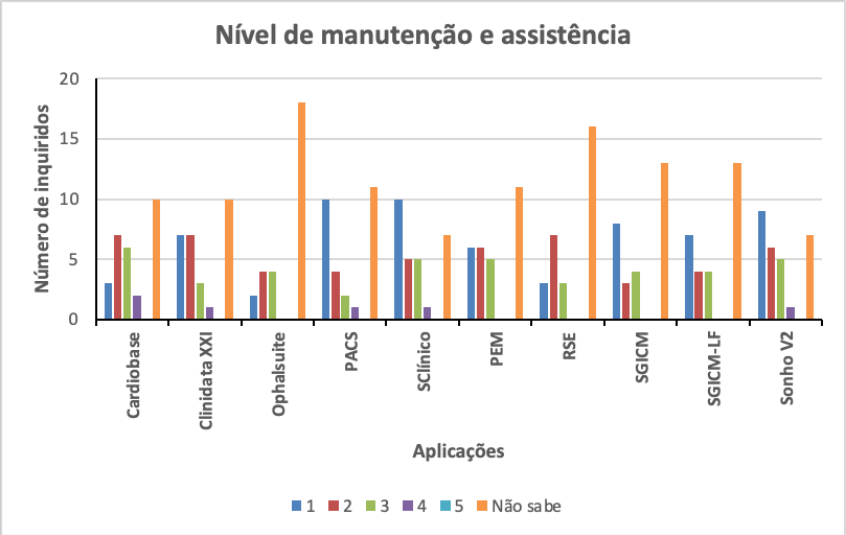


Figura 20 - Nível de manutenção e assistência

Para a proteção de acesso, abrangendo as dimensões física e lógica (Figura 36, no Apêndice 1), uma proteção fraca aumenta a probabilidade de acesso não autorizado aos dados ou SI. Ficou definido que 1 exemplificava segurança excecional com sistemas sofisticados de autenticação e monitorização, 2 níveis robustos de proteção física e lógica, 3 medidas suficientes, mas restritas, 4 proteção fraca com controlos fundamentais e 5 salvaguardas mínimas ou inadequadas.

De acordo com a Figura 21, este fator foi considerado suficiente, no entanto, muitos especialistas sublinharam a necessidade de implementar medidas mais sofisticadas, como a *Multifactor Authentication* (MFA). Os autores Suleski et al. (2023) ilustram que a MFA mitiga, substancialmente, o risco de tentativas de *phishing* e o acesso ilegal a sistemas críticos.

As respostas demonstraram que a SClínico e a PEM, por exemplo, precisam de métodos de segurança mais robustos, como a MFA, pois são usados com frequência e lidam com dados confidenciais. A maioria dos aplicativos tem proteção de acesso satisfatória, mas

plataformas transversais com milhares de utilizadores inevitavelmente, precisam de mais proteções. A Sonho V2 e a PACS são exemplos de sistemas com controlos de acesso rígidos.

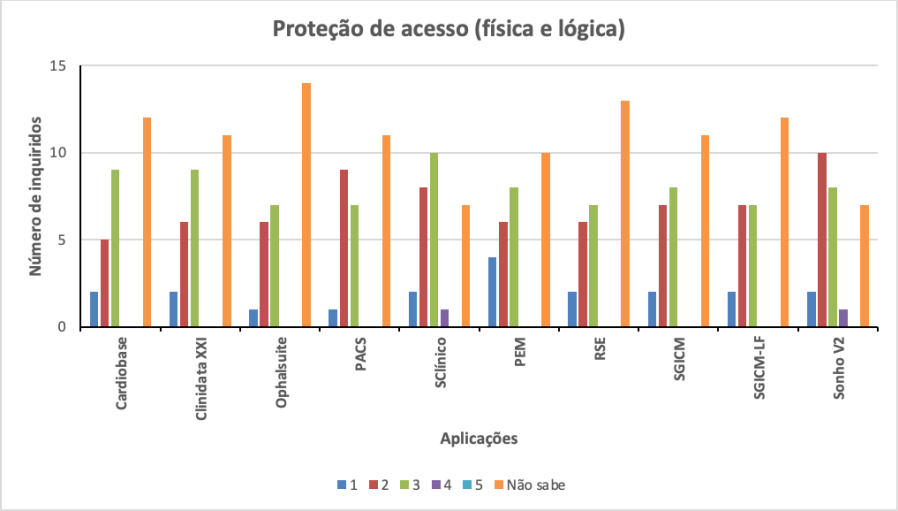


Figura 21 - Proteção de acesso (física e lógica)

Na sensibilidade e importância dos dados (Figura 37, no Apêndice 1), devido às aplicações que envolvem dados clínicos ou pessoais sensíveis terem um impacto muito maior em caso de violação ou perda, 1 indicava informações não confidenciais, 2 dados de baixa confidencialidade, 3 dados moderadamente confidenciais, 4 informações altamente confidenciais relativas a processos clínicos e 5 informações críticas e confidenciais de saúde, cuja divulgação resultaria em repercussões graves.

Os inquiridos classificaram, unanimemente, as informações geridas por estes programas como altamente sensíveis, abrangendo registos clínicos, diagnósticos e informações de identificação pessoal. Isto realça a necessidade de proteger a confidencialidade, integridade e disponibilidade, que são prioridades presentes na literatura encontrada.

Seh et al. (2020) demonstram que os dados de saúde são um dos setores mais sujeitos a ciberataques, com violações que podem resultar em repercussões significativas tanto para os pacientes, como para as instituições.

Através da Figura 22 e Figura 23, a RSE, SClínico, PEM e PACS foram reconhecidas como as melhores aplicações para gerir informações privadas e importantes, EHRs,

receitas médicas e imagens de diagnóstico. Esta classificação mostra a importância destes sistemas para guardar e enviar informações que identificam os pacientes.

Contudo, a Cardiobase e OphthalSuite são dois exemplos de sistemas ainda mais especializados que lidam com informações clínicas igualmente privadas, o que demonstra como as aplicações hospitalares são sensíveis em todos os aspetos, com base na documentação internada disponibilizada, sobre um plano de prevenção de riscos de gestão na ULS de Coimbra.

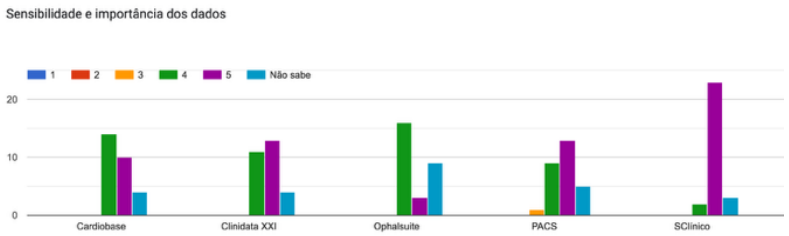


Figura 22 - Sensibilidade e importância dos dados

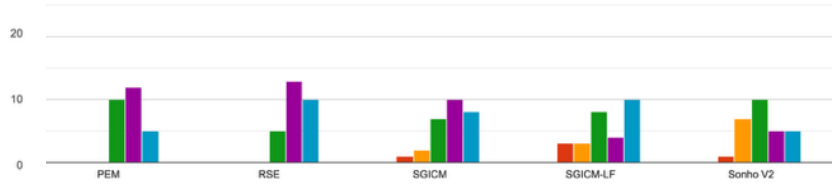


Figura 23 - Sensibilidade e importância dos dados

No âmbito da análise do nível de redundância (Figura 38, no Apêndice 1), em que a falta desta nos serviços aumenta o risco de falhas críticas, caso ocorra uma interrupção no serviço principal, 1 significava redundância abrangente e estratégias de *failover*, garantindo a continuidade do serviço em caso de falha do sistema, 2 redundância substancial com processos de *backup* fiáveis, 3 soluções de redundância parcial, 4 redundância mínima e pouco fiável e 5 ausência de mecanismos de redundância.

Esta questão obteve perceções variadas: certos sistemas possuíam fortes capacidades de redundância e *failover*, enquanto outros foram caracterizados como dependentes de soluções incompletas ou manuais, em que a falta de redundância contínua aumentava o

perigo de interrupções prolongadas. Kolowitz et al. (2012) afirmam que as soluções de redundância são essenciais para manter a continuidade do fluxo de trabalho em hospitais que dependem de SI.

Observando a Figura 24, aplicações como PACS e Cardiobase apresentam fortes recursos de redundância que são muito importantes em áreas de diagnóstico, cujo tempo de inatividade pode afetar gravemente os cuidados. Por outro lado, considerou-se que o SClínico dependia mais de soluções de redundância parcial ou manual, o que significaria interrupções mais longas no serviço se algo corresse mal.

Esta conclusão está em conformidade com a solução de contingência hospitalar apresentada numa documentação técnica da ULS de Coimbra, que relata como a redundância é essencial para sistemas antigos ou muito centralizados.

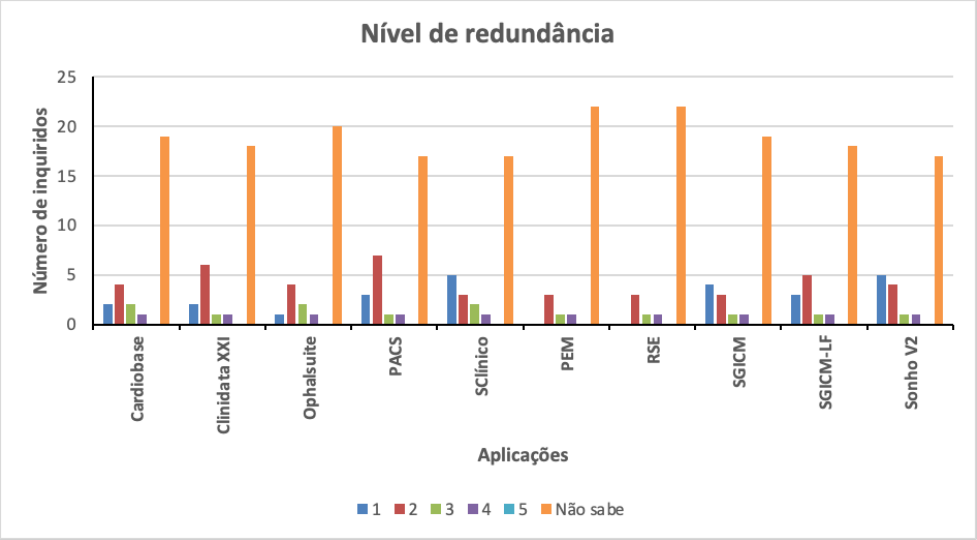


Figura 24 - Nível de redundância

A matriz de risco 5x5, baseada nos resultados anteriores, categoriza cada aplicação hospitalar com base em índices consolidados de vulnerabilidade e impacto. O eixo horizontal demonstra o impacto (mínimo 1 a crítico 5), enquanto o vertical indica a vulnerabilidade (muito baixa 1 a 5 crítico 5), assegurando coerência na representação gráfica. As cores variam de muito baixa (verde-claro) a crítica (vermelho).

Figura 25 - Matriz de risco com gráfico de dispersão

Inicialmente, a escala de vulnerabilidade no questionário estava alinhada inversamente com a escala de impacto, em que uma pontuação de 1 significava um nível muito alto de vulnerabilidade e 5 um nível muito baixo. De modo a manter a coerência entre os dois eixos, esta escala foi invertida, com 1 agora a indicar vulnerabilidade muito baixa e 5 muito alta.

O fator "sensibilidade e importância dos dados" foi a única exceção, uma vez que a escala original era a correta, ou seja, atribuía valores mais baixos a dados menos sensíveis e valores mais altos a informações críticas ou confidenciais logo, não necessitou de qualquer modificação.

Após isto, o valor médio de vulnerabilidade para cada aplicação foi calculado e combinado com a sua respetiva pontuação média de impacto. Os dados correspondentes foram subsequentemente apresentados num gráfico de dispersão, com o eixo horizontal a indicar o impacto e o eixo vertical a vulnerabilidade. A grelha de fundo da matriz de risco 5x5, representada na Figura 8, foi utilizada no gráfico para categorizar visualmente os níveis de risco em cinco classificações: muito baixo, baixo, médio, alto e crítico.

Esta representação gráfica facilita a compreensão da correlação entre o impacto e a vulnerabilidade de qualquer aplicação. As aplicações localizadas no quadrante inferior

esquerdo da matriz significam risco baixo, as da região central risco moderado e as próximas do quadrante superior direito, risco elevado ou crítico. Esta abordagem oferece uma representação clara da estrutura do SI da ULS de Coimbra, facilitando a priorização de métodos de mitigação, distribuição de recursos e tomada de decisões relativas a atualizações e manutenção do sistema.

Observa-se na Figura 25, na zona crítica (vermelho) não existe nenhuma aplicação presente, na alta (vermelho-claro) encontra-se a SClínico, Sonho V2, PACS e Clinidata XXI, na moderada (amarelo) está a RSE, PEM, Cardiobase, OphthalSuite, SGICM e SGICM-LF e na baixa (verde-claro) e muito baixa (verde) não se encontra nenhuma aplicação.

Isto vai de encontro com os resultados obtidos do nível de risco, presentes na Tabela 5.

Aplicações	Impacto	Vulnerabilidade	Risco
OphthalSuite	3,5	2,7	1,9
RSE	3,5	2,7	1,9
SGICM-LF	3,8	2,5	1,9
Cardiobase	3,5	2,8	2,0
PEM	3,9	2,6	2,0
PACS	4,2	2,4	2,0
SGICM	3,9	2,6	2,1
Sonho V2	4,3	2,5	2,1
Clinidata XXI	4,0	2,8	2,2
SClínico	4,3	2,7	2,4

Tabela 5 - Cálculo do risco

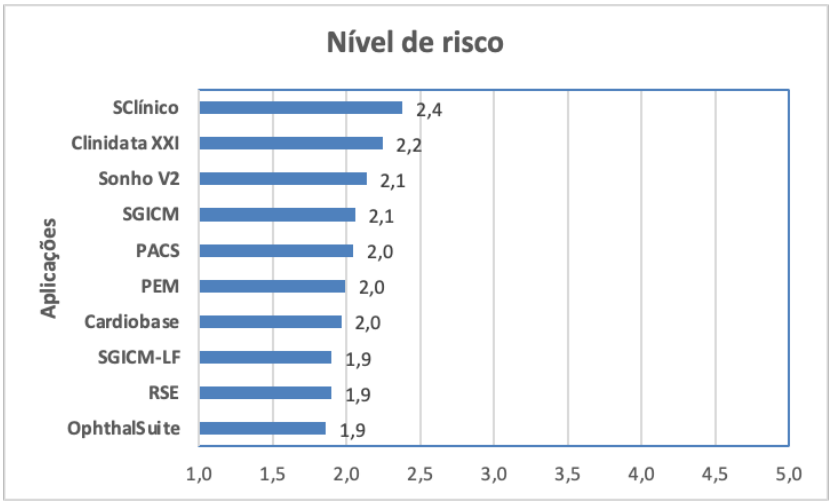


Figura 26 - Nível de risco

Os valores dos fatores (impacto entre 3,5 e 4,3 e vulnerabilidade entre 2,4 e 2,8) refletem riscos moderados a altos, que são resultados característicos de sistemas críticos no contexto hospitalar. De acordo com a ISO 31000:2018, o impacto traduz as consequências nos objetivos organizacionais, enquanto a ISO/IEC 27005:2022 define a vulnerabilidade como a suscetibilidade a falhas ou ameaças.

Como é possível observar na Figura 26, a aplicação com um maior nível de risco é a SClínico, que apresenta o valor de 2,4, exigindo medidas de mitigação prioritárias. Estes resultados confirmam a importância de uma monitorização contínua e da formulação de planos de contingência, em conformidade com estudos recentes sobre a gestão de risco em SI hospitalares (Alam, 2016; Bianco et al., 2022; Dumbravă & Iacob, 2013).

Isto deve-se ao facto de que, apesar das várias vantagens do uso de SI hospitalares e dos seus custos substanciais, estes podem apresentar falhas. Pesquisas recentes indicam que os SI hospitalares apresentam uma taxa de falha de aproximadamente 50 a 80% (Sayyadi Tooranloo & Saghafi, 2021) e, com base na investigação que Narayana Samy et al. (2010) fizeram, fatores como o erro humano, apresentam alta frequência de ocorrência, bem como falhas de energia, algo que requer resposta imediata de modo a evitar incidentes de segurança.

As instituições de saúde enfrentam vulnerabilidades relativas à segurança da informação, sendo suscetíveis a incidentes que comprometem conteúdos sensíveis, dada a relevância

crítica que estes possuem para o funcionamento dos serviços (Ayatollahi & Shagerdi, 2017).

A segurança das informações de saúde abrange três aspetos principais: proteger a confidencialidade, a integridade e a disponibilidade dos dados dos pacientes. Negligenciar qualquer um destes fatores pode resultar em várias complicações, incluindo prejuízos financeiros para hospitais e outras organizações de saúde (Ayatollahi & Shagerdi, 2017).

Apesar de, ao longo do tempo, existirem várias tentativas para se detetarem ameaças à segurança da informação, continuam a existir inúmeros riscos não identificados, principalmente a utilização ilegal de *software* e computadores para comunicação e atividades ilícitas (Ayatollahi & Shagerdi, 2017).

No trabalho de Ayatollahi & Shagerdi (2017), cujo objetivo foi avaliar os riscos que ameaçam a segurança da informação nos hospitais localizados numa das cidades do noroeste do Irão, foram analisados fatores de vulnerabilidade e impacto.

Nesse trabalho, em relação aos de vulnerabilidade, os resultados indicaram que muitas das causas fundamentais dos desastres naturais, como os incêndios, incluíam instalações elétricas desatualizadas, redes de transmissão de energia elétrica antiquadas e a ausência de sistemas de alarme de incêndio ou fumo (Ayatollahi & Shagerdi, 2017).

Relativamente ao risco humano, existiam plataformas de rede inadequadas, ausência de *firewalls*, proteções físicas, tecnológicas e administrativas insuficientes, entre outros. As ameaças físicas e ambientais podem decorrer de uma arquitetura de rede inadequada, negligência dos utilizadores e do pessoal informático ou alterações e reparações em edifícios, realizadas sem consulta ao departamento de TI (Ayatollahi & Shagerdi, 2017).

Ainda no trabalho de Ayatollahi & Shagerdi (2017), em relação ao impacto, e nos riscos humanos a eliminação de informações e vírus informáticos foram identificados como tendo a influência mais significativa na segurança da informação. Entre os riscos físicos e ambientais, a falta de conexão com a rede e fugas de fluídos em telhados ou tubos foram identificados como tendo o impacto mais significativo.

Ao implementar uma estratégia proativa para a gestão de riscos clínicos, as instituições de saúde podem estabelecer um ambiente mais seguro para pacientes, funcionários e todas as partes envolvidas relativamente aos cuidados de saúde, o que implica a realização de estudos abrangentes sobre potenciais riscos e vulnerabilidades (Longo et al., 2024).

Ao realizar esta análise, os profissionais de saúde podem executar intervenções direcionadas à gestão dos riscos, incluindo melhorias nos processos, iniciativas de formação e integração das melhores práticas, garantindo que os riscos potenciais sejam minimizados ou erradicados, antes que possam afetar negativamente a segurança do paciente, ou a qualidade do atendimento prestado. Uma estratégia proativa de gestão de riscos clínicos cultiva uma cultura de segurança e melhoria contínua, promove a comunicação transparente e evita possíveis acidentes (Longo et al., 2024).

A OphthalSuite é a aplicação que apresenta o nível mais baixo, o que pode indicar que segue uma monitorização com mais maturidade e controlada.

SI hospitalares bem estruturados trazem inúmeras vantagens para o contexto hospitalar, como uma maior precisão e organização na documentação de dados clínicos, acesso imediato a atualizações de registos em tempo real, recuperação remota de informações de pacientes, redução de erros médicos decorrentes de ilegibilidade e de imprecisões na introdução de pedidos e um maior apoio à tomada de decisões (Ngafeeson, 2014).

Ebnehoseini et al. (2019) indicam que, quando os utilizadores consideram o sistema intuitivo, fiável e congruente com as suas tarefas, a satisfação e a eficiência operacional melhoram significativamente. De acordo com a avaliação baseada no questionário realizado aos profissionais da ULS de Coimbra, a OphthalSuite demonstra suporte excecional ou louvável, níveis robustos de proteção física e lógica e um nível de redundância substancial com processos de *backup* fiáveis, minimizando assim os riscos.

A confiabilidade das informações documentadas e a estabilidade do sistema aumentam a confiança do utilizador e a continuidade das atividades terapêuticas, corroborando os indicadores de sucesso identificados por Ebnehoseini et al. (2017).

5.5 Especificação do conhecimento

A fase de especificação do conhecimento englobou a integração de dados empíricos com conhecimentos teóricos e práticos. O objetivo foi integrar a aprendizagem institucional e sugerir abordagens específicas para melhorar a resiliência, a governança e a segurança da informação em contextos de cuidados de saúde.

Os autores Alhawari et al. (2012) afirmam que uma abordagem orientada pelo conhecimento, permite que as organizações reconheçam e avaliem os riscos como fluxos de conhecimento entre sistemas e equipas.

Com base em documentação técnica interna disponibilizada pela ULS de Coimbra relativa a planos de contingência, que definem procedimentos operacionais em caso de falência dos SI, criar um repositório centralizado de conhecimento para dados de riscos e ocorrências seria uma iniciativa fundamental para a ULS de Coimbra, que permitiria consolidar dados de vários SI, combinando-os com relatórios regulares de incidentes produzidos. Esta plataforma facilitaria o estudo contínuo de vulnerabilidades recorrentes e serviria como base para modelos preditivos de risco operacional.

Durst & Zieba (2019) sublinham que o risco de conhecimento (a potencial perda ou uso indevido do conhecimento organizacional) pode comprometer a qualidade da tomada de decisões.

No âmbito da ULS de Coimbra, esta noção pode ser tratada através do estabelecimento de vias de comunicação oficiais entre o serviço de TI e os departamentos clínicos, visto que avaliações interdepartamentais sistemáticas de casos reais, juntamente com sessões de *feedback*, poderão melhorar a partilha interna de conhecimento sobre ameaças, vulnerabilidades e controlos, diminuindo assim a dependência da experiência individual.

Schmidt (2023) realça que a *Information Security Risk Management* (ISRM) deve ser considerada um processo sociotécnico, e não apenas um esforço técnico. A ULS de Coimbra pode estabelecer um programa de aprendizagem contínuo, focado em segurança da informação e governança de riscos para o pessoal de TI e usuários clínicos. O programa poderá incluir *briefings* frequentes sobre as normas ISO/IEC 27005:2022 e ISO

31000:2018, protocolos de resposta a incidentes e melhores práticas para a proteção de dados, em conformidade com o RGPD.

O trabalho de Taherdoost (2021) afirma que a ISRM é mais eficaz quando funciona como um processo cíclico, incluindo monitorização contínua e melhoria iterativa. Esta ideia pode auxiliar na criação de um ciclo regular de revisão de riscos na ULS de Coimbra, ao integrar avaliações quantitativas (tais como frequência de incidentes e tempo de inatividade) com qualitativas (contribuição dos utilizadores, importância do sistema e impacto percebido). Este método, alinhado com a ISO 31000:2018, permitirá aos decisores ajustar os limites de tolerância ao risco e rever as estratégias de mitigação com base no desempenho real.

Os hospitais enfrentam obstáculos significativos, quando os sistemas essenciais (clínicos, administrativos e de diagnóstico) funcionam de forma isolada (Cohen et al., 2016).

A implementação de um painel de integração na ULS de Coimbra, de acordo com o projeto presente na documentação técnica interna disponibilizada, relativa a uma plataforma de integração de sistemas clínicos em utilização, poderá facilitar a supervisão em tempo real da comunicação entre sistemas e o mapeamento de dependências. Isto permitirá a identificação imediata de falhas em cascata, que é um perigo destacado nos documentos de contingência da ULS de Coimbra e em normas internacionais como a ISO/IEC 27005:2022.

Além disto, a ULS de Coimbra poderá estabelecer um índice de risco baseado no conhecimento, consolidando dados de relatórios de incidentes, auditorias de sistemas e inquéritos aos utilizadores, tal como na realização do questionário presente no relatório. Este índice pode funcionar como um indicador da maturidade organizacional em matéria de segurança da informação e facilitar o planeamento estratégico de investimentos em infraestruturas, formação e contratos de manutenção.

Em resumo, esta investigação propõe várias ideias práticas para a ULS de Coimbra, entre elas, estabelecer repositórios de conhecimento que integrem dados de incidentes e riscos em todos os sistemas de saúde ou realizar ciclos iterativos de revisão de riscos, de acordo com as *frameworks* mencionadas ao longo deste relatório, de forma a facilitar a

adaptabilidade dinâmica. Outras ideias propostas consistem em melhorar a comunicação interdepartamental e criar comunidades de prática para a partilha de conhecimentos sobre riscos, desenvolver campanhas de formação e sensibilização específicas para profissionais de TI e outros departamentos, implementar painéis de integração e ferramentas de monitorização da interoperabilidade de modo a proporcionar visibilidade em todas as aplicações essenciais.

Ao implementar estas abordagens, a ULS de Coimbra pode fazer a transição de um modelo de gestão de riscos orientado para a conformidade, para um modelo centrado no conhecimento, melhorando a aprendizagem institucional e cultivando uma cultura de segurança proativa.

6 CONCLUSÃO

6.1 Contributos

O presente relatório de estágio proporcionou uma análise metódica da gestão de riscos em SI no ambiente hospitalar da ULS de Coimbra, com base em normas internacionais e diretivas nacionais para a cibersegurança e a continuidade operacional. A aplicação da metodologia de Investigação-Ação de Baskerville (1999) facilitou a criação de um ciclo que englobou o diagnóstico, o planeamento, a implementação, a avaliação e a especificação do conhecimento, envolvendo profissionais do DTSI.

Os resultados da investigação validaram a importância da gestão de riscos como uma ferramenta crucial para a segurança da informação, melhorar a eficiência dos processos e manter a continuidade e qualidade dos serviços de saúde. A aplicação prática de uma matriz de risco semi-quantitativa 5×5, com as dimensões de impacto e de vulnerabilidade, demonstrou a utilidade das abordagens teóricas apresentadas na revisão da literatura, validando a sua aplicabilidade no contexto hospitalar português.

Com base em documentação técnica interna disponibilizada pela ULS de Coimbra, relativa a uma plataforma de integração de sistemas clínicos em utilização, a análise revelou um nível significativo de interoperabilidade entre os sistemas, realçando a necessidade de uma vigilância contínua das vulnerabilidades.

O estudo, feito com recurso às *frameworks* ISO 31000:2018, ISO/IEC 27005:2022, COBIT 2019 e NIST CSF 2.0, ilustrou que a gestão de riscos deve ser um processo abrangente e consistente, incorporado à cultura organizacional e reforçado por políticas e planos de contingência (Steuperaert, 2019; Wu et al., 2024).

O plano de contingência da ULS de Coimbra presente na documentação técnica interna disponibilizada pela instituição, que define procedimentos operacionais em caso de falência dos SI, demonstrou a capacidade da instituição de manter a resiliência operacional e a continuidade clínica durante falhas do sistema. Estas ferramentas ilustram a sofisticação crescente da ULS de Coimbra na integração da governação, gestão de riscos e segurança da informação.

Os dados recolhidos a partir do questionário distribuído, indicaram que a perceção do utilizador é um fator crucial para compreender os elementos de vulnerabilidade e impacto relacionados com cada aplicação. Este método integrou a análise técnica com a experiência operacional, promovendo uma perspetiva abrangente e cooperativa sobre a segurança da informação, bem como um melhor entendimento acerca de quais aplicações necessitam de uma melhor manutenção.

6.2 Limitações

Uma das limitações durante o desenvolvimento deste trabalho, foi a escassez de tempo visto que, como o estágio ocorreu durante um período limitado, não foi possível avaliar um eventual impacto dos resultados das recomendações feitas à ULS de Coimbra, se estas forem aplicadas no futuro.

Apesar da amostra do questionário ter abrangido o DTSI e outros profissionais, não participaram inquiridos de outras áreas do hospital, o que pode limitar o contexto geral dos resultados, bem como o facto de o estudo ter sido realizado apenas na ULS de Coimbra que, apesar de ser uma instituição de saúde de grande dimensão, as conclusões podem não ser ajustadas a outras instituições. Para garantir uma melhor adequação do questionário e poder comparar a vulnerabilidade e os impactos das aplicações, recomenda-se a realização de pesquisas futuras com uma amostra maior e em outros contextos hospitalares.

Como alguns documentos técnicos fornecidos pela ULS de Coimbra são confidenciais, não puderam ser utilizados de forma integral, o que pode restringir a análise das aplicações. A área abrangida no relatório está em constante mudança e atualização, o que significa que novas alterações podem alterar o quadro de risco identificado.

6.3 Trabalhos futuros

Para investigações futuras, recomenda-se o reforço da monitorização contínua de riscos, empregando KPI, a realização de auditorias de segurança regulares, a atualização sistemática dos planos de contingência e o reforço da formação em cibersegurança para o pessoal de saúde, de acordo com, por exemplo, as diretrizes do CNCS (2025).

Como trabalho futuro, propõe-se ainda que seja desenvolvido um índice de risco baseado no conhecimento, para acompanhar a evolução da maturidade do risco e orientar as decisões de gestão, adotar uma ferramenta de avaliação de risco como parte integrante do processo de gestão de aplicações, criar *dashboards* dinâmicos para monitorização contínua dos riscos, integração com sistemas que detetem incidentes de segurança da informação (como proposto na iniciativa de um programa nacional, facultado para fins do estágio), definição de políticas de atualização e manutenção de *software* com base no nível de risco apurado.

De acordo com o supervisor deste estágio, neste momento, o estudo feito no âmbito deste estágio é "entendido como um trabalho académico e, certamente, que quando se puder abrir uma área de coordenação de Risco e Segurança, este será um excelente ponto de partida para a constituição de um Governança, Risco e Conformidade (GRC) (...) as matrizes e elementos produzidos poderão, eventualmente, ser tidos em consideração em análises futuras mas, atualmente, o departamento ainda está a ser constituído."

Em suma, a consolidação de uma cultura de gestão de riscos baseada no conhecimento e suportada por normas internacionais, revela-se um fator determinante para garantir a segurança dos pacientes, a eficiência organizacional e a sustentabilidade digital das organizações de saúde portuguesas.

REFERÊNCIAS BIBLIOGRÁFICAS

Acebes, F., González-Varona, J. M., López-Paredes, A., & Pajares, J. (2024). Beyond probability-impact matrices in project risk management: A quantitative methodology for risk prioritisation. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03180-5

Agrawal, V. (2017). A Framework for the Information Classification in ISO 27005 Standard. *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 264–269. https://doi.org/10.1109/CSCloud.2017.13

Ahmet, R., & Vladi, Dr. B. (2017). Risk Management in Public Sector: A Literature Review. *European Journal of Multidisciplinary Studies*, *2*(5), 323–329.

Alam, A. Y. (2016). Steps in the Process of Risk Management in Healthcare. *Journal of Epidemiology and Preventive Medicine*, *02*(02). https://doi.org/10.19104/jepm.2016.118

Alarfaj, K. A., & Rahman, M. M. H. (2024). The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix. In *Applied Sciences (Switzerland)* (Vol. 14, Issue 13). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app14135785

Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-Based Risk Management framework for Information Technology project. *International Journal of Information Management*, *32*(1), 50–65. https://doi.org/10.1016/j.ijinfomgt.2011.07.002

Al-Zuheri, A., Amer, Y., & Vlachos, I. (2019). Risk Assessment and Analysis of Healthcare System Using Probability-Impact Matrix. *Nursing & Primary Care*, *3*(5). https://doi.org/10.33425/2639-9474.1121

Antariksa, M. D. S., Angin, M. P., & Widodo, A. P. (2025). COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and

Benefits Across Various Industry Sectors. *Journal of Renewable Energy, Electrical, and Computer Engineering*, *5*(1), 99–105. https://doi.org/10.29103/jreece.v5i1.19501

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. In *BMC Medical Informatics and Decision Making* (Vol. 20, Issue 1). BioMed Central Ltd. https://doi.org/10.1186/s12911-020-01161-7

Arshed, N., & Danson, M. (2015). Research Methods for Business and Management. In K. O'Gorman & R. MacIntosh (Eds.), *Research Methods for Business and Management* (2nd ed.). Goodfellow Publishers Ltd.

Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. *The Open Medical Informatics Journal*, *11*(1), 37–43. https://doi.org/10.2174/1874431101711010037

Barati, S., & Mohammadi, S. (2008). Enhancing Risk Management with an Efficient Risk Identification Approach. *IEEE ICMIT*.

Baskerville, R. (1999). INVESTIGATING INFORMATION SYSTEMS WITH ACTION RESEARCH. *Communications of the Association for Information Systems*, *2*. https://doi.org/10.17705/1CAIS.00219

Bianco, L., Raffa, S., Fornelli, P., Mancini, R., Gabriele, A., Medici, F., Battista, C., Greco, S., Croce, G., Germani, A., Petrucci, S., Anibaldi, P., Bianco, V., Ronchetti, M., Banchieri, G., Napoli, C., & Piane, M. (2022). From Survey Results to a Decision-Making Matrix for Strategic Planning in Healthcare: The Case of Clinical Pathways. *International Journal of Environmental Research and Public Health*, *19*(13). https://doi.org/10.3390/ijerph19137806

BlueWorks. (2025). *OphthalSuite*. https://www.blueworks.pt/

Bonnie, E., & Leung, C. (2023, November 1). *The ISO 27005 Approach to Information Security Risk Management: 2022 Updates Explained*. Https://Secureframe.Com/Blog/Iso-27005.

Briner, M., Kessler, O., Pfeiffer, Y., Wehner, T., & Manser, T. (2010). Assessing hospitals' clinical risk management: Development of a monitoring instrument. *BMC Health Services Research*, *10*. https://doi.org/10.1186/1472-6963-10-337

Cagliano, A. C., Grimaldi, S., & Rafele, C. (2011). A systemic methodology for risk management in healthcare sector. *Safety Science*, *49*(5), 695–708. https://doi.org/10.1016/j.ssci.2011.01.006

Cardiobase. (2025). *Cardiobase - Cardiology Information System*. http://www.cardiobase.net

Cheng, P. H., Yang, C. H., Chen, H. S., Chen, S. J., & Lai, J. S. (2004). Application of HL7 in a Collaborative Healthcare Information System. *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, *2*, 3354–3357.

CNCS. (2025). *Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança*.

Cohen, J. F., Coleman, E., & Kangethe, M. J. (2016). An importance-performance analysis of hospital information system attributes: A nurses' perspective. *International Journal of Medical Informatics*, *86*, 82–90. https://doi.org/10.1016/j.ijmedinf.2015.10.010

Denney, A. S., & Tewksbury, R. (2013). How to Write a Literature Review. *Journal of Criminal Justice Education*, *24*(2), 218–234. https://doi.org/10.1080/10511253.2012.730617

Dhimas Azizah, N., Ramadani, U. R., & Andriawan, N. F. (2021). *Enhancing Software Quality Through the Integration of COBIT 2019 Framework : Compliance Requirements, A Study Case of Healthcare Applications*. https://doi.org/10.17509/SEICT

Dumbravă, V., & Iacob, V.-S. (2013). *Using Probability – Impact Matrix in Analysis and Risk Assessment Projects*. www.scientificpapers.org

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management. *Knowledge Management Research and Practice*, *17*(1), 1–13. https://doi.org/10.1080/14778238.2018.1538603

Ebnehoseini, Z., Tabesh, H., Deldar, K., Mostafavi, S. M., & Tara, M. (2019). Determining the hospital information system (HIS) success rate: Development of a new instrument and case study. *Open Access Macedonian Journal of Medical Sciences*, *7*(9), 1407–1414. https://doi.org/10.3889/oamjms.2019.294

Elmontsri, M. (2014). Review of the strengths and weaknesses of risk matrices. *Journal of Risk Analysis and Crisis Response*, *4*(1), 49–57. https://www.imperial.ac.uk

EVS. (2023, October 31). *EN, ISO, IEC standards – What is what?* Https://Www.Evs.Ee/En/Standard-What-Is-What.

Farokhzadian, J., Dehghan Nayeri, N., & Borhani, F. (2015). Assessment of Clinical Risk Management System in Hospitals: An Approach for Quality Improvement. *Global Journal of Health Science*, *7*(5), 294–303. https://doi.org/10.5539/gjhs.v7n5p294

Forêt, C. (2023, September 11). *Everything you need to know about ISO 27005: summary, requirements, pros and cons*. Https://Www.c-Risk.Com/Blog/Iso-27005.

Gebremedhin Kassa, S. (2017). IT Asset Valuation, Risk Assessment and Control Implementation Model. *ISACA Journal*, *3*, 1–9.

Hapon, A., Fedorchenko, V., Martovytskyi, V., Rykun, V., Sievierinov, O., & Oleshko, I. (2021). Measuring Vulnerabilities in Threat Modelling with Risk Matrix. *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, PIC S and T 2021 - Proceedings*, 617–619. https://doi.org/10.1109/PICST54195.2021.9772211

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. In *Journal of Medical*

Internet Research (Vol. 23, Issue 4). JMIR Publications Inc. https://doi.org/10.2196/21747

Heeks, R. (2006). Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics*, *75*(2), 125–137. https://doi.org/10.1016/j.ijmedinf.2005.07.024

ISO. (2018). *Risk management - Guidelines*.

ISO/IEC. (2022). *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*.

Jebb, A. T., Ng, V., & Tay, L. (2021). A Review of Key Likert Scale Development Advances: 1995–2019. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.637547

Jensen, R. C., Bird, R. L., & Nichols, B. W. (2022). Risk Assessment Matrices for Workplace Hazards: Design for Usability. *International Journal of Environmental Research and Public Health*, *19*(5). https://doi.org/10.3390/ijerph19052763

John Lynch & Associates. (2024, October 4). *Cybersecurity in Healthcare: NIST Framework 2.0*. Https://Johnlynchandassociates.Com/Navigating-Cybersecurity-in-Healthcare-with-Nists-Framework-2-0/.

Johnson, M. R. (2004). *HIPAA Risk Analysis* (1st ed.).

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, *7*(4), 396–403. https://doi.org/10.9734/bjast/2015/14975

Kaya, G. K., Ward, J., & Clarkson, J. (2019). A Review of Risk Matrices Used in Acute Hospitals in England. *Risk Analysis*, *39*(5), 1060–1070. https://doi.org/10.1111/risa.13221

Kolowitz, B. J., Lauro, G. R., Barkey, C., Black, H., Light, K., & Deible, C. (2012). Workflow continuity-moving beyond business continuity in a multisite 24-7 healthcare organization. *Journal of Digital Imaging*, *25*(6), 744–750. https://doi.org/10.1007/s10278-012-9504-4

Kubra Kaya, G., Ward, J., & Clarkson, J. (2016). *GJCIE 2016 Risk management in hospital settings: understanding and improving the current practice*.

Larsen, E., Hoffman, D., Rivera, C., Kleiner, B. M., Wernz, C., & Ratwani, R. M. (2019). Continuing Patient Care during Electronic Health Record Downtime. *Applied Clinical Informatics*, *10*(3), 495–504. https://doi.org/10.1055/s-0039-1692678

Lemmens, S. M. P., Lopes van Balen, V. A., Röselaers, Y. C. M., Scheepers, H. C. J., & Spaanderman, M. E. A. (2022). The risk matrix approach: a helpful tool weighing probability and impact when deciding on preventive and diagnostic interventions. *BMC Health Services Research*, *22*(1). https://doi.org/10.1186/s12913-022-07484-7

Longo, L., Tomarchio, O., & Trapani, N. (2024). A structured approach for enhancing clinical risk monitoring and workflow digitalization in healthcare. *Decision Analytics Journal*, *11*. https://doi.org/10.1016/j.dajour.2024.100462

Low, C., & Hsueh Chen, Y. (2012). Criteria for the evaluation of a cloud-based hospital information system outsourcing provider. *Journal of Medical Systems*, *36*(6), 3543–3553. https://doi.org/10.1007/s10916-012-9829-z

Lyon, R., Jones, A., Burke, R., & Baysari, M. T. (2023). What Goes Up, Must Come Down: A State-of-the-Art Electronic Health Record Downtime and Uptime Procedure in a Metropolitan Health Setting. *Applied Clinical Informatics*, *14*(3), 513–524. https://doi.org/10.1055/s-0043-1768995

Manser, T., Frings, J., Heuser, G., & Mc Dermott, F. (2016). The German clinical risk management survey for hospitals: Implementation levels and areas for improvement in 2015. *Zeitschrift Fur Evidenz, Fortbildung Und Qualitat Im Gesundheitswesen*, *114*, 28–38. https://doi.org/10.1016/j.zefq.2016.06.017

Maxdata Software, S. A. (2025). *Clinidata*. http://www.maxdata.pt/pt/home

MediaWiki. (2016). *Sistema de Gestão Integrado do Circuito do Medicamento*. https://aprendis.med.up.pt/index.php/Sistema_de_Gestão_Integrado_do_Circuito_do_Medicamento

Melo Gomes, E., & Macedo, M. (2024). *Registo de Saúde Eletrónico* (1st ed.). Instituto Português da Qualidade. https://www.ipq.pt/

Motevali Haghighi, S., & Torabi, S. A. (2020). Business continuity-inspired fuzzy risk assessment framework for hospital information systems. *Enterprise Information Systems*, *14*(7), 1027–1060. https://doi.org/10.1080/17517575.2019.1686657

Munnelly, J., & Clarke, S. (2009). HL7 Healthcare Information Management Using Aspect-Oriented Programming. *2009 22nd IEEE International Symposium on Computer-Based Medical Systems*, 1–4. https://doi.org/10.1109/CBMS.2009.5255349

Nair, A. (2021). *Introduction to Information Security Risk Assessment using FAIR (Factor Analysis of Information Risk)*. http://www.aujas.com

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. https://doi.org/10.1177/1460458210377468

Ngafeeson, M. N. (2014). Healthcare Information Systems Opportunities and Challenges. In *Encyclopedia of Information Science and Technology* (3rd ed., pp. 258–266). IGI Global. https://doi.org/10.4018/978-1-4666-5888-2.ch332

Pascarella, G., Rossi, M., Montella, E., Capasso, A., De Feo, G., Snr, G. B., Nardone, A., Montuori, P., Triassi, M., D'auria, S., & Morabito, A. (2021). Risk analysis in healthcare organizations: Methodological framework and critical variables. *Risk Management and Healthcare Policy*, *14*, 2897–2911. https://doi.org/10.2147/RMHP.S309098

Pickering, B., & Taylor, S. (2025). Individual perceptions of cybersecurity and risk management. *Open Research Europe*, *5*, 252. https://doi.org/10.12688/openreseurope.17332.1

Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study. *JMIR Formative Research*, *7*. https://doi.org/10.2196/41738

Presidência do Conselho de Ministros. (2023). *Decreto-Lei n.º 102/2023*. https://www.etf.gov.pt/uls-de-coimbra

Putra Eryawan, I. G. N. M., Arya Sasmita, G. M., Agung, A. A. K., & Wiranatha, C. (2021). Information Security Risk Strategy at PT. X Using NIST SP 800-30. *JURNAL ILMIAH MERPATI*, *9*(3).

Rampini, A. A., Sufi, A., & Viswanathan, S. (2014). Dynamic risk management. *Journal of Financial Economics*, *111*(2), 271–296. https://doi.org/10.1016/j.jfineco.2013.10.003

Reeder, B., Turner, A., & Demiris, G. (2010). *Use of Technology to Support Information Needs for Continuity of Operations Planning in Public Health: A Systematic Review*. https://doi.org/10.5210/ojphi.v2i1.2855

Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering and System Safety*, *59*, 49–62.

Sayyadi Tooranloo, H., & Saghafi, S. (2021). Assessing the risk of hospital information system implementation using IVIF FMEA approach. *International Journal of Healthcare Management*, *14*(3), 676–689. https://doi.org/10.1080/20479700.2019.1688504

Schmidt, M. (2023). Information security risk management terminology and key concepts. *Risk Management*, *25*(1), 1–23. https://doi.org/10.1057/s41283-022-00108-8

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. In *Healthcare (Switzerland)* (Vol. 8, Issue 2). MDPI AG. https://doi.org/10.3390/healthcare8020133

Singh, B., & Ghatala, M. H. (2012). Risk Management in Hospitals. *International Journal of Innovation, Management and Technology*, *3*.

Søhoel, H. M. (2018). *OWASP top ten - What is the state of practice among start-ups?* Norwegian University of Science and Technology.

SPMS. (2025a). *Clínico SClínico | Cuidados de Saúde Hospitalares (CSH)*. https://www.spms.min-saude.pt/2020/07/sclinico-hospitalar/

SPMS. (2025b). *PEM | Prescrição Eletrónica Médica*. https://www.spms.min-saude.pt/2020/07/pem/

SPMS. (2025c). *Registo de Saúde Eletrónico*. https://www.spms.min-saude.pt/2020/07/registo-de-saude-eletronico/

SPMS. (2025d). *Sobre a ULS Coimbra*. https://www.ulscoimbra.min-saude.pt/missao-e-valores/

SPMS. (2025e). *SONHO Hospitalar | Sistema Integrado de Informação Hospitalar*. https://www.spms.min-saude.pt/2019/01/product-sclinicohospitalar/

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

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. https://doi.org/10.6028/NIST.SP.800-30r1

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. In *Digital Health* (Vol. 9). SAGE Publications Inc. https://doi.org/10.1177/20552076231177144

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Computer Science*, *135*, 202–213. https://doi.org/10.1016/j.procs.2018.08.167

Sutejo, S., Prasetijo, A. B., & Agushyban, F. (2021). The Role of Information System for Risk Management in Hospital: A Narrative Review. *Jurnal Aisyah : Jurnal Ilmu Kesehatan*, *6*(3). https://doi.org/10.30604/jika.v6i3.1014

T, B., & Ganeshan, H. (2021). Supply chain risk identification and assessment by probability and impact matrix. *International Journal of Services and Operations Management*, *1*(1), 1. https://doi.org/10.1504/ijsom.2021.10043419

Taherdoost, H. (2021). A review on risk management in information systems: Risk policy, control and fraud detection. *Electronics (Switzerland)*, *10*(24). https://doi.org/10.3390/electronics10243065

TemplateLab. (2023). *42 Handy Risk Matrix Templates (Excel / Word)*. https://templatelab.com/risk-matrix/

Traoré, M., & Yamamoto, S. (2018). Healthcare CloudEcosystem Risk Analysis and Modeling: A FAIR Approach. *7th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 841–844. https://doi.org/10.1109/IIAI-AAI.2018.00171

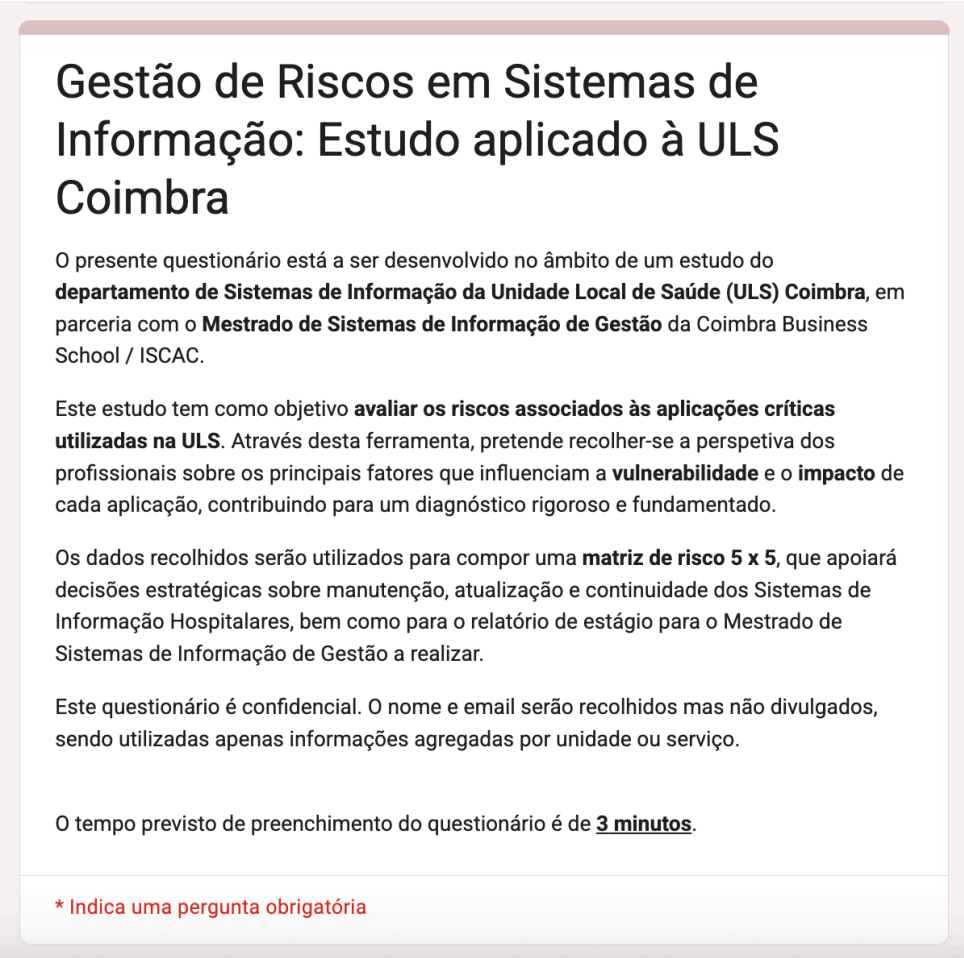
Tucker, D. (2022). *The Importance of a HIPAA Security Risk Analysis*. http://www.physicianleaders.org|800-562-8088

WeSecure. (2024, October 9). *Diferença entre a ISO 31000 e a ISO 27005: As Normas de Gestão de Risco*. https://blog.wesecure.pt/diferenca-iso-31000-iso-27005/

Wu, F.-T., Lee, W.-B., Cheng-Yuan Ku, C., Wu, Y.-S., & Shih, C.-Y. (2024). *Integrating ISO 27001, NIST CSF 2.0, and Cyber Defense Matrix for enhancing organizational cybersecurity governance*. https://ssrn.com/abstract=4991340

APÊNDICES

APÊNDICE 1. QUESTIONÁRIO COMPLETO.



Gestão de Riscos em Sistemas de Informação: Estudo aplicado à ULS Coimbra

O presente questionário está a ser desenvolvido no âmbito de um estudo do **departamento de Sistemas de Informação da Unidade Local de Saúde (ULS) Coimbra**, em parceria com o **Mestrado de Sistemas de Informação de Gestão** da Coimbra Business School / ISCAC.

Este estudo tem como objetivo **avaliar os riscos associados às aplicações críticas utilizadas na ULS**. Através desta ferramenta, pretende recolher-se a perspetiva dos profissionais sobre os principais fatores que influenciam a **vulnerabilidade** e o **impacto** de cada aplicação, contribuindo para um diagnóstico rigoroso e fundamentado.

Os dados recolhidos serão utilizados para compor uma **matriz de risco 5 x 5**, que apoiará decisões estratégicas sobre manutenção, atualização e continuidade dos Sistemas de Informação Hospitalares, bem como para o relatório de estágio para o Mestrado de Sistemas de Informação de Gestão a realizar.

Este questionário é confidencial. O nome e email serão recolhidos mas não divulgados, sendo utilizadas apenas informações agregadas por unidade ou serviço.

O tempo previsto de preenchimento do questionário é de **3 minutos**.

* Indica uma pergunta obrigatória

Figura 27 – Apresentação do Questionário Google Forms

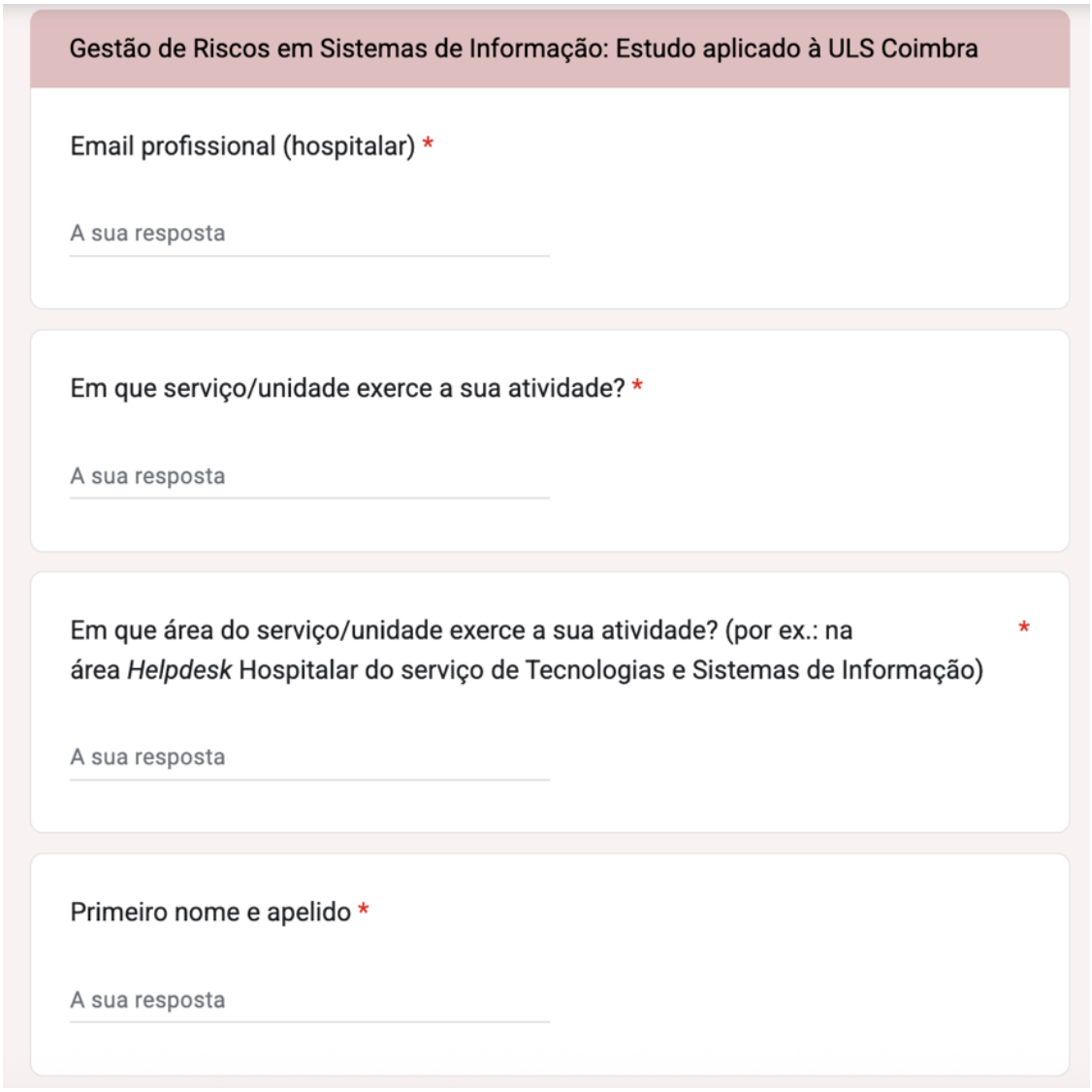


Figura 28 – Primeira parte do Questionário Google Forms

Número de utilizadores *

Este fator avalia quantos profissionais utilizam a aplicação regularmente. Aplicações com muitos utilizadores têm maior impacto organizacional em caso de falha e exigem maior robustez técnica e suporte.

Na sua perceção, quantos utilizadores utilizam esta aplicação regularmente no hospital (em simultâneo ou de forma distribuída)?

1. **< de 10 utilizadores**
2. **Entre 10 e 50 utilizadores**
3. **Entre 51 e 200 utilizadores**
4. **Entre 201 e 500 utilizadores**
5. **> de 500 utilizadores**

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 29 – Questão sobre o número de utilizadores

Disponibilidade da aplicação *

Este fator avalia o tempo em que a aplicação está disponível e funcional para os utilizadores, sem falhas ou interrupções. Uma baixa disponibilidade pode prejudicar o funcionamento dos serviços e o atendimento aos utentes.

Na sua perceção, como classifica a disponibilidade da aplicação ao longo do ano?

1. **Baixa** – Regista falhas frequentes e períodos prolongados de indisponibilidade.
2. **Moderada** – Funciona na maioria do tempo, mas com algumas interrupções mensais relevantes.
3. **Boa** – Raramente está indisponível; interrupções são pontuais e de curta duração.
4. **Muito boa** – Quase sempre disponível; falhas são raras e rapidamente resolvidas.
5. **Excelente** – Praticamente sempre disponível, sem falhas notórias ao longo do ano.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 30 – Questão sobre a disponibilidade da aplicação

Impacto reputacional *

Este fator avalia o impacto que a falha da aplicação pode ter na reputação do hospital. Quanto mais crítica a aplicação para o atendimento dos pacientes, maior o impacto em termos de imagem, confiança e credibilidade da instituição.

Na sua perceção, qual seria o impacto na reputação do hospital caso a aplicação falhasse por um período significativo (ex: horas ou dias)?

1. **Nenhum impacto externo**
2. **Impacto interno sem reflexo externo**
3. **Pode afetar a confiança interna**
4. **Pode causar perda de confiança pública**
5. **Pode levar a exposição mediática negativa e perda de credibilidade institucional**

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 31 – Questão sobre o impacto reputacional

Criticidade para os doentes

Este fator avalia o impacto direto da aplicação na prestação de cuidados aos utentes. Quanto mais crítica for a aplicação para o diagnóstico, terapêutica, monitorização ou emergência, maior a sua criticidade para os doentes.

Na sua perceção, qual é a criticidade da aplicação para a prestação direta de cuidados aos doentes?

1. **Nenhuma** – A aplicação não tem impacto na prestação de cuidados ao doente.
2. **Baixa** – A aplicação auxilia em tarefas não críticas, mas não afeta diretamente o cuidado ao doente.
3. **Moderada** – A aplicação está envolvida em tarefas clínicas, mas não essenciais, para a prestação de cuidados.
4. **Alta** – A aplicação é fundamental para tarefas clínicas importantes, como monitorização e prescrição, mas a falha não comprometeria a segurança imediata do doente.
5. **Crítica** – A aplicação é essencial para cuidados críticos, como diagnóstico ou tratamento de emergência, e a sua falha comprometeria diretamente a segurança do doente.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 32 – Questão sobre a criticidade para os doentes

Interoperabilidade *

Este fator avalia o grau de integração da aplicação com outros sistemas hospitalares. Quanto mais integrada for a aplicação, maior a sua dependência de outros sistemas e maior o risco de falhas em cadeia, caso algum sistema falhe.

Na sua perceção, qual é o grau de integração da aplicação com outros sistemas hospitalares?

1. **Isolada** – Não possui qualquer integração com outros sistemas.
2. **Pontual** – Integra-se apenas com 1 sistema, de forma simples e unidirecional.
3. **Moderada** – Integra-se com 2 a 3 sistemas.
4. **Alta** – Integra-se com vários sistemas.
5. **Crítica/Dependente** – Altamente integrada em tempo real com múltiplos sistemas nucleares (ex.: PACS), sendo afetada por ou afetando diretamente o funcionamento de outros.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 33 – Questão sobre a interoperabilidade

Grau de atualização da aplicação *

Este fator avalia a frequência e a regularidade das atualizações da aplicação. Aplicações desatualizadas podem estar sujeitas a falhas de segurança, incompatibilidades e perda de suporte técnico.

Na sua perceção, qual é o grau de atualização da aplicação?

1. **Obsoleta** – Sem suporte do fabricante, vulnerável, ou em fim de vida; risco elevado de falha ou ataque.
2. **Antiga** – Sem atualizações há mais de 4 anos; tem dependências críticas e vulnerabilidades conhecidas.
3. **Moderada** – Última atualização entre 2-4 anos; começa a apresentar limitações e riscos.
4. **Recente** – Atualizada nos últimos 1-2 anos; ainda compatível com requisitos técnicos e legais.
5. **Muito recente** – Aplicação atualizada nos últimos 12 meses; versão ativa é suportada e segura.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 34 – Questão sobre o grau de atualização da aplicação

Nível de manutenção e assistência *

Este fator avalia a qualidade e a disponibilidade do suporte técnico e da manutenção da aplicação. Sistemas com suporte inadequado ou sem manutenção regular estão mais suscetíveis a falhas operacionais e de segurança.

Na sua perceção, qual é o nível de manutenção e assistência disponível para esta aplicação?

1. **Inexistente** – Nenhum suporte técnico ou contrato de manutenção ativo. Não há garantias de correções ou atualizações.
2. **Fraco** – Suporte técnico limitado, com tempos de resposta elevados e manutenção esporádica.
3. **Adequado** – Suporte técnico básico com algumas limitações de horário ou tempo de resposta. Manutenção irregular.
4. **Bom** – Suporte técnico durante o horário útil, com atualizações periódicas e tempos de resposta razoáveis.
5. **Excelente** – Contrato de manutenção completo, com suporte 24/7, tempos de resposta garantidos e atualizações regulares.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 35 – Questão sobre o nível de manutenção e assistência

Proteção de acesso (física e lógica) *

Este fator avalia os mecanismos de controlo de acessos implementados na aplicação, tanto no nível lógico (autenticação, perfis de utilizador, segregação de funções) como físico (acesso ao servidor e infraestrutura).
A falta de proteção adequada aumenta o risco de acessos não autorizados, comprometendo a segurança dos dados e a continuidade operacional.
Na sua perceção, qual é o nível de proteção de acesso da aplicação?

1. **Inexistente ou negligenciada** – Sem controlo efetivo de acessos ou registos; qualquer utilizador pode aceder.
2. **Fraca** – Controlo de acessos básico e não padronizados, com logins limitados ou inexistentes e sem controlo físico dedicado.
3. **Moderada** – Acesso por senha com controlo parcial de perfis e funções, logins pouco sistemáticos com controlo físico básico.
4. **Robusta** – Perfis de utilizador definidos, autenticação por senha forte, logins ativos, controlo de acessos físicos básicos.
5. **Muito robusta** – Autenticação multifator, perfis bem definidos, logins auditáveis, segregação de funções, controlo físico e lógico com monitorização.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 36 – Questão sobre a proteção de acesso (física e lógica)

Sensibilidade e importância dos dados

Este fator avalia a criticidade dos dados processados pela aplicação. Aplicações que lidam com dados sensíveis, como informações pessoais de saúde ou diagnósticos, têm um risco mais elevado em caso de violação ou exposição desses dados.

Na sua perceção, qual é o nível de sensibilidade e importância dos dados processados pela aplicação?

1. **Dados não sensíveis** – Dados estatísticos ou agregados, sem impacto em caso de perda.
2. **Dados administrativos genéricos** – Gestão de recursos ou agendamentos, sem dados clínicos ou pessoais sensíveis.
3. **Dados parcialmente identificáveis** – Inclui dados de utentes (ex.: nome, contactos), mas não clínicos.
4. **Dados pessoais de saúde** – Contém dados clínicos, resultados de exames, histórico de saúde ou terapêutica.
5. **Dados críticos e sensíveis** – Dados de saúde altamente confidenciais (diagnósticos, psiquiatria, VIH, oncologia, etc.), combinados com identificadores pessoais.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 37 – Questão sobre a sensibilidade e importância dos dados

Nível de redundância

Este fator avalia a existência de mecanismos de continuidade operacional, como *backups*, servidores duplicados, ou *failover*. A ausência de redundância aumenta o risco de paragens prolongadas em caso de falhas nos sistemas.

Na sua perceção, qual é o nível de redundância implementado para a aplicação?

1. **Sem redundância** – Nenhum plano de continuidade documentado; falha implica paragem total e perda de dados possível.
2. **Limitada** – Apenas *backups* esporádicos ou sem testes de recuperação; sem duplicação do sistema.
3. **Parcial** – *Backups* periódicos e manuais; sem mecanismos de failover em tempo real.
4. **Elevada** – Servidores duplicados e *backups* regulares; *failover* manual previsto e testado.
5. **Total** – Sistema em alta disponibilidade com failover automático, *backups* frequentes e testados.

	1	2	3	4	5	Não sabe
Cardiobase	○	○	○	○	○	○
Clinidata XXI	○	○	○	○	○	○
Ophalsuite	○	○	○	○	○	○
PACS	○	○	○	○	○	○
SClínico	○	○	○	○	○	○
PEM	○	○	○	○	○	○
RSE	○	○	○	○	○	○
SGICM	○	○	○	○	○	○
SGICM-LF	○	○	○	○	○	○
Sonho V2	○	○	○	○	○	○

Figura 38 – Questão sobre o nível de redundância

APÊNDICE 2. PRINCIPAIS CARACTERÍSTICAS DAS APLICAÇÕES

Nome da aplicação	Descrição da aplicação	Fabricante	Interface	Integração real	Contrato de manutenção ativo	Interlocutor interno	Interlocutor externo	Interoperabilidade das bases de dados
CARDIOBASE	O CardioBase é um SI de Cardiologia desenvolvido para gerir o processo clínico dos pacientes desde a admissão até à alta no serviço de cardiologia. O sistema guarda os dados demográficos dos pacientes assim como os seus perfis de risco correspondentes.	InforTUCANO SI (PME)	HL7, MDM, QBP	Integra com SPMS (sumários clínicos, radiologia).	Sim	Pedro Soares	João Maltez	InforTUCANO SI (PME) - Compatível com bases de dados SQL *Server*, permitindo uma gestão fiável e estruturada dos dados clínicos e administrativos.
CLINIDATA XXI	Sistema inteligente de gestão global de laboratórios de análises clínicas e de diagnóstico, abrangendo aspetos técnicos e financeiro. Na ULS de Coimbra é amplamente utilizada nos serviços laboratoriais, incluindo o Serviço de Patologia Clínica e o Serviço de Hematologia Clínica.	Maxdata Software, S.A.	HL7, TCP/IP, File	Integra via HL7.	Sim	Joaquim Abreu	Dina Teresa	Maxdata Software, S.A. - Compatível com as principais bases de dados relacionais, incluindo soluções *open-source* como PostgreSQL e bases comerciais, promovendo flexibilidade e escalabilidade na implementação.
OPHTHALSUITE	A OphthalSuite centraliza dados de diversos dispositivos oftalmológicos numa única base de dados, independentemente do fabricante.	BlueWorks	HL7	Não identificado nas regras atuais do documento interno.	Sim	Pedro Soares	Paulo Barbeiro	BlueWorks - A OphalSuite é compatível com o HL7, um padrão de comunicação usado para o intercâmbio de informações clínicas e administrativas entre sistemas hospitalares.
PACS	Permite acesso remoto e rápido às imagens e aos relatórios associados, melhorando a eficiência clínica e a qualidade do atendimento.	SECTRA	HL7, DICOM	Integra com sistemas.	Sim	Pedro Soares	Carlos Cardoso	SECTRA - Utiliza o padrão HL7 (*Health Level Seven*) para a troca de dados clínicos, assegurando interoperabilidade com sistemas de informação hospitalar e soluções de imagiologia.
SCLÍNICO	O SClínico é um sistema de gestão do Processo Clínico Eletrónico (PCE), utilizado para registar, armazenar e consultar informações clínicas dos pacientes.	SPMS	HL7, Ensemble	Interoperável com sumários clínicos SPMS.	Sim	Margarida Marques	SPMS	SPMS - Integração via API FHIR (*Fast Healthcare Interoperability Resources*) e *web services*, assegurando conformidade com os *standards* internacionais de interoperabilidade em saúde digital.
PEM	Destinada à prescrição eletrónica de medicamentos e produtos de saúde.	SPMS	Web Services, HL7	Integrado com a plataforma SPMS (SCP - Prescrição). Presente no fluxo de sumários.	Sim	Margarida Marques	SPMS	SPMS - Ligação ao sistema regulatório Infarmed, permitindo a validação e integração de dados sobre medicamentos, dispositivos médicos e substâncias ativas.
RSE	Permite o registo e a partilha de dados clínicos entre utentes, profissionais de saúde e entidades prestadoras de serviços de saúde, assegurando a confidencialidade e a segurança da informação.	SPMS	Web Services, HL7	Presente no fluxo de sumários e pesquisas.	Sim	Margarida Marques	SPMS	SPMS - Disponibilização através de uma plataforma *web*, acessível a partir de navegadores modernos, promovendo a desmaterialização de processos e a acessibilidade multiplataforma.
SGICM	É um sistema informático desenvolvido para otimizar todas as atividades relacionadas com o circuito do medicamento nos hospitais.	GLINTT	HL7, TCP	Integra com sistemas de laboratório e hospitalares.	Sim	Joaquim Abreu	João Silva	GLINTT - Sistema interoperável, compatível com normas nacionais e internacionais, garantindo a integração de dados clínicos em diferentes pontos do circuito do medicamento e da gestão hospitalar.
SGICM-LF	Uma extensão do SGICM que abrange funcionalidades específicas de logística e farmácia.	GLINTT	HL7	Integra com vários.	Sim	Joaquim Abreu	João Silva	GLINTT - Plataforma interoperável com integração modular, adaptável a diferentes contextos hospitalares e serviços clínicos.
SONHO V2	Este sistema suporta serviços administrativos, como o controlo da produção, faturação e gestão de doentes, além de integrar informações clínicas essenciais para a prestação de cuidados de saúde.	SPMS	HL7, Web Services	Aparece como destino de múltiplas regras de encaminhamento.	Sim	Margarida Marques	SPMS	SPMS - Utiliza Oracle *Database* 11g R2 como motor de base de dados, assegurando desempenho, robustez e segurança no armazenamento de dados clínicos e administrativos.

Tabela 6 – Principais características das aplicações (parte 1)

Nome da aplicação	Número de utilizadores	Grupos profissionais	Data da última atualização	Localização dos servidores	Infraestruturas dos centros de dados	Proteção física e lógica do acesso	Quem pode extrair as informações?	Licenças de *software*
CARDIOBASE	350	Profissionais de cardiologia, incluindo médicos, enfermeiros e técnicos.	Compatível com Chrome, Firefox e Edge.	Localizado na Hyperv, na ULS de Coimbra.	Infraestrutura redundante	A aplicação é alojada em *data centers* internos da ULS de Coimbra com controlo de acesso físico, *backup* de energia (UPS) e redundância de sistemas para garantir alta disponibilidade. A proteção lógica inclui *Multifactor Authentication* (MFA), gestão de privilégios de utilizadores, criptografia de dados e monitorização contínua das atividades.	Administradores de sistema e responsáveis clínicos.	SQLSERVER
CLINIDATA XXI	750	Médicos, enfermeiros e técnicos, cada um com a sua credencial.	A versão mais recente é 100% web e compatível com os principais navegadores modernos, como Internet Explorer, Firefox, Chrome e Safari.	Servidores físicos, na ULS de Coimbra.	Infraestrutura redundante	Hospedado em *data centers* da ULS de Coimbra, com controlo físico de acessos e sistemas de *backup* de energia. A proteção lógica é garantida por autenticação forte, gestão de acessos e criptografia de dados para proteger as informações sensíveis, com auditorias regulares.	Administradores de sistema e responsáveis clínicos.	ORACLE
OPHTHALSUITE	350	Oftalmologistas, técnicos de diagnóstico, enfermeiros e outros membros da equipa de saúde oftalmológica.	Não disponível	Localizado na Hyperv, na ULS de Coimbra.	Infraestrutura redundante	A aplicação está protegida em *data centers* internos, com controlo físico de acessos e redundância de sistemas essenciais. A autenticação via *login* e senha e controlo de acessos, asseguram a proteção lógica, com criptografia de dados e monitorização de acessos.	Administradores de sistema e responsáveis clínicos.	SQLSERVER
PACS	750	Radiologistas, técnicos de radiologia, médicos de especialidades como oncologia, ortopedia, neurologia, entre outras.	Compatível com navegadores modernos, como Chrome, Edge ou Firefox.	*Data center* da ULS de Coimbra.	Infraestrutura redundante	O sistema de imagens médicas é hospedado em *data centers* especializados, com controlo de acesso físico e redundância de energia. A proteção lógica envolve criptografia das imagens DICOM, autenticação forte e controlo de acessos, além de auditoria contínua de acessos.	Administradores de sistema e responsáveis clínicos.	Licenciamento anual institucional
SCLÍNICO	1000+	Todos os clínicos podem aceder em contexto de doente, sem ser em contexto, só podem os médicos enfermeiros e psicólogos dados administrativos – preencher plataforma no RON (registo oncológico), 2 elementos de serviço gestão doentes/jurídico que precisam aceder aos processos para fins de resposta a tribunais.	Compatível com navegadores modernos.	Servidores físicos, na ULS de Coimbra.	Infraestrutura redundante	O sistema é alojado em *data centers* internos com controlo de acesso físico e *backup* de energia. A autenticação forte, gestão de privilégios e criptografia de dados asseguram a proteção dos dados clínicos, com monitorização contínua.	Administradores de sistema e responsáveis clínicos.	ORACLE
PEM	1000+ (≈1200)	Utilizada por médicos.	A PEM é uma plataforma realizada em ambiente *web*, compatível com os principais navegadores modernos.	Localizado externamente à ULS de Coimbra.	Infraestrutura redundante	A aplicação está protegida com controlo físico de acessos nos data centers da ULS de Coimbra, com sistemas de *backup* de energia. A proteção lógica é garantida por autenticação de utilizadores, gestão de privilégios e criptografia de dados.	Administradores de sistema e responsáveis clínicos.	Licenciamento anual institucional
RSE	1000+ (≈1200)	O RSE é utilizado por médicos e enfermeiros.	O RSE é uma plataforma web compatível com os principais navegadores modernos.	Localizado externamente à ULS de Coimbra.	Infraestrutura redundante	O sistema de registo está protegido em data centers com segurança física, com backup de energia e redundância. A autenticação multifatorial e controle de acessos asseguram a segurança, com criptografia e auditoria contínua.	Administradores de sistema e responsáveis clínicos.	Licenciamento anual institucional
SGICM	125	Os médicos o utilizam para prescrever, os enfermeiros para administrar medicamentos e os farmacêuticos para os dispensar.	Não disponível	Servidores físicos, na ULS de Coimbra.	Infraestrutura redundante	A aplicação está alojada em *data centers* internos, com controlo de acesso físico e redundância nos sistemas. A proteção lógica inclui autenticação forte, gestão de acessos e criptografia de dados, com monitorização constante.	Administradores de sistema e responsáveis clínicos.	ORACLE
SGICM-LF	125	Os enfermeiros o utilizam para pedir medicamentos, dispositivos médicos, pensos e outros materiais, e que os administrativos também o fazem.	Não disponível	Servidores físicos, na ULS de Coimbra.	Infraestrutura redundante	A aplicação é protegida com controlo de acesso físico no data center da ULS de Coimbra, e *backup* de energia. A autenticação forte e gestão de privilégios junto com criptografia de dados garantem a segurança, com monitorização de atividades.	Administradores de sistema e responsáveis clínicos.	ORACLE
SONHO V2	1000+ (≈1200)	Utilizado por administrativos.	Não disponível	Servidores físicos, na ULS de Coimbra.	Infraestrutura redundante	Hospedado em *data centers* internos com segurança física e vigilância, além de redundância de sistemas. A proteção lógica é garantida por autenticação de utilizadores, gestão de privilégios e criptografia de dados.	Administradores de sistema e responsáveis clínicos.	ORACLE

Tabela 7 - Principais características das aplicações (parte 2)