POLITÉCNICO DE LEIRIA

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Healthcare Data Watchdog - Ferramenta de monitorização de acessos a dados pessoais sensíveis em prestadores de MCDT com Imagiologia Médica

Mestrado em Cibersegurança e Informática Forense

Rui Lourenço de Campos Simões Pereira

Leiria, abril de 2026

POLITÉCNICO DE LEIRIA

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Healthcare Data Watchdog - Ferramenta de monitorização de acessos a dados pessoais sensíveis em prestadores de MCDT com Imagiologia Médica

Mestrado em Cibersegurança e Informática Forense

Rui Lourenço de Campos Simões Pereira

Projeto realizado sob orientação da Professora Doutora Maria Micaela Gonçalves Pinto Dinis Esteves (micaela.dinis@ipleiria.pt) e coorientação da Professora Doutora Ângela Margarida de Sousa Pereira (angela.pereira@ipleiria.pt) e Professora Doutora Eugénia Moreira Bernardino (eugenia.bernardino@ipleiria.pt).

Leiria, abril de 2026

ORIGINALIDADE E DIREITOS DE AUTOR

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionado o Autor e feita referência ao ciclo de estudos no âmbito do qual o mesmo foi realizado, a saber, Curso de Mestrado em Cibersegurança e Informática Forense, no ano letivo 2025/2026, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

AGRADECIMENTOS

Este trabalho não representa apenas uma etapa académica, mas uma caminhada de crescimento pessoal e profissional, que não teria sido possível concluir com sucesso sem o apoio de diversas pessoas.

À professora Micaela Esteves, à professora Ângela Pereira e à professora Eugénia Bernardino, pela orientação, coorientação, disponibilidade e ensinamentos ao longo de todo este processo, que foram fundamentais para a concretização deste trabalho.

À minha família, em especial à minha filha Ariana, por todo o apoio, paciência e compreensão ao longo deste período, sem os quais a realização deste trabalho não seria possível.

Aos colegas de Mestrado, pela troca de conhecimentos, pelo apoio mútuo e pelos momentos partilhados ao longo deste percurso académico.

A todos os que, direta ou indiretamente, fizeram parte desta jornada e contribuíram para a concretização deste projeto, fica o meu reconhecimento e gratidão.

RESUMO

Este trabalho estuda o contexto da cibersegurança nas organizações de saúde e apresenta a prova de conceito de um *software*, denominado *HealthCare Data Watchdog*, para a monitorização do acesso a dados pessoais sensíveis, incluindo relatórios de diagnóstico e imagem médica. O projeto dirige-se a entidades prestadoras de Meios Complementares de Diagnóstico e Terapêutica (MCDT) de pequena dimensão não abrangidas pela Diretiva de Segurança das Redes e da Informação 2 (Diretiva SRI2), que, tipicamente, não dispõem de soluções comerciais nem de equipas especializadas em cibersegurança.

A solução proposta visa capacitar utilizadores com conhecimentos limitados em cibersegurança, permitindo a deteção eficiente de acessos não autorizados a informação sensível. Ao facilitar a identificação precoce de incidentes de cibersegurança, a ferramenta contribui para a adoção atempada de medidas preventivas e corretivas, promovendo simultaneamente a conformidade com os requisitos legais de proteção de dados pessoais e de segurança da informação.

O trabalho inclui uma revisão das principais normas, regulamentos e boas práticas de cibersegurança, bem como das tecnologias, ferramentas e protocolos relevantes para o setor da saúde, com ênfase na utilização de soluções *open-source* para garantir a confidencialidade, integridade e disponibilidade dos dados.

A abordagem adotada compreendeu o desenho de uma arquitetura modular, capaz de recolher e centralizar dados de monitorização provenientes de sistemas heterogéneos, e o desenvolvimento de uma prova de conceito que integra e apresenta, de forma unificada, os controlos de segurança necessários. A simulação realizada evidenciou a viabilidade da solução, destacando os mecanismos de recolha, correlação e visualização da informação para apoio à decisão.

Palavras-chave: Cibersegurança em Saúde, Monitorização de Acessos, Dados Pessoais Sensíveis, Open-source, MCDT, NIS2, *HealthCare Data Watchdog*.

ABSTRACT

This work examines the cybersecurity context in healthcare organizations and presents a proof of concept of a *software*, named “HealthCare Data Watchdog”, designed to monitor access to sensitive personal data, including diagnostic reports and medical imaging. The project targets small-scale providers of Complementary Diagnostic and Therapeutic Services (MCDT) that are not covered by the Network and Information Security 2 Directive (NIS2 Directive), and which typically lack both commercial solutions and specialized cybersecurity teams.

The proposed solution aims to empower users with limited cybersecurity knowledge, enabling the efficient detection of unauthorized access to sensitive information. By facilitating the early identification of cybersecurity incidents, the tool supports the timely adoption of preventive and corrective measures, while simultaneously promoting compliance with the legal requirements for personal data protection and information security. The work includes a review of key cybersecurity standards, regulations, and best practices, as well as relevant technologies, tools, and protocols within the healthcare sector, with a focus on open-source solutions to ensure the confidentiality, integrity, and availability of medical data.

The adopted approach involved designing a modular architecture capable of collecting and centralizing monitoring data from heterogeneous systems, alongside the development of a proof of concept that integrates and presents the required security controls in a unified manner. The conducted simulation demonstrated the feasibility of the solution, highlighting the mechanisms for data collection, correlation, and visualization to support decision-making.

Keywords: Healthcare Cybersecurity, Access Monitoring, Sensitive Personal Data, Open-source, MCDT, NIS2, HealthCare Data Watchdog.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

ABAC	*Attribute-Based Access Control*
ACK	*Acknowledgement*
ACSS	Administração Central do Sistema de Saúde
API	*Application Programming Interface*
ARS	Administração Regional de Saúde
ASCII	*American Standard Code for Information Interchange*
B2B	*Business-to-Business*
BDNR	Base de Dados Nacional de Requisições
bit	Dígito binário
Byte	Unidade de informação digital composta por oito bits
CDA	*Clinical Document Architecture*
CDN	*Content Delivery Network*
CIA	*Confidentiality, Integrity and Availability*
CIS	*Center for Internet Security*
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
COBIT	*Control Objectives for Information and Related Technologies*
CSC	*Critical Security Controls*
CSIRT	Equipa de Resposta a Incidentes de Segurança Informática
DGS	Direção-Geral da Saúde
DHCP	*Dynamic Host Configuration Protocol*
DICOM	*Digital Imaging and Communications in Medicine*
DIMSE	*DICOM Message Service Element*
DLL	*Dynamic Link Library*
DLP	*Data Loss Prevention*
DNS	*Domain Name System*
DORA	*Digital Operational Resilience Act*
DPIA	Avaliação de Impacto de Proteção de Dados
DSR	*Design Science Research*

EDR	*Endpoint Detection and Response*
EE	Entidade Essencial
EHDS	Espaço Europeu de Dados de Saúde
EHR	*Electronic Health Records*
EI	Entidade Importante
EMEA	Europe, Middle East and Africa
ENISA	Agência da União Europeia para a Cibersegurança
EPD	Encarregado de Proteção de Dados
ERS	Entidade Reguladora da Saúde
EUA	Estados Unidos da América
FHIR	*Fast Healthcare Interoperability Resources*
FIDO2	*Fast IDentity Online 2*
FNS	Federação Nacional dos Prestadores de Cuidados de Saúde
FTP	*File Transfer Protocol*
GE	Grandes Entidades
GNS	Gabinete Nacional de Segurança
GRC	Governação, Risco e Conformidade
HCDW	*HealthCare Data Watchdog*
HIMSS	*Health Information and Management Systems Society*
HIPAA	*Health Insurance Portability and Accountability Act*
HL7	*Health Level Seven*
HTTPS	*HyperText Transfer Protocol Secure*
IA	Inteligência Artificial
IdM	*Identity Management*
IdP	*Identity Provider*
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IHE	*Integrating the Healthcare Enterprise*
IMT	Instituto de Mobilidade e Transportes
IoC	*Indicators of Compromise*
IP	*Internet Protocol*

IPS	*Intrusion Prevention System*
IPSS	Instituição Particular de Solidariedade Social
ISO	*International Standard Organization*
ISP	*Internet Service Provider*
JSON	*JavaScript Object Notation*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
LIGHt	*Local Interoperability Gateway for Healthcare*
MCDT	Meios Complementares de Diagnóstico e Terapêutica
ME	Médias Entidades
ML	*Machine Learning*
MLLP	*Minimal Lower Layer Protocol*
MSP	*Managed Service Provider*
MSSP	*Managed Security Service Provider*
MTTD	*Mean Time To Detect*
MWL	*Modality Worklist*
NCP	*National Contact Point*
NIS	*Network and Information Security*
NIS2	*Network and Information Security 2*
NIST	*National Institute of Standards and Technology*
OSI	*Open Systems Interconnection*
PaaS	*Platform-as-a-Service*
PBAC	*Policy-Based Access Control*
PACS	*Picture Archiving and Communication System*
PAM	*Privileged Access Management*
PDF	*Portable Document Format*
PII	*Personally Identifiable Information*
PIMS	*Privacy Information Management Systems*
PIN	*Personal Identification Number*
PME	Pequenas e Médias Empresas
PNB	*Portuguese National Broker*

PRR	Programa de Recuperação e Resiliência
PSD	Prestadores de Serviços Digitais
PSE	Prestadores de Serviços Essenciais
QNRCS	Quadro Nacional de Referência em Cibersegurança
RBAC	*Role-Based Access Control*
REST	*REpresentational State Transfer*
RGPD	Regulamento Geral de Proteção de Dados
RIM	*Reference Information Model*
RIS	*Radiology Information System*
RM	Ressonância Magnética
SaaS	*Software-as-a-Service*
SCP	*Service Class Provider*
SCU	*Service Class User*
SGBD	Sistema de Gestão de Base de Dados
SGPI	Sistemas de Gestão de Privacidade da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	*Security Information and Event Management*
SNS	Serviço Nacional de Saúde
SO	Sistema Operativo
SOAP	*Simple Object Access Protocol*
SOAR	*Security Orchestration, Automation and Response*
SP	*Special Publication*
SPMS	Serviços Partilhados do Ministério da Saúde
SRI	Segurança das Redes e da Informação
SRI2	Segurança das Redes e da Informação 2
SSO	*Single Sign-On*
SUS	*System Usability Scale*
TAC	Tomografia Axial Computorizada
TCP	*Transmission Control Protocol*
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação

TLD	*Top Level Domain*
TLS	*Transport Layer Security*
TS	*Technical Specification*
UE	União Europeia
UEBA	*User and Entity Behavior Analytics*
USD	Dólares Americanos
USF	Unidade de Saúde Familiar
VLAN	*Virtual Local Area Network*
VM	*Virtual Machines*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
XML	*Extensible Markup Language*

1. INTRODUÇÃO

Os sistemas informáticos são essenciais na área médica porque facilitam a recolha, integração de dados e centralização de toda a informação relevante para diagnóstico, apoiando a atividade dos recursos humanos envolvidos. Neste contexto, a "Estratégia Digital para o Serviço Nacional de Saúde 2024-2026", abordada pelo então Ministro da Saúde do XXIII Governo de Portugal, Dr. Manuel Pizarro, na conferência "Transição Digital na Saúde" que decorreu a 18 de abril de 2023, em Lisboa, apresentou o processo de transformação digital em curso no setor da saúde (Ministério da Saúde, 2024).

A digitalização dos processos melhorou a prestação dos serviços aos cidadãos, permitindo o acesso a serviços e dados através de plataformas digitais (Serviço Nacional de Saúde, 2023). Por sua vez, a facilidade no acesso e o valor que os dados clínicos têm, é necessário proteger os vários estágios da informação (produção, modificação, transmissão e armazenamento) contra eventos que possam comprometer a sua confidencialidade (*confidentiality*), integridade (*integrity*) e disponibilidade (*availability*), os três pilares da segurança da informação (também conhecidos pela sigla inglesa CIA),

A necessidade de proteger os dados advém não só da necessidade de preservar o bom funcionamento e a reputação das entidades, como também das obrigações legais dispostas no Lei n.º 58/2019, de 8 de agosto (Assembleia da República, 2019).

Os fluxos de informação criados no contexto de projetos de transição digital, como por exemplo o projeto “Exames Sem Papel” (ESP), que visa a disponibilização por meios informáticos de resultados médicos ao utente e aos médicos do Serviço Nacional de Saúde (SNS), exigem novos pontos de controlo do acesso aos dados.

A transformação digital amplia o âmbito da cibersegurança no contexto da segurança da informação de uma organização. À medida que se criam novos processos baseados somente em fluxos digitais, sem utilização do papel, as medidas de proteção sobre os sistemas informáticos têm de ser reforçadas, sendo um dos controlos a monitorização do acesso aos dados.

Como consequência da implementação de controlos de cibersegurança mais complexos e da necessidade de melhoria contínua, é necessário um acompanhamento constante por equipas especializadas, o que nem sempre é possível em organizações de pequena e média dimensão. Nestes casos, a solução pode ser contratar serviços externos especializados ou recorrer aos recursos técnicos e humanos internos existentes, adotando

soluções baseadas em *software open-source* e suportadas por comunidades de utilizadores.

Qualquer que seja a solução adotada, permanece a necessidade de apresentar os controlos de cibersegurança a elementos da organização autorizados para aceder a dados de monitorização e que não têm conhecimentos avançados para lidar com ferramentas de monitorização de cibersegurança. Podemos incluir neste perfil os gestores, ou quem é responsável pela proteção de dados pessoais. Neste sentido, é importante facilitar a disponibilização destes dados, através de painéis analíticos (*dashboards*).

1.1. MOTIVAÇÃO

Embora exista, ao nível da gestão de topo, uma perceção generalizada da necessidade de implementação de medidas de cibersegurança para a proteção de dados e sistemas no setor da saúde, as unidades prestadoras de MCDT de pequena dimensão – com um número de funcionários inferior a 50 pessoas ou nível de faturação inferior a 10 milhões de euros – não estão sujeitas ao cumprimento de normativos mais exigentes nesta matéria.

Nestes contextos, a infraestrutura informática e os mecanismos de cibersegurança tendem a ser dimensionados em função do grau de maturidade organizacional e da dimensão do negócio, o que frequentemente limita a adoção de soluções mais avançadas e dispendiosas, por não se alinharem com as prioridades estratégicas definidas pela gestão. Embora as soluções de cibersegurança de uso generalizado assegurem proteção eficaz contra acessos não autorizados a sistemas e informação, mostram-se inadequadas face às especificidades do contexto clínico, em particular no que respeita à análise contextual dos acessos legítimos a informação médica sensível.

Neste enquadramento, a principal motivação para o desenvolvimento deste projeto a necessidade de melhorar e simplificar a monitorização e a análise dos acessos a dados médicos e pessoais, através de uma solução informática de baixo custo. Para o efeito, propôs-se a criação de uma prova de conceito para uma aplicação informática capaz de disponibilizar informação de auditoria de forma clara, acessível e orientada ao contexto clínico, integrando componentes que permitam recolher e correlacionar eventos de acesso para uma monitorização mais eficaz e abrangente.

1.2. OBJETIVOS

Tendo em consideração a necessidade de proteção da informação, bem como a especificidade dos sistemas de imagiologia médica, o objetivo geral deste estudo consistiu

no desenvolvimento de uma prova de conceito de uma plataforma capaz de centralizar a monitorização do acesso a dados pessoais sensíveis. Paralelamente, pretendeu-se definir estratégias para a recolha de eventos de acesso, recorrendo a *software open-source* e à integração entre diferentes sistemas.

Atendendo a que o público-alvo inclui elementos da gestão e responsáveis por proteção de dados pessoais sem conhecimentos técnicos avançados em cibersegurança ou informática, a ferramenta deverá disponibilizar uma interface uniformizada, acessível através de um navegador *web*, concebida para facilitar a consulta, interpretação e análise da informação.

Como objetivos secundários temos:

- analisar o enquadramento legislativo e normativo aplicável a entidades com adoção voluntária da diretiva NIS2, no que concerne à proteção de dados pessoais e medidas de cibersegurança associadas;
- identificar e sistematizar os controlos de cibersegurança relevantes para o contexto do mercado-alvo;
- apresentar os principais protocolos e sistemas auxiliares relacionados com a temática do estudo;
- efetuar o levantamento de requisitos e a definição de casos de uso, incluindo as interações entre diferentes sistemas informáticos;
- descrever a arquitetura da solução proposta, bem como o funcionamento geral da aplicação.

O âmbito deste projeto evoluiu de forma deliberada ao longo do seu desenvolvimento. O objetivo inicial contemplava a implementação de uma solução funcional em ambiente operacional real; contudo, dois fatores estruturais conduziram a uma reorientação metodologicamente fundamentada. A transição profissional do autor para fora do setor da saúde eliminou o acesso à infraestrutura informática clínica que serviria de base ao desenvolvimento, integração e validação da solução em produção. Adicionalmente, a implementação real de um sistema desta natureza – que integra múltiplas infraestruturas críticas e processa dados pessoais sensíveis – requer autorizações específicas junto das entidades reguladoras competentes, cujo processo de obtenção é, por natureza, moroso e incompatível com o horizonte temporal de um projeto de mestrado.

Face a este enquadramento, e em consonância com os princípios do *Design Science Research* (DSR), a investigação foi reorientada para a construção de uma prova de conceito. Esta decisão não representa uma limitação do trabalho, mas antes uma escolha metodológica consciente: no quadro do DSR, a demonstração da viabilidade técnica de um artefacto constitui uma contribuição científica autónoma e reconhecida, que preserva o rigor da investigação sem depender de um contexto operacional específico.

1.3. PLANO DE TRABALHO

O plano de trabalho inicialmente proposto era composto por dois semestres letivos. No decurso do projeto, a conjugação de fatores já referidos – nomeadamente a transição profissional do autor para fora do setor da saúde e a consequente necessidade de reorientar o âmbito da solução – determinou a necessidade de solicitar uma prorrogação do prazo de entrega, tendo o projeto sido estendido por mais três semestres. Este período adicional, embora não previsto, revelou-se determinante para aprofundar a revisão de literatura, consolidar a arquitetura da solução e desenvolver os cenários de validação com o rigor adequado ao nível de um projeto de mestrado.

Considerando os objetivos apresentados na Secção 1.2, o plano de trabalho teve as seguintes tarefas:

T1. Definição dos objetivos gerais e específicos do trabalho e estudo do enquadramento;

T2. Levantamento do estado da arte e trabalho relacionado;

T3. Levantamento dos requisitos de sistema e definição da arquitetura de suporte;

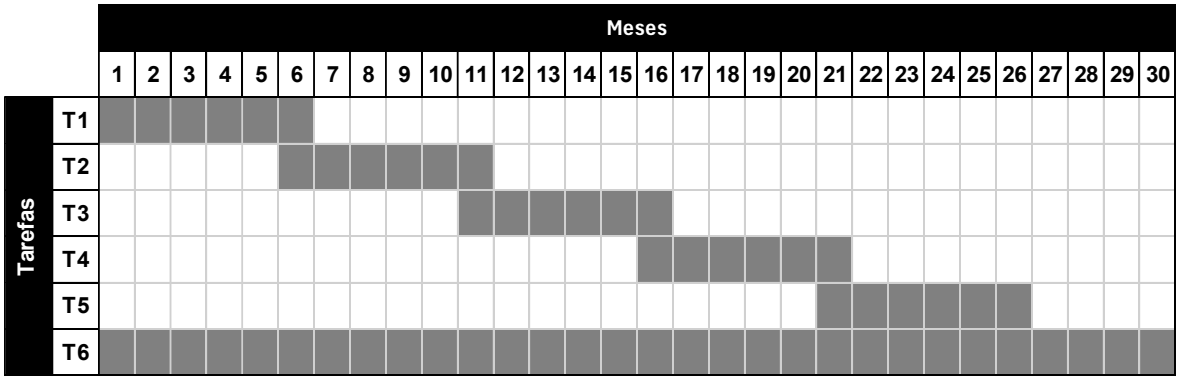
T4. Desenvolvimento da prova de conceito;

T5. Validação da prova de conceito através de dados simulados;

T6. Redação do relatório do projeto.

A Tabela 1 apresenta de forma detalhada a alocação das tarefas ao longo dos meses do projeto, começando em outubro de 2023 (no plano definido como mês um) até abril de 2026 (no plano definido como mês trinta).

Tabela 1 - Cronograma



1.4. METODOLOGIA

A metodologia utilizada para o desenvolvimento deste projeto assenta numa abordagem dual, combinando os princípios do *Design Science Research* (DSR) com as práticas das metodologias ágeis, de forma a garantir simultaneamente o rigor científico e a flexibilidade necessária à construção iterativa de uma prova de conceito.

O DSR constitui o enquadramento metodológico central desta investigação, orientando a produção de conhecimento científico através da conceção, implementação e avaliação de um artefacto tecnológico. Ao contrário das abordagens de investigação puramente descritivas, o DSR foca-se na criação de soluções inovadoras para problemas reais, avaliando a sua utilidade e pertinência no contexto organizacional em que se inserem. A metodologia segue seis estágios (identificação do problema, definição dos objetivos, conceção e desenvolvimento, demonstração, avaliação e comunicação), os quais estruturam as diferentes fases do presente trabalho, culminando na produção e validação de uma prova de conceito (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007).

Os seis estágios do DSR encontram correspondência direta na estrutura deste relatório. A identificação do problema é desenvolvida nas Secções 1.1 e 2, onde se caracteriza a lacuna de soluções acessíveis para entidades prestadoras de MCDT de pequena dimensão. A definição dos objetivos materializa-se nas Secções 1.2 e 1.3, com a formulação dos objetivos gerais e específicos e o respetivo plano de trabalho. A conceção e desenvolvimento do artefacto decorre ao longo do Capítulo 4, abrangendo o levantamento de requisitos, o modelo de dados, a arquitetura do sistema e o protótipo de baixa fidelidade. A demonstração e a avaliação concretizam-se na Secção 4.6, através da simulação de cenários de uso com dados fictícios que evidenciam o funcionamento da solução e verificam a sua adequação aos requisitos definidos. Por fim, a comunicação dos

resultados é assegurada pelo presente relatório e pela sua disseminação no contexto das provas públicas de mestrado.

A criação de uma prova de conceito é reconhecida como válida no contexto do DSR, uma vez que a demonstração da viabilidade de um artefacto constitui, por si só, uma contribuição relevante para o conhecimento científico.

Em complemento ao DSR, a construção da prova de conceito seguiu os princípios das metodologias ágeis, privilegiando ciclos iterativos e incrementais com períodos de trabalho curtos. Esta abordagem favorece a adaptação rápida a novos requisitos e a validação progressiva das funcionalidades implementadas, permitindo aferir, em cada iteração, a adequação da solução ao problema identificado. A adoção de práticas ágeis permitiu alinhar as decisões técnicas com as necessidades identificadas ao longo do processo de investigação (Sbrocco, 2012).

1.5. ESTRUTURA DO DOCUMENTO

Este relatório está estruturado em 5 capítulos.

O Capítulo 1 abrange a introdução, a motivação, os objetivos gerais e específicos, bem como a estrutura do documento.

O Capítulo 2 fornece o enquadramento do projeto, referindo-se aos principais regulamentos, normas e tecnologias relacionadas com o projeto, às principais entidades do setor da saúde, de cibersegurança e proteção de dados no âmbito europeu e nacional, bem como à caracterização das tecnologias existentes numa entidade prestadora de MCDT.

No Capítulo 3 apresenta-se o estado da arte de estudos no âmbito da segurança da informação e cibersegurança em entidades de saúde, de soluções de *software* existentes, bem como de tipos de sistemas que podem contribuir para a melhoria de cibersegurança na perspectiva específica de monitorização e auditoria de acesso a sistemas, fluxos e ficheiros contendo dados pessoais.

No Capítulo 4 realiza-se a análise de requisitos, identificando dados, atores, sistemas informáticos e fluxos de informação. Apresenta-se a arquitetura da plataforma, identificando os diversos componentes necessários para o funcionamento da solução e as estratégias de interligação de sistemas. Este capítulo finaliza com a verificação e validação da viabilidade conceitual da plataforma através de casos de uso e simulação dos fluxos de dados.

Finalmente, no Capítulo 5 apresentam-se as considerações finais e o trabalho futuro a ser desenvolvido.

2. ENQUADRAMENTO

Neste capítulo apresenta-se o contexto organizativo, legislativo, normativo e tecnológico relevante para a área da Imagiologia Médica. No âmbito organizativo, descrevem-se as principais entidades portuguesas com as quais as instituições prestadoras de MCDT mantêm relações (Secção 2.1) e os processos de transformação digital ocorridos no sector (Secção 2.2). São igualmente elencados os documentos pertinentes – incluindo legislação e regulamentos (Secções 2.3, 2.4, 2.5 e 2.6), normas e *frameworks* organizativas (Secções 2.7, 2.8, 2.9, 2.10 e 2.11) – de modo a fundamentar a definição dos requisitos no Capítulo 4. No domínio tecnológico, realiza-se uma resenha do ambiente expectável, com especial destaque para os sistemas de segurança e os protocolos de comunicação específicos do contexto médico (Secções 2.12, 2.13 e 2.14).

2.1. SISTEMA NACIONAL DE SAÚDE E PRESTADORES DE MEIOS COMPLEMENTARES DE DIAGNÓSTICO E TERAPÊUTICA

O Sistema Nacional de Saúde abrange todas as entidades, públicas e privadas, que operam no setor da saúde em Portugal. Por sua vez, o SNS, criado oficialmente a 15 de setembro de 1979 através da publicação da Lei nº 56/79, concretizou o direito à proteção da saúde previsto na Constituição portuguesa. Assegura o direito à saúde nas componentes de promoção, prevenção, diagnóstico, tratamento e reabilitação (Serviço Nacional de Saúde, 2025) (Varela, 2019). A Administração Central do Sistema de Saúde (ACSS) é a entidade responsável pela administração central, coadjuvada pelas Administrações Regionais da Saúde (ARS) que operam a nível regional. A Direção Geral da Saúde (DGS) é a entidade regulatória e coordena as normas clínicas e de prevenção em todo o território nacional (Direção Geral da Saúde, 2025).

O setor privado da saúde, constituído por entidades de iniciativa privada e social, mantém protocolos e convenções com o setor público para a prestação de cuidados de saúde primários, agudos e MCDT, para suprir as necessidades de resposta do setor público de saúde.

Tanto o setor público como o privado podem prestar serviços de MCDT, que são os procedimentos médicos e clínicos que visam o diagnóstico e a terapêutica, dos quais fazem parte a imagiologia médica, análises clínicas, fisioterapia, entre outros.

A Federação Nacional de Prestadores de Cuidados de Saúde (FNS), a entidade associativa que representa o setor privado de saúde, menciona que "a rede do setor

convencionado produz para o SNS mais de 300.000 atos por dia, mais de 100 milhões de atos por ano, dando resposta a cerca de 60.000 requisições médicas ao dia, ou seja, mais de 20 milhões de requisições por ano, o que representa mais de 90% da produção total do SNS, de MCDT em ambulatório." (Federação Nacional de Prestadores de Cuidados de Saúde, 2023).

Na Tabela 2 estão as principais entidades e a respetiva função no Sistema Nacional de Saúde.

Tabela 2 - Entidades e respetivas funções no sistema de saúde

Entidades	**Função principal**
Serviço Nacional de Saúde (SNS)	Prestação de cuidados primários, hospitalares (cirúrgicos), urgência, consulta e exames
Administração Central do Sistema de Saúde (ACSS)	Entidade de gestão nacional das entidades do setor
Administração Regional da Saúde (ARS)	Entidade de gestão regional das entidades do setor
Direção Geral da Saúde (DGS)	Entidade de coordenação do sistema nacional de saúde
Entidade Reguladora da Saúde (ERS)	Entidade de regulação do setor
Serviços Partilhados do Ministério da Saúde (SPMS)	Instituto público responsável pela gestão e operacionalização de iniciativas de transformação digital (protocolos e plataformas informáticas) no SNS
Hospitais privados / sociais / Instituição Particular de Solidariedade Social (IPSS)	Prestação de cuidados primários, hospitalares, urgência, consultas e exames, com acordos com o SNS
Prestadores MCDT convencionados	Prestação de atos de diagnóstico e terapêuticos para o SNS
Centros de Saúde	Entidade de saúde de atuação local, organizada em unidades funcionais
Unidades de Saúde Familiar (USF)	Unidades de saúde integradas nos centros de saúde, com autonomia e equipas multiprofissional e prestação de cuidados a utentes com e sem médico de família

2.2. TRANSFORMAÇÃO DIGITAL NA SAÚDE

Tal como acontece noutros setores e atividades económicas, a informatização de processos e fluxos de dados no sistema nacional de saúde português tem ocorrido progressivamente ao longo dos anos. O processo iniciou-se em 1988, com a automatização dos serviços financeiros e administrativos e a informatização dos processos clínicos (Pires, 2012) (Pontes, 2020).

Posteriormente, ao abrigo de iniciativas nacionais e internacionais (sobretudo europeias) de âmbito alargado, impulsionadas recentemente pelo Plano de Recuperação e Resiliência (PRR), a digitalização abarcou processos que até então se tinham mantido inalterados. O ano de 2020 foi declarado pela União como "Ano Europeu da Transformação Digital" (Comissão Europeia, 2025).

A telemedicina, prescrição eletrónica de medicamento e de exames são exemplos de processos informatizados com recursos à Internet para aproximar os serviços de saúde aos utentes, otimizar recursos e tempo. A desmaterialização dos processos traduz-se na eliminação do papel (por exemplo, nas prescrições) e evita deslocações aos locais de saúde por questões meramente administrativas. Segundo dados dos SPMS (Serviços Partilhados do Ministério da Saúde, 2024), desde 6 de maio de 2022 até 6 de maio de 2024, obtiveram-se os seguintes resultados: 49 milhões de requisições eletrónicas; 115 milhões de resultados partilhados pelos prestadores convencionados; 92% de taxa de desmaterialização.

Entre as vantagens da transição digital está a reutilização de dados existentes para informar e acompanhar os doentes com doenças crónicas, disponibilizar dados para investigação (com recurso à Inteligência Artificial (IA)), permitindo não só o diagnóstico e tratamento, como também a prevenção (Ladeia & Sousa, 2025).

Uma das faces visíveis da transformação digital é a aplicação "SNS24" (Figura 1), que congrega informação relativa ao utente (e aos seus dependentes), agendamento de consultas/teleconsultas, realização de teleconsultas, guias de prestação de exames e resultados, receitas farmacêuticas, lista de medicação habitual, lista de unidades de saúde do SNS com teleconsulta e boletim de vacinas, informação do centro de saúde, médico de família e contactos, entre outras informações.

Figura 1 - Interface Inicial da aplicação SNS24 para smartphones com sistema operativo Apple iOS

As entidades prestadoras de MCDT integram-se na cadeia de consumo e produção de informação para o SNS. Estas obtêm dados demográficos e exames a realizar das guias da prescrição desmaterializada e disponibilizam, após a realização do exame, os respetivos resultados (em formato de ficheiros *Portable Document Format* (PDF) e/ou dados estruturados) através do mesmo sistema.

O *Local Interoperability Gateway for Healthcare* (LIGHt) é uma plataforma de integração local, constituída por uma camada de integração (conhecida também pelo termo inglês *middleware*) que intermedia a troca de informação entre os produtos da SPMS e produtos de terceiros. As interfaces de comunicação são configuráveis e garantem o acesso aos dados sem necessidade de providenciar acesso direto às bases de dados, melhorando a segurança e auditoria de acessos. A comunicação interna é feita através de mensagens no formato *Health Level* 7 (HL7) v2.5. A comunicação entre este sistema e o *Portuguese National Broker* (PNB) é feita através do formato de mensagens HL7 *Fast Healthcare Interoperability Resources* (FHIR). (SPMS, 2017).

A Figura 2 representa o fluxo de informação mediado pelo LIGHt, do qual fazem parte:

- Registo Nacional de Utentes (RNU) é o sistema basilar constituído pela base de dados nacional com informação administrativa dos utentes do SNS, nomeadamente dados demográficos, número de identificação (entre outros, número de identificação fiscal, número de utente do SNS), centro de saúde e médico de família atribuído.

Este sistema fornece estes dados aos demais sistemas e aplicações, para melhorar a qualidade de informação, a gestão dos dados pessoais e a segurança/auditoria de acesso.

Figura 2 - Fluxo de informação mediado pelo LIGHt (SPMS, 2017)

- Sistema Clínico do SNS (SCLINICO), é o sistema informático utilizado pelos profissionais de saúde (por exemplo, médicos, enfermeiros) para gerir informação clínica dos utentes nos centros de saúde, bem como nalguns hospitais. Podem ser registados: dados relacionados com os episódios de consulta, diagnósticos, exames; prescrições de medicamentos (interligação com o sistema de Prescrição Eletrónica de Medicamentos (PEM)); e agendamento de consultas. Este sistema está interligado com diversos outros sistemas informáticos, entre os quais o Registo de Saúde Eletrónico (RSE) e o Sistema de Vigilância de Doenças de Declaração Obrigatória (SIVIDA).

- Sistema de Orientação Nacional para a Harmonização dos Hospitais (SONHO), é o sistema de informação administrativa hospitalar utilizado no SNS. É utilizado em hospitais públicos para: marcação de consultas e exames, gestão de internamentos e altas médicas, gestão da faturação e estatísticas de atividade hospitalar.

- Sistema de Vigilância de Doenças de Declaração Obrigatória é um sistema informático para a notificação e vigilância epidemiológica de: Doenças de Declaração Obrigatória (DDO) (por exemplo, tuberculose, hepatites virais, entre outras), infeções emergentes e eventos de saúde pública com impacto alargado (nacional e internacional). Este sistema é utilizado pelos profissionais de saúde em

centros de saúde e hospitais, delegados de saúde, técnicos da DGS e ARS, bem como laboratórios.

Outras aplicações e sistemas, como a aplicação "SNS24", integram-se neste ambiente de interoperabilidade.

O PNB é um sistema que envolve várias entidades e sistemas informáticos. Começou a ser desenvolvido em 2015 pela equipa de Interoperabilidade Técnica do SPMS, com o objetivo de promover a adoção de *standards* internacionais recomendados pela indústria de *eHealth* nos sistemas de âmbito nacional desenvolvidos pelo SPMS (SPMS, 2017).

O foco do projeto é garantir uma interoperabilidade organizacional, técnica, semântica e legal, através de um sistema central orientado a eventos, genérico e escalável, que permita manter e evoluir *workflows* para integração nacional e internacional (via *National Contact Point* (NCP)). Posteriormente foi expandido o seu âmbito e foi criado um circuito interministerial de intercâmbio de dados (SPMS, 2017).

Este sistema recorre a tecnologias e normas *open-source*, entre elas o protocolo HL7, baseando-se sobretudo na troca de mensagens entre sistemas (abordagem produtor-consumidor), com implementação de mecanismos de segurança como autenticação e controlos de acesso.

Tem especial relevância para os objetivos deste trabalho o projeto "Exames Sem Papel" (ESP). O projeto ESP "visa, através da utilização de múltiplas plataformas de serviços centrais, desmaterializar os processos de requisição, efetivação e faturação de Meios Complementares de Diagnóstico e Terapêutica" (SPMS, 2020) prestados por entidades públicas e privadas e disponibilizar o seu acesso às entidades públicas (hospitais e centros de saúde) e aos utentes (ou seus representantes legais).

No *website* oficial do projeto[1] é disponibilizada informação geral sobre o projeto, legislação, especificações, normas, dados de monitorização, bem como a possibilidade de submeter a manifestação de interesse na adesão ao mesmo (SPMS, 2020).

O diagrama da Figura 3 descreve o fluxo digital de prescrição, realização e faturação de MCDT no SNS. O processo pode ser dividido em três etapas: 1) prescrição e registo

[1] https://www.spms.min-saude.pt/2020/07/exames-sem-papel/

pelo médico do SNS; 2) realização e partilha de resultados pelos prestadores de MCDT convencionados; e 3) conferência da faturação e pagamento pelas entidades do SNS;

Na primeira etapa, o médico prescreve o exame através do *software* SCLINICO. A prescrição é registada centralmente de forma imediata (BDNR). O utente recebe uma guia de prestação que contém dois códigos: o *Personal Identification Number* (PIN) de acesso e o PIN de prestação.

Na segunda etapa, o utente dirige-se a uma entidade prestadora de MCDT convencionada para a realização do exame. Esta entidade usa o PIN de acesso para consultar a requisição na BDNR do exame a realizar. Após a realização do exame, o PIN de prestação é usado para registar que o serviço foi concluído. Os resultados do exame são partilhados digitalmente através do RSE, ficando disponíveis para o médico e para o utente via SNS 24.

Na última etapa. o prestador envia a fatura eletrónica para o Centro de Conferência de Faturas do SNS. Após a verificação da informação com a base de dados de requisições, a ARS procede ao pagamento.

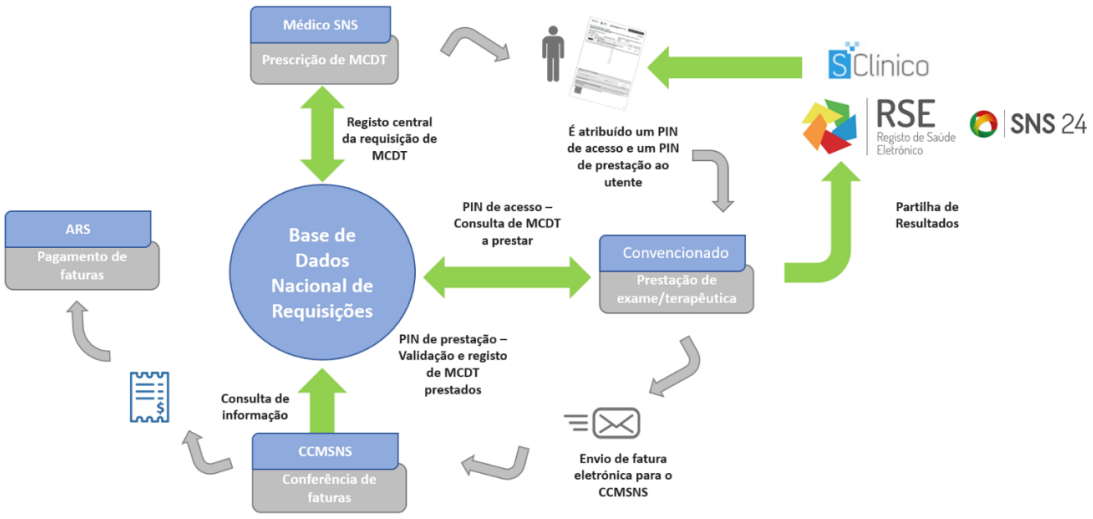


Figura 3 - Sistemas e fluxos de requisições e resultados de MCDT (SPMS, 2017)

A Base de Dados Nacional de Requisições (BDNR) é um repositório de dados dos sistemas informáticos criados pela SPMS, que permite o acesso das entidades autorizadas à sua *Application Programming Interface* (API) para obtenção de dados e ações sobre as requisições de MCDT (Figura 4). O desiderato deste repositório central é evitar a duplicação de dados, permitindo que os vários serviços do SNS possam consumir dados para fins administrativos ou clínicos.

Entre outros fluxos de trabalho existentes, destacam-se:

1. agendamento e efetivação de requisições MCDT;
2. comunicação e consulta de resultados de MCDT.

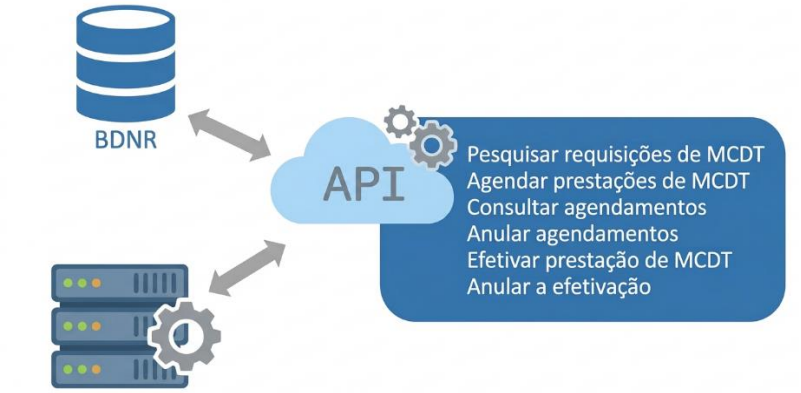


Figura 4 - BDNR e API de acesso a MCDT (SPMS, 2017)

No primeiro fluxo de trabalho, através do acesso a *webservices* baseados em *Single Object Access Protocol* (SOAP) e mensagens no formato estruturado *Extensible Markup Language* (XML), é feita a pesquisa da requisição. Após obtenção da requisição, pode ser feito o agendamento (reserva da requisição a um prestador de MCDT para posterior realização do exame) e efetivação (que ocorre no momento da prestação do serviço).

No segundo fluxo de trabalho, que recorre a *webservices* baseados em *Representational State Transfer* (REST) com mensagens HL7 FHIR, é efetuada a comunicação do resultado assim que o relatório médico está disponível. O sistema é notificado de que é possível consultar o relatório em formato digital (PDF) armazenado e disponibilizado pelos sistemas do prestador.

2.3. LEIS E REGULAMENTOS DO SETOR DA SAÚDE

O setor da saúde em Portugal é regulado por um conjunto de leis, decretos-lei, portarias e normas técnicas específicas. O desiderato da regulação é garantir a qualidade, segurança e eficácia dos cuidados prestados pelas diversas entidades públicas e privadas. No âmbito do projeto, enfatizam-se os seguintes regulamentos:

- Normas e Circulares Normativas da DGS, com orientações clínicas e operacionais para os serviços de saúde;
- Licenciamento de Estabelecimentos de Saúde, com regras para abertura e funcionamento (Decreto-Lei n.º 127/2014);

- Portaria n.º 1303/2006, de 21 de novembro, que define os requisitos técnicos e funcionais dos sistemas de informação de saúde, incluindo obrigações de registo de acessos, integridade do processo clínico eletrónico e conservação de dados pessoais;

- Lei n.º 15/2014, de 21 de março, que consolida a legislação em matéria de direitos e deveres do utente dos serviços de saúde; no qual prevê o direito de acesso ao processo clínico e o dever de confidencialidade por parte dos profissionais;

- Normas da DGS e da SPMS de regulação da Telemedicina e Saúde Digital.

A Entidade Reguladora da Saúde (ERS) é a entidade pública portuguesa com "poderes de regulação, regulamentação, supervisão, fiscalização e sancionatórios" e "tem por missão a regulação da atividade dos estabelecimentos prestadores de cuidados de saúde dos setores público, privado, cooperativo e social" (Entidade Reguladora da Saúde, 2025). No *website*[2] da instituição está listada a legislação específica para cada área referida.

2.4. CIBERSEGURANÇA NO CONTEXTO EUROPEU E NACIONAL

Um dos objetivos do plano de Transformação Digital na Saúde é a resiliência dos sistemas a ataques de cibersegurança. Para alcançar os diversos objetivos da cibersegurança, as entidades europeias produziram diretivas relacionadas com a cibersegurança, de forma a uniformizar a resposta coletiva dos Estados-membros. Posteriormente, estas diretivas foram transpostas com adaptações para os quadros legais de cada país, em consonância com a legislação já existente e particularidades societárias. Entre outros resultados, a legislação estabeleceu a criação de entidades e redes de colaboração (Comissão Europeia, 2025).

A estratégia da cibersegurança na União Europeia (UE) assenta em três pilares:

1. resiliência, soberania tecnológica e liderança;

2. capacidade operacional de prevenção, deteção, resposta e dissuasão;

3. cooperação para promover um ciberespaço global e aberto.

[2] https://www.ers.pt/pt/legislacao/selecionar/prestadores/

A Figura 5 sintetiza os instrumentos existentes associadas às capacidades operacionais, os âmbitos de cooperação e as entidades e programas existentes.

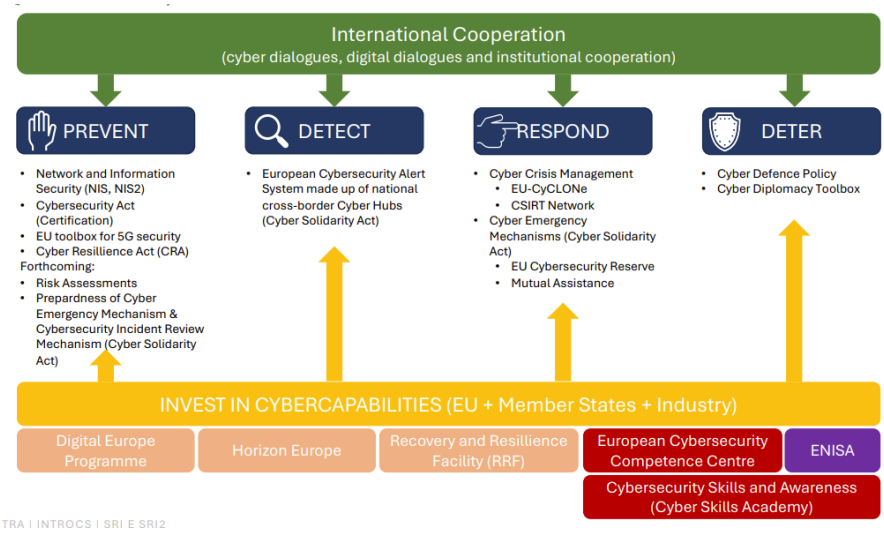


Figura 5 - Estratégia Europeia de Cibersegurança (European Commission, 2025)

O Centro Nacional de Cibersegurança (CNCS) é autoridade nacional responsável pelo ciberespaço em Portugal. Esta entidade está sob a alçada do Gabinete Nacional de Segurança (GNS) e é o representante nacional nas iniciativas e projetos europeus sob coordenação da *European Union Agency for Cybersecurity* (ENISA). Esta agência europeia apoia na definição das políticas europeias de cibersegurança da UE, permitindo a cooperação e coordenação estratégica e técnica (sob a forma de orientações técnicas e formação) entre várias entidades europeias e nacionais. Um exemplo recente de política europeia de segurança é a *Network and Information Security Directive* (NIS).

Ao nível da resposta a incidentes de cibersegurança, o CNCS criou a rede nacional de equipas de resposta a incidentes de segurança informática (*Computer Security Incident Response Team* (CSIRT)), da qual faz parte a sua própria equipa, a CERT.PT, sendo esta equipa a representante nacional na Rede Europeia de CSIRT, estabelecida pela Diretiva UE 2016/1148 (Parlamento Europeu e do Conselho, 2016).

Ao nível técnico, o CNCS tem produzido documentação diversa, destacando-se o Quadro Nacional de Referência em Cibersegurança (QNRCS), documento cuja primeira versão data de 2019. Neste documento faz-se o enquadramento legislativo e organizacional da cibersegurança nacional e apresenta uma base de trabalho para a implementação dos requisitos mínimos nesta matéria nas organizações nacionais de qualquer dimensão ou atividade económica, sendo de aplicação obrigatória para os serviços públicos, os Prestadores de Serviços Essenciais (PSE) e os Prestadores de

Serviços Digitais (PSD) em território nacional, tais como a saúde, energia, comunicações, entre outros (Centro Nacional de Cibersegurança, 2019).

No QNRCS aborda-se o processo de gestão de risco de uma forma prática, explicando a importância da identificação de ativos críticos, vulnerabilidades, riscos, partes interessadas, classificação por grau de impacto e probabilidade de ocorrência.

Os cinco objetivos da gestão de cibersegurança são: identificar, proteger, detetar, responder e recuperar. No objetivo "identificar" encontram-se medidas orientadas para identificar o contexto da organização, os ativos e atividades que suportam os processos críticos, bem como identificar os riscos associados. No objetivo "proteger" encontram-se medidas destinadas a proteger os processos e ativos da organização, visando proteger as três dimensões da organização: Pessoas, Processos e Tecnologia. No objetivo "detetar" estão mencionadas as formas de definir e implementar medidas que visem a identificação atempada de incidentes de cibersegurança. No objetivo "responder" estão descritas medidas de ação no caso de deteção de incidente, de modo a reduzir os potenciais efeitos adversos na organização. No objetivo "recuperar" são mencionadas estratégias de definição e implementação de planos de recuperação de processos e serviços afetados por incidentes de cibersegurança, de modo a retomar as atividades fundamentais da organização no menor tempo útil possível. Os cinco objetivos formam um ciclo iterativo de melhoria contínua (Centro Nacional de Cibersegurança, 2019).

Os objetivos e medidas de segurança estão segmentados em categorias e subcategorias, com uma breve descrição do objetivo específico da subcategoria, modos de implementação técnica e processual, evidências a produzir e mapeamento para *frameworks* e normas de cibersegurança (por exemplo, mapeamento com controlos da *Center for Internet Security* (CIS) *Critical Security Controls* (CSC) 8, *Control Objectives for Information and Related Technologies* (COBIT) 5, *Internation Standard Organization* (ISO) / *Internation Electrotechnical Commission* (IEC) 27001:2013 e *National Institute of Standards and Technology* (NIST) *Special Publication* (SP) 800) (Centro Nacional de Cibersegurança, 2019).

2.5. DIRETIVA DE SEGURANÇA DAS REDES E DA INFORMAÇÃO 2

A Diretiva de Segurança das Redes e da Informação 2 (SRI2) (Diretiva UE 2022/2555), também conhecida por NIS2, está em vigor na UE desde 16 de janeiro de 2023 e a sua transposição para os ordenamentos jurídicos nacionais dos Estados-Membros estava prevista até 17 de outubro de 2024. A transposição em Portugal ocorreu a 4 de dezembro

de 2025, através do Decreto-Lei n.º 125/2025 (Portugal. Presidência do Conselho de Ministros, 2025).

Esta nova diretiva, que substitui a anterior SRI em vigor desde 2018, uniformiza a estratégia de cibersegurança na UE, nomeadamente no que se relaciona com: redes de comunicação eletrónica, dispositivos ou grupos de dispositivos interconectados que processam dados digitais; dados digitais recebidos, transmitidos e armazenados. Esta nova versão clarifica e amplia o âmbito de entidades e setores visados, e estabelece também um quadro sancionatório mais penalizador.

Aplica-se a incidentes provenientes do ciberespaço ou de origem física, que tenham impacto num serviço com efeito perturbador significativo como interrupções de fornecimento de energia ou desastres naturais.

As entidades podem ser classificadas em Grandes Empresas (GE), Médias Empresas (ME) ou Pequenas e Médias Empresas (PME) em função do seu setor de atividade, do número de funcionários e do volume de faturação. Considera-se que uma GE é uma organização com 250 funcionários ou mais ou com um volume de faturação superior a 50 milhões de euros; uma ME tem entre 50 a 249 funcionários ou um volume de faturação entre 10 e 50 milhões de euros; uma PME tem menos de 50 funcionários ou volume de faturação inferior a 10 milhões de euros). Salvo exceções, as PMEs estão excluídas do âmbito da NIS2.

A NIS2 apresenta as entidades em dois anexos, classificadas por Entidade Essencial (EE), Entidade Importante (EI) ou "não aplicável / fora do âmbito" (N/A), como presente nas Tabela 3 e Tabela 4.

Tabela 3 - Classificação de Entidades segundo o Anexo I (Setores de Alta Criticidade – NIS2)

Setor	**Subsector**	**GE**	**ME**	**PME**
Energia	Eletricidade, gás, hidrogénio, petróleo	EE	EI	N/A
Transporte	Aéreo, ferroviário, marítimo	EE	EI	N/A
Banca	Instituições de crédito (exceto reguladas pela dora)	EE	EI	N/A
Infraestrutura Financeira	Bolsas, contrapartes centrais (exceto entidades reguladas pela *Digital Operational Resilience Act* (DORA)	EE	EI	N/A

Setor	Subsector	GE	ME	PME
Saúde	Prestadores de cuidados de saúde, laboratórios, medicamentos, dispositivos médicos	EE	EI	N/A
Saúde (caso especial)	Entidades com autorização de distribuição de medicamentos	EE	EI	N/A
Água potável	Abastecimento de água potável	EE	EI	N/A
Águas residuais	Apenas se parte essencial da atividade	EE	EI	N/A
Infraestrutura Digital	Prestadores qualificados de serviços de confiança	EE	EE	EE
	Serviços *Domain Name Service* (DNS) (exceto domínios *root*)	EE	EE	EE
	Top-Level Domain Registries	EE	EE	EE
	Redes públicas de comunicações	EE	EE	EE
	Serviços de confiança não qualificados	EE	EE	EI
	Pontos de troca de internet	EE	EI	EI
	Computação em nuvem	EE	EI	N/A
	Centros de dados	EE	EI	N/A
	Redes de entrega de conteúdo (*Content Delívery Network* (CDN))	EE	EI	N/A
Serviços de Tecnologias de Informação e Comunicação (*Business to Business* (B2B))	*Managed Security Service Providers* (MSSP) - Prestadores de serviços de segurança geridos, ou seja, entidades externas que fornecem serviços de monitorização, gestão e resposta a incidentes de cibersegurança	EE	EI	N/A
Administração Pública	Autoridades centrais (exceto justiça, parlamentos, entre outros)	EE	EE	EE
	Autoridades regionais	EI	EI	EI
Espaço	Operadores de infraestrutura terrestre	EE	EI	N/A

Tabela 4 - Classificação de Entidades segundo o Anexo II (Outros Setores Críticos – NIS2)

Setor	**GE**	**ME**	**PME**
Serviços postais e de correio	EI	EI	N/A
Gestão de resíduos (se for atividade económica principal)	EI	EI	N/A
Químicos – fabrico, produção, distribuição	EI	EI	N/A
Alimentar – produção e processamento industrial e grossista	EI	EI	N/A
Manufatura – dispositivos médicos, eletrónica, maquinaria, veículos, entre outros.	EI	EI	N/A
Prestadores digitais – *marketplaces*, motores de busca, redes sociais	EI	EI	N/A
Investigação – organizações de investigação (exceto ensino; entidades de educação é de aplicação voluntária)	EI	EI	N/A
Registo de domínios (entidades que fornecem serviços de registo de nomes de domínio)	sujeitas apenas aos Artigos 3 e 28		

Para além do âmbito e dos objetivos gerais já apresentados, a NIS2 caracteriza-se por:

- a governança está mais centralizada, através da criação de um grupo europeu de cooperação de cibersegurança, melhorando a robustez de resposta;
- os requisitos de segurança são mais específicos e detalhados, alinhados com o contexto atual da organização, com os requisitos regulamentares e com as melhores práticas internacionais de cibersegurança;
- a notificação de incidentes significativos tem critérios harmonizados e processos de notificação mais claros, com os seguintes prazos de comunicação de incidentes às autoridades nacionais (CNCS ou CSIRT): a notificação inicial a ser feita até 24 horas desde que se deteta o incidente; notificação intermédia até 72 horas; entrega de relatório final até um (1) mês;
- as autoridades nacionais têm o poder para realizar auditorias e inspeções; as organizações devem realizar auditorias, processos de monitorização contínua e avaliações de risco são obrigatórios e devem ser realizados periodicamente, para definir prioridades de proteção e recuperação, aferir a eficácia das medidas, identificar as vulnerabilidades e mitigar as ameaças;

- as sanções foram harmonizadas, com penalizações financeiras e outras medidas corretivas; as autoridades nacionais têm o poder de aplicar as seguintes sanções: 1) para EE, até 10 milhões de euros ou 2% do volume de negócios anual global (o que for maior); 2) para EI, até 7 milhões de euros ou 1,4% do volume de negócios anual global (o que for maior);

- a resiliência ganha destaque na estratégia, com colaboração entre diversas entidades, de modo a permitir a recuperação e continuidade dos negócios em caso de incidente;

- a gestão de topo da organização deve estar envolvida na supervisão da cibersegurança, é responsável por violações de conformidade e deve receber formação específica em cibersegurança para a correta definição e avaliação das estratégias globais; os gestores devem promover a capacitação de recursos humanos e entidades, através da contratação e formação, bem como de certificações de cibersegurança aplicáveis à entidade;

- o investimento em tecnologia e processos de cibersegurança, através da implementação de diversos tipos de tecnologia para monitorização, deteção e resposta a incidentes, bem como na atualização da infraestrutura e redução de sistemas legados (ou seja, sistemas informáticos descontinuados e que não têm suporte nem atualizações do seu fabricante);

- a harmonização de medidas de segurança e requisitos entre estados-membros, com uma implementação uniforme para ser eficaz.

- a existência de documentação acerca das políticas, procedimentos e relato dos incidentes relevantes, que sirvam de orientação para os recursos humanos e de prova de conformidade no âmbito das auditorias.

As organizações devem implementar medidas técnicas e organizacionais adequadas, tais como:

- a gestão de riscos e segurança da informação, para identificar, avaliar e tratar os riscos com impacto significativo;

- a gestão de incidentes, com o registo e deteção de eventos e incidentes, com o registo das ocorrências e detalhe do processo de investigação;

- a gestão e comunicação de incidentes com terceiros, com ações para identificar, gerir, mitigar e comunicar a autoridades e partes interessadas os incidentes de segurança;
- os planos de recuperação e continuidade de negócio, com a gestão efetiva de cópias de segurança e preparação dos recursos humanos;
- a gestão da segurança em redes e sistemas de informação;
- uso de criptografia para garantir a confidencialidade, integridade e disponibilidade de informação e respetivos sistemas;
- a gestão de vulnerabilidades em sistemas informáticos.

Considerando o âmbito deste projeto, uma PME prestadora de MCDT não é obrigada a cumprir a NIS2, embora seja recomendado o seu cumprimento voluntário.

2.6. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, doravante designado Regulamento Geral de Proteção de Dados (RGPD), constitui o diploma jurídico da União Europeia que estabelece o regime aplicável à proteção de dados pessoais dos cidadãos da UE. O regulamento entrou em vigor em 25 de maio de 2018, sendo diretamente aplicável em todos os Estados-Membros. No ordenamento jurídico português, a sua execução foi concretizada pela Lei n.º 58/2019, de 8 de agosto, que assegura a execução e conformidade nacionais. O âmbito de aplicação do RGPD estende-se a todas as entidades, públicas ou privadas, estabelecidas dentro ou fora do território da União Europeia, desde que procedam à recolha, ao tratamento ou ao armazenamento de dados pessoais relativos a cidadãos da UE.

Nos termos do RGPD, entende-se por dados pessoais (em inglês, *Personally Identifiable Information* - PII) qualquer informação que permita identificar, direta ou indiretamente, uma pessoa singular. Esta abrangência aplica-se independentemente do suporte ou formato em que os dados se encontrem, incluindo meios físicos ou digitais, textuais ou audiovisuais. Exemplos comuns incluem o nome, o número de identificação fiscal, a imagem fotográfica ou dados biométricos. Estes elementos podem surgir isoladamente ou em combinação, potenciando o seu poder identificador. O regulamento abarca igualmente identificadores digitais associados às comunicações eletrónicas, como endereços de *Internet Protocol* (IP) ou outros marcadores tecnológicos (Magalhães & Pereira, 2020).

Para além da categoria geral de dados pessoais, o RGPD prevê ainda a existência de categorias especiais de dados, cuja natureza é particularmente sensível. Entre estes contam-se os dados de saúde, genéticos, biométricos, bem como aqueles que revelem opiniões políticas, convicções filosóficas ou religiosas e filiação sindical. O tratamento destas categorias encontra-se sujeito a um regime reforçado, estando, em regra, proibido, salvo em circunstâncias excecionais e sob condições estritas. Em Portugal, a decisão quanto à licitude da recolha e tratamento compete à Comissão Nacional de Proteção de Dados (CNPD), enquanto autoridade de controlo competente. Atendendo ao risco acrescido que tais dados representam para os direitos e liberdades fundamentais dos titulares, o legislador europeu estabeleceu regras particularmente rigorosas quanto à sua utilização e proteção (Magalhães & Pereira, 2020).

Os quatro papéis definidos no âmbito do RGPD são:

- Titular dos dados pessoais - pessoa singular aos quais os dados pessoais se referem;
- Controlador de dados - pessoa singular ou coletiva responsável pela definição da motivação para recolha de dados e as suas finalidades, bem como pela supervisão de subcontratantes;
- Operadores de dados - pessoa singular ou coletiva que trata os dados em nome do controlador, seguindo as suas instruções;
- Encarregado de Proteção de Dados (EPD) - é o especialista que assegura a conformidade da organização com as leis e regulamentos de proteção de dados; informa, aconselha e monitoriza o tratamento realizado pelos controladores e operadores.

O regulamento estipula que os titulares dos dados pessoais têm os seguintes direitos em relação aos seus dados pessoais:

- direito de informação (artigos 12, 13 e 14) - o titular tem direito a ser informado de forma transparente sobre quem faz o tratamento dos seus dados, as finalidades do tratamento e quais são os seus direitos;
- direito de acesso (artigo 15) - o titular tem o direito de ser informado sobre se os seus dados estão a ser tratados, quais, com que finalidade, se foram ou serão divulgados, e o seu período de armazenamento;

- direito de retificação (artigo 16) - o titular pode solicitar a correção dos dados que estão incorretos ou desatualizados;

- direito ao esquecimento (artigo 17) - o titular pode pedir para que os dados sejam excluídos, nas situações em que os dados já não são necessários, alterar o consentimento anterior ou quando existir tratamento ilícito;

- direito à limitação do tratamento (artigo 18) - o titular opta por solicitar a restrição ao tratamento dos dados ao invés da sua eliminação;

- direito à portabilidade dos dados (artigo 20) - o titular pode solicitar que os seus dados lhe sejam fornecidos em formato estruturado digitalmente legível e que sejam transmitidos a outro responsável pelo tratamento;

- direito de oposição (artigo 21) - o titular pode opor-se ao tratamento adicional dos dados no contexto do uso e interesse legítimo do controlador;

- direito de não ser submetido a decisões automatizadas (artigo 22) - o titular não pode ser submetido a decisões exclusivamente baseadas em algoritmos e processos automatizados, quando estiver associado a efeitos jurídicos.

Os titulares de dados têm os seguintes deveres:

- fornecer informações verdadeiras - não sendo explicitamente obrigatório no RGPD, implica a perda de direitos em caso de litígio;

- exercer os direitos com boa-fé - o uso abusivo dos direitos pode implicar a limitação do uso dos mesmos;

- proteção individual de informação e dispositivos - o titular deve evitar comportamentos que coloquem em risco os seus dados pessoais.

O RGPD apresenta um conjunto de obrigações para os controladores e operadores de dados. Em resumo, os controladores de dados têm as seguintes obrigações:

- princípio de tratamento dos dados (artigo 5) - o controlador deve garantir o tratamento lícito, leal e transparente, recolhendo somente os dados necessários para fins específicos, explícitos e legítimos; os dados devem ser mantidos pelo tempo necessário, garantir que são exatos e permanecem atualizados; garantir a sua segurança e confidencialidade;

- tratamento com base legal (artigo 6) - o tratamento deve ser feito com base legal, com base em consentimento do titular, cumprimento de obrigação legal ou interesse legítimo;

- garantir os direitos dos titulares (artigos 12 a 22) - garantir os direitos dos titulares dos dados pessoais anteriormente mencionados;

- transparência e informação (artigos 13 e 14) - o titular deve ser informado de quem é o controlador, a finalidade e a base legal do tratamento, e os eventuais operadores de dados externos;

- segurança dos dados (artigo 32) - devem ser adotadas medidas técnicas organizativas na proteção dos dados (confidencialidade, integridade e disponibilidade);

- notificação de violações de dados (artigos 33 e 34) - proceder à comunicação de incidentes à autoridade local (em Portugal, a CNPD em até 72 horas após conhecimento da violação; informar os titulares se estiverem em risco os seus direitos;

- realizar Avaliação de Impacto de Proteção de Dados (sigla em inglês, DPIA) - realizar a avaliação em caso de tratamentos com elevado risco, como os que envolvem dados sensíveis ou são efetuados sistematicamente e em larga escala;

- formalizar contratos e monitorizar operadores (artigo 28) - devem existir contratos escritos entre controlador e operador, bem como monitorização contínua de que estão a ser cumpridas as orientações do tratamento;

- nomear EPD, quando exigido (artigo 37) - nomear o responsável de supervisão do cumprimento dos dispostos no RGPD no controlador e nos operadores, nos casos previstos.

No caso dos operadores, estes devem:

- ajudar o controlador a cumprir com as obrigações legais do regulamento, nomeadamente nas respostas aos pedidos dos titulares dos dados, avaliação de impacto e notificações de violação;

- não subcontratar o tratamento a terceiros sem autorização do controlador (artigo 28), quando a empresa tem mais de 250 funcionários ou quando trata dados sensíveis;

- devolver e eliminar os dados findo o contrato com o controlador (artigo 28)
- seguir estritamente as instruções do controlador (artigo 29) - só lhe é permitido o que o controlador autorizar;
- manter o registo da atividade do tratamento (artigo 30);
- garantir a segurança dos dados (artigo 32).

2.7. ISO/IEC 27001:2022 - SISTEMAS DE GESTÃO DE SEGURANÇA DE INFORMAÇÃO

No âmbito da implementação e gestão de Sistema de Gestão de Segurança da Informação (SGSI), destaca-se, no contexto empresarial português, a norma ISO/IEC 27001:2022, desenvolvida e mantida pela ISO em colaboração com a IEC. Esta norma integra a série ISO/IEC 27000, dedicada aos sistemas de gestão da segurança da informação, cuja versão mais recente foi publicada em 2022 (ISO/IEC, 2022).

As orientações práticas relativas ao estabelecimento de um SGSI encontram-se complementadas por outros documentos da mesma série, designadamente a ISO/IEC 27002:2022, que apresenta, de forma detalhada e aplicável, os controlos de segurança recomendados. Os documentos da série 27000 apresentam uma estrutura modular e interdependente, permitindo dar resposta a requisitos legais, regulamentares e setoriais, tanto de carácter geral como específico. As revisões periódicas destes documentos asseguram a atualização dos controlos de segurança, de modo a refletir as necessidades emergentes.

De forma mais específica, a ISO/IEC 27001:2022 organiza o ciclo de vida de um SGSI em quatro etapas fundamentais: estabelecer, implementar, manter e melhorar.

Estes controlos de segurança estão listados num anexo da norma, designado por “Anexo A”, constituindo uma referência para a seleção e aplicação das medidas de segurança mais adequadas ao perfil de risco de cada organização.

Os controlos estão organizados por grupos, existindo:

- 37 controlos organizacionais, com enfoque em políticas, processos e responsabilidades gerais, onde se incluem a conformidade legal, a gestão de ativos e a relação com terceiros;

- 8 controlos de pessoas, com enfoque na segurança de recursos humanos, desde a sua contratação até à sua saída, incluindo trabalho remoto, formação e responsabilidades de confidencialidade;
- 14 controlos físicos, com enfoque na proteção de instalações e equipamentos contra ameaças físicas;
- 34 controlos tecnológicos, com enfoque em medidas de controlo de acesso, criptografia, proteção contra aplicações maliciosas e segurança das redes informáticas.

No contexto do setor da saúde podem ser implementadas orientações complementares, tais como:

- ISO 27799 - Segurança da informação na área da saúde;
- ISO/IEC 27701 - Extensão para a gestão da privacidade (SGPI);
- ISO/TS 81001-1 - Segurança, eficácia e proteção de *software* e sistemas informáticos em saúde.

Como o perímetro de análise da segurança deste trabalho se restringe aos sistemas internos da organização e os sistemas externos são somente encarados como "produtores" e "consumidores" de dados, os documentos ISO/IEC 27017 (segurança de informação de sistemas na nuvem) e ISO/IEC 27018 (proteção de dados pessoais em sistemas de nuvem pública) não serão considerados.

2.8. ISO/IEC 27701:2019 - GESTÃO DA PRIVACIDADE DA INFORMAÇÃO

Enquanto a ISO/IEC 27001 contém os requisitos para o estabelecimento de um SGSI e a ISO/IEC 27002 contém os detalhes dos controlos para cumprir os requisitos, existem outros documentos que estendem os requisitos originais, cumprindo objetivos específicos. No contexto do setor da saúde pode-se destacar a ISO/IEC 27701, que aborda os Sistemas de Gestão de Privacidade de Informação (SGPI) (em inglês, *Privacy Information Management System* (PIMS)), com o intuito de endereçar os requisitos dos diversos regulamentos de proteção de dados pessoais, como o RGPD (ISO/IEC, 2019).

A ISO/IEC 27701 menciona as adaptações dos controlos especificados na ISO/IEC 27002 para o contexto da privacidade e proteção de dados pessoais, a avaliação dos riscos de privacidade, políticas integradas de privacidade e segurança de informação, bem como a definição de funções e responsabilidades específicas na proteção de dados pessoais.

A estrutura desta norma contém cláusulas com os requisitos e orientações centrais, os requisitos para a adoção de um SGPI baseados nesta norma, as orientações e adaptações aos controlos mencionados ISO/IEC 27002 e os controlos adicionais específicos para os controladores e processadores de dados pessoais.

Nos Anexos A e B da norma constam os objetivos de controlo e controlos SGPI específicos para controladores e processadores de PII.

2.9. ISO 27799:2016 - GESTÃO DA SEGURANÇA DA INFORMAÇÃO NA INFORMÁTICA MÉDICA

A ISO 27799 é uma extensão da ISO/IEC 27001 e ISO/IEC 27002 para a área da saúde (Thales Group, 2024) (ISO, 2016). Providencia orientações para a segurança da informação neste setor específico, com foco na proteção de dados de saúde de pacientes (considerados como dados sensíveis pelo RGPD) e alinhado com leis e regulamentos (por exemplo, a *Health Insurance Portability and Accountability Act* (HIPAA), aplicada nos Estados Unidos da América (EUA).

Os requisitos e controlos específicos estão orientados para:

- descoberta e classificação de dados confidenciais dentro da organização, promovendo a digitalização dos dados, para monitorização e proteção mais apropriadas;
- gestão e monitorização de acessos privilegiados a dados;
- aplicação de técnicas de criptografia e de anonimização / pseudonimização de dados em processamento (em "trânsito") ou arquivados (em "repouso");
- gestão centralizada e seguro das chaves de criptografia;
- proteção dos dados através do registo do acesso a dados para deteção de ações irregulares.

A ISO 27799 serve de ponte entre documentos gerais e específicos da área da saúde.

2.10. ISO 81001-1:2021 - SEGURANÇA, EFICÁCIA E PROTEÇÃO DE *SOFTWARE* E SISTEMAS INFORMÁTICOS EM SAÚDE

A ISO 81001-1:2021 integra uma família de documentos normativos dedicada à segurança (*safety*), eficácia e proteção (*security*) do *software* e dos sistemas de tecnologias de informação na área da saúde. Destina-se "a organizações e pessoas que criam, adquirem, operam, mantêm, utilizam ou desativam *software* e sistemas de TI na área da saúde (incluindo dispositivos médicos), sendo aplicável a todas as organizações envolvidas, independentemente da sua dimensão, complexidade ou modelo de negócio" (ISO, 2025).

Os três pilares fundamentais da norma são:

1. segurança - para evitar danos ao paciente, técnicos e operadores de sistemas médicos;
2. eficácia - para alcançar os resultados clínicos desejados para o procedimento;
3. segurança - proteger de acessos indesejados os dados e sistemas médicos.

A adoção da ISO 81001-1:2021 é de carácter voluntário, embora o seu cumprimento seja fortemente recomendado para organizações que desenvolvem, adquirem ou operam *software* e sistemas de TI na área da saúde. A adesão a esta norma evidencia uma predisposição organizacional para a melhoria contínua, bem como o compromisso de integrar a gestão da segurança e da privacidade da informação com os processos operacionais do setor da saúde .

2.11. *HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT*

Para além das normas e *frameworks* de segurança de informação e cibersegurança já abordadas, pelas quais as organizações se podem certificar, existem outras *frameworks* e certificações específicas para o setor da saúde. A HIPAA, lei aprovada em 1996 nos EUA, é tida como referência por diversos motivos, entre os quais: por ter sido precursora no estabelecimento de padrões de proteção de privacidade e segurança da informação na saúde das pessoas, por ter um grande mercado interno de consumo de equipamentos médicos e por ser um dos principais fabricantes e exportadores de equipamentos médicos. Esta lei aplica-se a hospitais, clínicas e seguradoras que processam dados médicos nos EUA (Blobel, 2007).

No âmbito da proteção de dados pessoais de saúde, a HIPAA define:

- regras de privacidade - quem pode aceder e em que situações o pode fazer;
- regras de segurança - quais são os requisitos técnicos e administrativos para proteger os dados em formato digital;
- regras de notificação de exfiltração[3] de dados - obrigação de notificar os pacientes e autoridades no caso de apropriação ilegítima de dados pessoais.

O tratamento dos dados pessoais é explicitamente autorizado em atividades de tratamento médico, processos administrativos e de faturação de serviços. Outros tipos de tratamento requerem autorização do titular dos dados pessoais.

O titular dos dados pessoais tem o direito de aceder e solicitar cópia dos seus registos médicos, solicitar correções dos dados pessoais e obter histórico de acesso aos mesmos.

2.12. TIPOS E GRUPOS DE UTILIZADORES

Para uma correta aplicação da cibersegurança na organização, é relevante identificar e agrupar os utilizadores pelas seguintes funções no fluxo de informação:

- pacientes, as pessoas que são submetidas a exames médicos;
- médicos, que acedem e analisam os dados obtidos pelas modalidades (tipos de exame) e produzem relatórios com o diagnóstico;
- técnicos, que auxiliam o trabalho dos médicos na aquisição de dados para diagnóstico;
- gestores, têm apenas acesso a dados demográficos do paciente, para fins de gestão e administrativos;
- diretor clínico, têm acesso aos dados de diagnóstico do paciente em contexto específico;
- administrativos / auxiliares, que inserem os dados de admissão dos pacientes;

[3] Exfiltração de dados (*data exfiltration*) é o ato de transferir dados de um sistema ou organização, sem ter autorização para tal, para um destino externo, normalmente de forma intencional. Pode ser feita através de vários métodos, como envio por correio eletrónico, cópia para dispositivos externos ou computadores pessoais, ou através de comunicações encriptadas criadas para o efeito. A exfiltração pode envolver dados pessoais sensíveis, propriedade intelectual ou informação estratégica (IBM, n.d.).

- administradores de sistema, que geram o sistema informático e têm acesso à infraestrutura informáticos, sistemas de processamento e aos dados (o acesso aos dados é feito num contexto de resolução de problemas, requerendo justificação).

O paciente é o detentor dos dados pessoais sensíveis, usufruindo de todos os direitos e deveres definidos pelo RGPD e pela legislação conexa. Os médicos têm acesso a dados de estudos anteriores, com privilégio de leitura. Os técnicos têm acesso de escrita e leitura ao estudo atual, enquanto autores da recolha de dados para diagnóstico. Os administrativos e auxiliares têm somente acesso a dados demográficos, com acesso de escrita e leitura para confirmação e correção. Os administradores de sistema têm acesso aos dados para fins técnicos, sem permissão para manipulação de dados em ficheiros e bases de dados. Os restantes utilizadores não têm acesso aos dados pessoais sensíveis.

2.13. REDE DE INFORMÁTICA MÉDICA

A Figura 6 apresenta um diagrama ilustrativo de uma rede informática médica de carácter genérico, no qual se encontram igualmente identificados pontos específicos de acesso remoto à informação armazenada no perímetro da organização.

As funções genéricas dos dispositivos dentro do perímetro da organização são:

- equipamentos de rede (*Switch* / *Router* / *Firewall*) - asseguram a comunicação informática com segregação e controlo de fluxos entre dispositivos e redes (rede local e Internet);

- servidor controlador de domínio - garantir a gestão de identidades, dispositivos e políticas de segurança;

- servidor *Radiology Information System* (RIS) - sistema de informação radiológica para gestão administrativa dos exames, com informação demográfica (utentes, médicos, técnicos e administrativos), exames (obtenção de prescrições, agendamento de exames) e resultados de diagnóstico. Através de serviços de interoperabilidade, podem também disponibilizar informação para equipamentos médicos em formatos *Digital Imaging and Communications in Medicine* (DICOM) e *Health Level Seven (*HL7);

- servidor de ficheiros - armazenamento local de relatórios médicos;

- servidor web - disponibilização de serviços e informação para serviços externos (por exemplo, para envio e receção de pedidos tendo como interlocutor sistemas do SPMS);
- estação de trabalho administrativo - entrada, processamento e saída de dados presentes no RIS (dados demográficos, exames e relatórios médicos);
- equipamento médico - aquisição de dados para diagnóstico;
- estação de trabalho técnico radiologista - tratamento de dados adquiridos por dispositivo médico;
- estação de trabalho médico - acesso a imagens médicas (obtidas no contexto do exame atual ou anteriores) e dados demográficos para diagnóstico e produção do relatório médico.

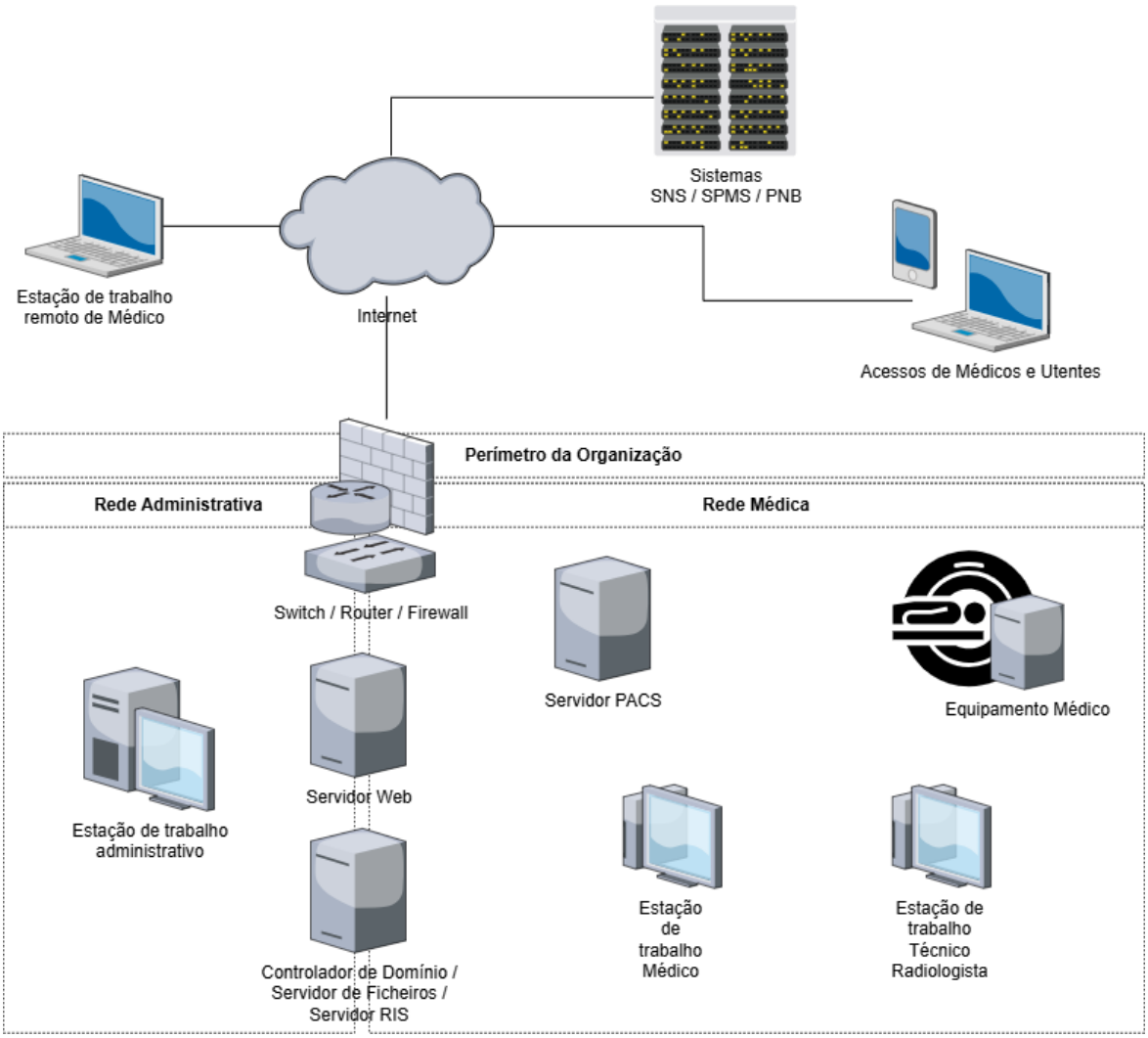


Figura 6 - Diagrama de rede médica

As funções genéricas dos dispositivos fora do perímetro da organização são:

- sistemas de intermediação de dados da SPMS, nomeadamente o PNB, para encaminhamento de pedidos entre sistemas informáticos do SNS e prestadores de MCDT;
- estação de trabalho remoto do médico - acesso a imagens médicas e dados demográficos para diagnóstico e produção (ou revisão) do relatório médico;
- estação de trabalho de médico de família - acesso ao relatório de diagnóstico;
- equipamentos informáticos do utente, como aplicações para dispositivos móveis, para acesso a prescrições e relatórios de diagnóstico médico.

2.14. PROTOCOLOS DE COMUNICAÇÃO

Para além dos protocolos de comunicação informáticos comummente presentes numa rede informática, existem protocolos específicos para a comunicação de dados de saúde entre sistemas e equipamentos médicos. A utilização destes protocolos não se circunscreve ao perímetro da organização, mas são também utilizados para comunicação de informação com sistemas exteriores (como, por exemplo, o PNB). Nas subsecções seguintes são apresentados os protocolos mais relevantes para o âmbito deste trabalho.

2.14.1. *Health Level 7*

A *Health Level 7 International* (HL7) é uma organização sem fins lucrativos e mantém um conjunto de normas e protocolos para troca, integração, partilha e recuperação de informação médica em formato eletrónico (HL7 International, 2025). A normalização melhora a comunicação entre sistemas e equipamentos médicos de diferentes fabricantes, ao invés do uso de soluções proprietárias.

Os padrões HL7 mais utilizados no momento são HL7 v2.x, HL7 v3, *Clinical Document Architecture* (CDA) e FHIR. A primeira versão do HL7 v2.x surgiu em 1989 e é amplamente utilizado na troca de informação entre sistemas médicos e laboratoriais. As várias versões mantêm retro-compatibilidade entre elas, permitindo que coexistam num sistema informático médico (HL7 International, 2025). Baseia-se em mensagens de texto padronizadas de estrutura fixa. A informação é separada por *pipe* (|) e cada segmento da mensagem começa com um identificador de três letras (*Message Code*), ao qual pode acrescer um código de dois a três caracteres separado por acento circunflexo (), com o

evento de gatilho (que indica situação ou ação específica) (Figura 7) (Castro, Domingo, Colomé, & Estévez, 2011) (Surety Systems , 2023) (HL7 International, 2025).

Como principais segmentos são:

- MSH (*Message Header*);
- MSH-9 (*Message Type*) que está contido no MSH;
- ADT (*Admit, Discharge, Transfer*) para mensagens administrativas com dados de pacientes: ADT^A01 - admissão de paciente; ADT^A08 - atualização de informações do paciente;
- ORM (*Order Message*) para ordens ou pedidos de exames e procedimentos: ORM^O01 para pedido de exame ou procedimento;
- ORU (*Observation Result*) para mensagens de resultados de exames: ORU^R01 - resultado de exame;
- DFT (*Detailed Financial Transaction*) para mensagens de transações financeiras;
- SIU (*Scheduling Information Unsolicited*) para mensagens de agendamento: SIU^S12 - agendamento de consulta ou procedimento;
- MDM (*Medical Document Management*) para gestão de documentos clínicos: MDM^T02 - envio de relatório médico
- QRY RSP (*Query Response*) - mensagens de pedido de consulta e resposta ao pedido: QRY^A19 - consulta por paciente; RSP^K21 - resposta à consulta.

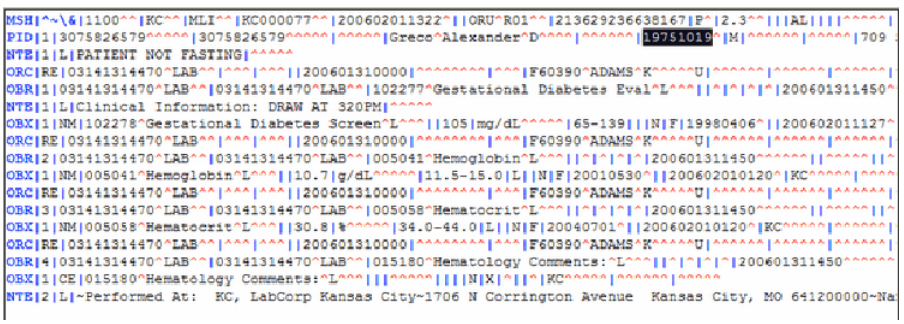


Figura 7 - Exemplo de mensagem HL7 v2.x

Recorre-se normalmente ao protocolo de comunicação *Minimal Lower Layer Protocol* (MLLP), protocolo de aplicação (camada 7 do modelo OSI), que encapsula a mensagem de texto recorrendo a delimitadores (0x0B no início da mensagem, 0x1C 0x0D no fim da

mensagem) a ser enviado através de *Transport Communication Protocol* (TCP)/IP *sockets*, usando a porta TCP 2575 por omissão.

Recorre a mensagens de confirmação (em inglês, *Acknowledgement* (ACK)):

- *Acknowledgement Accept* ("AA"), correspondente ao "ACK" do TCP/IP, no caso da mensagem ter sido corretamente processada;
- *Application Error* ("AE"), correspondente a "NACK" do TCP/IP, caso ocorra erro, com retorno da mensagem de erro.

Este protocolo não implementa controlo de rede nem segurança. A segurança terá de ser implementada recorrendo a outros protocolos de rede que possam encapsular os dados em trânsito entre os sistemas envolvidos (por exemplo, utilizando *Virtual Local Area Network* (VLAN), *Transport Layer Security* (TLS) sobre TCP ou *Virtual Private Network* (VPN)).

A versão 3 deste protocolo é uma evolução do padrão anterior, com adoção limitada. Tem por base um modelo de referência informativa (*Reference Informational Model* (RIM)), que torna a estrutura mais rígida e um maior rigor formal, com uma estrutura semântica mais consistente. As mensagens usam o formato XML e estão divididas em três partes:

1. *message wrapper*, que contém informações sobre o remetente, destinatário e detalhes de interação;
2. *control wrapper*, que contém o evento de gatilho, com as respetivas situações ou ações;
3. *domain payload*, que contém os dados demográficos ou de resultados que se pretendem transmitir.

O CDA é um padrão para codificação, formatação e estruturação de documentos clínicos baseado em XML, com vista a facilitar a interoperabilidade e troca de informação médica. São usados modelos de referência para tipos de documentos específicos. Estes documentos podem ser utilizados para troca de dados de saúde (*Eletronic Health Records* (EHR)) entre sistemas informáticos internos, bem como entre entidades externas privadas (por exemplo, outros prestadores de MCDT) ou públicas (por exemplo, organismos que gerem as iniciativas de saúde pública) (Health Level Seven International - CDA, 2025).

O padrão FHIR distingue-se dos anteriores por se basear em tecnologias web, nomeadamente XML e *Java Object Notation* (JSON) e APIs REST, que melhoram a

agilidade, segurança e troca de informação entre sistemas informáticos internos e externos à instituição. Em concreto, podem ser utilizados os mecanismos de segurança de comunicação associados ao protocolo *HyperText Transport Portocol Secure* (HTTPS) (Health Level Seven International - FHIR, 2023).

A estrutura é modular e organizada em recursos, presente na Figura 8 (Zamani Forooshani, 2020). Os recursos agrupam dados específicos (por exemplo, paciente, médico) e podem ser combinados numa única mensagem. Os formatos das mensagens são previamente definidos para permitir a interoperabilidade entre sistemas de comunicação. O conteúdo da mensagem é alfanumérico, permitindo a interoperabilidade semântica em alguns campos através da integração de terminologias médicas, como SNOMED CT e LOINC (MediCollector, 2025).


```
{
   "name": [{ "use": "official", "text": "Sarah", "family": ["Bor"], "given": ["Sarah Olaf"]}],
   "gender": { "coding": [{ "system": "http://hl7.org/fhir/v3/AdministrativeGender", "code": "F",
"display": "Female" }] },
   "telecom": [{ "system": "phone", "value": "+31612345678", "use": "mobile" },
         {"system": "phone",  "value": "+31201234567", "use": "home" }],
   "birthDate": "1960-03-13",
   "address": [{ "use": "home", "line": ["Bos en Lommerplein 280"], "city": "Amsterdam", "zip":
"1055RW", "country": "NLD" }],
   "managingOrganization": { "reference": "Organization/1", "display": "Burgers University Medical
Centre" },
   "active": true
}
```


Figura 8 - Exemplo de mensagem HL7 FHIR

Este padrão é utilizado na troca de mensagens entre as entidades prestadoras de MCDT e as plataformas dos SPMS, como por exemplo no âmbito do projeto "Exames sem Papel".

2.14.2. *Digital Imaging and Communications in Medicine*

O *Digital Imaging and Communications in Medicine* (DICOM) é o padrão internacional para armazenamento, transmissão e partilha de imagens médicas e informação clínica associada. Embora seja frequentemente utilizado em conjunto com o HL7 (padrão dedicado à troca de dados clínicos e administrativos), os dois são normas independentes com propósitos complementares, existindo em ambos serviços com funcionalidades sobreponíveis em determinados contextos (PostDICOM, n.d.) (NEMA, 2025).

Os protocolos DICOM operam na camada de aplicação e utilizam normalmente *TCP/IP* para comunicar (portas 104 e 11112). Ao nível da segurança, podem ser implementados diversos mecanismos de segurança:

1. assegurar que a comunicação só ocorra caso o serviço que solicita o serviço (*Service Class User* (SCU), ou seja, o cliente) esteja autorizado pelo serviço que responde ou fornece aos dados (*Service Class Provider* (SCP), ou seja, o servidor);

2. comunicação cifrada recorrendo a TLS, proposta na especificação DICOM *Part Section* (PS) 3.15, *Security and System Management Profiles*, define perfis de segurança para: cifra de dados em arquivo, integridade atestada por assinatura digital, regras para partilha segura de dados, auditoria de transmissão de dados, anominimzação/pseudonomização de dados, entre outros (NEMA, 2025).

O *DICOM Message Service Element* (DIMSE) é a camada de mensagens de DICOM e define um conjunto de métodos de comunicação entre aplicações e dispositivos médicos (por exemplo, *Picture Archiving and Communication System* (PACS), estações de trabalho, modalidades de imagem médica e sistemas de informação).

O DIMSE está dividido em dois tipos de serviços, em função do tipo de operação e objetos. Para objetos compostos, como imagens ou relatórios, são utilizados os seguintes métodos:

- C-STORE, para enviar um objeto DICOM, como no envio de imagens de equipamentos para o PACS;
- C-FIND, para consulta de informação numa fonte de dados;
- C-MOVE, para que objetos sejam movidos de um servidor para outro destino;
- C-GET, para obter imagens (idêntico ao C-MOVE, mas retorna os dados na mesma associação DICOM);
- C-ECHO, para testar a conectividade com um dispositivo ou serviço DICOM.

Para objetos normalizados, com estruturas predefinidas, relacionadas com comunicações em fluxos de trabalho, existem os seguintes métodos:

- N-CREATE, para criar um objeto;
- N-SET, para modificar atributos de um objeto já existente;
- N-GET, para obter os atributos de um objeto;

- N-ACTION, para executar uma ação num objeto;
- N-EVENT-REPORT, para notificação de eventos.

Em função do tipo de operação (obter, modificar, transferir ou eliminar) e do serviço requerido, os mecanismos de segurança nativos do DICOM devem ser complementados por controlos genéricos de segurança informática, como autenticação por identidade do utilizador, controlo de acesso baseado em funções, registos de auditoria e VPN.

Os serviços relevantes para este projeto foram: 1) pesquisa de dados (por exemplo, obter lista de trabalho e exames arquivados); e 2) envio e recuperação de dados do PACS.

2.15. MAPEAMENTO ENTRE REQUISITOS DE PROTEÇÃO DE INFORMAÇÃO, REGULAMENTOS E *FRAMEWORKS* DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

No Anexo A apresenta-se um resumo dos regulamentos, *frameworks* de segurança de informação e cibersegurança, com os principais requisitos de cibersegurança definidos para este projeto e requisitos conexos. No mapeamento apresentado são mencionadas cinco categorias de requisitos: controlo de acessos; registo e auditoria; notificação e resposta a incidentes; proteção de dados e minimização; cadeia de abastecimento e continuidade.

Este mapeamento serve de base aos requisitos funcionais da plataforma e para a seleção dos componentes a incluir na arquitetura de suporte.

3. ESTADO DA ARTE

A pesquisa de trabalho relacionado foi orientada para o estudo de diversos fatores associados à gestão da cibersegurança em entidades de saúde, abrangendo tanto dimensões técnicas como organizacionais. Neste contexto, foram analisados estudos relevantes sobre cibersegurança no setor da saúde (Secção 3.1), bem como sistemas informáticos genéricos com funcionalidades semelhantes disponíveis no mercado (Secção 3.2). Adicionalmente, foram considerados sistemas específicos da área da informática médica, nomeadamente soluções para controlo e auditoria de acessos, roteamento, transformação e integração de fluxos de dados, bem como plataformas de monitorização centralizada (Secção 3.3).

3.1. REVISÃO DE LITERATURA

A cultura da cibersegurança de várias organizações do setor da saúde geograficamente distintas, com diferentes dimensões, é abordada em (Gioulekas, et al., 2022). Os autores salientam a importância de identificar, classificar e abordar vulnerabilidades e fraquezas de cibersegurança.

Embora a ENISA mencione no relatório "*Threat Landscape Report 2018: 15 Top Cyberthreats and Trends*" publicado em 2019 que o setor da saúde representa 27% dos ataques cibernéticos, Gioulekas et al. referem no seu estudo que se desconhece o número real efetivo de ataques, porque algumas entidades não têm noção de que foram alvo de um ciberataque. Estes ataques informáticos implicam perda e exfiltracão de dados de pacientes, bem como disrupção e indisponibilidade de sistemas de informação (ENISA, 2019).

Gioulekas et al. (2022) identificaram, até à data do seu estudo, que a maior ameaça à privacidade e segurança das entidades de saúde advém do seu próprio pessoal. É identificado o erro humano como a causa mais comum para os incidentes de segurança, motivados por falta de cultura em cibersegurança, consciencialização, negligência ou malícia dos funcionários. No relatório da ENISA de 2018, 50,6% das entidades identificaram estas ameaças internas como o seu adversário mais sério, fruto da falta de cultura de cibersegurança.

No relatório da ENISA com dados até 2024, *Threat Landscape 2024* (European Union Agency for Cybersecurity, 2024), a ENISA salienta que no setor da saúde ocorreu um decremento de casos de *ransomware* (45% face a 54% registado entre 2021 e 2023), um

aumento na ocorrência e comunicação de incidentes significativos (309 casos) e um crescimento das violações de dados (28%). Neste relatório também foi sinalizada a diversidade do tipo de ameaças.

A cultura de cibersegurança de uma entidade resulta da combinação de atitudes, comportamentos, conhecimento e consciência de todas as pessoas da organização perante riscos e ameaças. A avaliação pode incluir auditorias de infraestrutura e de políticas de segurança, culminando em ações de sensibilização e formação, para melhorar o senso de responsabilidade das pessoas que utilizam os sistemas informáticos e processam informação.

Em países com baixos orçamentos para o setor da saúde, como Portugal, Grécia e Roménia, Gioulekas et al. mencionam que a percentagem reservada para cibersegurança do orçamento geral para tecnologias de informação é baixa (cerca de 10%), comparativamente a países da América do Norte, norte e centro da Europa (Gioulekas, et al., 2022).

É relevante destacar as vertentes individuais e organizacionais na cultura de cibersegurança. A *"Cybersecurity Culture Framework"*, desenvolvido em 2019 no contexto do projeto *"EnergyShiled"* da UE direcionado à cibersegurança no setor da energia, é uma metodologia de avaliação da cultura em cibersegurança nas organizações. Esta *"framework"* combina diversos fatores organizacionais (ativos, continuidade, acesso e confiança, operações, defesa e governação de segurança) e individuais (atitude, sensibilização, atitudes e competência) e facilita a avaliação de políticas e procedimentos de segurança organizacional, juntamente com as características, comportamentos, atitudes e habilidades dos funcionários. Deste modo é possível aferir o nível de maturidade dos responsáveis pela gestão e operação da infraestrutura tecnológica, bem como dos utilizadores em geral, de uma determinada instituição. A perceção da importância da cibersegurança numa organização é a base para a instauração e manutenção de políticas e medidas orientadas para a proteção de dados, sistemas, pessoas e processos de negócio (Georgiadou, Mouzakitis, Bounas, & Askounis, 2020).

Portugal não é exceção ao panorama internacional no que respeita às ameaças de cibersegurança no setor da saúde. De acordo com o Relatório "Cibersegurança em Portugal - Riscos & Conflitos" (5.ª edição), publicado pelo CNCS em 2024, o setor da saúde foi o terceiro mais afetado em 2023, representando 8% do total de incidentes registados pelo CERT.PT, apenas superado pelos Prestadores de Serviços de Internet (26%) e pela Banca (10%). O mesmo relatório regista um aumento de 106% nos incidentes de cibercrime neste setor face ao ano anterior, totalizando 107 ocorrências (CNCS, 2024).

No que concerne aos requisitos de proteção de dados, são obrigatórios a encriptação de dados sensíveis, controlo de acessos, auditoria de acessos, gestão dos consentimentos dos utentes e supervisão por entidades europeias da transferência de dados para países fora da UE. Como menciona Gonçalves, a interoperabilidade de dados na saúde com o desiderato de melhorar a eficiência dos dados de saúde sincronizados entre sistemas aumenta a complexidade na proteção (Gonçalves, 2025).

Conhecidos os riscos e desafios do setor da saúde, o foco volta-se para a busca de uma metodologia integrada de cibersegurança e ferramentas de suporte para sistemas de informação que possa ser utilizada no setor da saúde. Os sistemas médicos são caracterizados por um conjunto de plataformas que normalmente se encontram interligadas entre si: sistema de informação médica (*Radiological Information System* (RIS), *Hospital Information System* (HIS), ou *Clinical Information System* (CIS)), sistema de consulta e arquivamento de imagens (PACS), DICOM *Storage*), serviços de informação entre equipamentos (DICOM *Worklist*, DICOM *Print*, HL7). Como proposto por Coutinho et al. (2023), ao ecossistema devem estar associados sistemas de deteção e prevenção de intrusões (*Intrusion Detection System* (IDS)/ *Intrusion Prevention System* (IPS)), gerenciamento de eventos e informações de segurança (*Security Information and Event Management* (SIEM)), tratamento e resolução de incidentes (por exemplo, através de sistemas *Security orchestration, automation, and response* (SOAR)), proteção contra perda de dados (*Data Loss Prevention* (DLP)). Deste modo é possível automatizar todas as fases do ciclo de vida da resposta a incidentes no contexto de ciberataques (identificar, proteger, detetar, responder, recuperar) (Coutinho, Ferreira, Yevseyeva, & Basto-Fernandes, 2023).

A *"All-in-one Cybersecurity Methodology"* proposta assenta em sete etapas: 1) Definição dos sistemas a serem integrados; 2) Integração dos sistemas na plataforma de monitorização (SIEM); 3) Definição de casos de usos e ajuste de regras; 4) Criação de incidentes de segurança de informação; 5) Definição do procedimento de resolução de incidentes; 6) Resolução de incidentes; e 7) Acompanhamento (Coutinho, Ferreira, Yevseyeva, & Basto-Fernandes, 2023).

Os controlos de segurança devem incidir, sobretudo, sobre os sistemas de suporte e os protocolos de imagem médica, como o DICOM e o HL7. A sua implementação tem um impacto positivo ao nível da Governação, Risco e Conformidade (GRC), ao contribuir para: 1) o reforço da governação e a melhoria dos processos; 2) o cumprimento normativo, nomeadamente através da *NIST Cybersecurity Framework* e da série de publicações NIST SP 800; e 3) a gestão do risco (Coutinho, Ferreira, Yevseyeva, & Basto-Fernandes, 2023).

A expansão da superfície de ataque que ocorre por via de proliferação de dispositivos médicos ligados em rede é também identificada como um crescente problema da cibersegurança no setor da saúde (Ahmed, Naqvi, & Josephs, 2019). As quatro dimensões identificadas são: 1) infraestrutura envelhecida, com a existência de sistemas legados por longos períodos; 2) dispositivos médicos cada vez mais conectados à Internet e historicamente desenvolvidos sem preocupações de cibersegurança; 3) baixa cultura de cibersegurança, como a utilização de palavras-passe fracas, e resistência a controlos adicionais; e 4) o cumprimento de requisitos legais e regulamentares (RGPD). Neste sentido, é relevante a adição de um conjunto de métricas de cibersegurança: Indicadores de Comprometimento (IOC), Indicadores de Ataque (IOA), Avaliação de Risco, Testes de Intrusão (*Penetration Testing*), Avaliação de Vulnerabilidades, Equipas de Ataque e Defesa (*Red and Blue Teaming*) e Resiliência e Defesa Baseada em Inteligência de Ameaças. Estas métricas visam permitir às organizações de saúde quantificar o seu estado de segurança, apoiar a tomada de decisão por parte dos gestores e reforçar proactivamente as defesas dos seus sistemas de informação. Embora as métricas propostas sejam aplicáveis a qualquer setor, o seu impacto será particularmente relevante na área da saúde, dada a complexidade dos ambientes tecnológicos, a elevada sensibilidade dos dados geridos e as implicações diretas que as falhas de segurança podem ter na segurança dos doentes.

Os recursos humanos e tecnológicos mobilizados para a preservação da confidencialidade, integridade e disponibilidade dos sistemas e dados médicos estão diretamente dependentes da capacidade financeira das organizações e da consciencialização das administrações para a sua importância.

Os sistemas de informação médica são sistemas informáticos críticos, sobretudo por: primeiramente, porque é vital estarem operacionais para auxiliar na prestação de cuidados de saúde; porque operam com dados sensíveis que podem colocar em risco os direitos e garantias dos seus detentores; o elevado custo de aquisição, operação e manutenção dos equipamentos médicos (*hardware* e *software*), que requerem recursos humanos com conhecimentos técnicos específicos.

3.2. SISTEMAS INFORMÁTICOS AUXILIARES

Seguidamente são apresentados alguns dos tipos de *software* que podem agregar valor à cadeia de proteção de dados num sistema informático médico. Na Secção 3.2.1 é abordada a gestão de identidades e acessos. Na Secção 3.2.2 são abordados os sistemas de deteção e prevenção de intrusões. Também associados à deteção de intrusões e

prevenção de incidentes, abordam-se na Secção 3.2.3 os sistemas de deteção e resposta a incidentes. Os sistemas de gestão de eventos e informação de cibersegurança abordam-se na Secção 3.2.4, a orquestração e automatização na Secção 3.2.5 e a prevenção de perda ou roubo de dados na Secção 3.2.6

3.2.1. *Identity and Access Management*

De modo a garantir a gestão de identidade e acessos, desde a criação, autenticação, autorização e auditoria de identidades e respetivas ações, podem ser implementados tecnologias e procedimentos dentro da organização. Deve ser proporcionado acesso a sistemas e informação pelas pessoas autorizadas e negado às restantes.

Um Sistema de Gestão de Identidades e Acessos (conhecido como *IDentity Management* (IDM) ou *Identiy and Access Management* (IAM)) endereça as seguintes necessidades (IBM Corporation, 2025):

- gerir o ciclo de vida da identidade digital dos utilizadores (internos e externos) que se ligam ao sistema informático da organização, através da criação de contas de utilizador, atribuição e modificação de permissões, bem como a desativação e eliminação de contas;
- autenticar o utilizador, através de métodos com um ou vários fatores de autenticação, de modo a garantir a legitimidade do acesso;
- autorizar o acesso aos recursos pelos utilizadores com esse direito e negar o acesso aos restantes utilizadores;
- rastrear e auditar o acesso a sistemas e recursos, em todas as fases do ciclo de vida de utilização da conta (criação, autenticação, autorização, desativação, eliminação);
- simplificar os métodos de acesso aos sistemas, com recursos a autenticação federada ou de início de sessão único (*Single Sign-On* (SSO)).

Através dos registos providenciados por este tipo de sistema é possível fornecer as evidências para auditorias e cumprir com os requisitos regulatórios.

A definição de políticas de autorização num sistema IAM assenta em modelos de controlo de acesso, intrinsecamente relacionados com granularidade e a flexibilidade das permissões atribuídas. Os modelos mais adotados são o *Role-Based Access Control*

(RBAC), o *Attribute-Based Access Control* (ABAC) e o *Policy-Based Access Control* (PBAC).

No modelo RBAC, as permissões são associadas a papéis (*roles*) e os utilizadores são atribuídos a esses papéis, em vez de receberem permissões diretamente. Esta abordagem simplifica a administração em organizações com estruturas hierárquicas definidas, sendo amplamente utilizada em sistemas de saúde, onde os perfis de acesso são determinados pela função clínica ou administrativa do utilizador – por exemplo, médico, enfermeiro, técnico de diagnóstico ou administrativo (Sandhu, Coyne, Feinstein, & Youman, 1996). O modelo ABAC complementa o RBAC ao avaliar atributos dinâmicos do utilizador, do recurso e do contexto ambiental (por exemplo, o horário de acesso, a localização ou o nível de classificação dos dados), permitindo definir políticas de controlo de acesso mais granulares e adaptáveis (Hu, et al., 2014).

Em ambientes de saúde, a adoção de RBAC é frequentemente exigida por normas regulatórias. A norma HIPAA nos Estados Unidos e o RGPD na União Europeia determinam que o acesso a dados clínicos deve ser limitado ao mínimo necessário para o exercício das funções do utilizador, aplicando o princípio conhecido como *need-to-know* ou *least privilege*.

A autenticação multifator (em inglês, *Multi-Factor Authentication* (MFA)) constitui um mecanismo essencial para reforçar a verificação da identidade dos utilizadores, exigindo a apresentação de dois ou mais fatores de autenticação de categorias distintas: algo que o utilizador sabe (palavra-passe), algo que possui (*token* físico ou aplicação de autenticação) e algo que é (biometria). A adoção de MFA reduz significativamente o risco de comprometimento de contas por roubo de credenciais, sendo reconhecida como uma das medidas de segurança de maior impacto por organismos como o NIST e a ENISA (Grassi, Garcia, & Fenton, 2017).

Outro conceito importante é a federação de identidades, que permite que uma identidade digital estabelecida num domínio seja reconhecida e aceite noutros domínios, sem necessidade de criar credenciais adicionais. Protocolos como o *Security Assertion Markup Language* (SAML 2.0), o *OpenID Connect* (OIDC) e o OAuth 2.0 são os *standards* mais utilizados para implementar federação de identidades e SSO em ambientes empresariais e de saúde (Recordon & Reed, 2006). Em contexto hospitalar, a federação de identidades é particularmente relevante na integração entre sistemas clínicos de diferentes fornecedores, permitindo que um profissional de saúde aceda, com as mesmas credenciais, ao sistema de informação hospitalar (HIS), ao arquivo de imagens médicas (PACS) e a portais externos de referenciação.

Uma componente especializada dos sistemas IAM é o *Privileged Access Management* (PAM), orientado para o controlo, monitorização e auditoria de contas com privilégios elevados, como administradores de sistemas, engenheiros de infraestrutura e contas de serviço. Estas contas representam um vetor de ataque crítico, dado que o seu comprometimento pode conferir ao atacante controlo total sobre sistemas e dados sensíveis (Gartner, 2022). As soluções PAM implementam mecanismos como o acesso *just-in-time* (JIT), em que os privilégios são concedidos temporariamente para uma tarefa específica e revogados no seu término, e o registo de sessões privilegiadas, que permite a gravação e auditoria de todas as ações efetuadas durante uma sessão com privilégios elevados (Hansche, Berti, & Hare, 2004).

Em ambientes de saúde, a aplicação de PAM é especialmente relevante para proteger sistemas que processam dados de pacientes, equipamentos de imagiologia médica e infraestruturas críticas como servidores PACS e sistemas de arquivo clínico. A monitorização contínua das contas privilegiadas, integrada com plataformas SIEM, permite detetar comportamentos anómalos e acionar respostas automáticas de contenção.

A gestão de identidades e acessos em organizações de saúde está sujeita a um conjunto de requisitos regulatórios e normativos específicos. O RGPD impõe, nos seus artigos 5.º, 25.º e 32.º, a obrigatoriedade de implementar medidas técnicas e organizativas adequadas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais, incluindo dados de saúde, classificados como categoria especial de dados. A rastreabilidade dos acessos (nomeadamente, quem acedeu, a quê, quando e a partir de onde) é um requisito implícito para efeitos de auditoria e de demonstração de conformidade.

3.2.2. *Intrusion Detection System / Intrusion Prevention System*

Os sistemas de deteção (IDS) e prevenção (IPS) de intrusões, normalmente integrados em dispositivos denominados de *firewall*, realizam a análise da comunicação de dados que circula através do dispositivo. No caso dos IDS, apenas alertam ou enviam informação para outros sistemas auxiliares. No caso dos IPS, estes agem ativamente e desencadeiam uma ação sobre um determinado fluxo (por exemplo, bloquear a comunicação).

A análise pode ser feita baseada em padrões (*signature-based*) de dados presentes numa comunicação ou ficheiro em trânsito, ou através de análise comportamental (*behavioral / anomaly-based*). As assinaturas, também designadas por IOC, são inseridas previamente no dispositivo que efetua a análise e contêm um conjunto de atributos, nomeadamente IP ou DNS de origem, partes de mensagem, entre outros elementos que

possam atestar a segurança da comunicação. Na análise por comportamento, como o exemplo dos sistemas *User and Entity Behavior Analytics* (UEBA) (baseados em *machine learning*), o sistema deteta desvios ao padrão habitual de comportamento de rede, utilizador ou aplicação. Este recorre à aprendizagem contínua e a sua ação é mais eficaz em ataques não padronizados e exfiltração de dados (Blue Goat Cyber, 2025).

3.2.3. *Endpoint Detection and Response*

Um *Endpoint Detection and Response* (EDR) complementa a função dos IDS/IPS através da distribuição de agentes nos vários dispositivos finais, para que a ação de deteção e resposta possa ser feita nesses pontos, de modo a isolar dispositivos caso estes sofram um ataque. A ação de cada agente pode ser coordenada centralmente e de forma autónoma e isolada.

Um EDR também audita eventos ocorridos no dispositivo. A sua integração com outros sistemas, nomeadamente SIEM, permite a análise centralizada da rede através da correlação de eventos provenientes de diversos dispositivos e aplicações de rede (Ferreira, 2025).

3.2.4. *Security Information and Event Management*

Um SIEM é uma plataforma que combina as funções de recolha, armazenamento e análise de *logs* e eventos provenientes de diferentes sistemas com as funções de monitorização, correlação de eventos e criação de alertas em tempo real. Através de uma gestão centralizada e normalização dos dados recebidos pelos diversos sistemas, é possível detetar ataques mais complexos e permitir orientar outros sistemas conexos para uma ação localizada (por exemplo, recorrendo a EDR e SOAR) (Crowley, Filkins, & Pescatore, 2022).

Para obter informação da rede, o SIEM disponibiliza *dashboards* e relatórios. Os relatórios automáticos são úteis para dar resposta a auditorias e a requisitos de conformidade. A integração de várias fontes de informação e a existência de um histórico permitem a análise forense digital para investigação de incidentes.

Um exemplo de SIEM *open-source* é o Wazuh, que combina recursos de SIEM com EDR, através da utilização de um agente que é instalado nos sistemas a monitorizar. O Wazuh é relevante para o âmbito deste projeto, porque faz parte da arquitetura de sistema de suporte ao HCDW (Wazuh, 2015) .

3.2.5. *Security Orchestration, Automation and Response*

Um SOAR é uma plataforma que complementa as funções de um SIEM e EDR, pois permite automatizar, orquestrar e gerir as respostas a incidentes através da informação fornecida pelo SIEM e despoletar ações nos diversos dispositivos através do EDR.

A orquestração possibilita a realização de ações em múltiplos dispositivos (previamente integrados), para alterar fluxos de dados ou lançar ações específicas nos diversos sistemas.

A automatização baseia-se em roteiros de resposta (*playbooks*) previamente definidos para a realização de tarefas repetidas ou previstas como, por exemplo, bloqueio automático de comunicações envolvendo IP maliciosos ou enriquecimento de IOC.

A resposta a incidentes através deste tipo de plataforma reduz o tempo de resposta entre a deteção do incidente e a sua resolução, facilita a gestão de incidentes em todo o seu ciclo de vida (deteção, análise, resposta e lições aprendidas), permite uma prévia definição de ações que podem ser executadas automaticamente ou executadas pelos analistas de cibersegurança (Crowley, Filkins, & Pescatore, 2022).

3.2.6. *Data Loss Prevention*

O *Data Loss Prevention* (DLP) é um conceito que abrange *software* e políticas de segurança da informação que permitem a deteção, monitorização e prevenção da divulgação não autorizada de dados sensíveis, nomeadamente dados pessoais, financeiros, protegidos por regulação e propriedade intelectual.

Através da definição de padrões e de técnicas de inspeção e aprendizagem, é efetuada a classificação e identificação dos dados. A monitorização ocorre sobre dados armazenados para arquivo, transmitidos ou em utilização nos dispositivos finais, e permite a aplicação de restrições e bloqueios automáticos em caso de ações não autorizadas (por exemplo, cópia dos ficheiros para unidades de armazenamento externas ou envio por correio eletrónico), dando visibilidade adicional do uso dos dados.

Através de um DLP é possível gerar alertas e relatórios para dar resposta a requisitos legais, de modo a evitar multas e danos de reputação (CrowdStrike, 2025).

3.3. SISTEMAS INFORMÁTICOS ESPECÍFICOS DE INFORMÁTICA MÉDICA

Nesta secção são apresentados tipos de sistemas e soluções existentes no mercado específicos para o contexto clínico, tais como o controlo e auditoria de acesso a dados (Secção 3.3.1), gestão e tratamento de fluxos (Secção 3.3.2) e monitorização centralizada (Secção 3.3.3).

3.3.1. Controlo e auditoria de acesso a dados

As ferramentas de controlo e auditoria de acesso a dados permitem conceder ou negar a visualização e edição de dados sensíveis aos utilizadores numa rede informática. Este tipo de ferramenta pode ser integrado com outras ferramentas de fornecimento de identidade (*Identity Provider*(IDP)) e DLP.

A plataforma *Edison Datalogue Connect*, da *GE HealthCare* permite a colaboração de dados de forma segura, integrada com os serviços de diretório *Microsoft Active Directory* para centralização de utilizadores, permitindo SSO. Tem funcionalidades integradas de auditoria e rastreamento de acesso a protocolos e imagens DICOM (GE Healthcare, 2025).

Tendo em consideração que o *software PACS* proposto para a arquitetura estudada (*Orthanc*) pode ser executado em soluções de *Platform-as-a-Service* (PaaS), importa também mencionar as soluções em *cloud* pública. Os principais fornecedores de *cloud* disponibilizam serviços de armazenamento em conformidade com os requisitos de saúde, mas para dados armazenados nos seus servidores. Entre os serviços temos o *Google Cloud Healthcare API* que fornece ferramentas para gerir e auditar dados médicos, incluindo nos formatos HL7 v2 e FHIR, DICOM e API de anonimização (Google Cloud, 2025). O *Microsoft Azure Health Data Services* disponibiliza igualmente APIs para HL7 FHIR e DICOM, disponibiliza controlo e auditoria de acessos, integração com outras aplicações de saúde, transformação de dados e integração com análise de dados utilizando IA e ML. O serviço menciona conformidade com o HIPAA e o RGPD (Microsoft, 2025). A *Amazon Web Services* disponibiliza serviços e plataformas de suporte a atividades médicas em conformidade com os regulamentos em vigor para o setor. Através de ferramentas genéricas integradas, permite a auditoria e o controlo de acesso a dados (Amazon Web Services, 2022) (Amazon Web Services, 2025).

3.3.2. Roteamento, transformação e integração de fluxos

As ferramentas que permitem roteamento, transformação e integração de fluxos de comunicações médicas podem providenciar informações sobre os dados que circulam através delas.

A *Unifier*, da *DICOM Systems* é uma plataforma que permite fazer o roteamento de serviços DICOM e HL7 com base em regras inteligentes, com possibilidade de anonimização, integração de fluxos com encriptação de dados, integração com serviços de diretório *Microsoft Active Directory*, assegurando a conformidade com regulamentação como o HIPAA (Dicom Systems, 2025).

O *Mercure Imaging* é uma plataforma *open-source* de orquestração de comunicações entre serviços DICOM, com funcionalidades de roteamento semelhantes ao *Unifier*. A monitorização das comunicações é realizada pelo serviço *bookkeeper analysis*, que recolhe os dados presentes nas *tags* dos ficheiros DICOM (Mercure Imaging Org, 2025).

O *software NextGen Healthcare*, versão atual e comercial do original *software open-source Mirth Connect*, permite efetuar a interoperabilidade entre sistemas e transformação de dados em formatos de texto estruturado, como o HL7, JSON e XML. Através da inspeção de dados é possível efetuar a monitorização dos dados que circulam pelos canais de comunicação estabelecidos (Yeh, 2020). O acesso aos canais de dados, para envio ou receção de informação, pode ser auditado (através dos *Channel History*) e o acesso condicionado através de regras, multi-fator de autenticação e integração com serviços de diretório LDAP (NEXTGen, 2025).

3.3.3. Monitorização centralizada

As plataformas e ferramentas de monitorização de comunicações através do protocolo TCP/IP permitem monitorizar dados DICOM e HL7 em trânsito (Paessler AG, 2025). A integração de monitorização de rede com outras plataformas, nomeadamente IDS, IPS, SIEM e SOAR melhora a monitorização e resposta a incidentes através da deteção de acessos ilegítimos aos dados, através da criação de regras específicas e contextualizadas.

Para a monitorização de fluxos de dados em redes informáticas médicas, além dos serviços genéricos habitualmente supervisionados, as ferramentas utilizadas devem disponibilizar sensores específicos para os protocolos HL7 e DICOM (C-STORE, C-ECHO, C-FIND), de forma a permitir a avaliação contínua do desempenho, da disponibilidade e da

integridade dos sistemas clínicos, bem como a recolha e o armazenamento estruturado de eventos para fins de auditoria (Paessler AG, 2025).

A correlação entre eventos de segurança e o contexto de identidade melhora a eficácia operacional do SIEM. Num ambiente de saúde, um evento de segurança isolado adquire significado muito diferente consoante o utilizador associado seja um médico ou um utilizador genérico do serviço (Cyberout Security, 2024).

O uso de conectores de integração, como o *Wazuh Integration Framework*, ou de soluções de SOAR, permite automatizar a consulta de gestores de identidades e acessos em tempo real aquando da geração de alertas, adicionando atributos de identidade aos eventos e permitindo a definição de regras de correlação baseadas em papéis (RBAC-aware correlation). Esta abordagem é alinhada com os princípios de *Zero Trust Architecture* (ZTA), preconizados pelo NIST SP 800-207 (Rose, Borchert, Mitchell, & Connelly, 2020), segundo os quais nenhuma entidade é implicitamente confiável, independentemente da sua localização na rede.

A implementação desta integração de dados e centralização da monitorização melhora a eficácia das medidas de cibersegurança através da redução do tempo de deteção (*Mean Time To Detect* (MTTD)) e do aumento da qualidade dos alertas, com redução significativa de falsos positivos (IBM Security, 2023). Como apresentado no Anexo A, a existência de eventos de segurança enriquecidos com informação de identidade e acessos é um requisito implícito do RGPD para efeitos de auditoria, permitindo demonstrar que o acesso a dados pessoais de saúde é devidamente registado e rastreável (Parlamento Europeu e Conselho da União Europeia, 2016).

3.4. AUDITORIA DE EVENTOS DE CIBERSEGURANÇA NO CONTEXTO DE SISTEMAS MÉDICOS

A especificidade dos sistemas de informação médica reside no facto de os protocolos de comunicação predominantes no sector (nomeadamente, DICOM e HL7 FHIR) incorporarem mecanismos de auditoria próprios e padronizados, que permitem o registo estruturado e interoperável de eventos de acesso independentemente do fabricante dos sistemas envolvidos.

No domínio da imagiologia médica, a norma DICOM PS3.15 define o perfil *Audit Trail Message Format Profile*, que especifica o formato, o vocabulário e o mecanismo de transporte das mensagens de auditoria geradas por sistemas DICOM. Os eventos auditáveis (incluindo acessos a estudos, operações de transferência de imagens e

tentativas de autenticação) são codificados em mensagens XML estruturadas e transmitidos via protocolo *Syslog* para um repositório centralizado (DICOM Standards Committee, 2025). O perfil *Audit Trail and Node Authentication* (ATNA) promovido pela iniciativa *Integrating the Healthcare Enterprise* (IHE) operacionaliza este mecanismo numa arquitetura de atores bem definida, estabelecendo requisitos de autenticação mútua por TLS e de integridade das mensagens (IHE International, 2023). Gregg *et al.* (2006) demonstraram, num estudo publicado no *Journal of Digital Imaging*, a viabilidade de consolidar registos ATNA provenientes de múltiplos sistemas PACS heterogéneos num repositório centralizado, concluindo que esta abordagem é a mais pragmática para a gestão de informação de auditoria em ambiente hospitalar (Gregg, D'Agostino, & Toledo, 2006).

No contexto dos sistemas de interoperabilidade baseados em HL7 FHIR, o recurso *AuditEvent* cumpre função equivalente, sendo concebido para o registo estruturado de eventos de acesso e modificação de dados clínicos. O vocabulário de eventos utilizado é partilhado com o perfil DICOM ATNA, garantindo uma base conceptual comum entre os dois *standards*. A especificação FHIR é explícita na obrigatoriedade de registo das decisões de controlo de acesso, tanto as autorizações como as negações. Ao adotar o suplemento IHE *RESTful* ATNA, é possível ainda a pesquisa de registos por parâmetros como data, utilizador e tipo de evento, facilitando a integração com plataformas de monitorização centralizadas (IHE International, 2015).

3.5. SÍNTESE

A literatura evidencia que o setor da saúde é altamente vulnerável a ciberataques, sendo o erro humano e a baixa cultura de cibersegurança fatores críticos. Destaca-se a necessidade de abordagens integradas que combinem tecnologia, processos e formação para mitigar riscos. A adoção de *frameworks*, métricas e soluções como SIEM, IAM e SOAR permite reforçar a capacidade de deteção e resposta a incidentes. Paralelamente, o cumprimento regulatório e a proteção de dados exigem mecanismos robustos de controlo e auditoria.

Face ao exposto, propõe-se o desenvolvimento de um sistema de monitorização e auditoria de acessos a dados clínicos em ambientes digitais de saúde, destinado especificamente a pequenas entidades prestadoras de MCDT, designadamente clínicas de imagiologia que operam em ambiente digital. Estas entidades caracterizam-se por processar volumes significativos de dados pessoais sensíveis, nomeadamente imagens médicas e relatórios de diagnóstico, estando sujeitas às mesmas obrigações regulatórias

que as grandes instituições hospitalares ao abrigo do RGPD, sem que, na generalidade dos casos, disponham de recursos humanos especializados em cibersegurança ou de orçamento para implementar soluções comerciais de monitorização.

O sistema a desenvolver (HCDW) recolhe eventos de acesso provenientes das diferentes fontes da infraestrutura tecnológica da entidade, nomeadamente sistemas PACS, servidores de relatórios, plataformas de interoperabilidade e o componente de gestão de identidades e acessos (IAM). A informação recolhida é processada, normalizada e armazenada numa base de dados centralizada, sendo apresentada através de *dashboards* interativos que tornam a informação de monitorização acessível a utilizadores que não estão exclusivamente dedicados à área de cibersegurança, como gestores clínicos e EPD.

Além da visualização de acessos, o sistema auxilia-se do SIEM e do IAM para identificar padrões de utilização e detetar comportamentos anómalos, como acessos não justificados ou tentativas de acesso a dados de pacientes sem relação clínica estabelecida. Esta estratégia permite reforçar os mecanismos de controlo de acesso, contribuindo para a proteção da confidencialidade, integridade e disponibilidade dos dados clínicos, em linha com os princípios da tríade CIA e com os requisitos do artigo 32.º do RGPD (Parlamento Europeu e Conselho da União Europeia, 2016).

O sistema proposto distingue-se das soluções existentes, nomeadamente na forma como integra e apresenta informação de monitorização de cibersegurança de forma acessível a perfis não especializados, no contexto específico da saúde. Enquanto as soluções SIEM tradicionais se dirigem predominantemente a equipas de operações de segurança (SOC) com competências técnicas avançadas, o HCDW diferencia-se por:

- privilegiar a visualização através de *dashboards* intuitivos, orientados à tomada de decisão e não à análise forense técnica;
- adaptar a informação a perfis não especializados, nomeadamente gestores clínicos e EPD de pequenas entidades, que necessitam de evidências de conformidade regulatória sem conhecimentos aprofundados em cibersegurança;
- enquadrar-se especificamente nos fluxos digitais do setor da saúde, integrando nativamente os protocolos predominantes neste contexto, nomeadamente DICOM, HL7, *DICOMweb* e o ecossistema SPMS/SNS;
- assentar exclusivamente em ferramentas *open-source*, nomeadamente *Orthanc*, *Wazuh*, *Keycloak* e *PostgreSQL*, eliminando custos de licenciamento e tornando a

solução economicamente viável para entidades de pequena dimensão, que constituem a maioria dos prestadores de MCDT em Portugal.

4. DESENVOLVIMENTO

Neste capítulo é apresentado o levantamento dos requisitos funcionais e não funcionais (Secção 4.1) que servem de base à construção do modelo de dados (Secção 4.2), arquitetura de sistema (Sesção 4.3) e à escolha das tecnologias utilizadas (Secção 4.4). Seguidamente é apresentado um protótipo de baixa fidelidade (Secção 4.5) e a validação e avaliação da solução ao nível conceptual (Secção 4.6).

4.1. LEVANTAMENTO DE REQUISITOS

Os requisitos de um sistema constituem as especificações dos serviços que este deve fornecer, bem como as restrições sob as quais deve operar, em resposta às necessidades identificadas para a resolução de um problema concreto (Sommerville, 2011). Integram esta categoria, entre outros, as regras de negócio, os mecanismos de interação com o utilizador, as restrições de desempenho e de volume de dados, os requisitos de integração com sistemas externos, a conformidade com normativos legais e organizacionais, e os atributos de segurança da informação.

Sommerville (2011) classifica os requisitos em duas categorias fundamentais. Os requisitos funcionais descrevem os serviços que o sistema deve prestar, o modo como deve reagir a entradas específicas e o comportamento esperado em determinadas situações – incluindo, quando aplicável, a especificação explícita do que o sistema não deve fazer. Os requisitos não funcionais, por sua vez, definem as propriedades e restrições globais do sistema (como desempenho, fiabilidade, segurança, escalabilidade e conformidade com normas), aplicando-se frequentemente ao sistema como um todo e não a funcionalidades isoladas. Importa sublinhar que os requisitos não funcionais podem revelar-se mais críticos do que os funcionais: a sua não satisfação pode inviabilizar a utilidade prática do sistema, independentemente do correto cumprimento das funções especificadas.

4.1.1. Requisitos funcionais

No levantamento dos requisitos funcionais consideram-se os fluxos de informação e cenários de utilização anteriormente apresentados, para identificar o que o sistema faz. Para cada cenário foram elencados os atributos de comportamento e uso da plataforma.

Na Tabela 5 estão listados os requisitos funcionais, tendo cada um atribuído um identificador (ID) começado pela sigla “RF”, uma breve descrição, o objetivo do requisito e

a classificação essencial, importante e desejável. Um requisito essencial é de implementação obrigatória porque está relacionado com uma funcionalidade e objetivo da plataforma, sem o qual o sistema não pode ser operacionalizado nem considerado completo. Um requisito importante não condiciona a operacionalidade do sistema, mas contribui de forma significativa para o seu comportamento e usabilidade, devendo por isso ser implementado após a satisfação dos requisitos essenciais. Por fim, um requisito desejável é de natureza opcional: a sua ausência não compromete os objetivos principais do sistema, representando uma melhoria incremental que poderá ser considerada em fases posteriores do desenvolvimento

Tabela 5 - Requisitos funcionais

ID	**Descrição**	**Objetivo**	**Perfil**	**Classificação**
RF01	Lista de acessos justificados	O utilizador pode listar os acessos autorizados, com código de paciente, código de médico e código de utilizador, data e hora de acesso, origem do acesso.	Auditor	Essencial
RF02	Lista de acessos não justificados	O utilizador pode listar os acessos que não se correlacionam com listagem providenciada pelo RIS, com código de paciente, código de médico e código de utilizador, data e hora de acesso, origem do acesso.	Auditor	Essencial
RF03	Lista de acessos externos	O utilizador pode listar os acessos efetuados através dos webservices para partilha de resultados, com código de paciente, código de médico e código de utilizador, data e hora de acesso, origem do acesso.	Auditor	Essencial

ID	Descrição	Objetivo	Perfil	Classificação
RF04	Lista de atividade do utilizador	O utilizador pode consultar o histórico de atividade da conta do utilizador, nomeadamente acessos a sistemas e documentos, alteração da palavra-passe, data e hora do evento e origem do acesso (IP).	Auditor	Essencial
RF05	Lista de eventos adversos	O utilizador pode consultar a correlação de dados e filtros, que disponibilizam eventos adversos, identificando a origem do acesso, documento acedido e paciente visado	Auditor	Essencial
RF06	Exportação de relatórios em PDF	O utilizador pode permitir a exportação de listagens em PDF com possibilidade de pseudonimização dos dados	Administrador	Importante
RF07	Pesquisa global por identificador	O utilizador pode efetuar uma pesquisa global de dados por código de paciente, código de médico e código de utilizador	Auditor	Desejável
RF08	Eliminação de registos com tempo de retenção superior ao legalmente permitido	O utilizador pode permitir a eliminação automática de registos com tempo de retenção superior ao legalmente permitido, ou a identificação para remoção manual.	Administrador	Essencial
RF09	Preservação de registos com exclusão de remoção automática	O utilizador pode definir quais os registos que devem ser preservados (por exemplo, por ordem judicial) por um período superior ao definido na retenção geral de dados (RF08).	Auditor	Essencial

A plataforma HCDW define dois perfis de utilizador (Gestor e Administrador), cujas responsabilidades são descritas nos cenários de uso (Subsecção 4.6.2). No contexto de sistemas de informação em saúde, a adoção de um modelo baseado em funções (RBAC) é a abordagem mais comum e recomendada por referenciais como a ISO/IEC 27001:2022 e o NIST SP 800-162, por permitir a atribuição de permissões de acordo com a função organizacional do utilizador, respeitando o princípio do menor privilégio. A cada perfil deverão corresponder permissões explicitamente definidas: ao Gestor, a consulta de eventos de acesso, a emissão de relatórios e a pesquisa geral; ao Administrador, adicionalmente, a gestão de utilizadores, a configuração da plataforma e a manutenção das tabelas auxiliares. A formalização destas permissões numa matriz de controlo de acesso constitui um requisito de completude da especificação e uma condição prévia a qualquer implementação em ambiente de produção.

4.1.2. Requisitos não funcionais

No levantamento dos requisitos não funcionais, ou seja, como o sistema funciona, foram analisados os cenários de uso e elencados os atributos de qualidade, restrições e desempenho.

Na Tabela 6 estão listados os requisitos não funcionais, seguindo a estrutura da tabela anterior: um identificador de requisito (coluna ID) começado pela sigla “RNF”, breve descrição, objetivo e classificação (essencial, importante e desejável).

Tabela 6 - Requisitos não funcionais

ID	Descrição	Objetivo	Perfil	Classificação
RNF01	Portabilidade da aplicação	A aplicação deve ser agnóstica de sistema operativo, podendo ser instalada em SO Microsoft Windows ou distribuições Linux/Unix.	N/A	Essencial
RNF02	Acesso por Web com protocolo de comunicação segura	A plataforma deve estar acessível exclusivamente por protocolo HTTPS, requerendo o uso de certificado SSL válido.	N/A	Essencial

ID	Descrição	Objetivo	Perfil	Classificação
RNF03	Todos os serviços, recursos e bibliotecas em uso ou para consumo da aplicação devem estar *on-premises*	Todos as fontes de dados, recursos informáticos ou bibliotecas a integrar na plataforma não devem requerer o uso de ligação a redes exteriores à rede informática da entidade.	N/A	Importante
RNF04	Autenticação e autorização no acesso às funcionalidades da plataforma	O utilizador deve poder criar e gerir as contas de acesso à plataforma HCDW, com atribuição individualizada de acessos às listagens e funcionalidades de exportação de dados	Administrador	Essencial
RNF05	Os dados pessoais temporários e cifrados	Todos os dados pessoais devem ser obtidos seletivamente das fontes de dados externas (quando necessários) e devem permanecer temporariamente e serem cifrados.	N/A	Essencial

4.2. MODELO DE DADOS

Nesta seção é apresentado o modelo de dados de suporte à aplicação proposta, com descrição das entidades, relações e restrições. Na definição do modelo de dados teve-se em consideração que todos os dados que identifiquem indivíduos e relatórios devem conter um identificador de pseudonimização, permitindo estabelecer relações entre registos na aplicação, sem identificar o utilizador, médico e paciente (não são guardados dados pessoais que permitam a identificação dos indivíduos).

4.2.1. Modelo conceptual e lógico

O modelo conceptual tem as seguintes entidades:

- Utilizador – representa as contas de acesso ao sistema, relacionadas com uma pessoa (paciente, técnico ou médico), e tem como atributos um identificador de pseudonimização de utilizador e o identificador único do IAM;
- Médico – representa os médicos registados no sistema, internos ou externos à organização, e tem como atributos um identificador de pseudonimização de médico e identificador do RIS/PACS;
- Paciente – representa as pessoas às quais um determinado registo diz respeito, e tem como atributos um identificador de pseudonimização do paciente, o identificador de paciente no RIS / PACS;
- Sistema – representa o sistema através do qual se consegue aceder aos dados, identificando também a entidade de origem do acesso, e tem como atributos um identificador de pseudonimização de sistema, tipo de sistema (interno, externo) e o identificador único de sistema (entidade presente nos dados estruturados HL7);
- Objeto Informacional – representa os registos relacionados com o paciente, com os dados obtidos e gerados antes, durante e depois do exame, nomeadamente dados estruturados, imagens e relatórios médicos, e tem como atributos um identificador de pseudonimização de objeto, o tipo de objeto (imagem, relatório, dados estruturados), data e hora relacionados com a produção do objeto, o identificador de objeto presente no RIS/PACS;
- Evento – representa o evento de acesso aos registos por parte de um utilizador ou de origem não identificada, e tem como atributos um identificador de pseudonimização do evento, data e hora de ocorrência do evento e os identificadores do registo, utilizador, sistema e taxionomia.
- Taxionomia – representa o tipo de evento e tem como atributos um identificador, uma codificação uniforme de taxionomia e a respetiva descrição.
- Configurações – representa as configurações específicas da aplicação e tem como atributos um identificador, uma chave e um valor, o autor e a data de modificação.

A Figura 9 representa o modelo lógico de dados recorrendo à notação "*Crow's foot*" para diagramas de Entidade-Relação, com as seguintes restrições e regras de integridade:

- um utilizador pode ser associado a um médico ou nenhum (relação 0:1);
- um utilizador pode ser associado a um paciente ou nenhum (relação 0:1);
- um objeto informacional deve ser associado a um médico (condição obrigatória);
- um objeto informacional deve ser associado a um paciente (condição obrigatória);
- um objeto informacional gera vários eventos (condição obrigatória)
- um evento pode ser associado a um utilizador ou nenhum;
- um utilizador pode originar vários eventos;
- um evento deve ser associado a um sistema (condição obrigatória);
- um utilizador tem várias configurações (condição obrigatória);
- um evento deve ter uma taxionomia associada (condição obrigatória).

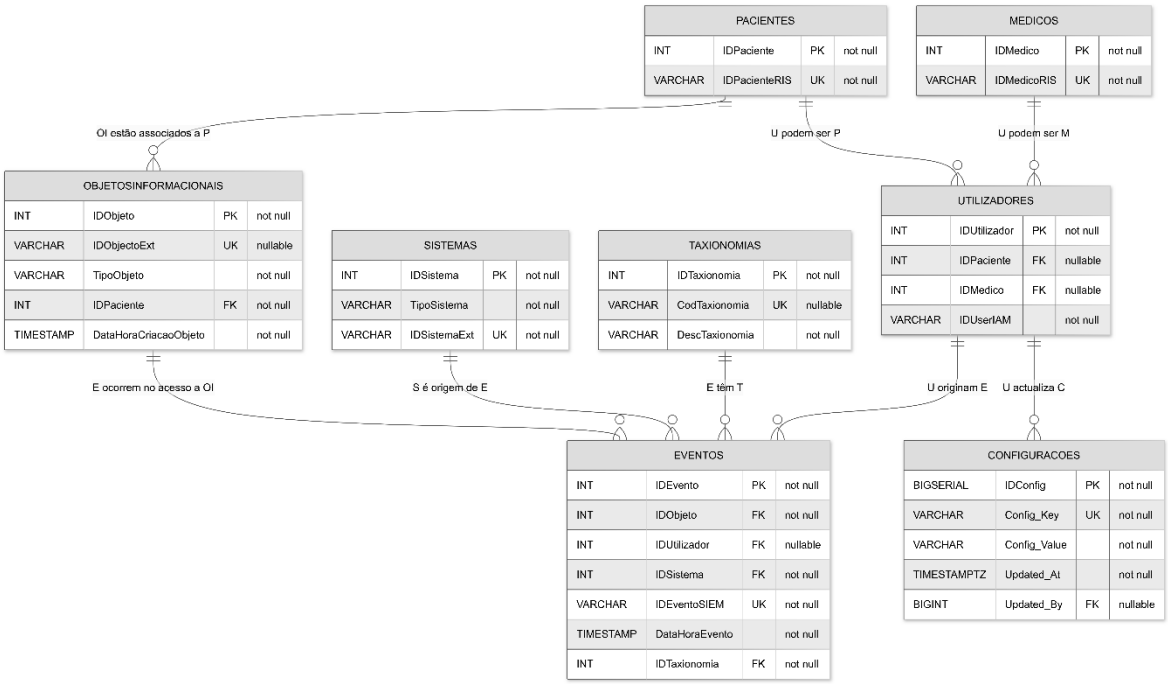


Figura 9 - Diagrama Entidade-Relação da aplicação

4.2.2. Modelo físico

Nesta Subsecção apresenta-se o código SQL utilizado para criar as tabelas, para sistema de gestão de base de dados (SGBD) *PostgreSQL* versão 18, tendo em consideração o modelo lógico definido e otimizações de acesso aos dados.

As tabelas “Pacientes”, “Medicos”, “Sistemas” e “Utilizadores” (Figura 10) constituem as entidades de referência do modelo de dados. Os identificadores primários de todas as tabelas utilizam o tipo “BIGSERIAL”, que gera automaticamente valores inteiros de 64 bits com incremento sequencial, garantindo unicidade e escalabilidade para volumes elevados de registos. Os identificadores externos (“IDPacienteRIS”, “IDMedicoRIS”, “IDSistemaExt” e “IDUserIAM”) são definidos como “VARCHAR(255)”, acomodando os identificadores alfanuméricos provenientes de sistemas externos heterogéneos, como o RIS, o PACS e o sistema IAM, sem impor restrições de formato. Na tabela “Utilizadores”, as chaves estrangeiras “IDPaciente” e “IDMedico” são do tipo “BIGINT”, compatível com o “BIGSERIAL” das tabelas referenciadas, e a restrição “CHECK” implementada garante que um utilizador não pode assumir simultaneamente os papéis de paciente e médico, assegurando a integridade semântica dos dados.

```sql
-- Tabela Pacientes
CREATE TABLE Pacientes (
    IDPaciente BIGSERIAL PRIMARY KEY,
    IDPacienteRIS VARCHAR(255) UNIQUE NOT NULL);
-- Tabela Medicos
CREATE TABLE Medicos (
    IDMedico BIGSERIAL PRIMARY KEY,
    IDMedicoRIS VARCHAR(255) UNIQUE NOT NULL);
-- Tabela Sistemas
CREATE TABLE Sistemas (
    IDSistema BIGSERIAL PRIMARY KEY,
    TipoSistema VARCHAR(255) NOT NULL,
    IDSistemaExt VARCHAR(255) UNIQUE NOT NULL);
-- Tabela Utilizadores
CREATE TABLE Utilizadores (
    IDUtilizador BIGSERIAL PRIMARY KEY,
    IDPaciente BIGINT,
    IDMedico BIGINT,
    IDUserIAM VARCHAR(255) NOT NULL,
    CONSTRAINT FK_Utilizadores_Pacientes
        FOREIGN KEY (IDPaciente) REFERENCES Pacientes(IDPaciente),
    CONSTRAINT FK_Utilizadores_Medicos
        FOREIGN KEY (IDMedico) REFERENCES Medicos(IDMedico),
    -- Garante que um utilizador não é simultaneamente paciente e médico
    CONSTRAINT CHK_Utilizador_Tipo
        CHECK (
            (IDPaciente IS NOT NULL AND IDMedico IS NULL) OR
            (IDPaciente IS NULL AND IDMedico IS NOT NULL) OR
            (IDPaciente IS NULL AND IDMedico IS NULL)
        )
);
```

Figura 10 – Criação de tabelas Pacientes, Medicos, Sistemas e Utilizadores no SGBD

As tabelas “ObjetosInformacionais”, “Taxionomias” e “Configuracoes” (Figura 11) suportam o registo dos objetos clínicos monitorizados e os metadados de configuração da

plataforma. Na tabela “ObjetosInformacionais”, o campo “TipoObjeto” utiliza o tipo “SMALLINT”, adequado para armazenar um conjunto limitado e estável de categorias de objetos (por exemplo, imagem DICOM, relatório PDF), minimizando o espaço de armazenamento. O campo “DataHoraCriacaoObjeto” é do tipo “TIMESTAMP WITH TIME ZONE”, garantindo o registo da data e hora com referência ao fuso horário, essencial para a rastreabilidade temporal em ambientes distribuídos. Na tabela “Configuracoes”, o campo “Update_At” segue o mesmo tipo, assegurando um registo de auditoria fiável das alterações às configurações da plataforma, enquanto o par “Config_Key”/”Config_Value” em “VARCHAR(255)“ confere flexibilidade para armazenar parâmetros de configuração de natureza variável sem necessidade de alterações ao esquema da base de dados.

```
-- Tabela ObjetosInformacionais
CREATE TABLE ObjetosInformacionais (
    IDObjeto BIGSERIAL PRIMARY KEY,
    IDObjetoExt VARCHAR(255) UNIQUE,
    TipoObjeto SMALLINT NOT NULL,
    IDPaciente BIGINT NOT NULL,
    DataHoraCriacaoObjeto TIMESTAMP WITH TIME ZONE DEFAULT
CURRENT_TIMESTAMP,
    CONSTRAINT FK_ObjetosInformacionais_Pacientes
        FOREIGN KEY (IDPaciente) REFERENCES Pacientes(IDPaciente));
-- Tabela Taxionomias
CREATE TABLE Taxionomias(
    IDTaxionomia BIGSERIAL PRIMARY KEY,
    CodTaxionomia VARCHAR(255) UNIQUE,
    DescTaxionomia VARCHAR(255) NOT NULL);
-- Tabela Configurações
CREATE TABLE Configuracoes(
    IDConfig BIGSERIAL PRIMARY KEY,
    Config_Key VARCHAR(255) UNIQUE NOT NULL,
    Config_Value VARCHAR(255) NOT NULL,
    Update_At TIMESTAMP WITH TIME ZONE DEFAULT CURRENT_TIMESTAMP NOT NULL,
    Update_By BIGINT NOT NULL,
    CONSTRAINT FKConfiguracoesUtilizadores FOREIGN KEY (Updated_By)
        REFERENCES Utilizadores(IDUtilizador));
```

Figura 11 – Criação de tabelas ObjetosInformacionais, Taxionomias e Configuracoes no SGBD

A tabela “Eventos” (Figura 12) constitui o núcleo do modelo de dados, registando todos os acessos a objetos informacionais detetados pelos sistemas de monitorização. O identificador “IDEventoSIEM”, do tipo “VARCHAR(255)” com restrição “UNIQUE”, permite referenciar de forma unívoca cada evento proveniente do SIEM, evitando duplicações em caso de reingestão de dados. O campo “DataHoraEvento”, definido como “TIMESTAMP WITH TIME ZONE” com valor por omissão “CURRENT_TIMESTAMP”, assegura o registo automático do momento do evento com precisão e consistência temporal, independentemente da zona horária do sistema que o gera. As chaves estrangeiras “IDObjeto”, “IDUtilizador”, “IDSistema” e “IDTaxionomia”, todas do tipo “BIGINT” ou “INT”,

estabelecem as relações com as restantes entidades do modelo, garantindo a integridade referencial dos dados de auditoria.

A criação de índices sobre as colunas de chave estrangeira da tabela “Eventos” e das tabelas “ObjetosInformacionais” e “Utilizadores” visa otimizar o desempenho das operações de consulta, que constituem o caso de uso predominante da plataforma. A instrução “CREATE INDEX CONCURRENTLY” foi deliberadamente utilizada em detrimento do índice padrão, permitindo a criação dos índices sem bloquear operações de leitura e escrita concorrentes na tabela (uma consideração relevante em ambientes onde a ingestão de eventos e a consulta da interface HCDW ocorrem em simultâneo). Os índices cobrem as colunas com maior seletividade nas consultas de filtragem e agregação previstas nos cenários de uso, nomeadamente a pesquisa por objeto informacional, por utilizador, por sistema de origem e por taxonomia de evento.

```
-- Tabela Eventos
CREATE TABLE Eventos (
    IDEvento BIGSERIAL PRIMARY KEY,
    IDObjeto BIGINT NOT NULL,
    IDUtilizador BIGINT,
    IDSistema BIGINT NOT NULL,
    IDEventoSIEM VARCHAR(255) UNIQUE NOT NULL,
    DataHoraEvento TIMESTAMP WITH TIME ZONE DEFAULT CURRENT_TIMESTAMP,
    IDTaxionomia INT NOT NULL,
    CONSTRAINT FK_Eventos_ObjetosInformacionais
        FOREIGN KEY (IDObjeto) REFERENCES ObjetosInformacionais(IDObjeto),
    CONSTRAINT FK_Eventos_Utilizadores
        FOREIGN KEY (IDUtilizador) REFERENCES Utilizadores(IDUtilizador),
    CONSTRAINT FK_Eventos_Sistemas
        FOREIGN KEY (IDSistema) REFERENCES Sistemas(IDSistema)
    CONSTRAINT FK_Eventos_Taxionomias
        FOREIGN KEY (IDTaxionomia) REFERENCES Taxionomias(IDTaxionomia));
-- Índices para performance
CREATE INDEX CONCURRENTLY idx_eventos_objeto ON Eventos(IDObjeto);
CREATE INDEX CONCURRENTLY idx_eventos_utilizador ON Eventos(IDUtilizador);
CREATE INDEX CONCURRENTLY idx_eventos_sistema ON Eventos(IDSistema);
CREATE INDEX CONCURRENTLY idx_eventos_taxionomia ON Eventos(IDTaxionomia);
CREATE INDEX CONCURRENTLY idx_objetos_paciente ON
ObjetosInformacionais(IDPaciente);
CREATE INDEX CONCURRENTLY idx_utilizadores_paciente ON
Utilizadores(IDPaciente);
CREATE INDEX CONCURRENTLY idx_utilizadores_medico ON
Utilizadores(IDMedico);
```

Figura 12 – Criação de tabelas Eventos e índices de performance no SGBD

Cada uma das tabelas “Pacientes”, “Medicos” e “Utilizadores” tem uma tabela auxiliar temporária (*temp_pacientes*, *temp_medicos* e *temp_utilizadores*), sendo a chave primária e chave estrangueira da tabela permanente. Os dados pessoais são copiados para o campo “Descrição”.

Através do tipo de tabelas "*unlogged*", os dados presentes nestas tabelas não são persistentes (ficam maioritariamente em RAM) e a escrita e leitura são mais rápidas (porque não utilizam o mecanismo de *Write-Ahead Logging* (WAL), responsável pela escrita das alterações em ficheiros log antes de aplicar na tabela final) (Figura 13).

```
-- Tabela temporária relacionada com Pacientes
CREATE UNLOGGED TABLE temp_pacientes (
    IDPaciente BIGINT PRIMARY KEY,
    Descricao BYTEA NOT NULL,
    CONSTRAINT FK_temp_pacientes
        FOREIGN KEY (IDPaciente)
        REFERENCES Pacientes(IDPaciente));
-- Tabela temporária relacionada com Medicos
CREATE UNLOGGED TABLE temp_medicos (
    IDMedico BIGINT PRIMARY KEY,
    Descricao BYTEA NOT NULL,
    CONSTRAINT FK_temp_medicos
        FOREIGN KEY (IDMedico)
        REFERENCES Medicos(IDMedico));
-- Tabela temporária relacionada com Utilizadores
CREATE UNLOGGED TABLE temp_utilizadores (
    IDUtilizador BIGINT PRIMARY KEY,
    Descricao BYTEA NOT NULL,
    CONSTRAINT FK_temp_utilizadores
        FOREIGN KEY (IDUtilizador)
        REFERENCES Utilizadores(IDUtilizador));
```

Figura 13 - Modelo de dados físico das tabelas temporárias

Como camada de segurança adicional, requisito RNF05 (Subsecção 0, Tabela 6), o campo descrição é cifrado recorrendo às funcionalidades de cifragem nativas do SGBD adotado, com a ativação da extensão e utilização das funções de criptografar (*pgp_sym_encrypt*) e descriptografar (*pgp_sym_decrypt*) com recurso a "chave_secreta" (Figura 14).

```
-- Activar a extensão
CREATE EXTENSION IF NOT EXISTS pgcrypto;

-- Exemplo de criptografar e inserir dados na tabela temporária
INSERT INTO temp_pacientes (descricao)
VALUES (pgp_sym_encrypt({"nome":"Rui"}, 'chave_secreta'));

-- Exemplo de descriptografar na consulta dos dados
SELECT pgp_sym_decrypt(descricao, 'chave_secreta') AS descricao_text
FROM temp_pacientes;
```

Figura 14 - Funcionalidade de encriptação aplicado às tabelas temporárias

4.3. ARQUITETURA DO SISTEMA

Seguidamente é apresentada a arquitetura da plataforma, HCDW, a desenvolver considerando a análise de requisitos, os componentes a integrar e as fontes de dados a consumir.

Na Figura 15 identificam-se os elementos que compõem o sistema, com referência aos servidores de apoio ao negócio (origem dos dados), aplicações auxiliares (IAM, SIEM), camada de processamento de dados (responsável pela recolha, tratamento, correlação, integração de dados e gestão dos dados presentes no SGBD) e camada de visualização dos dados.

Os *logs* funcionais e de acesso são gerados nos sistemas presentes na rede informática médica: controlador de domínio / serviço de diretório (*Active Directory*), servidor de ficheiros (*WebDAV*), servidor de serviços web HL7, servidor PACS.

A gestão de identidades e acessos possui a informação replicada dos serviços de diretório (*Active Directory*), disponibilizando os serviços de autenticação e autorização para os sistemas não integrados com o *Active Directory*.

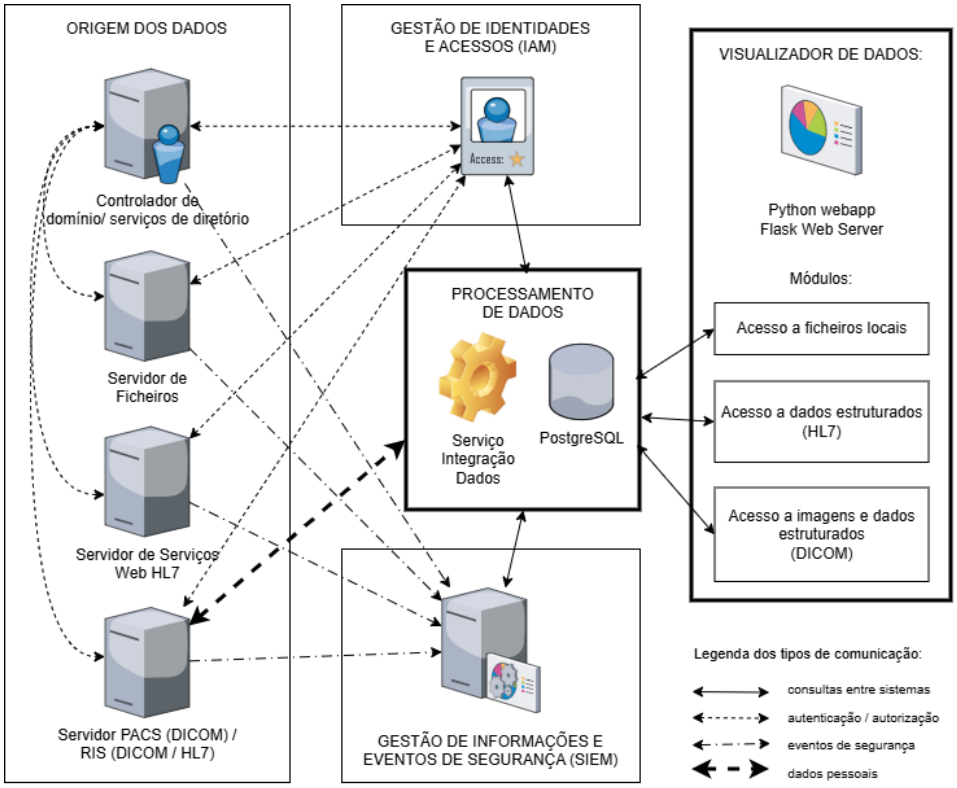


Figura 15 - Identificação dos componentes do sistema

O SIEM recebe informação dos vários equipamentos através do agente instalado em cada equipamento, que é correlacionada com registos da base de dados. Os *logs*

funcionais são disponibilizados por cada aplicação a monitorizar nos servidores de apoio ao negócio.

A camada de processamento de dados é responsável por fazer os pedidos ao SIEM, através de *Wazuh Indexer API*, e registar os eventos relevantes na base de dados, correlacionando com dados consultados no IAM. Toda a lógica de integração de dados reside nesta camada, que opera de forma autónoma em relação à camada de apresentação (visualizador de dados).

O visualizador de dados fornece a informação processada que está armazenada na base de dados (*PostgreSQL*). Para a apresentação de dados pessoais associados aos registos, a camada de apresentação faz um pedido à camada de processamento de dados para obter os dados do RIS, que mantém temporariamente guardados em tabelas temporárias, por um curto período de tempo.

4.3.1. Identidades e Acessos

Num contexto de acesso interno e remoto por utilizadores da entidade, a gestão de identidades e acessos recorre usualmente a um diretório centralizado, integrado com o servidor de VPN. No caso da rede informática de referência, essa centralização é feita pelo *Microsoft Active Directory* do controlador de domínio.

Neste projeto e para os objetivos pretendidos, para facilitar a centralização das identidades e acessos, bem como a manutenção de dados de auditoria, adota-se um gestor de identidades e acessos para integrar os repositórios de identidades locais ao *Microsoft Active Directory*.

Para o efeito foi selecionado o *software Keycloak*[4], "*Open Source Identity and Access Management"*. Esta plataforma permite replicar a informação presente no serviço de diretório e disponibilizar métodos de autenticação e autorização para outros sistemas e aplicações, nomeadamente através dos protocolos SAML, OIDC e FIDO2. Os adaptadores disponibilizados, nomeadamente o proxy IAM "*oauth2-proxy"*, permitem disponibilizar mecanismos de autenticação e de registo de acessos através de um *proxy* que atua como intermediário entre o cliente e os serviços web (aplicações), aplicando um nível adicional de controlo e segurança de forma desacoplada das aplicações.

[4] https://www.keycloak.org/

O diagrama de sequência apresenta o fluxo de requisições, dados recolhidos e destinatários entre os sistemas envolvidos na requisição do objeto informacional (Figura 16).

No diagrama apresentado, todos os serviços web de acesso interno redirecionam a autenticação para o gestor de identidades e acessos através do *Proxy IAM*, configurado num *reverse proxy* NGINX. O *reverse proxy* tem a função de intermediar e validar as conexões entre o cliente e o serviço web requisitado. Por ser o primeiro ponto de contacto de requisição pelo cliente, o *reverse proxy* é o primeiro a enviar o evento de requisição de objeto informacional ao SIEM.

Esta requisição inicia um processo de autenticação e autorização perante o IAM, usando o *proxy* IAM presente no *reverse proxy*. No caso de ausência de *token* ou *token* inválido, o pedido é redirecionado para a página de *login*. Após autenticação ou se o *token* já existir, se for válido, a requisição é aceite, o serviço web envia para o SIEM o evento ocorrido detalhado. Se o *token* for inválido mesmo após a autenticação, retorna código de resposta HTTP (*HTTP status code*) 401 ou 403, referente respetivamente a “não autorizado” (para falha na autenticação) e “Proibido” (para falha na autorização).

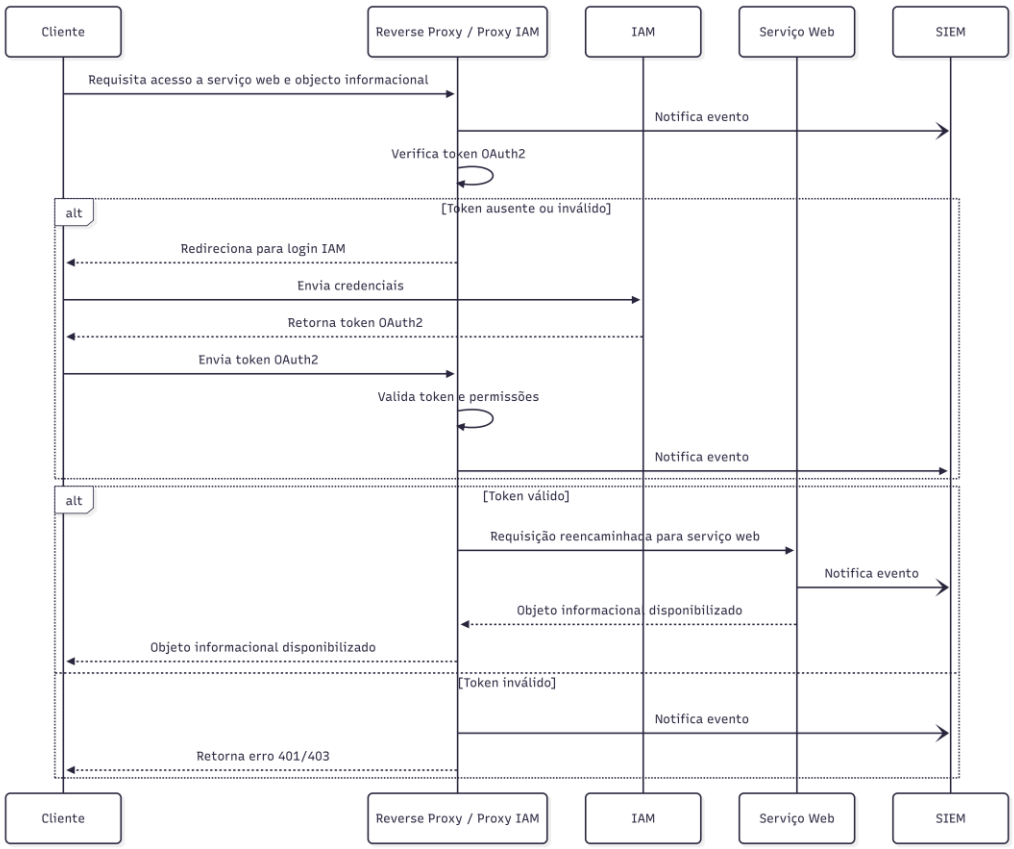


Figura 16 - Diagrama de sequência da requisição de objeto informacional a serviços web internos

Quando o *token* é válido, o serviço web recebe o pedido de objeto informacional a servir e envia para o SIEM os detalhes do pedido com dados conexos (identificadores de paciente, de estudo e data e hora de criação). Cada serviço web tem a responsabilidade de enviar estes detalhes para o SIEM nos eventos de requisição aceite (que precedem a disponibilização do objeto informacional).

No caso de acessos por sistemas internos a serviços disponibilizados pelo PACS através de protocolo DIMSE (Figura 17), cabe ao PACS garantir quais os sistemas clientes que podem aceder através da inclusão dos *Application Entity Title* (AET) do sistema requerente (cliente) na lista de AET autorizados. Este evento de acesso é comunicado ao SIEM diretamente pelo PACS *Orthanc*, recorrendo a *scripts* LUA. A comunicação é feita por registo em *logs* em detrimento da interação direta com o REST API do *Wazuh*, para possibilitar a comunicação assíncrona de dados com o SIEM e evitar eventos perdidos caso o SIEM ou a REST API não estejam disponíveis.

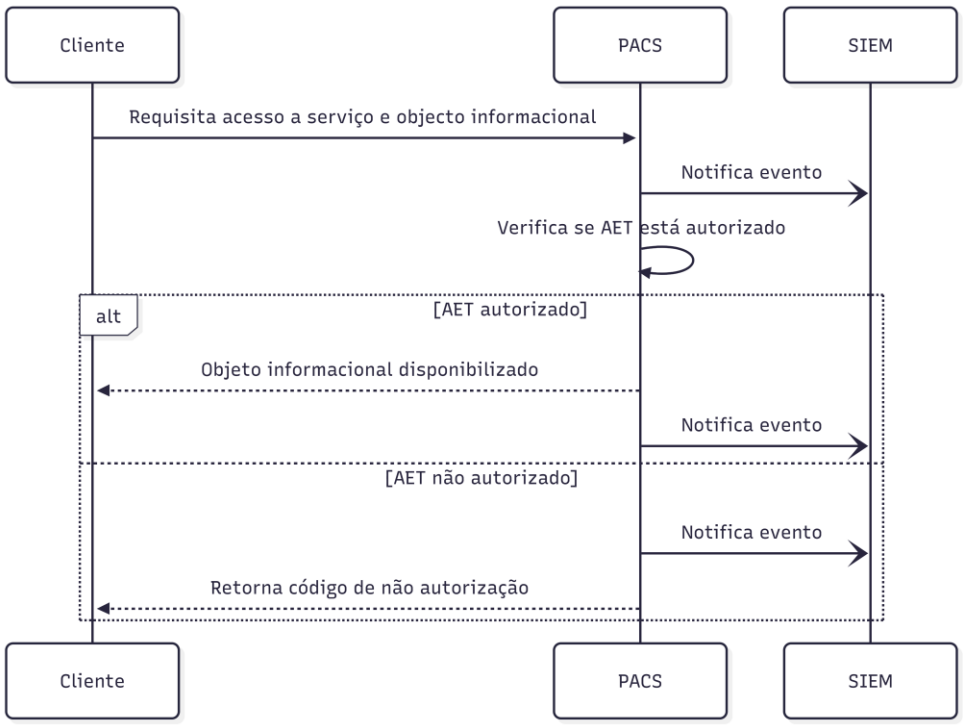


Figura 17 - Diagrama de sequência de requisição de objeto informacional por sistemas internos ao repositório PACS, através de DICOM (DIMSE)

4.3.2. Gestão de eventos e informações de segurança

Na arquitetura do sistema, o SIEM *Wazuh* é o repositório de eventos de segurança, para o qual são enviados eventos específicos relativos a cada pedido de acesso a objetos informacionais. A comunicação do evento pode ser feita pelos diversos sistemas (*reverse*

proxy, serviço *WebDAV*, *Orthanc DICOMweb*, serviços web HL7 e controlador de domínio) através do agente do SIEM ou envio de pedidos por *HTTP webwooks* da *Wazuh* API.

Na solução adotada, o agente nativo do SIEM *Wazuh*, "*OSEC client*", é instalado no sistema e configurado para consumir os *logs* dos serviços a monitorizar, através da inclusão da entrada "<localfile>" no ficheiro de configuração "/var/ossec/etc/ossec.conf" (*Linux*) ou "C:\Program Files (x86)\ossec-agent\ossec.conf" (Windows). A periodicidade da comunicação do agente com o servidor é ajustada para comunicação de dados a cada 10 segundos.

Para a configuração do *Orthanc* foi efetuada a confguração descrita na Figura 18.

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/orthanc/orthanc.log</location>
</localfile>
```

Figura 18 - Configuração do agente *Wazuh* no *Orthanc*

Na configuração do *OSEC Client* no *reverse proxy*, é configurado o local de armazenamento dos logs de acessos e erros (Figura 19).

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/nginx/access.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/nginx/error.log</location>
</localfile>
```

Figura 19 - Configuração do agente *Wazuh* no *Reverse Proxy*

A informação que conta nos *logs* do *Orthanc* é ajustada por *scripts* LUA. No Anexo B, Anexo C, Anexo D e Anexo E são apresentados formas de integração dos dados para vários tipos de pesquisa e os protocolos DICOM utilizados.

No caso do *Reverse Proxy*, os *logs* também são ajustados para refletir a *query string* presente na URL do recurso a consultar (mencionado na Secção 4.3.4).

4.3.3. Repositório central dos dados da plataforma

Os dados encontram-se distribuídos por diversos sistemas e a sua correlação e fornecimento para a HCDW ocorrem num ponto central. O SGBD utilizado nesta arquitetura

é o *PostgreSQL* Server, que permite as seguintes funcionalidades relevantes para a arquitetura:

1) tabelas *unlogged*, tabelas permanentes que não são registadas no *Write-Ahead Log*, melhorando o desempenho, para funcionar como *cache* temporária de dados;
2) existência de biblioteca para guardar dados encriptados / desencriptados nos campos das tabelas;
3) vistas materializadas (*materialized views*) que armazenam os resultados numa tabela *snapshot* de consultas complexas e com reduzido grau de mutação dos dados, para permitir consultas rápidas;
4) particionamento de tabelas baseadas em tempo ou recorrendo à extensão *TimescaleDB* (para suportar base de dados de séries temporais), para segmentação temporal dos dados e consolidação de dados mais antigos.

O SGBD *PostgreSQL* integra-se com as bases de dados que podem ser usadas pelos IAM e RIS, através da funcionalidade de *Foreign Data Wrappers* (FDW), permitindo expor tabelas ou vistas remotas como tabelas locais, de modo que sejam expostos temporariamente os dados necessários ao preenchimento das tabelas temporárias com dados pessoais. Para o caso específico, tanto o IAM como o RIS usam também o SGBD *PostgreSQL*. Na Figura 20 é apresentado o exemplo de acesso à tabela remota de IAM para obter o identificador e nome de utilizador presentes no IAM.

```
-- 1) Ativação da extensão no SGBD central
CREATE EXTENSION IF NOT EXISTS postgres_fdw;
-- 2) Criar o servidor remoto
CREATE SERVER iam_pg
  FOREIGN DATA WRAPPER postgres_fdw
  OPTIONS (host iam.host', port '5432', dbname 'iamdb');
-- 3) Mapear utilizador local -> utilizador remoto
CREATE USER MAPPING FOR shared_user_local
  SERVER iam_pg
  OPTIONS (user 'shared_user_remote', password 'pwd');
-- 4) Criar tabela remota (foreign table)
CREATE FOREIGN TABLE ft_users (
  id      integer,
  username    text,
  email   text
)
  SERVER iam_pg
  OPTIONS (schema_name 'public', table_name 'users');
-- 5) Usar como se fosse local
SELECT * FROM ft_users;
```

Figura 20 - Acesso a tabelas remotas através de FDW

As integrações com o SIEM requerem outra abordagem porque o *Wazuh* não utiliza um SGBD relacional. Para este fim são feitas requisições à *Wazuh Indexer* API, cuja resposta é dada pelo indexador *OpenSearch*. Para a utilização de sintaxe SQL nas requisições, pode ser instalado o "*SQL plugin*", que permite limitar os campos e aplicar filtros de pesquisa. As duas opções podem ser utilizadas em paralelo, em função do tipo de pesquisa a efetuar, do volume de dados a obter e da velocidade de resposta ao pedido. O processo inicia na requisição dos dados, seleção e inserção dos dados relevantes na camada de processamento de dados.

4.3.4. Fluxos de dados

Nesta secção são apresentados os quatro fluxos de disponibilização de objetos informacionais: fluxo de relatórios em edição, fluxo de relatórios finalizados, fluxo de dados estruturados (PACS/DICOM) e fluxo de dados estruturados (HL7) para entidades externas (através de serviços web).

Para o fluxo de relatórios em edição, consideram-se os seguintes estágios do documento e os formatos utilizados:

1. Criação inicial do relatório – formato *OpenDocument Text (ODT)* em uso;
2. Revisão do relatório – formato *ODT* em uso;
3. Validação do relatório – formato *ODT* arquivado, geração de *Portable Document File (PDF)*.

No terceiro estágio do relatório, o ficheiro PDF é assinado digitalmente, sendo este o documento a disponibilizar através dos serviços web HL7 e em posteriores consultas de estudos anteriores.

Para disponibilização dos ficheiros no formato *OpenDocument Text* para edição através de processadores de texto (*LibreOffice versão 25*), instalados em *clientes Microsoft Windows 11*, foram consideradas soluções somente baseadas em servidores de ficheiros *on-premise* (instalados e geridos fisicamente na entidade), com sistemas operativos *Windows Server 2022 Standard* ou *Linux*, com o serviço de partilha de ficheiros instalado e ativado.

Através dos servidores, e para o propósito de acesso e edição remota de documentos, podem ser adotados os protocolos FTP/SFTP, SMB/CIFS, NFS e *WebDAV*. A integração de acesso direto através do processador de texto é facilitada quando se recorre aos

protocolos SMB/CIFS e *WebDAV*, sem necessitar de instalação de componentes adicionais aos instalados no serviço de partilha de ficheiros. A análise dos protocolos SMB/CIFS e respetivas funcionalidades de auditoria de acesso a ficheiros (*Audit Object Access*) revela que é possível identificar a listagem e o acesso a ficheiros através dos eventos registados no *Event Viewer* apresentados na Tabela 7.

Tabela 7 - Lista de eventos gerados pelo *Audit Object Access*

ID	**Descrição do Evento**	**Dados apresentados**
4656	Pedido para aceder a um objeto (intenção de abrir/apagar antes do resultado)	Objeto
4663	Tentativa de ação num objeto (leitura, escrita, eliminação, permissões alteradas)	Utilizador, processo, ação específica e caminho do ficheiro
4658	Identificador (*handle*) de um objeto é fechado	(sem dados apresentados)
4660	Objeto eliminado	(sem dados apresentados)
4670	Permissões de objeto alteradas	(sem dados apresentados)
5145	Acesso a partilha de rede (específico para ficheiros partilhados no servidor)	(sem dados apresentados)

A utilização da auditoria de acesso a ficheiros tende a gerar um número elevado de eventos por cada acesso e uma elevada ocorrência de falsos positivos no SIEM.

Ao nível do controlo de acessos aos recursos, a autenticação em SMB/CIFS com *Microsoft Active Directory* utiliza primordialmente o protocolo *Kerberos* para validar identidades de forma segura num domínio. No processo, o cliente solicita um *ticket* ao *Domain Controller* usando as credenciais do utilizador. O *ticket* é apresentado posteriormente ao servidor de ficheiros para aceder à partilha.

Para facilitar a integração com os demais sistemas e permitir um controlo mais granular dos recursos recorrendo ao *reverse proxy* e IAM, rejeita-se o uso de SMB/CIFS em detrimento da solução baseada em *WebDAV*, recorrendo ao servidor NGNIX com módulos *nginx-dav-ext-module*[5] e *ngx_https_dav_module*, com ativação da funcionalidade de *locking* para evitar edição simultânea e configuração de autenticação por OIDC. Na

[5] https://github.com/arut/nginx-dav-ext-module

autenticação recorre-se ao *OpenResty*, conjugado com o script *lua-resty-openidc,* para a integração entre NGINX e *Keycloak*.

As consultas efetuadas através do *WebDAV* são também registadas no *log* para posterior envio para o SIEM, com os seguintes dados: IP do utilizador, nome da conta do utilizador, documento solicitado, métodos *WebDAV*, data e hora do acesso.

No fluxo de relatórios finalizados e fluxo de dados para entidades externas, o registo é feito ao nível aplicacional bem como no servidor web (NGINX), que neste caso funciona como *reverse proxy*, que direciona pedidos externos para os serviços internos HL7.

O uso de comunicações cifradas de *endpoints* exteriores invalida a recolha de todos os dados necessários à identificação da entidade externa que efetuou o pedido através do *reverse proxy*. Deste modo, considerando que estes serviços web HL7 registam dados de auditoria na base de dados e em *logs.* Estes registos são recolhidos através do agente SIEM e por acesso direto do *PostgreSQL* aos registos de auditoria (tabelas existentes no RIS para registo de acessos a relatórios médicos), para disponibilização dos dados na plataforma HCDW.

Nos fluxos de dados estruturados (internos), nomeadamente na utilização de comunicações *DICOMweb* e HL7 FHIR no modelo cliente-servidor, o servidor aplicacional disponibiliza integração com IAM e *logs* de acesso para consumo do agente SIEM

No caso do PACS no cenário, *Orthanc* versão 1.12.10, a integração com o IAM é feita através da utilização da API REST e protocolos *DICOMweb*, utilizando o *Orthanc Auth Service* e plugin *authorization*.

Para o registo de acessos às chamadas de *DICOMweb*, existe a necessidade de utilizar a estratégia de *reverse proxy* explicada anteriormente, de modo a intercetar os dados de *request* do protocolo HTTP, nomeadamente da query do método *GET*, para obter *PatientID* (identificador único do paciente), *StudyInstanceUID* (identificador único de estudo). O utilizador e a autorização associada estão também presentes no cabeçalho do *request*. Na resposta aos pedidos (HTTP *response*) pode ser confirmado se o acesso ao recurso foi autorizado e os dados que foram fornecidos ao sistema requerente.

4.3.5. Plataforma

A plataforma de visualização de dados dos acessos aos objetos informacionais comunica somente com a camada de tratamento de dados, onde reside o sistema de gestão de base de dados. As ações na camada de apresentação podem despoletar na

camada de tratamento de dados a requisição a outros sistemas, nomeadamente IAM, SIEM e RIS, sendo esta última camada a intermediária das ações requeridas pelo utilizador.

A plataforma tem uma estrutura base que assegura a autenticação e autorização perante o IAM. As vistas e funcionalidades são implementadas em módulos recorrendo ao paradigma *Model-View.Controller* (MVC), com dois ficheiros por módulo e modelos baseados nas entidades mencionadas na secção 4.2.1 Modelo conceptual e lógico .

4.4. TECNOLOGIAS APLICÁVEIS

As tecnologias selecionadas seguem a premissa inicial de um sistema baseado em componentes *open-source* ou de licenciamento sem custos para fins comerciais.

Os sistemas de IAM, SIEM, SGBD e HCDW, por serem compatíveis com distribuições *Linux*, foram instalados em máquinas virtuais *Ubuntu Server 24.04 LTS*, com recursos de CPU, memória RAM e de armazenamento partilhados.

Para o suporte da aplicação HCDW é utilizada a linguagem de programação *Python*, com recurso ao módulo *Flask*[6] e implementado o paradigma MVC. A estrutura de ficheiros segue o seguinte padrão:

```
app/
├── models/      # Dados + lógica de negócio (SQLAlchemy)
│   └── paciente.py
├── views/       # Templates HTML/Jinja2
│   └── consulta1.html
├── controllers/ # Rotas Flask + processamento
│   └── rotas_consulta1.py
└── __init__.py  # Factory pattern + inicialização
```

Figura 21 - Exemplo de estrutura da aplicação com *Flask* MVC

O recurso ao paradigma MVC permite a separação do código para a realização de testes unitários por camada, é escalável (adicionar uma funcionalidade não implica mudanças nas restantes funcionalidades já implementadas), facilidade de acesso e manutenção dos dados. A componente de *model* é assegurada pelo módulo *SQLAlchemy*[7]. Os dados são obtidos diretamente do *PostgreSQL* através do módulo

[6] https://flask.palletsprojects.com/en/stable/

[7] https://www.sqlalchemy.org/

SQLAlchemy, e carregados em memória para o módulo Pandas[8]. Para análise de dados com componente gráfica e tabelas é utilizado o módulo *Dash*[9].

4.5. PROTÓTIPO DE BAIXA FIDELIDADE

Nesta seção é apresentado um protótipo de baixa fidelidade da aplicação HCDW. Na Figura 22 está o fluxo de utilização da camada de apresentação com as interfaces de autenticação do utilizador, listagens e detalhes de vários tipos de acessos (justificados, injustificados, externos, eventos adversos), pesquisas gerais de informação, emissão e histórico de relatórios, configurações do utilizador e histórico de acesso dos utilizadores à aplicação.

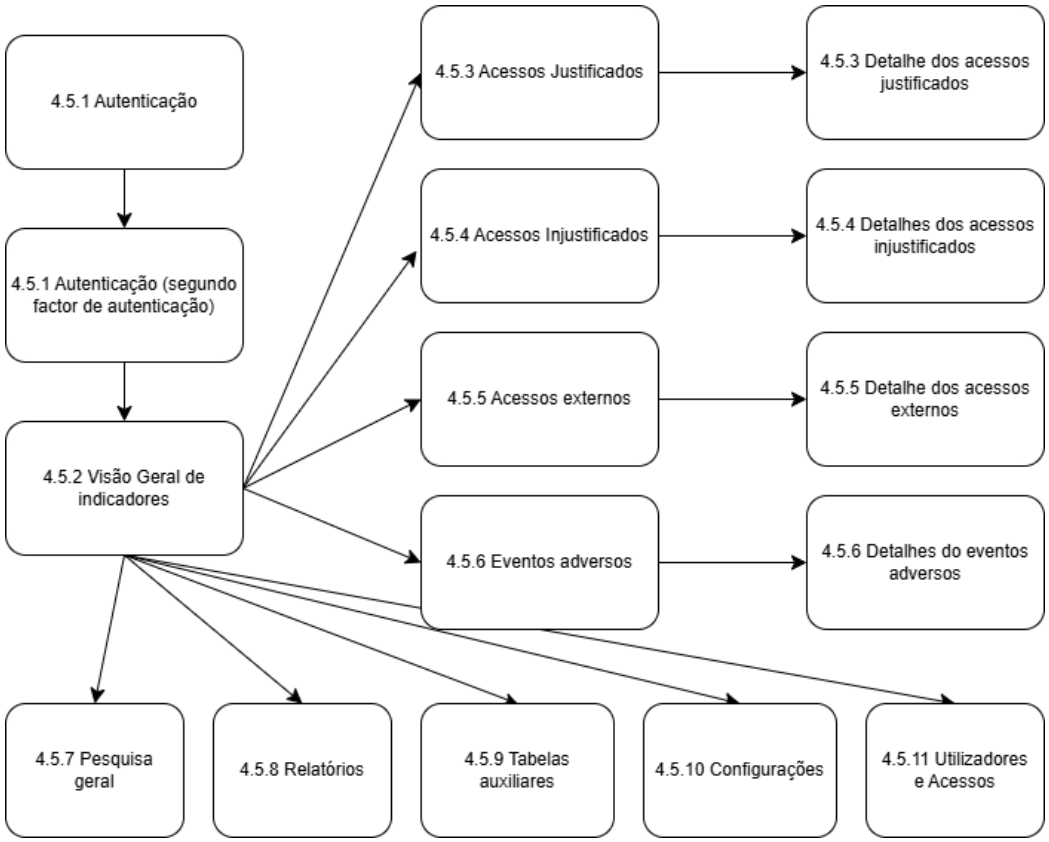


Figura 22 - Fluxo de utilização do HCDW

[8] https://pandas.pydata.org/

[9] https://dash.plotly.com/tutorial

4.5.1. Autenticação

Na interface de autenticação é solicitado o utilizador e palavra-chave (Figura 23). A autenticação é gerida pelo IAM.

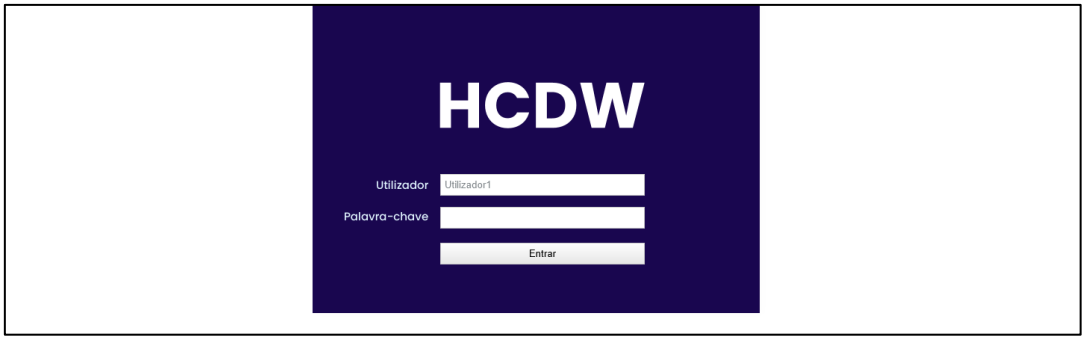


Figura 23 - Interface HCDW de autenticação do utilizador

Se a opção de “Habilitar TOPT” estiver selecionada no painel de configurações, é apresentada ao utilizador uma validação através de um segundo fator de autenticação (*Two Factor Authentication - 2FA)* (Figura 24), sendo esta realizada através do mecanismo de *Time-based One Time Password* (TOTP). Este método requer a utilização de uma aplicação TOTP (por exemplo, a aplicação *Authy*) e o registo de uma chave secreta partilhada.

Figura 24 - Interface HCDW de validação TOTP do utilizador

4.5.2. Visão geral e indicadores

Após autenticado, o utilizador entra numa nova página web onde tem um menu lateral para aceder às várias listagens de informação. Nesta página inicial são apresentados quatro indicadores mensais e um gráfico com a evolução anual dos acessos justificados e injustificados aos objetos informacionais (Figura 25).

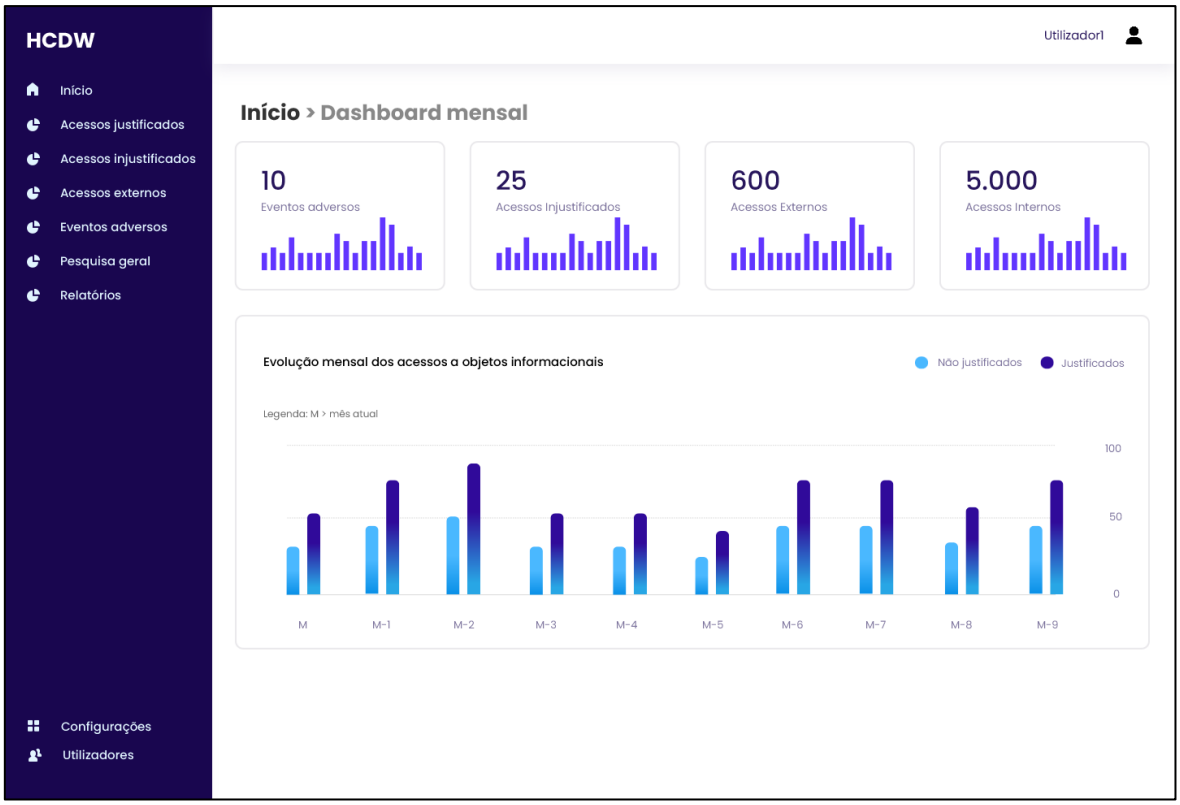


Figura 25 - Interface HCDW de vista geral e indicadores

4.5.3. Acessos justificados

Na interface de acessos justificados são listados os registos da tabela “eventos”, que tenham associado uma taxionomia de justificação do acesso ao objeto informacional (Figura 26). A listagem apresenta propositadamente apenas os códigos associados aos registos, de forma a não apresentar dados pessoais.

Por cada linha são apresentados o identificador do evento, a data/hora de ocorrência do evento, o código do paciente associado ao objeto informacional, o código do utilizador associado ao evento e o código de médico se o utilizador estiver associado a um médico.

O filtro dos registos é feito através das taxionomias que classificam o evento de acesso justificado, ou seja, todas as taxionomias cujo código contenha o conjunto de caracteres “AJUS”.

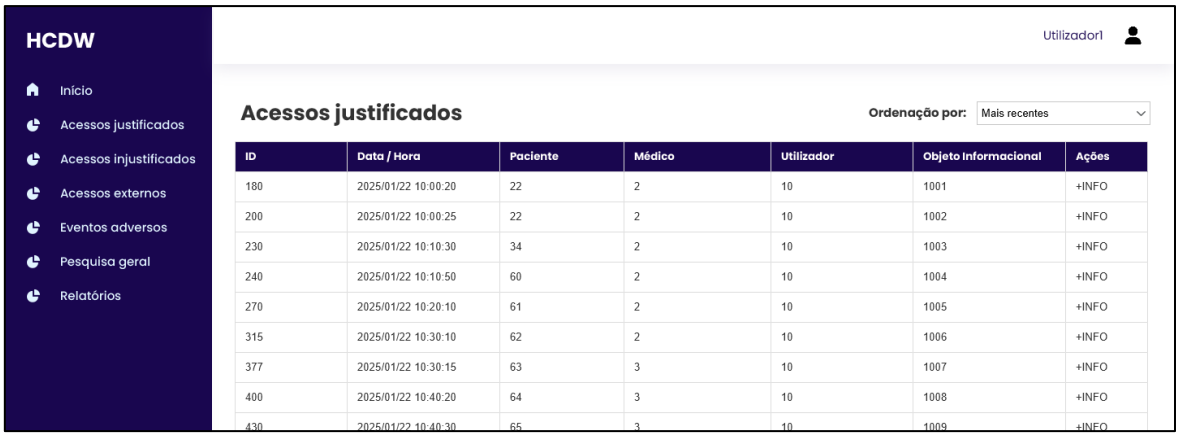


Figura 26 - Interface HCDW de listagem de acessos justificados

Os dados pessoais são apresentados no detalhe da linha (Figura 27), com requisição direta às fontes de dados e armazenamento em tabelas temporárias. Os dados apresentados são: identificador do evento; data e hora de ocorrência do evento; código e detalhe do OI (tipo de estudo realizado) com data e hora de sua criação: paciente associado; médico associado (se o utilizador que gerou o evento estiver associado a um médico); sistema de origem do acesso; utilizador (que no caso de ser um médico, acrescenta à descrição o texto “(Médico)”); e a justificação baseada na taxionomia.

O utilizador poderá ser um médico ou um utilizador interno da organização, em função da taxionomia do evento.

Figura 27 - Interface HCDW de detalhe de acesso justificado

4.5.4. Acessos injustificados

Na Figura 28 é apresentada a interface de listagem de acessos injustificados. Os acessos injustificados são todos os eventos classificados com taxionomias cujo código contenha o conjunto de caracteres “NJUS”.

Figura 28 - Interface HCDW de listagem de acessos injustificados

No detalhe do acesso injustificado (Figura 29) são apresentados os mesmos campos de informação mencionados nos detalhes dos acessos justificados.

Na ausência de taxionomia, o campo justificação é preenchido com o texto “sem justificação”. Pode ocorrer o acesso por parte de um utilizador sem ter justificado o seu acesso no RIS, ou acesso ao recurso por utilizador não identificado.

Figura 29 - Interface HCDW de detalhe de acesso injustificado

4.5.5. Acessos externos

Na listagem de acessos externos aos OI (Figura 30), são apresentados os mesmos campos mencionados nas listagens anteriores. Os eventos têm associado taxionomias com código contendo o conjunto de caracteres “ACEXT”.

Estes eventos estão sempre associados a um paciente, médico e sistema externo. Por sua vez, não sendo um acesso com um utilizador interno, o evento fica sem utilizador associado. Nos acessos externos é feita sempre a associação do evento SIEM (*IDEventoSIEM*).

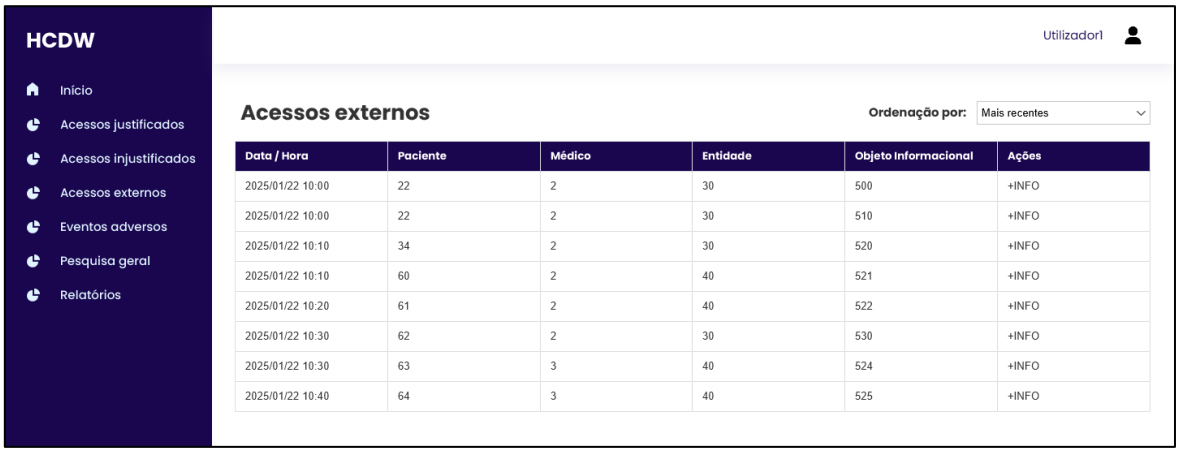


Figura 30 - Interface HCDW de listagem de acessos externos

No detalhe do acesso externo (Figura 31) são apresentados os campos: identificador do evento, OI acedido, paciente ao qual pertence o OI; sistema de acesso.

Figura 31 - Interface HCDW de detalhe de acesso externo

4.5.6. Eventos adversos

A listagem de eventos adversos (Figura 32) refere-se a eventos criados através do SIEM que envolvem o acesso a um OI identificável, mas sem existir uma justificação para o mesmo. Pode ser atribuído ao evento o identificador de sistema, mas pode ser omisso o identificador de utilizador. Distinguem-se dos eventos legítimos classificados com acesso externo porque a origem do acesso é um sistema considerado ilegítimo (por exemplo, acesso por sistema de ficheiros ao documento).

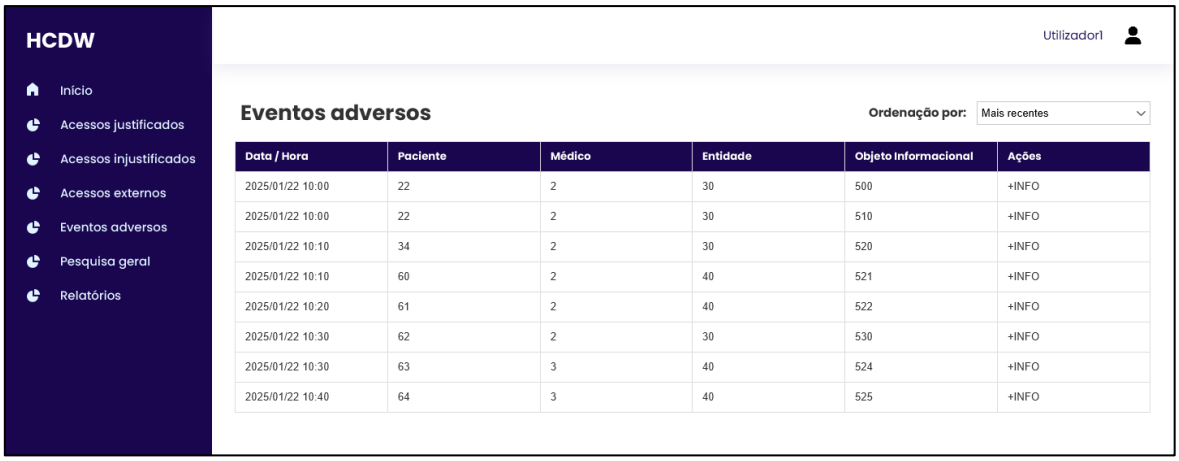


Figura 32 - Interface HCDW de listagem de eventos adversos

O detalhe do evento adverso contém informação semelhante aos anteriores (Figura 33)

Figura 33 - Interface HCDW de detalhe de evento adverso

4.5.7. Pesquisa geral

A página de pesquisa geral permite a pesquisa na tabela de todos os eventos (Figura 34). Através do acesso ao link “+INFO” presente em cada linha da tabela, na coluna ações, é possível aceder ao detalhe, sendo encaminhado para uma página do tipo de evento que se trata (justificado, injustificado, acesso externo ou evento adverso).

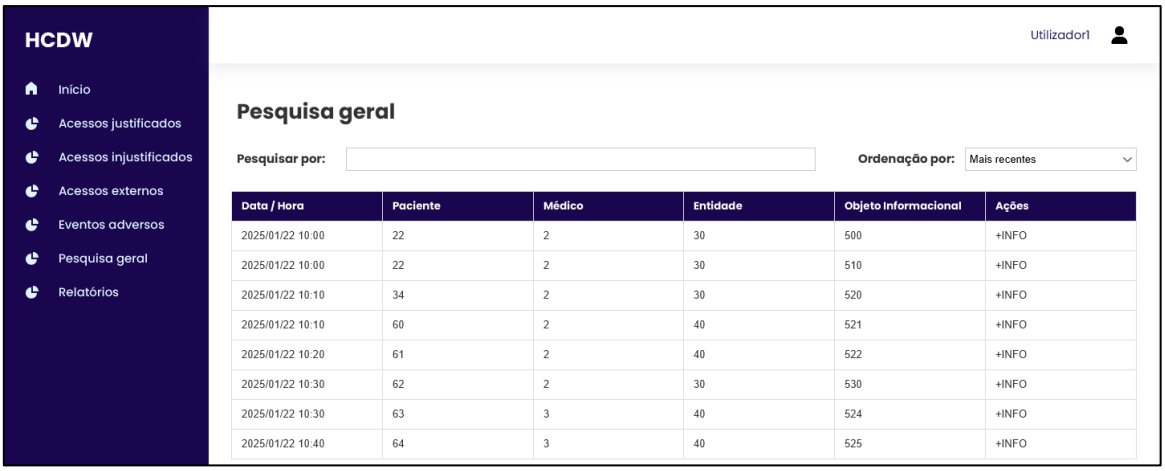


Figura 34 - Interface HCDW de pesquisa geral de informação (eventos)

4.5.8. Relatórios

A página de emissão de relatórios disponibiliza um formulário de parametrização dos dados a serem incluídos no relatório (Figura 35). Através desta mesma página são listados os relatórios emitidos. Para consultar os relatórios em formato PDF, aciona-se o link “VER RELATÓRIO” presente em cada linha do registo.

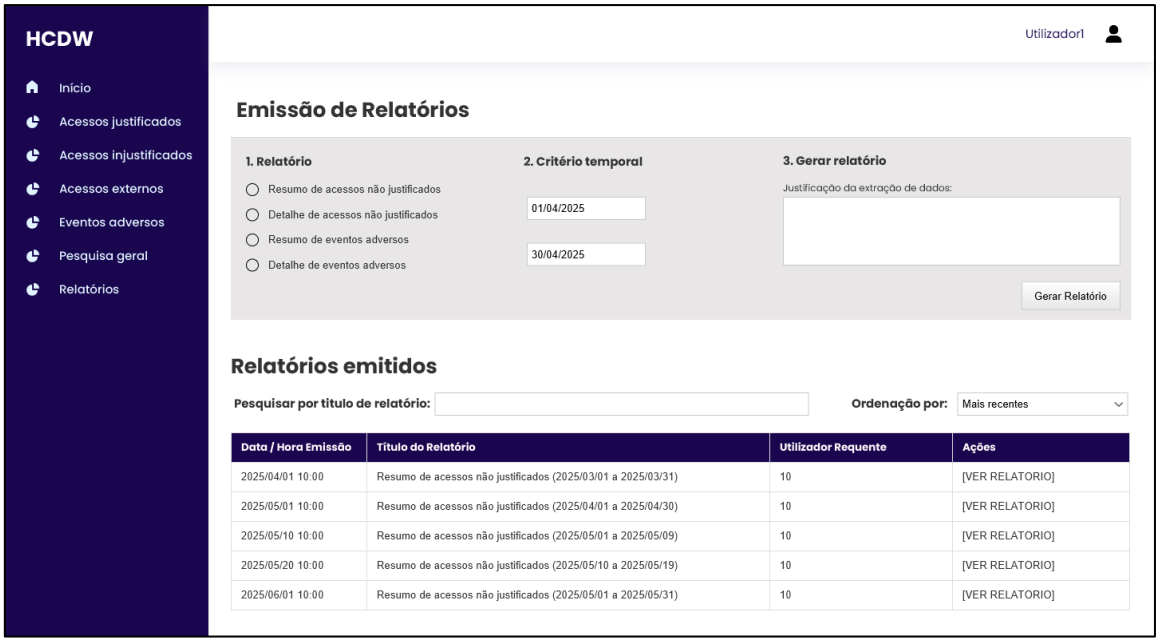


Figura 35 - Interface HCDW de emissão e consulta de histórico de relatórios

4.5.9. Tabelas auxiliares

A interface de gestão de tabelas auxiliares (Figura 36) permite gerir os dados presentes nas tabelas de base de dados “Sistemas” e “Taxionomias”.

Os dados presentes nestas tabelas não são inseridos de forma dinâmica pelo serviço de processamento de dados, sendo que tanto os sistemas como as taxionomias têm de ser inseridos manualmente. Os registos destas tabelas que estejam correlacionados com registos de outras tabelas não podem ser modificados ou eliminados.

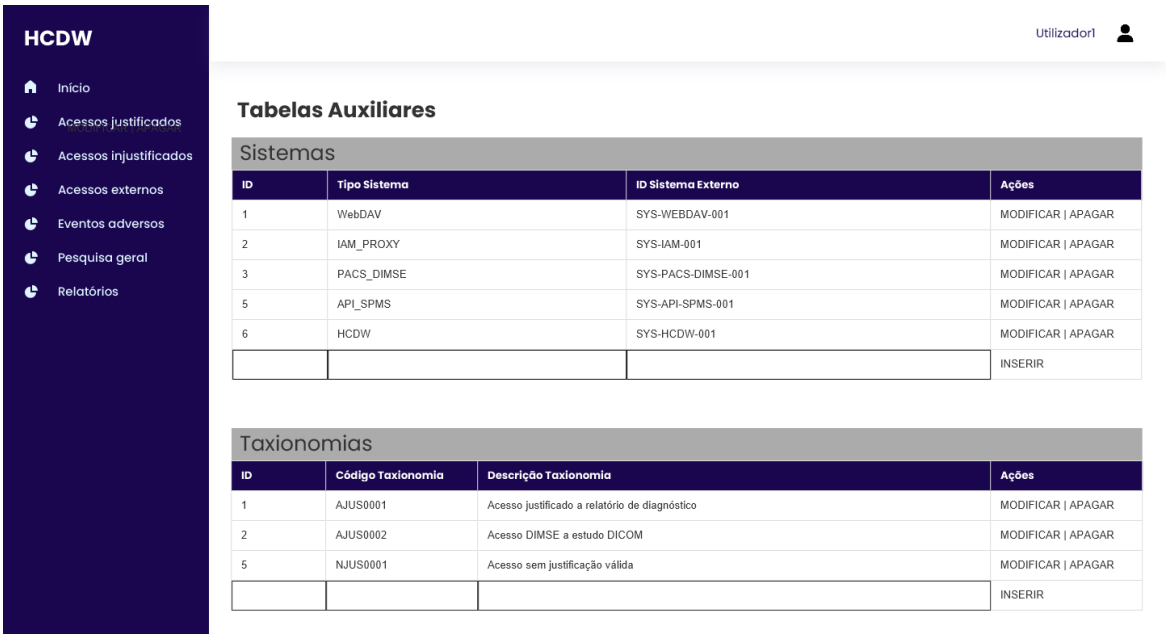


Figura 36 - Interface HCDW de gestão de tabelas auxiliares

4.5.10. Configurações

A interface de configurações (Figura 37) permite habilitar a funcionalidade de duplo fator de autenticação (2FA) e configurar a chave secreta para TOTP.

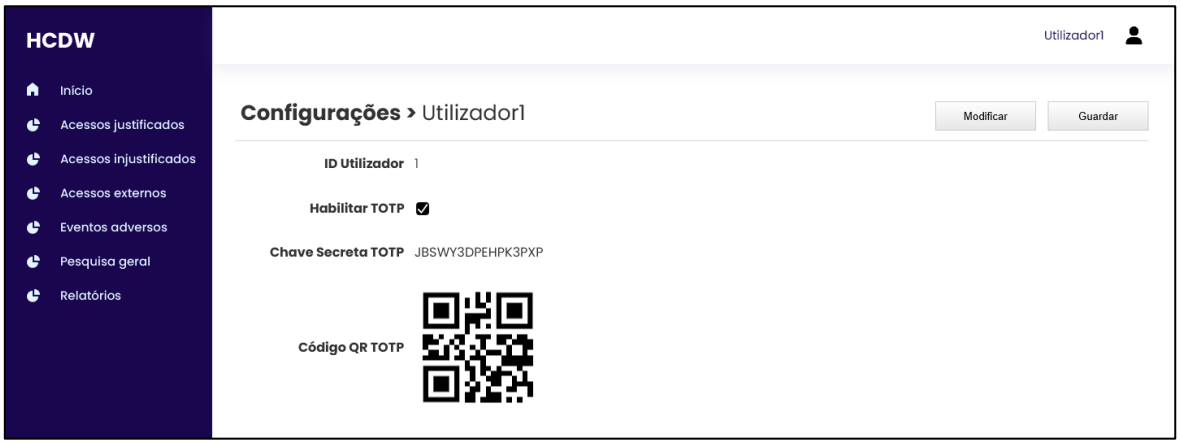


Figura 37 - Interface HCDW de configurações do utilizador

4.5.11. Utilizadores e acessos

Na interface de utilizadores e acessos, são listados os acessos e ações efetuadas na aplicação HCDW (Figura 38).

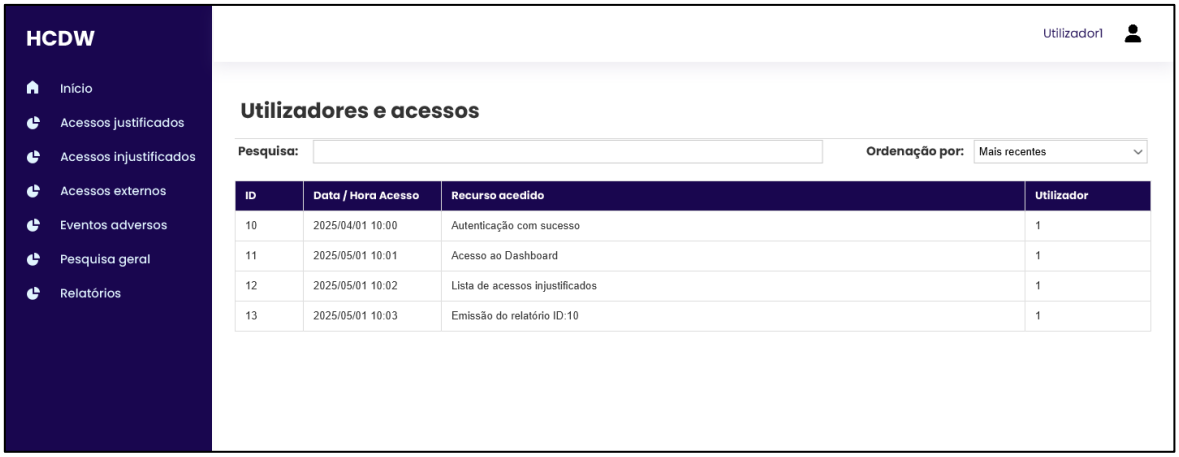


Figura 38 - Interface HCDW de histórico de acessos dos utilizadores

4.6. VALIDAÇÃO E AVALIAÇÃO

Nesta Secção apresenta-se a validação e avaliação da prova de conceito, através de cenários de uso e simulação dos fluxos.

Antes da apresentação das simulações dos cenários, são apresentados na Subsecção 4.6.1 os dados que devem constar nas tabelas de suporte, necessários para as consultas. Na Subsecção 4.6.2 são apresentados os vários cenários de uso com a respetiva simulação baseada em dados fictícios.

4.6.1. Dados de referência necessários para as consultas

Para o correto funcionamento da plataforma HCDW, as tabelas de base de dados “Taxionomias” e “Sistemas” devem conter previamente os valores de exemplo listados na Tabela 8 e Tabela 9, respetivamente.

Tabela 8 - Dados da tabela Taxionomias

IDTaxionomia	CodTaxionomia	DescTaxionomia
1	AJUS0001	Acesso justificado a relatório de diagnóstico
2	AJUS0002	Acesso DIMSE a estudo DICOM
3	AJUS0003	Acesso DICOMweb a estudo DICOM

IDTaxionomia	CodTaxionomia	DescTaxionomia
4	AJUS0004	Acesso externo via SPMS/SNS
5	NJUS0001	Acesso sem justificação válida
6	NJUS0002	Evento adverso – analisar no SIEM
8	AJUS0006	Acesso a página do HCDW

Tabela 9 - Dados da tabela Sistemas

IDSistema	TipoSistema	IDSistemaExt
1	WebDAV	SYS-WEBDAV-001
2	IAM_PROXY	SYS-IAM-001
3	PACS_DIMSE	SYS-PACS-DIMSE-001
4	PACS_DICOMWEB	SYS-PACS-DCMWEB-001
5	API_SPMS	SYS-API-SPMS-001
6	HCDW	SYS-HCDW-001

Para a simulação apresentada na próxima Secção, considera-se que existem dados nas tabelas de base de dados “Pacientes”, “Medicos” e “Utilizadores”, tal como apresentado na Tabela 10, Tabela 11 e

Tabela 12. De referir que estes dados, numa utilização real da plataforma, são inseridos automaticamente pela interação entre sistemas, nomeadamente na recolha de dados existentes no RIS e no IAM.

Tabela 10 - Dados da tabela Pacientes

IDPaciente	IDPacienteRIS
10	RIS-PAC-00012
11	RIS-PAC-00019

Tabela 11 - Dados da tabela Medicos

IDMedico	IDMedicoRIS
20	RIS-MED-00005
21	RIS-MED-00008

Tabela 12 - Dados da tabela Utilizadores

IDUser	IDPaciente	IDMedico	IDUserIAM
1	NULL	20	iam-user-med-00005
2	NULL	21	iam-user-med-00008
4	NULL	NULL	iam-user-adm-00010
5	10	NULL	iam-user-pac-00012
6	NULL	NULL	iam-user-mgm-00001

4.6.2. Cenários de uso e simulação com dados fictícios

Para o estudo da solução foram definidos doze cenários de uso: os primeiros quatro correspondem a fluxos de acesso a objetos informacionais, ou seja, os fluxos a serem monitorizados pela solução apresentada (Tabela 13, Tabela 15, Tabela 17 e Tabela 19). Os restantes cenários apresentam a interação do utilizador com a plataforma HCDW , Tabela 21, Tabela 23, Tabela 25, Tabela 27, Tabela 29, Tabela 31, Tabela 33, Tabela 35 e Tabela 38).

Em cada cenário são mencionados: o ator com autorização para acesso ao recurso, as pré-condições do cenário, o fluxo normal de execução de tarefas e os fluxos alternativos (por exemplo, falha de autenticação ou autorização, indisponibilidade do recurso), bem como pós-condição com menção ao que é esperado ter no final do fluxo de interação com o sistema. No caso dos cenários de uso relativos à interação com a plataforma HCDW, também é apresentado no campo “Ator” o papel autorizado a executar a operação, tal como definido previamente nos requisitos do sistema.

Na simulação associada a cada cenário são apresentados: os dados produzidos e recolhidos nos sistemas de origem e enviados para o SIEM, o fluxo de informação expectável entre sistemas, os tratamentos efetuados, as pesquisas SQL executadas e a informação apresentada ao utilizador final. Os cenários são apresentados nas Tabela 14, Tabela 16, Tabela 18, Tabela 20, Tabela 22, Tabela 24, Tabela 26, Tabela 28, Tabela 30, Tabela 32, Tabela 34, Tabela 36 e Tabela 39.

Reforça-se que os dados presentes neste capítulo são sintéticos, gerados apenas para a finalidade de simulação e não correspondem a sistemas, indivíduos ou relatórios reais.

O primeiro cenário refere-se ao acesso ao sistema de armazenamento de ficheiros para a criação e edição do relatório de diagnóstico, com a simulação dos eventos gerados em cada passo (Tabela 13 e Tabela 14).

Tabela 13 - Cenário 1 - Criação e edição do relatório de diagnóstico médico

Identificador	1
Cenário	Criação e edição do relatório de diagnóstico médico
Ator(es)	Médico
Pré-condições	O utilizador deve possuir conta de acesso ao sistema (presente no IAM) com autenticação válida e autorização para visualização e edição do relatório. O relatório deve existir no servidor WebDAV, identificado pelo seu identificador único.
Fluxo normal	1) O utilizador autentica-se no sistema de consulta e edição de relatórios, sendo criado um *token* de acesso pelo IAM. 2) O utilizador insere ou seleciona a justificação de acesso ao relatório a partir de uma lista pré-definida. 3) O utilizador acede ao recurso (relatório) através do link correspondente ao servidor WebDAV. 4) O utilizador visualiza ou edita o relatório de diagnóstico.
Fluxos alternativos	1.1) O utilizador falha na autenticação (credenciais inválidas) – o acesso ao recurso é negado e o evento registado no SIEM. 1.2) O utilizador autentica-se com sucesso, mas não possui autorização para aceder ao recurso – o acesso é negado e o evento é registado no SIEM
Pós-condição	Registo no SIEM do evento de acesso, incluindo a identificação do utilizador, do recurso acedido, da justificação apresentada, do endereço IP de origem e do resultado da operação

Tabela 14 - Simulação de dados gerados e consumidos no Cenário 1

Fluxos	**Dados**
1. Pedido de autenticação do	[Proxy IAM envia para SIEM] eventid: 1; parenteventid: 1; system: auth_iam; source_ip: 192.168.1.10; state: request_auth; destination_url: https://webdav-server/reports/

Fluxos	**Dados**
utilizador (Proxy IAM)	5c6ffbdd40d9556b73a21e63c3e0e904f5303c3d1b6e8e2a5f8f8f9b1a5c1c2; timestamp: 2025-11-05T10:46:00Z
2. Autenticação bem-sucedida (fluxo normal)	[Proxy IAM envia para SIEM] eventid: 2; parenteventid: 1; system: auth_iam; source_ip: 192.168.1.10; state: access_allowed; userid: 1; destination_url: https://webdav-server/reports/5c6ffbdd40d9556b73a21e63c3e0e904f5303c3d1b6e8e2a5f8f8f9b1a5c1c2; timestamp: 2025-11-05T10:48:00Z
2.1. Autenticação sem sucesso (utilizador incorreto) (fluxo alternativo)	[Proxy IAM envia para SIEM] eventid: 2; parenteventid: 1; system: auth_iam; source_ip: 192.168.1.10; state: access_denied; username: utilizador123; destination_url: https://webdav-server/reports/5c6ffbdd40d9556b73a21e63c3e0e904f5303c3d1b6e8e2a5f8f8f9b1a5c1c2; timestamp: 2025-11-05T10:48:00Z
2.2. Autenticação sem sucesso (utilizador sem permissões para aceder ao recurso) (fluxo alternativo)	[Proxy IAM envia para SIEM] eventid: 2; parenteventid: 1; system: auth_iam; source_ip: 192.168.1.10; state: no_authoriz; userid: 4; destination_url: https://webdav-server/reports/5c6ffbdd40d9556b73a21e63c3e0e904f5303c3d1b6e8e2a5f8f8f9b1a5c1c2; timestamp: 2025-11-05T10:48:00Z
3. Relatório é disponibilizado pelo servidor WebDAV	[WebDAV envia para SIEM] eventid: 3; parenteventid: 1; system: webdav_server; source_ip: 192.168.1.10; state: document_accessed; userid: 1; patientid:10; justification: 1; timestamp: 2025-11-05T10:50:00Z
4. Inserção do evento na base de dados (HCDW)	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (101, 10, 2, 'wazuh-evt-20251105-00001', '2025-11-05T10:50:00+00', 1);

O segundo cenário refere-se ao acesso interno para armazenar ou recuperar estudos DICOM do PACS, através dos protocolos DIMSE, para acesso às imagens de suporte ao diagnóstico médico (Tabela 15 e Tabela 16).

Tabela 15 - Cenário 2 - Acesso interno ao PACS via DIMSE

Identificador	2
Cenário	Acesso interno ao PACS através de DIMSE para armazenar ou recuperar estudos DICOM
Ator(es)	Médico, Técnico de radiologia
Pré-condições	O sistema cliente deve estar previamente registado na lista de AET autorizados a aceder ao sistema PACS. O estudo DICOM deve existir no repositório.
Fluxo normal	1) O utilizador interage com o sistema de origem, que submete um envio (C-STORE) ou recuperação (C-FIND/C-MOVE) do estudo DICOM ao PACS. 2) O HCDW é notificado do acesso e insere automaticamente a justificação de acesso com base no contexto clínico detetado (por exemplo, pedido de exame em curso no RIS) 3) O PACS processa o pedido do utilizador e o utilizador visualiza ou armazena o estudo DICOM.
Fluxos alternativos	2.1) O HCDW não consegue identificar um contexto válido de acesso – a justificação não é inserida e o evento é registado no SIEM como acesso potencialmente indevido. 2.2) O AET de origem não se encontra na lista de sistemas autorizados – a ligação é recusada pelo PACS e o evento é registado no SIEM.
Pós-condição	Registo no SIEM do evento DIMSE, incluindo o AET de origem, o AET de destino, o tipo de operação (C-STORE, C-FIND, C-MOVE), o identificador do estudo DICOM e o resultado da operação.

Tabela 16 - Simulação de dados gerados e consumidos no Cenário 2

Fluxos	**Dados**
1. Pedido DIMSE de recuperação de estudo (C-MOVE) – sistema PACS	[PACS envia para SIEM] eventid: 10; parenteventid: 10; system: pacs_dimse; aet_source: RIS-WORKSTATION-01; aet_destination: ORTHANC-PACS; operation: C-MOVE; study_instance_uid: 1.2.840.10008.5.1.4.1.1.2.20251105.001; state: request; timestamp: 2025-11-05T09:00:00Z

Fluxos	**Dados**
2. Justificação automática inserida pelo sistema	[PACS envia para o SIEM] eventid: 11; parenteventid: 10; system: pacs_dimse; aet_source: RIS-WORKSTATION-01; justification: APEDEXM00042; context: pedido_exame_ativo; state: justification_ok; timestamp: 2025-11-05T09:00:02Z
2.1. Contexto inválido – justificação não inserida (fluxo alternativo)	[PACS envia para o SIEM] eventid: 11; parenteventid: 10; system: pacs_dimse; aet_source: RIS-WORKSTATION-01; justification: null; context: no_valid_context; state: justification_missing; severity: warning; timestamp: 2025-11-05T09:00:02Z
2.2. AET não autorizado – acesso recusado (fluxo alternativo)	[PACS envia para o SIEM] eventid: 11; parenteventid: 10; system: pacs_dimse; aet_source: UNKNOWN-STATION-99; state: access_denied; reason: aet_not_registered; severity: alert; timestamp: 2025-11-05T09:00:02Z
3. Estudo recuperado com sucesso (fluxo normal)	[PACS envia para o SIEM] eventid: 12; parenteventid: 10; system: pacs_dimse; aet_source: RIS-WORKSTATION-01; aet_destination: ORTHANC-PACS; operation: C-MOVE; study_instance_uid: 1.2.840.10008.5.1.4.1.1.2.20251105.001; patientid: 7; state: success; timestamp: 2025-11-05T09:00:05Z
4. Inserção do evento na base de dados (HCDW) – (fluxo normal)	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (202, 5, 3, 'wazuh-evt-20251105-00012', '2025-11-05T09:00:05+00', 2);
4.1. Inserção do evento na base de dados (HCDW) – acesso sem justificação (fluxo alternativo)	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (202, 5, 3, 'wazuh-evt-20251105-00013', '2025-11-05T09:00:05+00', 5);

O terceiro cenário refere-se ao acesso interno para visualizar estudos DICOM do PACS através dos protocolos *DICOMweb*, para acesso às imagens de suporte ao diagnóstico médico (Tabela 17 e Tabela 18).

Tabela 17 - Cenário 3 - Acesso interno ao PACS via *DICOMweb*

Identificador	3
Cenário	Acesso interno ao PACS através de DICOMweb (WADO-RS/STOW-RS/QIDO-RS) para visualizar estudos DICOM
Ator(es)	Médico, Técnico de radiologia
Pré-condições	O utilizador deve possuir conta de acesso ao sistema PACS com autenticação válida e autorização para visualização de estudos DICOM, através da integração com IAM.
Fluxo normal	1) O utilizador autentica-se no sistema de visualização de estudos DICOM, mediante integração com IAM (*token* OAuth2/ OpenID Connect). 2) O sistema insere automaticamente a justificação de acesso com base no contexto clínico ativo (nomeadamente consulta de exame realizado ou estudos anteriores). 3) O utilizador visualiza o estudo DICOM através do visualizar web.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao recurso é negado e o evento é registado no SIEM. 2.1) Não existe contexto válido de acesso – a justificação não é inserida e o acesso é classificado como potencialmente indevido.
Pós-condição	Registo no SIEM do evento DICOMweb, incluindo o identificador do utilizador, o identificador do estudo DICOM, a justificação de acesso e o resultado da operação.

Tabela 18 - Simulação de dados gerados e consumidos no Cenário 3

Fluxos	**Dados**
1. Pedido de autenticação (Proxy IAM)	[Proxy IAM envia para o SIEM] eventid: 20; parenteventid: 20; system: auth_iam; source_ip: 192.168.2.55; state: request_auth; destination_url: https://pacs-server/wado-rs/studies/1.2.840.10008.5.1.4.1.1.2.20251106.002; timestamp: 2025-11-06T08:30:00Z
1. Autenticação bem-sucedida (fluxo normal)	[Proxy IAM envia para o SIEM] eventid: 21; parenteventid: 20; system: auth_iam; source_ip: 192.168.2.55; state: access_allowed; userid: 8; destination_url: https://pacs-server/wado-

Fluxos	**Dados**
	rs/studies/1.2.840.10008.5.1.4.1.1.2.20251106.002; timestamp: 2025-11-06T08:30:02Z
1.1. Autenticação falhada (fluxo alternativo)	[Proxy IAM envia para o SIEM] eventid: 21; parenteventid: 20; system: auth_iam; source_ip: 192.168.2.55; state: access_denied; username: tecrad99; reason: invalid_credentials; timestamp: 2025-11-06T08:30:02Z
2. Justificação automática inserida	[PACS envia para o SIEM] eventid: 22; parenteventid: 20; system: pacs_dicomweb; userid: 8; justification: ACONS00017; context: consulta_ativa; state: justification_ok; timestamp: 2025-11-06T08:30:03Z
2.1. Contexto inválido – justificação ausente (fluxo alternativo)	[PACS envia para o SIEM] eventid: 22; parenteventid: 20; system: pacs_dicomweb; userid: 8; justification: null; context: no_valid_context; state: justification_missing; severity: warning; timestamp: 2025-11-06T08:30:03Z
3. Estudo DICOM visualizado com sucesso (fluxo normal)	[PACS envia para o SIEM] eventid: 23; parenteventid: 20; system: pacs_dicomweb; source_ip: 192.168.2.55; state: study_accessed; userid: 8; patientid: 33; study_instance_uid: 1.2.840.10008.5.1.4.1.1.2.20251106.002; justification: ACONS00017; timestamp: 2025-11-06T08:30:10Z
4. Inserção do evento na base de dados (HCDW) – fluxo normal	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (305, 8, 3, 'wazuh-evt-20251106-00023', '2025-11-06T08:30:10+00', 3);
4. Inserção do evento na base de dados (HCDW) – acesso sem justificação	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (305, 8, 3, 'wazuh-evt-20251106-00024', '2025-11-06T08:30:10+00', 5);

O quarto cenário refere-se a acessos encaminhados pelo PNB/SPMS para os *webservices* de disponibilização de resultados (Tabela 19 e Tabela 20). A origem do pedido está previamente identificada. Os dois pontos de comunicação interagem através de mensagens HL7 FHIR. A necessidade incide sobre o registo dos dados que estão a ser acedidos.

Tabela 19 - Cenário 4 - Acesso externo via *webservices* de partilha de resultados com o SPMS/SNS

Identificador	4
Cenário	Acesso externo a relatórios em formato PDF através dos *webservices* de partilha de resultados com o SPMS/SNS.
Ator(es)	Utente, Médico do SNS (Médico de Família, de Especialidade ou em contexto de urgência hospitalar)
Pré-condições	O utilizador deve possuir acesso à aplicação MySNS ou aplicações do ecossistema SNS. Deve existir um relatório em formato PDF disponível para consulta, associado ao utente e ao médico que realizou o diagnóstico.
Fluxo normal	1) O utilizador autentica-se na aplicação MySNS ou aplicações do ecossistema do SNS. 2) O sistema externo (SPMS) efetua a requisição do recurso estruturado à entidade prestadora de MCDT. 3) O sistema interno responde à requisição com o ficheiro PDF cifrado. 4) O sistema externo desencripta e disponibiliza os dados estruturados do exame (por exemplo, médico que realizou o diagnóstico, tipo de exame) e relatório em formato PDF ao utilizador.
Fluxos alternativos	3.1) Falha na entrega do recurso – o relatório não existe, ou ocorre erro de comunicação entre sistemas; o evento é registado no SIEM.
Pós-condição	Registo no SIEM do evento de acesso externo, incluindo o identificador do sistema externo requisitante, o identificador do recurso solicitado, o resultado da operação e o *timestamp*.

Tabela 20 - Simulação de dados gerados e consumidos no Cenário 4

Fluxos	**Dados**
1. Pedido de recurso pelo sistema externo SPMS	[Reverse Proxy envia para SIEM] eventid: 30; parenteventid: 30; system: spms_gateway; source_ip: 193.137.200.5; state: resource_request; resource_id: REL-PDF-20251107-00099; patientid_ext: SNS123456789; timestamp: 2025-11-07T14:20:00Z

Fluxos	**Dados**
2. Sistema interno localiza e prepara o recurso	[Monitorização de *Webservices* enviam para SIEM] eventid: 31; parenteventid: 30; system: internal_api; resource_id: REL-PDF-20251107-00099; patientid: 19; state: resource_found; timestamp: 2025-11-07T14:20:01Z
3. Mensagem HL7 FHIR com PDF cifrado entregue com sucesso (fluxo normal)	[Monitorização de *Webservices* enviam para SIEM] eventid: 32; parenteventid: 30; system: internal_api; resource_id: REL-PDF-20251107-00099; patientid: 19; state: resource_delivered; destination_system: spms_gateway; timestamp: 2025-11-07T14:20:02Z
3.1. Falha na entrega do recurso (fluxo alternativo)	[Monitorização de *Webservices* enviam para SIEM] eventid: 32; parenteventid: 30; system: spms_gateway; resource_id: REL-PDF-20251107-00099; state: decryption_failed; reason: invalid_certificate; severity: alert; timestamp: 2025-11-07T14:20:03Z
4. Inserção do evento na base de dados (HCDW) – fluxo normal	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (407, NULL, 4, 'wazuh-evt-20251107-00032', '2025-11-07T14:20:02+00', 4);
4. Inserção do evento na base de dados (HCDW) – evento adverso	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (407, NULL, 4, 'wazuh-evt-20251107-00033', '2025-11-07T14:20:03+00', 6);

De mencionar que nas inserções mencionadas no passo 4 da Tabela 20, o valor do campo *IDUtilizador* é *NULL* porque o acesso é efectuado por um sistema externo (SPMS), não por um utilizador directamente registado na plataforma HCDW.

Os próximos cenários apresentam a interação com a plataforma HCDW. O quinto cenário refere-se à interação com a listagem de acessos justificados (Tabela 21 e Tabela 22).

Tabela 21 - Cenário 5 - Listagem de acessos justificados na HCDW

Identificador	5
Cenário	Listagem de acessos justificados na plataforma HCDW

Ator(es)	Gestor
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com perfil de Gestor, integrada com o IAM
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Acessos Justificados”. 3) O sistema executa a consulta à base de dados e devolve a listagem de eventos com justificação válida. 4) O utilizador consulta a listagem, podendo filtrar por intervalo temporal, sistema de origem ou utilizador.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM.
Pós-condição	Registo no SIEM de pesquisa efetuada, incluindo identificação do gestor, critérios de filtragem e *timestamp*.

Tabela 22 - Simulação de dados gerados e consumidos no Cenário 5

Fluxos	**Dados**
1. Autenticação do gestor no HCDW (integrado com IAM)	[HCDW envia para o SIEM] eventid: 40; parenteventid: 40; system: auth_iam; source_ip: 10.0.0.5; state: access_allowed; userid: 20; destination_url: https://hcdw/acessos-justificados; timestamp: 2025-11-10T09:00:00Z
1.1. Falha na autenticação do gestor no HCDW	[HCDW envia para o SIEM] eventid: 40; parenteventid: 40; system: auth_iam; source_ip: 10.0.0.5; state: access_denied; username: utilizador123; destination_url: https://hcdw/acessos-justificados; timestamp: 2025-11-10T09:00:00Z
2. Consulta à base de dados HCDW	SELECT e.IDEvento, e.DataHoraEvento, u.IDUserIAM, o.IDObjectoExt, o.TipoObjeto, t.DescTaxionomia, s.TipoSistema FROM Eventos e JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto JOIN Taxionomias t ON e.IDTaxionomia = t.IDTaxionomia JOIN Sistemas s ON e.IDSistema = s.IDSistema LEFT JOIN Utilizadores u ON e.IDUtilizador = u.IDUtilizador WHERE t.CodTaxionomia IN ('AJUS0001', 'AJUS0002', 'AJUS0003',' AJUS0004') ORDER BY e.DataHoraEvento DESC;

Fluxos	**Dados**
3. Resultado devolvido ao utilizador	3 registos encontrados: (i) acesso a relatório por med-00010 em 2025-11-05T11:00:00Z; (ii) acesso DIMSE por med-00005 em 2025-11-05 T12:00:00Z; (iii) acesso DICOMweb por med-00008 em 2025-11-06 T09:00:00Z
4. Registo da pesquisa do gestor no SIEM	[HCDW envia para o SIEM] eventid: 41; parenteventid: 40; system: hcdw; userid: 20; action: list_justified_accesses; filter: none; result_count: 3; timestamp: 2025-11-10T09:00:05Z

O sexto cenário refere-se à interação com a listagem de acessos não justificados (Tabela 23 e Tabela 24).

Tabela 23 - Cenário 6 - Listagem de acessos não justificados na HCDW

Identificador	6
Cenário	Listagem de acessos não justificados na plataforma HCDW
Ator(es)	Gestor
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Gestor, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Acessos Não Justificados”. 3) O sistema executa a consulta à base de dados, filtrando eventos classificados com taxionomia de acesso sem justificação válida. 4) O utilizador consulta a listagem, podendo filtrar por intervalo temporal, sistema de origem ou utilizador.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM.
Pós-condição	Registo no SIEM de pesquisa efetuada, incluindo a identificação do gestor e *timestamp.*

Tabela 24 - Simulação de dados gerados e consumidos no Cenário 6

Fluxos	**Dados**
1. Autenticação do gestor no HCDW (integrado com IAM)	[HCDW envia para o SIEM] eventid: 50; parenteventid: 50; system: auth_iam; source_ip: 10.0.0.5; state: access_allowed;

Fluxos	**Dados**
	userid: 20; destination_url: https://hcdw/acessos-nao-justificados; timestamp: 2025-11-10T09:10:00Z
1.1. Falha na autenticação do gestor no HCDW	[HCDW envia para o SIEM] eventid: 50; parenteventid: 50; system: auth_iam; source_ip: 10.0.0.5; state: access_denied; username: utilizador123; destination_url: https://hcdw/acessos-nao-justificados; timestamp: 2025-11-10T09:10:00Z
2. Consulta à base de dados HCDW	SELECT e.IDEvento, e.DataHoraEvento, u.IDUserIAM, o.IDObjectoExt, o.TipoObjeto, s.TipoSistema, e.IDEventoSIEM FROM Eventos e JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto JOIN Taxionomias t ON e.IDTaxionomia = t.IDTaxionomia JOIN Sistemas s ON e.IDSistema = s.IDSistema LEFT JOIN Utilizadores u ON e.IDUtilizador = u.IDUtilizador WHERE t.CodTaxionomia = 'NJUS0001' ORDER BY e.DataHoraEvento DESC;
3. Resultado devolvido ao utilizador	2 registos encontrados: (i) acesso DIMSE sem justificação por med-00005 em 2025-11-05; (ii) acesso DICOMweb sem justificação por med-00008 em 2025-11-06
4. Registo da pesquisa do gestor no SIEM	[HCDW envia para o SIEM] eventid: 51; parenteventid: 50; system: hcdw; userid: 20; action: list_unjustified_accesses; filter: none; result_count: 2; timestamp: 2025-11-10T09:10:05Z

No sétimo cenário é apresentada a interação do utilizador com a listagem de acessos externos (Tabela 25 e Tabela 26).

Tabela 25 - Cenário 7 - Listagem de acessos externos na HCDW

Identificador	7
Cenário	Listagem de acessos externos na plataforma HCDW
Ator(es)	Gestor
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Gestor, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Acessos Externos”. 3) O sistema executa a consulta à base de dados, filtrando eventos originados por sistemas externos (por exemplo, SPMS/SNS). 4)

	O utilizador consulta a listagem, podendo filtrar por intervalo temporal e sistema de origem.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM.
Pós-condição	Registo no SIEM de pesquisa efetuada.

Tabela 26 - Simulação de dados gerados e consumidos no Cenário 7

Fluxos	**Dados**
1. Autenticação do gestor no HCDW (integrado com IAM)	[HCDW envia para o SIEM] eventid: 60; parenteventid: 60; system: auth_iam; source_ip: 10.0.0.5; state: access_allowed; userid: 20; destination_url: https://hcdw/acessos-externos; timestamp: 2025-11-10T09:20:00Z
1.1. Falha na autenticação do gestor no HCDW	[HCDW envia para o SIEM] eventid: 60; parenteventid: 60; system: auth_iam; source_ip: 10.0.0.5; state: access_denied; username: utilizador123; destination_url: https://hcdw/acessos-externos; timestamp: 2025-11-10T09:20:00Z
2. Consulta à base de dados HCDW	SELECT e.IDEvento, e.DataHoraEvento, s.TipoSistema, s.IDSistemaExt, o.IDObjectoExt, o.TipoObjeto, p.IDPacienteRIS, e.IDEventoSIEM FROM Eventos e JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto JOIN Sistemas s ON e.IDSistema = s.IDSistema JOIN Pacientes p ON o.IDPaciente = p.IDPaciente WHERE s.TipoSistema = 'API_SPMS' ORDER BY e.DataHoraEvento DESC;
3. Resultado devolvido ao utilizador	1 registo encontrado: acesso externo via SPMS ao relatório REL-PDF-20251107-00099 do paciente RIS-PAC-00019 em 2025-11-07
4. Registo da pesquisa do gestor no SIEM	[HCDW envia para o SIEM] eventid: 61; parenteventid: 60; system: hcdw; userid: 20; action: list_external_accesses; filter: system_type=API_SPMS; result_count: 1; timestamp: 2025-11-10T09:20:05Z

O oitavo cenário refere-se à interação com a listagem de eventos adversos (Tabela 27 e Tabela 28).

Tabela 27 - Cenário 8 - Listagem de eventos adversos na HCDW

Identificador	8
Cenário	Listagem de eventos relacionados com acessos não autorizados na plataforma HCDW
Ator(es)	Gestor
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com perfil de Gestor, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Eventos Adversos”. 3) O sistema executa a consulta à base de dados, filtrando eventos classificados como eventos adversos de segurança (por exemplo, falhas de autenticação, acessos de sistema não autorizados). 4) O utilizador consulta a listagem.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM.
Pós-condição	Registo no SIEM de pesquisa efetuada, incluindo a identificação do gestor e *timestamp*.

Tabela 28 - Simulação de dados gerados e consumidos no Cenário 8

Fluxos	**Dados**
1. Autenticação do gestor no HCDW (integrado com IAM)	[HCDW envia para o SIEM] eventid: 70; parenteventid: 70; system: auth_iam; source_ip: 10.0.0.5; state: access_allowed; userid: 20; destination_url: https://hcdw/eventos-adversos; timestamp: 2025-11-10T09:30:00Z
1.1. Falha na autenticação do gestor no HCDW	[HCDW envia para o SIEM] eventid: 70; parenteventid: 70; system: auth_iam; source_ip: 10.0.0.5; state: access_denied; username: utilizador123; destination_url: https://hcdw/eventos-adversos; timestamp: 2025-11-10T09:30:00Z
2. Consulta à base de dados HCDW	SELECT e.IDEvento, e.DataHoraEvento, u.IDUserIAM, s.TipoSistema, o.IDObjectoExt, t.DescTaxionomia, e.IDEventoSIEM FROM Eventos e JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto JOIN Taxionomias t ON e.IDTaxionomia = t.IDTaxionomia JOIN Sistemas s ON e.IDSistema = s.IDSistema LEFT JOIN Utilizadores u ON

Fluxos	**Dados**
	e.IDUtilizador = u.IDUtilizador WHERE t.CodTaxionomia = ' NJUS0002' ORDER BY e.DataHoraEvento DESC;
3. Resultado devolvido ao utilizador	1 registo encontrado: falha de desencriptação via SPMS para o relatório REL-PDF-20251107-00099 em 2025-11-07, classificado como evento adverso
4. Registo da pesquisa do utilizador no SIEM	[HCDW envia para o SIEM] eventid: 71; parenteventid: 70; system: hcdw; userid: 20; action: list_adverse_events; filter: none; result_count: 1; timestamp: 2025-11-10T09:30:05Z

O nono cenário refere-se à interação com a pesquisa geral de eventos na plataforma HCDW (Tabela 29 e Tabela 30).

Tabela 29 - Cenário 9 - pesquisa geral na HCDW

Identificador	9
Cenário	Pesquisa geral de eventos na plataforma HCDW
Ator(es)	Gestor
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Gestor, integrada com o IAM
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Pesquisa Geral”. 3) O utilizador define os critérios da pesquisa no campo “Pesquisar por” (por exemplo, identificador do paciente, identificador do utilizador, intervalo temporal, tipo de sistema, taxionomia do evento) e aciona a pesquisa. 4) O sistema executa a consulta à base de dados com os critérios definidos e devolve a listagem de eventos correspondentes.
Fluxos alternativos	1.1 Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM. 3.1) A pesquisa não retorna resultados – o sistema apresenta uma mensagem informativa ao utilizador.
Pós-condição	Registo no SIEM da pesquisa efetuada, incluindo a identificação do gestor, critérios utilizados e número de resultados obtidos.

Tabela 30 - Simulação de dados gerados e consumidos no Cenário 9

Fluxos	**Dados**
1. Autenticação do gestor no HCDW (integrado com IAM)	[HCDW envia para o SIEM] eventid: 80; parenteventid: 80; system: auth_iam; source_ip: 10.0.0.5; state: access_allowed; userid: 20; destination_url: https://hcdw/pesquisa-geral; timestamp: 2025-11-10T10:00:00Z
1.1. Falha na autenticação do gestor no HCDW	[HCDW envia para o SIEM] eventid: 80; parenteventid: 80; system: auth_iam; source_ip: 10.0.0.5; state: access_denied; username: utilizador123; destination_url: https://hcdw/pesquisa-geral; timestamp: 2025-11-10T10:00:00Z
2. Critérios de pesquisa definidos pelo gestor	Critérios: patientid = 'RIS-PAC-00033'; intervalo: 2025-11-01 a 2025-11-30
3. Consulta à base de dados HCDW	SELECT e.IDEvento, e.DataHoraEvento, u.IDUserIAM, s.TipoSistema, o.IDObjectoExt, o.TipoObjeto, t.DescTaxionomia, e.IDEventoSIEM FROM Eventos e JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto JOIN Pacientes p ON o.IDPaciente = p.IDPaciente JOIN Taxionomias t ON e.IDTaxionomia = t.IDTaxionomia JOIN Sistemas s ON e.IDSistema = s.IDSistema LEFT JOIN Utilizadores u ON e.IDUtilizador = u.IDUtilizador WHERE p.IDPacienteRIS = 'RIS-PAC-00033' AND e.DataHoraEvento BETWEEN '2025-11-01T00:00:00Z' AND '2025-11-30T23:59:59Z' ORDER BY e.DataHoraEvento DESC;
4. Resultado devolvido ao utilizador	1 registo encontrado: acesso DICOMweb por med-00008 ao estudo 1.2.840.10008.5.1.4.1.1.2.20251106.002 em 2025-11-06
5. Registo da pesquisa do gestor no SIEM	[HCDW envia para o SIEM] eventid: 81; parenteventid: 80; system: hcdw; userid: 20; action: general_search; filter: patientid=RIS-PAC-00033, date_range=2025-11-01/2025-11-30; result_count: 1; timestamp: 2025-11-10T10:00:08Z

O décimo cenário apresenta a interação com a interface de emissão de relatórios de auditoria na plataforma HCDW (Tabela 31 e Tabela 32).

Tabela 31 - Cenário 10 - emissão de relatório na HCDW

Identificador	10
Cenário	Emissão de relatório na plataforma HCDW
Ator(es)	Gestor
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Gestor, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Relatórios”. 3) O utilizador seleciona o tipo de relatório a emitir: 3.a) resumo de acessos não justificados; 3.b) detalhe de acessos não justificados; 3.c) resumo de eventos adversos; 3.d) detalhe de eventos adversos. 4) O utilizador define intervalo temporal da recolha de dados. 5) O utilizador insere a justificação para emissão do relatório. 6) O utilizador aciona a pesquisa através do botão “Gerar Relatório”. 7) O sistema executa as consultas necessárias, gera o documento PDF e disponibiliza-o na listagem de relatórios emitidos.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM. 6.1) Erro na geração de relatório (por exemplo, não existem dados para o intervalo definido) – o sistema apresenta mensagem de erro e regista o evento no SIEM.
Pós-condição	Registo no SIEM da emissão do relatório, incluindo identificação do gestor, tipo de relatório, intervalo temporal, justificação apresentada e *timestamp*.

Tabela 32 - Simulação de dados gerados e consumidos no Cenário 10

Fluxos	**Dados**
1. Autenticação do gestor no HCDW (integrado com IAM)	[HCDW envia para SIEM] eventid: 90; parenteventid: 90; system: auth_iam; source_ip: 10.0.0.5; state: access_allowed; userid: 20; destination_url: https://hcdw/relatorios; timestamp: 2025-11-10T11:00:00Z

Fluxos	**Dados**
1.1. Falha na autenticação do gestor no HCDW	[HCDW envia para SIEM] eventid: 90; parenteventid: 90; system: auth_iam; source_ip: 10.0.0.5; state: access_denied; username: utilizador123; destination_url: https://hcdw/relatorios; timestamp: 2025-11-10T11:00:00Z
2. Parâmetros de emissão do relatório	Tipo: detalhe de acessos não justificados; intervalo: 2025-11-01 a 2025-11-30; justificação: AUDITORIA-2025-11
3. Consulta à base de dados HCDW para geração do relatório	SELECT e.IDEvento, e.DataHoraEvento, u.IDUserIAM, s.TipoSistema, s.IDSistemaExt, o.IDObjectoExt, o.TipoObjeto, p.IDPacienteRIS, t.DescTaxionomia, e.IDEventoSIEM FROM Eventos e JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto JOIN Pacientes p ON o.IDPaciente = p.IDPaciente JOIN Taxionomias t ON e.IDTaxionomia = t.IDTaxionomia JOIN Sistemas s ON e.IDSistema = s.IDSistema LEFT JOIN Utilizadores u ON e.IDUtilizador = u.IDUtilizador WHERE t.CodTaxionomia = ' NJUS0001' AND e.DataHoraEvento BETWEEN '2025-11-01T00:00:00Z' AND '2025-11-30T23:59:59Z' ORDER BY e.DataHoraEvento DESC;
4. Relatório gerado e disponibilizado (fluxo normal)	Ficheiro: relatorio-acessos-nao-justificados-detalhe-202511.pdf; 2 registos incluídos: acesso DIMSE sem justificação (2025-11-05) e acesso DICOMweb sem justificação (2025-11-06)
5. Registo da emissão do relatório no SIEM	[HCDW envia para SIEM] eventid: 91; parenteventid: 90; system: hcdw; userid: 20; action: report_generated; report_type: detail_unjustified_accesses; date_range: 2025-11-01/2025-11-30; justification: AUDITORIA-2025-11; result_count: 2; timestamp: 2025-11-10T11:00:15Z
6. Inserção do evento de emissão	INSERT INTO Eventos (IDObjeto, IDUtilizador, IDSistema, IDEventoSIEM, DataHoraEvento, IDTaxionomia) VALUES (NULL, 20, 6, 'wazuh-evt-20251110-00091', '2025-11-10T11:00:15+00', 1);

O décimo primeiro cenário apresenta o acesso ao painel de configuração geral da plataforma HCDW, onde se encontram as definições gerais da aplicação, como a retenção de registos (Tabela 33 e Tabela 34).

Tabela 33 - Cenário 11 – Configurações gerais da plataforma HCDW

Identificador	11
Cenário	Configurações gerais da plataforma HCDW
Ator(es)	Gestor, administrador
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Gestor ou Administrador, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Configurações Gerais”. 3) O utilizador pode habilitar ou desabilitar o uso de segundo fator de autenticação (2FA)
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM.
Pós-condição	Registo no SIEM da alteração das configurações gerais, incluindo identificação do utilizador, definições alteradas e o *timestamp*.

Tabela 34 - Simulação de dados gerados e consumidos no Cenário 11

Fluxos	**Dados**
1. Pedido de autenticação do utilizador (integrado com IAM)	HCDW envia para SIEM: { eventid: 200, parenteventid: 200, system: "auth-iam", sourceip: "192.168.1.15", state: "request-auth", destinationurl: "hcdw/configuracoes", timestamp: "2025-11-14T09:00:00Z" }
1.1. Autenticação falhada - credenciais inválidas (fluxo alternativo)	HCDW envia para SIEM: { eventid: 201, parenteventid: 200, system: "auth-iam", sourceip: "192.168.1.15", state: "access-denied", username: "gestor99", reason: "invalid-credentials", timestamp: "2025-11-14T09:00:05Z" }
2. Autenticação bem-sucedida (fluxo normal)	HCDW envia para SIEM: { eventid: 202, parenteventid: 200, system: "auth-iam", sourceip: "192.168.1.15", state: "access-allowed", userid: 6, destinationurl: "hcdw/configuracoes", timestamp: "2025-11-14T09:00:10Z" }
3. Acesso à página Configurações Gerais	HCDW envia para SIEM: { eventid: 203, parenteventid: 200, system: "hcdw", userid: 6, action: "page-access", page: "configuracoes-gerais", timestamp: "2025-11-14T09:00:15Z" }

Fluxos	**Dados**
4. Consulta do estado atual das configurações - base de dados HCDW	SELECT config_key, config_value FROM Configuracoes WHERE config_key IN ('2fa_enabled', 'totp_secret_set') ORDER BY config_key;
4. Resultado devolvido ao utilizador	2 registos encontrados: i) 2fa_enabled = false ii) totp_secret_set = false
5. Utilizador habilita o 2FA	HCDW envia para SIEM: { eventid: 204, parenteventid: 200, system: "hcdw", userid: 6, action: "config-update", config_key: "2fa_enabled", old_value: "false", new_value: "true", state: "success", timestamp: "2025-11-14T09:00:30Z" }
5. Atualização na base de dados HCDW	UPDATE Configuracoes SET config_value = 'true', updated_at = '2025-11-14T09:00:30Z', updated_by = 6 WHERE config_key = '2fa_enabled';
5.1. Erro na atualização - permissão insuficiente (fluxo alternativo)	HCDW envia para SIEM: { eventid: 205, parenteventid: 200, system: "hcdw", userid: 5, action: "config-update", config_key: "2fa_enabled", state: "error", reason: "insufficient-permissions", severity: "warning", timestamp: "2025-11-14T09:00:30Z" }
Pós-condição - registo final no SIEM	HCDW envia para SIEM: { eventid: 206, parenteventid: 200, system: "hcdw", userid: 6, action: "config-session-end", changes: [{ config_key: "2fa_enabled", old_value: "false", new_value: "true" }], state: "success", timestamp: "2025-11-14T09:00:35Z" }

O décimo segundo cenário refere-se à gestão das tabelas auxiliares da base de dados da plataforma HCDW, nomeadamente inserir, modificar e apagar registos associados a “Sistemas” e “Taxionomias”. Estes registos não são inseridos automaticamente no HCDW, ao contrário do que acontece com as restantes tabelas. (Tabela 35 e Tabela 36).

Complementarmente à auditoria criada através de eventos gerados para o SIEM e registados em paralelo nos eventos do HCDW, podem ser implementadas *triggers PostgreSQL* nas tabelas mencionadas, como forma de garantir registos de auditoria em todas as operações de *Create, Remove, Update, Delete* (CRUD) de forma autónoma e independente da disponibilidade do SIEM. Utilizando esta técnica, é implementada uma

segunda estratégia de auditoria registada de forma permanente e diretamente na base de dados.

Tabela 35 - Cenário 12 – Gestão das tabelas auxiliares da plataforma HCDW

Identificador	12
Cenário	Gestão das tabelas auxiliares da plataforma HCDW
Ator(es)	Administrador
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Administrador, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Tabelas auxiliares”. 3) O utilizador pode inserir nos dados nas tabelas, desde que os valores dos campos “Tipo Sistema”, “ID Sistema Externo”, “Código Taxionomia” e “Descrição Taxionomia” sejam únicos e preenchidos. 4) O utilizador pode modificar e apagar os registos sem correlações com registos de outras tabelas.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM. 3.1) Erro ao inserir dados (por exemplo, o valor inserido para os campos mencionados não é único) – o sistema apresenta mensagem de erro.4.1) Erro na eliminação de registo (por exemplo, registo utilizado noutra tabela (chave estrangeira)) – o sistema apresenta mensagem de erro.
Pós-condição	Registo no SIEM da inserção, modificação ou eliminação do registo, incluindo identificação do administrador, ID do registo, valores inseridos ou modificados e *timestamp*.

Tabela 36 - Simulação de dados gerados e consumidos no Cenário 12

Fluxos	**Dados**
1. Autenticação do administrador no HCDW (integrado com IAM)	[HCDW envia para SIEM] eventid: 100; parenteventid: 100; system: auth_iam; source_ip: 10.0.0.3; state: access_allowed; userid: 1; role: administrator; destination_url:

Fluxos	**Dados**
	https://hcdw/tabelas-auxiliares; timestamp: 2025-11-12T08:00:00Z
1.1. Autenticação falhada – credenciais inválidas (fluxo alternativo)	[HCDW envia para SIEM] eventid: 100; parenteventid: 100; system: auth_iam; source_ip: 10.0.0.3; state: access_denied; username: admin99; reason: invalid_credentials; timestamp: 2025-11-12T08:00:00Z
2. Acesso à página "Tabelas Auxiliares"	[HCDW envia para SIEM] eventid: 101; parenteventid: 100; system: hcdw; userid: 1; action: page_access; page: tabelas-auxiliares; timestamp: 2025-11-12T08:00:05Z
3a. Inserção de novo registo na tabela Sistemas (fluxo normal)	INSERT INTO Sistemas (TipoSistema, IDSistemaExt) VALUES ('RIS', 'SYS-RIS-001');
3a. Registo da inserção em Sistemas no SIEM	[HCDW envia para SIEM] eventid: 102; parenteventid: 100; system: hcdw; userid: 1; action: record_insert; table: Sistemas; record_id: 7; values: {TipoSistema: 'RIS', IDSistemaExt: 'SYS-RIS-001'}; state: success; timestamp: 2025-11-12T08:01:00Z
3b. Inserção de novo registo na tabela Taxionomias (fluxo normal)	INSERT INTO Taxionomias (CodTaxionomia, DescTaxionomia) VALUES ('AJUS0005', 'Acesso privilegiado por administrador de sistema');
3b. Registo da inserção em Taxionomias no SIEM	[HCDW envia para SIEM] eventid: 103; parenteventid: 100; system: hcdw; userid: 1; action: record_insert; table: Taxionomias; record_id: 7; values: {CodTaxionomia: AJUS0005', DescTaxionomia: 'Acesso privilegiado por administrador de sistema'}; state: success; timestamp: 2025-11-12T08:01:30Z
3.1a. Erro na inserção em Sistemas – IDSistemaExt duplicado (fluxo alternativo)	INSERT INTO Sistemas (TipoSistema, IDSistemaExt) VALUES ('RIS', 'SYS-RIS-001'); → Erro PostgreSQL: ERROR: duplicate key value violates unique constraint "sistemas_idsistemaext_key" DETAIL: Key (IDSistemaExt)=(SYS-RIS-001) already exists.

Fluxos	**Dados**
3.1a. Registo do erro de inserção no SIEM	[HCDW envia para SIEM] eventid: 104; parenteventid: 100; system: hcdw; userid: 1; action: record_insert; table: Sistemas; state: error; reason: duplicate_key; field: IDSistemaExt; value: 'SYS-RIS-001'; severity: warning; timestamp: 2025-11-12T08:02:00Z
3.1b. Erro na inserção em Taxionomias – CodTaxionomia duplicado (fluxo alternativo)	INSERT INTO Taxionomias (CodTaxionomia, DescTaxionomia) VALUES (' AJUS0001', 'Acesso justificado a relatório de diagnóstico'); → Erro PostgreSQL: ERROR: duplicate key value violates unique constraint "taxionomias_codtaxionomia_key" DETAIL: Key (CodTaxionomia)=(AJUS0001) already exists.
3.1b. Registo do erro de inserção no SIEM	[HCDW envia para SIEM] eventid: 105; parenteventid: 100; system: hcdw; userid: 1; action: record_insert; table: Taxionomias; state: error; reason: duplicate_key; field: CodTaxionomia; value: ' AJUS0001'; severity: warning; timestamp: 2025-11-12T08:02:30Z
4a. Modificação de registo na tabela Sistemas (fluxo normal)	UPDATE Sistemas SET TipoSistema = 'RIS_V2', IDSistemaExt = 'SYS-RIS-002' WHERE IDSistema = 7;
4a. Registo da modificação em Sistemas no SIEM	[HCDW envia para SIEM] eventid: 106; parenteventid: 100; system: hcdw; userid: 1; action: record_update; table: Sistemas; record_id: 7; previous_values: {TipoSistema: 'RIS', IDSistemaExt: 'SYS-RIS-001'}; new_values: {TipoSistema: 'RIS_V2', IDSistemaExt: 'SYS-RIS-002'}; state: success; timestamp: 2025-11-12T08:03:00Z
4b. Modificação de registo na tabela Taxionomias (fluxo normal)	UPDATE Taxionomias SET DescTaxionomia = 'Acesso privilegiado por administrador de sistema ou técnico TI' WHERE IDTaxionomia = 7;
4b. Registo da modificação em Taxionomias no SIEM	[HCDW envia para SIEM] eventid: 107; parenteventid: 100; system: hcdw; userid: 1; action: record_update; table: Taxionomias; record_id: 7; previous_values: {DescTaxionomia: 'Acesso privilegiado por administrador de sistema'}; new_values:

Fluxos	**Dados**
	{DescTaxionomia: 'Acesso privilegiado por administrador de sistema ou técnico TI'}; state: success; timestamp: 2025-11-12T08:03:30Z
4c. Eliminação de registo sem correlações na tabela Sistemas (fluxo normal)	DELETE FROM Sistemas WHERE IDSistema = 7;
4c. Registo da eliminação em Sistemas no SIEM	[HCDW envia para SIEM] eventid: 108; parenteventid: 100; system: hcdw; userid: 1; action: record_delete; table: Sistemas; record_id: 7; deleted_values: {TipoSistema: 'RIS_V2', IDSistemaExt: 'SYS-RIS-002'}; state: success; timestamp: 2025-11-12T08:04:00Z
4d. Eliminação de registo sem correlações na tabela Taxionomias (fluxo normal)	DELETE FROM Taxionomias WHERE IDTaxionomia = 7;
4d. Registo da eliminação em Taxionomias no SIEM	[HCDW envia para SIEM] eventid: 109; parenteventid: 100; system: hcdw; userid: 1; action: record_delete; table: Taxionomias; record_id: 7; deleted_values: {CodTaxionomia: ' AJUS0005', DescTaxionomia: 'Acesso privilegiado por administrador de sistema ou técnico TI'}; state: success; timestamp: 2025-11-12T08:04:30Z
4.1a. Erro na eliminação em Sistemas – registo referenciado em Eventos (fluxo alternativo)	DELETE FROM Sistemas WHERE IDSistema = 3; → Erro PostgreSQL: ERROR: update or delete on table "sistemas" violates foreign key constraint "fk_eventos_sistemas" on table "eventos" DETAIL: Key (IDSistema)=(3) is still referenced from table "Eventos".
4.1a. Registo do erro de eliminação no SIEM	[HCDW envia para SIEM] eventid: 110; parenteventid: 100; system: hcdw; userid: 1; action: record_delete; table: Sistemas; record_id: 3; state: error; reason: foreign_key_violation;

Fluxos	Dados
	referenced_table: Eventos; severity: warning; timestamp: 2025-11-12T08:05:00Z
4.1b. Erro na eliminação em Taxionomias – registo referenciado em Eventos (fluxo alternativo)	DELETE FROM Taxionomias WHERE IDTaxionomia = 1; → Erro PostgreSQL: ERROR: update or delete on table "taxionomias" violates foreign key constraint "fk_eventos_taxionomias" on table "eventos" DETAIL: Key (IDTaxionomia)=(1) is still referenced from table "Eventos".
4.1b. Registo do erro de eliminação no SIEM	[HCDW envia para SIEM] eventid: 111; parenteventid: 100; system: hcdw; userid: 1; action: record_delete; table: Taxionomias; record_id: 1; state: error; reason: foreign_key_violation; referenced_table: Eventos; severity: warning; timestamp: 2025-11-12T08:05:30Z
Consulta de verificação do estado atual das tabelas auxiliares	SELECT s.IDSistema, s.TipoSistema, s.IDSistemaExt FROM Sistemas s ORDER BY s.IDSistema; SELECT t.IDTaxionomia, t.CodTaxionomia, t.DescTaxionomia FROM Taxionomias t ORDER BY t.IDTaxionomia;

O décimo terceiro cenário refere-se à listagem de acessos à plataforma HCDW, que inclui por cada acesso o *timestamp* de acesso, o recurso acedido e o utilizador que o efetuou.

Para que seja possível obter o mesmo nível de detalhe de auditoria no acesso aos objetos informacionais, cada página é tratada como sendo ela própria um objeto informacional, estando associado um identificador de paciente neutro (ou seja, zero). O identificador utilizado para o tipo de objeto das páginas é o zero, sendo este identificador reservado para objetos internos da aplicação. O identificador de objeto externo corresponde ao URL da página (Tabela 37).

Tabela 37 - Pré-registo das páginas do HCDW como Objetos Informacionais

IDObjectoExt	TipoObjeto	IDPaciente
hcdw/dashboard	0	0
hcdw/acessos-justificados	0	0
hcdw/acessos-nao-justificados	0	0

IDObjectoExt	TipoObjeto	IDPaciente
hcdw/acessos-externos	0	0
hcdw/eventos-adversos	0	0
hcdw/pesquisa-geral	0	0
hcdw/relatórios	0	0
hcdw/configurações	0	0
hcdw/tabelas-auxiliares	0	0
hcdw/utilizadores-acessos	0	0

Esta abordagem assegura que os acessos à própria plataforma HCDW são tratados com o mesmo rigor de auditoria que os acessos a dados pessoais e relatórios de diagnóstico, permitindo ao administrador identificar sessões anómalas ou acessos indevidos à plataforma de monitorização, sendo relevante dado o carácter sensível da informação nela contida.

O cenário e a simulação são apresentados baseados nestes pressupostos (Tabela 38 e Tabela 39).

Tabela 38 - Cenário 13 – Listagem dos acessos à plataforma HCDW

Identificador	13
Cenário	Listagem dos acessos à plataforma HCDW
Ator(es)	Administrador
Pré-condições	O utilizador deve possuir conta de acesso ao HCDW com o perfil de Administrador, integrada com o IAM.
Fluxo normal	1) O utilizador autentica-se no HCDW (integrado com IAM). 2) O utilizador acede à página “Utilizadores e Acessos”. 3) O utilizador define os critérios da pesquisa no campo “Pesquisar” (por exemplo, intervalo temporal, recurso acedido, identificador do utilizador), escolhe a ordenação pretendida para a listagem e aciona a pesquisa. 4) O sistema executa a consulta à base de dados com os critérios definidos e devolve a listagem de eventos correspondentes.
Fluxos alternativos	1.1) Falha na autenticação – o acesso ao HCDW é negado e o evento é registado no SIEM.

Pós-condição	Registo no SIEM da pesquisa efetuada, incluindo identificação do Administrador e critérios de pesquisa.

Tabela 39 - Simulação de dados gerados e consumidos no Cenário 13

Fluxos	**Dados**
1. Autenticação do administrador no HCDW (integrado com IAM) – fluxo normal	[HCDW envia para SIEM] eventid: 120; parenteventid: 120; system: auth_iam; source_ip: 10.0.0.3; state: access_allowed; userid: 1; role: administrator; destination_url: https://hcdw/utilizadores-acessos; timestamp: 2025-11-13T09:00:00Z
1.1. Autenticação falhada – credenciais inválidas (fluxo alternativo)	[HCDW envia para SIEM] eventid: 120; parenteventid: 120; system: auth_iam; source_ip: 10.0.0.3; state: access_denied; username: admin99; reason: invalid_credentials; timestamp: 2025-11-13T09:00:00Z
2. Acesso à página "Utilizadores e Acessos"	[HCDW envia para SIEM] eventid: 121; parenteventid: 120; system: hcdw; userid: 1; action: page_access; page: utilizadores-acessos; timestamp: 2025-11-13T09:00:05Z
3. Critérios de pesquisa definidos pelo administrador	[HCDW envia para SIEM] userid: 'iam-user-med-00008'; intervalo: 2025-11-01 a 2025-11-30; ordenação: DataHoraEvento DESC
4. Consulta à base de dados HCDW – acessos ao HCDW pelo utilizador indicado	SELECT e.IDEvento, e.DataHoraEvento, u.IDUserIAM, s.TipoSistema, s.IDSistemaExt, o.IDObjectoExt, t.CodTaxionomia, t.DescTaxionomia, e.IDEventoSIEM FROM Eventos e JOIN Taxionomias t ON e.IDTaxionomia = t.IDTaxionomia JOIN Sistemas s ON e.IDSistema = s.IDSistema LEFT JOIN Utilizadores u ON e.IDUtilizador = u.IDUtilizador LEFT JOIN ObjetosInformacionais o ON e.IDObjeto = o.IDObjeto WHERE s.IDSistemaExt = 'SYS-HCDW-001' AND u.IDUserIAM = 'iam-user-med-00008' AND e.DataHoraEvento BETWEEN '2025-11-01T00:00:00Z' AND '2025-11-30T23:59:59Z' ORDER BY e.DataHoraEvento DESC;
4. Resultado devolvido ao administrador	3 registos encontrados: (i) pesquisa geral efectuada por iam-user-med-00008 em 2025-11-10T10:00:08Z (AJUS0006); (ii) acesso à página de acessos justificados em 2025-11-

Fluxos	Dados
	10T09:00:05Z (AJUS0006); (iii) autenticação bem-sucedida no HCDW em 2025-11-10T09:00:00Z (AJUS0006)
5. Registo da pesquisa do administrador no SIEM	[HCDW envia para SIEM] eventid: 122; parenteventid: 120; system: hcdw; userid: 1; action: hcdw_access_log_search; filter: {userid: 'iam-user-med-00008', date_range: '2025-11-01/2025-11-30', sort: 'DataHoraEvento DESC'}; result_count: 3; timestamp: 2025-11-13T09:00:12Z

Os cenários e as simulações apresentados nesta secção apresentam o detalhe das interações entre os diversos componentes presentes na arquitetura da solução.

A redundância de alguns registos, que são enviados simultaneamente para o SIEM e para a base de dados da plataforma HCDW é propositada e afigura-se como uma redundância de monitorização, que permite a operação da plataforma em caso de indisponibilidade do SIEM. Nestes casos, os eventos identificados como “HCDW envia para o SIEM” permanecem guardados em ficheiro de *logs* locais, que podem ser enviados logo que os componentes estiverem disponíveis.

No caso da indisponibilidade do IAM, a operação fica comprometida, visto que é o ponto central de autenticação. Para este sistema, e nos cenários apresentados, não existe um fluxo alternativo de autenticação e autorização.

Os cenários consideram que a componente de processamento de informação e da base de dados associada, bem como a componente de apresentação estão disponíveis e operacionais.

Os fluxos prevendo a indisponibilidade dos vários componentes mencionados não são apresentados neste contexto porque são considerados como medidas de mitigação a serem implementadas na arquitetura geral do sistema, não diretamente relacionadas com o HCDW.

5. CONCLUSÃO

Neste capítulo apresentam-se as considerações finais acerca deste projeto (secção 5.1) e do trabalho futuro (secção 5.2).

5.1. CONSIDERAÇÕES FINAIS

O presente projeto cumpriu os objetivos definidos na Secção 1.2, demonstrando a viabilidade técnica de uma plataforma de monitorização de acessos a dados pessoais sensíveis em entidades prestadoras de MCDT de pequena dimensão. O objetivo geral – o desenvolvimento de uma prova de conceito capaz de centralizar a monitorização de acessos, recorrendo a soluções open-source e à integração entre sistemas heterogéneos – foi atingido através da conceção de uma arquitetura modular, do desenvolvimento de um protótipo de baixa fidelidade e da validação por simulação de treze cenários de uso. Os objetivos secundários foram igualmente cumpridos: foi realizado o enquadramento legislativo e normativo aplicável (RGPD, NIS2, ISO 27001/27701/27799), identificados os controlos de cibersegurança relevantes para o contexto clínico, apresentados os principais protocolos e sistemas auxiliares (DICOM, HL7, PACS, SIEM, IAM) e descrita a arquitetura da solução proposta. Do ponto de vista das contribuições, o trabalho oferece, por um lado, uma contribuição científica ao propor e validar concetualmente uma arquitetura de monitorização orientada ao contexto clínico, alinhada com os referenciais normativos europeus; e, por outro, uma contribuição prática ao disponibilizar um modelo de referência acessível a entidades que, pela sua dimensão, não dispõem de equipas especializadas em cibersegurança.

As opções metodológicas e técnicas adotadas ao longo deste projeto beneficiaram de cerca de oito anos de experiência profissional do autor no setor da saúde, durante os quais foi possível observar, em contexto real, os desafios quotidianos da gestão da cibersegurança numa entidade prestadora de MCDT. Algumas das decisões de desenho da solução (nomeadamente a separação entre acessos justificados e injustificados, a classificação de eventos adversos e a estrutura dos painéis de monitorização) foram informadas por essa experiência empírica, com o objetivo de responder a necessidades concretas de gestores e responsáveis pela proteção de dados que, no dia a dia, carecem de ferramentas acessíveis e orientadas ao contexto clínico. Reconhece-se, contudo, que esta ancoragem na experiência prática, embora válida como ponto de partida, não substitui uma validação formal junto de utilizadores reais, a qual constitui uma das principais limitações do presente trabalho e um passo essencial a concretizar em investigação futura.

Adicionalmente, a ausência de uma DPIA e de uma análise de risco formal sobre a própria plataforma, bem como a validação exclusivamente baseada em dados simulados, delimitam o alcance das conclusões aqui apresentadas, sem prejuízo da relevância e validade da prova de conceito desenvolvida.

O presente trabalho evidenciou que a ausência de mecanismos de monitorização e auditoria de acessos a dados pessoais sensíveis representa uma lacuna na postura de segurança das entidades prestadoras de MCDT de pequena dimensão, não abrangidas pela Diretiva SRI2. Neste contexto, desenvolveu-se o protótipo *HealthCare Data Watchdog* (HCDW) com o intuito de validar que é tecnicamente viável, recorrendo exclusivamente a soluções *open-source*, centralizar a gestão de identidades, bem como a recolha, a correlação e visualização de eventos de acesso provenientes de sistemas heterogéneos (nomeadamente o PACS, o servidor de armazenamento de relatórios e os *webservices* de integração com o SPMS/SNS), numa interface acessível a utilizadores sem conhecimentos técnicos em cibersegurança ou informática avançada.

A adoção voluntária de *frameworks* ou boas práticas de cibersegurança, como as definidas no Quadro Nacional de Referência em Cibersegurança (QNRCS), por parte de entidades que não são juridicamente obrigadas a tal, evidencia maturidade organizacional. Esta adoção voluntária vai além da conformidade regulamentar, pois permite melhorar os processos internos, promove uma organização mais coerente e estruturada dos dados e da informação e reduz a superfície de ataque da organização ao identificar e classificar os seus ativos críticos. Nas entidades prestadoras de MCDT, cujo produto final é o relatório médico (baseado nos dados recolhidos durante o exame ao paciente), os dados pessoais sensíveis são simultaneamente o maior ativo e a maior responsabilidade. A degradação da sua integridade, confidencialidade ou disponibilidade compromete não só a conformidade regulatória, mas também a missão da entidade.

A reputação das organizações de saúde e dos profissionais que nelas exercem funções está intrinsecamente ligada à capacidade de efetuar um correto tratamento dos dados dos seus pacientes. Os estudos analisados no âmbito deste trabalho identificam o erro humano (motivado por falta de cultura em cibersegurança, negligência ou intenção maliciosa) como a principal causa de incidentes de segurança no setor. A inexistência de controlos de acesso adequados e de mecanismos de registo auditável expõe os profissionais a situações de vulnerabilidade, nas quais a responsabilidade individual por atos de acesso indevido se torna impossível de demonstrar ou refutar. O sistema HCDW, ao registar de forma sistemática e independente cada evento de acesso a objetos informacionais (registando o utilizador, o recurso acedido, a justificação apresentada, o sistema de origem

e a data e hora de acesso), cria um elemento dissuasor relevante: o conhecimento de que o acesso fica registado e é passível de auditoria constitui, por si só, um mecanismo de controlo comportamental.

Os equipamentos e sistemas legados representam uma realidade permanente no parque informático das entidades da área da saúde, cuja capacidade de renovação tecnológica é condicionada por restrições orçamentais e pela complexidade de substituição de sistemas críticos em ambientes clínicos. A evolução acelerada da tecnologia médica e informática acentua esta disparidade. Neste contexto, a segurança de perímetro – materializada através da segmentação de redes, do controlo de fluxos por *firewall*, da implementação de um *Reverse Proxy* com autenticação centralizada no IAM e da monitorização contínua via SIEM – é utilizada como medida compensatória e estratégica, baseada em soluções de baixo custo e adequadas à dimensão da entidade.

Mais do que a implementação de tecnologia ou alteração de processos, é importante que a definição e a priorização destes controlos resultem sempre de uma avaliação de risco formal e documentada, proporcional ao contexto e à criticidade dos sistemas. A organização deve empreender esse esforço para que exista uma cultura de prevenção e não de reação, evitando que sejam só implementados controlos em resposta a incidentes já ocorridos.

A simulação realizada no âmbito desta prova de conceito demonstrou a viabilidade do modelo de dados proposto e dos fluxos de integração definidos. Através dos cenários de uso identificados e da simulação com dados fictícios, confirmou-se que a arquitetura modular da solução é adequada aos objetivos propostos.

5.2. TRABALHO FUTURO

Neste subcapítulo é abordado o trabalho futuro, do ponto de vista da plataforma HCDW, bem como da própria arquitetura do sistema.

Numa primeira instância, a transição da prova de conceito da plataforma, através do seu desenvolvimento e implementação em produção em ambiente real, com testes funcionais e de carga e políticas formais de retenção de dados. A arquitetura modular proposta facilita esta evolução, nomeadamente na substituição ou adição de componentes sem impacto nos restantes módulos. Outra possibilidade é estruturar e distribuir os componentes da aplicação por *containers*, que permitirá criar uma camada de abstração face ao sistema informático onde está a ser executado, através de tecnologias como

Docker, *Kubernetes*, ou *OpenShift*, que simplificam o processo de instalação, atualização e operação em diferentes tipos de infraestrutura.

Um aspeto relevante a desenvolver em trabalho futuro prende-se com a realização de uma análise de risco formal sobre a própria plataforma HCDW. Embora o trabalho aborde a avaliação de risco como boa prática no âmbito do QNRCS e da Diretiva NIS2, não foi conduzida uma DPIA nem uma análise de risco específica à solução desenvolvida. Esta lacuna é relevante dado que o HCDW, ao centralizar registos de auditoria de acessos a dados pessoais sensíveis, constitui ele próprio um ativo crítico de informação. O seu eventual comprometimento – por acesso não autorizado, adulteração ou indisponibilidade – poderia ter implicações diretas na confidencialidade, integridade e rastreabilidade dos dados que a ferramenta visa proteger. A elaboração de uma DPIA, em conformidade com o artigo 35.º do RGPD, e de uma análise de risco alinhada com a ISO/IEC 27001:2022, constituem, assim, passos essenciais para a maturação da solução antes de qualquer implementação em ambiente de produção.

No que respeita à validação da solução junto dos utilizadores finais, um passo importante em trabalho futuro será a realização de uma avaliação de usabilidade formal, envolvendo profissionais de saúde e responsáveis pela proteção de dados pessoais. Esta avaliação poderá assumir a forma de entrevistas estruturadas ou da aplicação de um questionário de usabilidade padronizado (como o *System Usability Scale* (SUS)) dirigido a utilizadores representativos do público-alvo da ferramenta, nomeadamente gestores de entidades prestadoras de MCDT e EPD. Os resultados obtidos permitiriam identificar oportunidades de melhoria na interface e na experiência de utilização, contribuindo para uma solução mais acessível e adequada às necessidades reais do contexto clínico

A evolução da solução deverá igualmente contemplar a integração com os padrões e iniciativas emergentes no domínio da interoperabilidade em saúde. Em particular, a adoção do standard HL7 FHIR R4/R5 como protocolo de troca de dados clínicos permitiria ampliar a capacidade de recolha e correlação de eventos de acesso em ambientes de saúde mais modernos e interoperáveis. Paralelamente, o Espaço Europeu de Dados de Saúde (EHDS), regulamento aprovado pela União Europeia em 2025, estabelece um novo quadro para a partilha transfronteiriça de dados de saúde e impõe requisitos adicionais de controlo de acesso, auditoria e soberania dos dados – áreas diretamente abrangidas pelo âmbito do HCDW. A integração da plataforma com os mecanismos de governação e auditoria previstos no EHDS representa, assim, uma oportunidade estratégica de evolução da solução e de alinhamento com o futuro enquadramento regulatório europeu.

Outra possível melhoria é o alargamento da integração da plataforma HCDW com todos os sistemas que armazenem ou processem dados pessoais sensíveis no contexto da entidade prestadora de MCDT. Sistemas como o RIS, o HIS/CIS e os equipamentos de modalidade médica com interface DICOM *Worklist* e DICOM *Storage* constituem fontes de eventos de acesso ainda não contempladas na versão atual da solução. A integração com sistemas médicos que utilizem o HL7 também representa igualmente uma extensão de elevado valor, dada a prevalência deste protocolo no ecossistema de interoperabilidade da saúde em Portugal. Em particular, a integração com o protocolo HL7 FHIR, adotado pelo ecossistema SPMS/SNS, permitiria melhorar a recolha de eventos de acesso associados a consultas e partilhas de resultados realizadas através da BDNR e do PNB, enriquecendo o mapa de acessos externos monitorizados pelo HCDW. Esta extensão seria especialmente relevante para o rastreio de acessos realizados por médicos do SNS no contexto do projeto Exames Sem Papel, cujos fluxos de acesso são monitorizados de forma parcial na solução apresentada.

De modo a garantir a manutenção permanente da monitorização, é relevante o desenvolvimento de mecanismos de deteção da indisponibilidade do SIEM e IAM, visto que existe uma dependência funcional do HCDW face a estes sistemas de origem de eventos. Neste caso, a capacidade de monitorização fica comprometida, sem que o utilizador do HCDW se aperceba da indisponibilidade destes sistemas e dos fluxos de dados esperados. Sugere-se a implementação de sinais de funcionamento (*heartbeat*) e a criação de um módulo que possa consumir estes sinais, de modo a alertar caso não esteja a receber informação, bem como a execução de verificações funcionais periódicas nos diversos sistemas (SIEM, IAM, SGBD), de modo a verificar a disponibilidade e integridade dos dados.

Considerando que o modelo de dados atual do HCDW é centrado em taxionomia de eventos e na relação entre utilizadores, objetos informacionais e sistemas, existe uma base sólida para a implementação futura de mecanismos de deteção comportamental, recorrendo a técnicas de *Data Mining, Machine Learning* e *User and Entity Behavior Analytics* (UEBA). Deste modo é possível a criação de modelos para classificação automática dos eventos, de modo a detetar acessos anómalos, nomeadamente elevado número de acessos a objetos informacionais, acessos de IPs não autorizados e a objetos informacionais de pacientes que não têm um contexto clínico ativo no RIS.

Em relação à geração de relatórios de conformidade regulatória, a plataforma HCDW deverá evoluir no sentido de suportar a geração automática dos mesmos, nomeadamente relatórios periódicos exigidos no âmbito do RGPD (nomeadamente, registos de atividades

de tratamento, relatórios de incidentes para a CNPD) e da Diretiva SRI2 (nomeadamente, notificação de incidentes significativos ao CNCS no prazo de 24 horas). A automatização deste processo permitiria a redução da carga administrativa associada ao cumprimento regulatório e minimizaria o risco de incumprimento de prazos legais de notificação, que podem implicar sanções financeiras significativas.

Por último, a taxionomia de eventos atualmente definida – centrada em acessos justificados, não justificados, externos e eventos adversos – representa um ponto de partida adequado, mas poderá ser progressivamente enriquecida. Sugere-se o alinhamento desta taxionomia com classificações internacionais de auditoria de acessos em sistemas de saúde, como as definidas pelo perfil *Audit Trail and Node Authentication* (ATNA) da integração IHE (*Integrating the Healthcare Enterprise*), bem como com os eventos de auditoria previstos na norma DICOM para o perfil de segurança associado. Esta harmonização facilitaria a interoperabilidade do HCDW com outros sistemas de auditoria existentes no ecossistema de saúde e permitiria a utilização de comunicação normalizada de eventos a entidades supervisoras.

BIBLIOGRAFIA

Ahmed, Y., Naqvi, S., & Josephs, M. (2019). Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. *13th International Symposium on Medical Information and Communication Technology (ISMICT)*, (pp. 1-9). doi:10.1109/ISMICT.2019.8744003

Amazon Web Services. (2022, 11 17). *Detective Controls — Healthcare Industry Lens (Well-Architected Framework).* Retrieved from AWS Documentation: https://docs.aws.amazon.com/wellarchitected/latest/healthcare-industry-lens/detective-controls.html

Amazon Web Services. (2025). *AWS CloudTrail – Features.* Retrieved from AWS: https://aws.amazon.com/cloudtrail/features/

Assembleia da República. (2019). Lei n.º 58/2019, de 8 de agosto. *Diário da República, 1.ª Série*(151/2019), 3-40. Obtido em 26 de 07 de 2024, de https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Blobel, B. (2007). Comparing approaches for advanced e-health security infrastructures. *International Journal of Medical Informatics, 76*(5-6), pp. 454–459. Obtido de https://pubmed.ncbi.nlm.nih.gov/17074532/

Blue Goat Cyber. (2025, 09 15). *Signature Vs. Anomaly-Based Detection: Which Is More Effective?* Retrieved from Blue Goat Cyber Blog: https://bluegoatcyber.com/blog/signature-vs-anomaly-based-detection-which-is-more-effective/

Castro, J., Domingo, A., Colomé, J., & Estévez, S. (08 de 2011). HL7 in Personal Health System Component's Integration for Mental Health Treatment. *Journal of Health Informatics*.

Centro Nacional de Cibersegurança. (2019). *Quadro Nacional de Referência em Cibersegurança*. Obtido de https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

CNCS. (2024). *Cibersegurança em Portugal - Riscos & Conflitos: 5.ª edição*. Observatório de Cibersegurança / CNCS. Obtido de https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf

Comissão Europeia. (16 de 06 de 2025). *Década Digital 2025: Estudo sobre indicadores de saúde em linha*. Obtido de https://digital-strategy.ec.europa.eu/pt/library/digital-decade-2025-ehealth-indicator-study

Comissão Europeia. (2025). *Políticas da UE em Matéria de Cibersegurança*. Obtido em 01 de 06 de 2025, de https://digital-strategy.ec.europa.eu/pt/policies/cybersecurity-policies

Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated Cybersecurity Methodology and Supporting Tools for Healthcare Operational

Information Systems. *Computers & Security, 129*, 103189. doi:10.1016/j.cose.2023.103189

CrowdStrike. (2025). *CrowdStrike*. Obtido em 23 de 11 de 2025, de What Is Data Loss Prevention (DLP)?: https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-loss-prevention-dlp/

Crowley, C., Filkins, B., & Pescatore, J. (2022). *Security Operations Center: Building, Operating, and Maintaining Your SOC* (2ª ed.). Sebastopol, California, USA: O'Reilly Media.

Cyberout Security. (2024). *Gestão Avançada com SIEM e SOAR*. Obtido em 04 de 12 de 2025, de Cyberout Security: https://www.cyberout.com.br/blog/4/siem-soar-gestao

DICOM Standards Committee. (2025). PS3.15: Security and system management profiles — A.5 Audit Trail Message Format Profile. Obtido de https://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_a.5.html

Dicom Systems. (2025). *Unifier Enterprise Imaging Platform*. Obtido de Dicom Systems: https://dcmsys.com/solutions/unifier-enterprise-imaging-platform/

Direção Geral da Saúde. (2025). *Missão e Atribuições*. Obtido de DGS: https://www.dgs.pt/a-dgs/missao-e-atribuicoes.aspx

ENISA. (2019). *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends*. European Union Agency for Cybersecurity. Obtido em 10 de 09 de 2025, de https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Entidade Reguladora da Saúde. (2025). *Entidade Reguladora da Saúde*. Obtido de https://www.ers.pt/pt/institucional/a-ers/

Entidade Reguladora da Saúde. (2025). *Ligação à Legislação – Prestadores de Saúde*. Obtido de https://www.ers.pt/pt/legislacao/selecionar/prestadores/

European Commission. (2025). *The EU's Cybersecurity Strategy for the Digital Decade*. Obtido em 10 de 09 de 2025, de European Commission: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape 2024*. ENISA Threat Landscape 2024. Obtido em 05 de 07 de 2025, de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Federação Nacional de Prestadores de Cuidados de Saúde. (2023). *Prestadores Privados de Cuidados de Saúde Preocupados Com Reforma Anunciada Do SNS*. Obtido de https://www.fns.pt/prestadores-privados-de-cuidados-de-saude-preocupados-com-reforma-anunciada-do-sns/

Ferreira, D. (2025). *Segurança de Rede, Defesa Cibernética e Operações*. Lisboa: FCA - Editora de Informática.

GE Healthcare. (2025). *Edison Datalogue Connect*. Retrieved from https://appsource.microsoft.com/en-us/product/web-apps/gehealthcare.edison_datalogue_connect_2020?tab=overview

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing and evaluating current security awareness and behavior. *Journal of Computer Information Systems*. Obtido em 10 de 03 de 2024, de https://doi.org/10.1080/08874417.2020.1845583

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., . . . Ntanos, C. (09 de 02 de 2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare, 10*(2). doi:10.3390/healthcare10020327

Gonçalves, E. (2025). Comprehensive Analysis for Cybersecurity and Interoperability in Portuguese Healthcare Systems Under NIS2. *ARIS2 - Advanced Research on Information Systems Security, 5*(1), 38-56. Obtido de https://aris-journal.com/aris/index.php/journal/article/view/59

Google Cloud. (2025). *Cloud Healthcare API*. Retrieved from https://cloud.google.com/healthcare-api?hl=en_gb

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital Identity Guidelines*. National Institute of Standards and Technology. Obtido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Gregg, B., D'Agostino, H., & Toledo, E. G. (18 de 09 de 2006). Creating an IHE ATNA-based audit. *Journal of Digital Imaging*, 307–315. Obtido de https://pmc.ncbi.nlm.nih.gov/articles/PMC3045161/

Hansche, S., Berti, J., & Hare, C. (2004). *Official (ISC)² Guide to the CISSP Exam*. Florida, USA: Auerbach Publications / CRC Press.

Health Level Seven International - CDA. (2025). *CDA-Core-Sd Overview*. Retrieved from https://build.fhir.org/ig/HL7/CDA-core-sd/overview.html

Health Level Seven International - FHIR. (2023). *Summary – FHIR V5.0.0*. Obtido de https://www.hl7.org/fhir/summary.html

Health Level Seven International. (s.d.). *Health Level Seven International*. Obtido em 20 de 04 de 2025, de https://www.hl7.org/

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly*, 75-75.

HL7 International. (2025). *HL7 International — Homepage*. Retrieved 04 20, 2025, from https://www.hl7.org/

HL7 International. (2025). *HL7 Version 2 Product Suite – Standards Product Brief*. Retrieved from https://www.hl7.org/implement/standards/product_brief.cfm?product_id=185

HL7 International. (s.d.). AuditEvent — FHIR R6 specification. Obtido de https://build.fhir.org/auditevent.html

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. National Institute of Standards and Technology (NIST). Obtido de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf

IBM Corporation. (2025). *Visão Geral — Identity Manager (SIG and i 10.0.2)*. Obtido de https://www.ibm.com/docs/pt-br/sig-and-i/10.0.2?topic=overview-identity-manager

IBM. (s.d.). *O que é exfiltração de dados?* Obtido em 28 de 06 de 2025, de IBM: https://www.ibm.com/br-pt/think/topics/data-exfiltration

IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach: IBM.

IHE International. (08 de 06 de 2015). Technical framework supplement: Add RESTful ATNA (query and feed). (IHE, Ed.) Obtido de https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA_Rev1.0_PC_2015-06-08.pdf

IHE International. (04 de 08 de 2023). Audit trail and node authentication (ATNA). *IHE ITI Technical Framework, 1 (rev 20.0)*. Obtido de https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html

ISO. (2016). ISO 27799:2016 — Health informatics: Information security management in health using ISO/IEC 27002. (2ª). (I. O. Standardization, Ed.) Obtido em 21 de 07 de 2025

ISO. (2025, 1). *ISO/TS 81001-2-1:2025 - Health software and health IT systems safety, effectiveness and security — Part 2-1: Coordination — Guidance and requirements for the use of assurance cases for safety and security*. Geneva: ISO. Retrieved from https://cdn.standards.iteh.ai/samples/82210/09f24571ed9e4659bb6b648a614c95c0/ISO-TS-81001-2-1-2025.pdf

ISO/IEC. (2019). ISO/IEC 27701:2019 — Security techniques: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. (I. O. Standardization, Ed.) Obtido em 20 de 07 de 2025, de https://www.iso.org/standard/71670.html

ISO/IEC. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection: Information security management systems —

Requirements. (I. O. Standardization, Ed.) Obtido de https://www.iso.org/standard/27001

Kizer, H. (2020). *Designing a Secure IAM Architecture with NGINX, OAuth2-Proxy, Redis, Keycloak, and Flask.* Obtido de https://kizerh.medium.com/designing-a-secure-iam-architecture-with-nginx-oauth2-proxy-redis-keycloak-and-flask-993d4ea0f39f

Ladeia, Y., & Sousa, N. (2025). A Reutilização Dos Dados Dos Doentes Para Treinar Inteligência Artificial Para Dispositivos Médicos Na União Europeia. *Acta Médica Portuguesa, 38*(5), 285-287. doi:10.20344/amp.22509

Magalhães, F., & Pereira, M. (2020). *Regulamento Geral de Proteção de Dados - Manual Prático* (3 ed.). Lisboa: Grupo Editorial Vida Económica.

MediCollector. (2025). *TCP & HL7 Streaming Interface*. Obtido de https://www.medicollector.com/uploads/3/1/0/6/31064385/medicollector_-_tcp___hl7_streaming_interface.pdf

Mercure Imaging Org. (2025). *Monitoring — Mercure DICOM Orchestrator Documentation.* Retrieved from https://mercure-imaging.org/docs/monitoring.html

Microsoft. (2025). *Appendix L: Events to Monitor.* Obtido de Microsoft Learn: https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Microsoft. (2025, 06 02). *Frequently Asked Questions about Azure Health Data Services.* Retrieved from https://learn.microsoft.com/en-us/azure/healthcare-apis/healthcare-apis-faqs

Ministério da Saúde. (2024). Plano Estratégico 2024-2026. Em M. d. Saúde (Ed.), *Transição Digital na Saúde.* Lisboa. Obtido de https://www.sg.min-saude.pt/wp-content/uploads/2024/04/PE_2024-2026_web.pdf

NEMA. (2025). *DICOM Part 3.15: Security and System Management Profiles*. Retrieved 12 29, 2025, from https://dicom.nema.org/medical/dicom/current/output/pdf/part15.pdf

NEMA/DICOM Standards Committee. (2025). *PS 3.15 — Security and System Management Profiles*. Obtido em 29 de 12 de 2025, de National Electrical Manufacturers Association: https://www.dicomstandard.org/standards/view/security-and-system-management-profiles

NEXTGen. (2025). *Healthcare Integration Engine – Mirth Connect.* Obtido de https://www.nextgen.com/solutions/interoperability/mirth-integration-engine

Paessler AG. (10 de 06 de 2025). *How can I monitor DICOM and HL7 with PRTG?* Obtido em 04 de 12 de 2025, de Paessler - The Monitoring Experts:

https://helpdesk.paessler.com/en/support/solutions/articles/76000068619-how-can-i-monitor-dicom-and-hl-with-prtg

Parlamento Europeu e Conselho da União Europeia. (2016). Regulamento (UE) 2016/679 - Regulamento Geral sobre a Proteção de Dados. *Jornal Oficial da União Europeia*, L119, páginas 1–88. Obtido em 21 de 07 de 2025, de https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis

Parlamento Europeu e do Conselho. (6 de 7 de 2016). *Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L1148

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77.

Pires, R. I. (2012). *Os Sistemas de Informação nas Organizações de Saúde: Avaliação da Maturidade dos Sistemas de Informação Hospitalares*. Universidade de Évora, Évora. Obtido de https://dspace.uevora.pt/rdpc/bitstream/10174/17966/1/Tese%20de%20Mestrado.pdf

Pontes, C. M. (2020). *Avaliação do uso de Sistemas de Informação pelos gestores de nível intermédio em contexto hospitalar*. Universidade do Minho, Braga. Obtido de https://repositorium.uminho.pt/entities/publication/bf62e7c1-1c4d-4f46-8d42-f0e6c45adac4

Portugal. Presidência do Conselho de Ministros. (4 de 12 de 2025). Decreto-Lei n.º 125/2025, de 4 de dezembro. *Diário da República Eletrónico*. Obtido em 12 de 02 de 2026, de https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

PostDICOM. (s.d.). *Compreender o Protocolo de Comunicação DICOM*. Obtido em 25 de 07 de 2025, de PostDICOM: https://www.postdicom.com/pt/blog/understanding-dicom-communication-protocol

(2024). *Prioritising eHealth Cybersecurity Against Emerging Challenges*. Retrieved from https://www.enisa.europa.eu/news/prioritising-ehealth-cybersecurity-against-emerging-challenges

Recordon, D., & Reed, D. (2006). OpenID 2.0: A platform for user-centric identity management. *Proceedings of the Second ACM Workshop on Digital Identity Management* (pp. 11-16). ACM. Obtido de https://dl.acm.org/doi/abs/10.1145/1179529.1179532

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. Obtido de https://doi.org/10.6028/NIST.SP.800-207

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer, 29*(2), pp. 30-47. doi:https://doi.org/10.1109/2.485845

Sbrocco, J. H. (2012). *Metodologias Ágeis: Engenharia de Software sob Medida*. São Paulo: Érica.

Serviço Nacional de Saúde. (2023). *Transição Digital Na Saúde*. Obtido em 26 de 07 de 2024, de https://www.sns.gov.pt/: https://www.sns.gov.pt/noticias/2023/04/19/transicao-digital-na-saude-2/

Serviço Nacional de Saúde. (2025). *História Do SNS*. Obtido de https://www.sns.gov.pt/sns/servico-nacional-de-saude/historia-do-sns/

Serviços Partilhados do Ministério da Saúde. (05 de 2024). *Dois Anos de Exames Sem Papel e Mais de 115 Milhões de Resultados Partilhados*. Obtido de https://www.spms.min-saude.pt/2024/05/dois-anos-de-exames-sem-papel-e-mais-de-115-milhoes-de-resultados-partilhados/

Siemon, D. (2024). *Introduction to Design Science Research (DSR)*. Obtido de https://www.softwareengineering.fi/wp-content/uploads/2024/11/FAST_introduction_to_DSR.pdf

Sommerville, I. (2011). *Software Engineering* (9ª ed.). Addison-Wesley (Pearson).

SPMS. (2017). *Base de Dados Nacional de Requisições (BDNR) e API de acesso a MCDT*. Obtido em 20 de 04 de 2025, de SPMS: https://www.spms.min-saude.pt

SPMS. (06 de 2017). *Interoperabilidade Técnica – LIGHt, PNB e NCP*. Obtido de https://www.spms.min-saude.pt/2017/06/interoperabilidade-tecnica-light-pnb-ncp/

SPMS. (03 de 2017). *PNB Estreia Circuito Interministerial*. Obtido em 24 de 11 de 2025, de https://www.spms.min-saude.pt/2017/03/pnb-portuguese-national-broker/

SPMS. (07 de 2020). *Exames Sem Papel*. Obtido de https://www.spms.min-saude.pt/2020/07/exames-sem-papel/

Surety Systems . (2023). *Tapping into the Power of HL7 Message Structures with Surety Systems*. Obtido de https://www.suretysystems.com/insights/tapping-into-the-power-of-hl7-message-structures-with-surety-systems/

Thales Group. (2024, 1 1). *ISO 27799:2016 Compliance | Health Informatics*. Retrieved from https://cpl.thalesgroup.com/compliance/iso-277992016-compliance

Varela, R. (2019). *História Do Serviço Nacional de Saúde Em Portugal: A Saúde e a Força de Trabalho, Do Estado Novo Aos Nossos Dias*. Âncora Editora.

Wazuh. (2015). *Wazuh - The Open Source Security Platform. Unified XDR and SIEM protection*. Obtido em 22 de 06 de 2025, de GitHub: https://github.com/wazuh/wazuh

Yeh, J. (20 de 09 de 2020). *Setup Mirth Connect Monitoring in a Day*. Obtido de https://medium.com/teamzerolabs/setup-mirth-connect-monitoring-in-a-day-76c8db2cca15

Zamani Forooshani, M. (2020). *A Tool for Integrating Dynamic Healthcare Data Sources*. PhD thesis. doi:10.13140/RG.2.2.22074.82885

ANEXOS

Anexo A - Mapeamento entre requisitos, legislação e *frameworks* de segurança da informação e cibersegurança

Requisito de controlo e auditoria	RGPD	NIS2	QNRCS	Legislação portuguesa
Controlo de acessos baseado em funções (RBAC) Acesso limitado ao papel clínico e necessidade de conhecimento; princípio do menor privilégio	Proteção por omissão; medidas técnicas de segurança adequadas à sensibilidade dos dados de saúde (Artigos 5.º, 25.º e 32.º)	Políticas de controlo de acesso como medida técnica obrigatória para entidades essenciais de saúde (Artigo 21.º)	Identidades geridas com base em funções; contas e privilégios atribuídos segundo o princípio do menor privilégio; controlo de acesso físico e lógico a sistemas e dados (PR.GA-1, PR.GA-4)	Acesso ao processo clínico condicionado ao papel profissional; segredo médico como limite ao acesso; CNPD fiscaliza (Lei 58/2019 Artigo 28.º, Portaria 1303/2006)
Autenticação forte (MFA) Verificação com múltiplos fatores antes do acesso a registos médicos e sistemas clínicos	Medida técnica de segurança adequada ao risco; confidencialidade e integridade do tratamento (Artigo 32.º Considerenado 83)	MFA ou autenticação contínua expressamente exigida para entidades essenciais; listada como medida obrigatória (Artigo 21.º)	Autenticação obrigatória para todos os utilizadores; recomendação de autenticação multifator em sistemas e serviços críticos; gestão de credenciais e palavras-passe seguras (PR.GA-6, PR.GA-7)	Transposição NIS1: medidas técnicas para acesso seguro; obrigação implícita de autenticação robusta em sistemas de saúde (Lei 58/2019 Artigo 28.º, Decreto de Lei (DL) 109-D/2021)

Gestão de identidades privilegiadas (PAM) Controlo reforçado de contas de administrador e de acesso a dados altamente sensíveis	*Privacy by design*; medidas técnicas proporcionais à sensibilidade dos dados de categorias especiais (Artigos 25.º e 32.º)	Políticas de acesso privilegiado e uso de criptografia como medidas explícitas para entidades essenciais (Artigo 21.º)	Gestão do ciclo de vida de contas privilegiadas; separação de funções administrativas; controlo e registo de operações realizadas com privilégios elevados (PR.GA)	Acesso a sistemas clínicos dependente de identificação profissional verificada; responsabilidade disciplinar e civil em caso de acesso indevido (Lei 46/2004 Artigo 8.º, Portaria 1303/2006 Artigo 12.º)
Revisão e revogação periódica de acessos Remoção de acessos obsoletos; revisão regular dos direitos atribuídos após mudança de função ou saída	Limitação da conservação; direito ao apagamento; medidas técnicas e organizativas contínuas (Artigos 5.º, 17.º e 32.º)	Ciclo de vida de credenciais integra as políticas de controlo de acesso obrigatórias para entidades essenciais (Artigo 21.º)	Revisão periódica de direitos de acesso; desativação imediata de contas após cessação de funções ou contrato; procedimento formal de revogação documentado (PR.GA)	Dever de atualização de perfis de acesso; responsabilidade do responsável pelo tratamento pela gestão de acessos ativos (Lei 58/2019 Artigo 28.º, Lei 46/2004)
Registo e auditoria de acessos Logs com identidade do utilizador, timestamp, recurso acedido e origem; conservação adequada	Responsabilidade e capacidade de demonstrar conformidade; resiliência contínua dos sistemas de tratamento	Gestão de incidentes e práticas básicas de cibersegurança impõem registo sistemático de eventos de acesso a sistemas essenciais	Recolha e análise de logs de atividade de utilizadores e sistemas; registo de eventos de autenticação, autorização e acesso a dados; conservação dos registos por período definido em política interna	Registo obrigatório de acessos ao processo clínico eletrónico; prazo mínimo de conservação de 5 anos; rastreabilidade exigida por lei

	(Artigos 5.º, 24.ºe 32.º)	(Artigo 21.º)	(DT.MA)	(Lei 46/2004 Artigo 8.º, Portaria 1303/2006 Artigo 12.º, Lei 15/2014 Artigo 5.º)
Integridade e proteção dos logs Registos de auditoria não adulteráveis nem elimináveis sem autorização formal	Integridade e confidencialidade como princípios nucleares do tratamento; medidas técnicas de proteção adequadas (Artigos 5.º e 32.º)	Segurança na aquisição e manutenção de sistemas inclui integridade dos dados de registo; os logs são evidência em notificações de incidente (Artigo 21.º)	Proteção da integridade de dados e registos críticos; controlos contra modificação ou eliminação não autorizadas; centralização de logs em sistema protegido contra adulteração (PR.SD)	Integridade do processo clínico eletrónico legalmente exigida; responsabilidade civil e disciplinar em caso de alteração não autorizada de registos clínicos (Portaria 1303/2006 Artigo 12.º, Lei 46/2004 Artigo 8.º)
Deteção de acessos anómalos Identificação em tempo real de padrões suspeitos: acessos massivos, fora de horário, contas inativas	Capacidade de restaurar disponibilidade; deteção precoce como pressuposto da notificação em 72h à CNPD (Artigos 32.º e 33.º)	Alerta precoce em 24h implica capacidade de deteção contínua; impacto em serviços de saúde tem limiar de notificação baixo (Artigos 21.º e 23.º)	Monitorização contínua de sistemas e redes; deteção automatizada de comportamentos anómalos; correlação de eventos de segurança; alertas gerados e escalonados por processo definido (DT.MA, DT.DE)	Sem disposição legal explícita; (aplica-se o dever geral de segurança da Lei 58/2019 e das obrigações de gestão de incidentes do DL 109-D/2021 para operadores de serviços essenciais de saúde)

Notificação de violações e incidentes Comunicação atempada à autoridade de controlo e, se necessário, aos titulares; reporte ao CNCS	Notificação à CNPD em 72h; comunicação ao titular se risco elevado; documentação interna obrigatória (Artigos 33.º e 34.º)	Três fases: alerta ao CNCS (24h) → notificação (72h) → relatório final (30 dias); prazos mais curtos e processo mais exigente que o RGPD (Artigo 23.º)	Plano de resposta a incidentes documentado e testado; procedimentos de notificação a autoridades competentes; comunicação interna e externa definida; análise pós-incidente e lições aprendidas (RS.CO, RS.GI)	CNPD como autoridade de controlo para dados pessoais; CNCS como autoridade NIS; obrigações de reporte cumulativas em incidentes de dados de saúde (Lei 58/2019 Artigo 27.º, DL 109-D/2021 Artigo 12.º)
Pseudonimização e minimização de dados Redução da exposição de identificadores diretos em logs, relatórios e sistemas de monitorização	Minimização, limitação da finalidade e pseudonimização como medidas técnicas de proteção adequadas (Artigos 4.º, 5.º, 25.º e 32.º)	NIS2 remete para RGPD em matéria de dados pessoais; pseudonimização integra medidas de proteção de sistemas (Artigo 21.º, Considerando 89)	Classificação de dados por sensibilidade; encriptação de dados em repouso e em trânsito; aplicação de técnicas de anonimização e pseudonimização em contextos de menor necessidade de identificação (PR.SD, PR.PI)	Anonimização obrigatória para investigação clínica; pseudonimização como medida preferencial de proteção de dados de saúde em tratamentos secundários (Lei 58/2019 Artigo 2.º, Lei 21/2014 Artigo 4.º)
Conservação e eliminação segura de dados Cumprimento de prazos de retenção; eliminação	Limitação da conservação como princípio; direito ao apagamento; dados não mantidos além	Ciclo de vida dos sistemas inclui ciclo de vida dos dados; aplicável indiretamente; sem disposição autónoma explícita	Política de retenção e eliminação de dados documentada; eliminação segura e verificável de suportes e dados; inventário de dados	Processo clínico conservado por mínimo de 10 anos após o último ato; arquivamento regulamentado pelo IGFSS e ARS regionais

verificável após o prazo legal ou contratual	do necessário à finalidade (Artigo 5.º e 17.º)	(Artigos 21.º)	com prazos de retenção definidos por categoria (PR.SD, PR.PI)	(Lei 46/2004 Artigo 10.º, Portaria 1303/2006)
Segurança da cadeia de abastecimento Controlo de acessos de fornecedores e subcontratantes a sistemas e dados clínicos	Contrato com subcontratante obrigatório; fornecedor vinculado às mesmas obrigações de segurança do responsável pelo tratamento (Artigos 28.º e 32.º)	Requisito autónomo e explícito: avaliação das práticas de segurança de fornecedores TIC é medida obrigatória para entidades essenciais (Artigos 21.º e 22.º)	Identificação e avaliação de fornecedores críticos; cláusulas de segurança em contratos com terceiros; controlo de acessos remotos de fornecedores; auditoria de conformidade de subcontratantes (ID.GR)	Subcontratantes de dados de saúde sujeitos às mesmas obrigações; notificação ao CNCS em incidentes que envolvam fornecedores de serviços essenciais (Lei 58/2019 Artigo 28.º, DL 109-D/2021 Artigo 10.º)
Continuidade e recuperação de serviços Manutenção ou restauro rápido de sistemas clínicos críticos após incidente ou desastre	Resiliência contínua dos sistemas; capacidade de restaurar disponibilidade e acesso em tempo útil (Artigo 32.º)	Continuidade, backups e recuperação de desastres como medidas obrigatórias; saúde classificada como setor de alta criticidade no Anexo I da diretiva (Artigo 21.º)	Plano de continuidade de negócio documentado e testado; backups regulares, protegidos e verificados; objetivos de tempo de recuperação (RTO) e ponto de recuperação (RPO) definidos; exercícios periódicos de simulação (RC.PL, RC.ME)	SNS obrigado a manter planos de continuidade operacional; SPMS coordena resiliência dos sistemas de informação de saúde nacionais (DL 109-D/2021, Lei 95/2019 Artigo 24.º)

Anexo B - Orthanc-wazuh-store-audit.lua

```lua
-- /etc/orthanc/orthanc-wazuh-store-audit.lua

local logFile = "/var/log/orthanc/dicom_store_audit.log"

local function writeLog(line)
  local f = io.open(logFile, "a")
  if f ~= nil then
    f:write(line .. "\n")
    f:close()
  end
end

-- ocorre por cada inserção de imagem / recurso
function OnStoredInstance(instanceId, tags, metadata, origin)
  local remoteAet = ""
  local remoteIp = ""
  if origin ~= nil then
    remoteAet = origin["RemoteAet"] or ""
    remoteIp = origin["RemoteIp"] or ""
  end
  local studyUid  = tags["StudyInstanceUID"] or ""
  local patientId = tags["PatientID"] or ""
  local modality  = tags["Modality"] or ""
  -- StudyDate + StudyTime = datetime de criação do estudo (da modalidade)
  local studyDate = tags["StudyDate"] or ""
  local studyTime = tags["StudyTime"] or ""
  local studyDatetime = studyDate .. " " .. studyTime  -- YYYYMMDD HHMMSS
  -- data/hora de receção no Orthanc (UTC)
  -- não sofre alterações de DST/fuso
  local ts = os.date("!%Y-%m-%dT%H:%M:%SZ")
  -- formato key=value para Wazuh
  local line = string.format(
    'event=stored_instance ts=%s remote_aet=%s studyuid=%s patientid=%s
modality=%s study_datetime=%s',
    ts, remoteAet, studyUid, patientId, modality, studyDatetime
  )

  writeLog(line)
end

-- ocorre quando estudo fica estável
-- (ultima receção de imagem > StableAge)
-- registo agregador
function OnStableStudy(studyId, tags, metadata)
  local studyUid  = tags["StudyInstanceUID"] or ""
  local patientId = tags["PatientID"] or ""
  -- StudyDate + StudyTime do estudo (da primeira instância)
  local studyDate = tags["StudyDate"] or ""
  local studyTime = tags["StudyTime"] or ""
  local studyDatetime = studyDate .. " " .. studyTime
  -- data/hora quando estudo ficou estável (UTC)
  local ts = os.date("!%Y-%m-%dT%H:%M:%SZ")
```

```
  -- formato key=value para Wazuh (sem AET, pois é agregado)
  local line = string.format(
    'event=stable_study ts=%s studyuid=%s patientid=%s study_datetime=%s',
    ts, studyUid, patientId, studyDatetime
  )

  writeLog(line)
end
```

Anexo C - Orthanc-wazuh-find-audit.lua

```
-- /etc/orthanc/orthanc-wazuh-find-audit.lua

local logFile = "/var/log/orthanc/dicom_find_audit.log"

local function writeLog(line)
  local f = io.open(logFile, "a")
  if f ~= nil then
    f:write(line .. "\n")
    f:close()
  end
end

function IncomingFindRequestFilter(source, origin)
  local remoteAet = origin["RemoteAet"] or ""
  local remoteIp  = origin["RemoteIp"] or ""

  -- Tags da query C-FIND (ex: PatientID, StudyInstanceUID, etc.)
  local patientId = source["PatientID"] or ""
  local studyUid  = source["StudyInstanceUID"] or ""
  local modality  = source["Modality"] or ""

  -- data/hora da query (UTC)
  local ts = os.date("!%Y-%m-%dT%H:%M:%SZ")

  -- formato key=value para Wazuh
  local line = string.format(
    'event=find_request ts=%s remote_aet=%s remote_ip=%s patientid=%s
studyuid=%s modality=%s',
    ts, remoteAet, remoteIp, patientId, studyUid, modality
  )

  writeLog(line)

  -- Devolve a source original (não altera a query)
  return source
end
```

Anexo D - Orthanc-wazuh-dicomweb-wado-audit.lua

```
-- /etc/orthanc/orthanc-wazuh-dicomweb-wado-audit.lua

local logFile = "/var/log/orthanc/dicomweb_wado_audit.log"

local function writeLog(line)
  local f = io.open(logFile, "a")
  if f ~= nil then
    f:write(line .. "\n")
    f:close()
  end
end

function OnStartedRequest(method, uri, ip)
  if string.match(uri, "/studies/") or string.match(uri, "/series/") then
    local ts = os.date("!%Y-%m-%dT%H:%M:%SZ")
    writeLog(string.format('event=wado_retrieve ts=%s remote_ip=%s
uri=%s', ts, ip, uri))
  end
end
```

Anexo E - Orthanc-dicom-audit-log-rotate

```
# /etc/logrotate.d/orthanc-dicom-audit

/var/log/orthanc/dicom_store_audit.log {
    daily          # rodar todos os dias
    rotate 14      # manter 14 dias de histórico
    missingok
    notifempty
    compress       # comprimir ficheiros antigos em .gz
    delaycompress
    create 0640 orthanc adm
}

/var/log/orthanc/dicom_find_audit.log {
    daily          # rodar todos os dias
    rotate 14      # manter 14 dias de histórico
    missingok
    notifempty
    compress       # comprimir ficheiros antigos em .gz
    delaycompress
    create 0640 orthanc adm
}

/var/log/orthanc/dicomweb_wado_audit.log {
    daily          # rodar todos os dias
    rotate 14      # manter 14 dias de histórico
    missingok
    notifempty
    compress       # comprimir ficheiros antigos em .gz
    delaycompress
    create 0640 orthanc adm
}
```