P.PORTO

INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

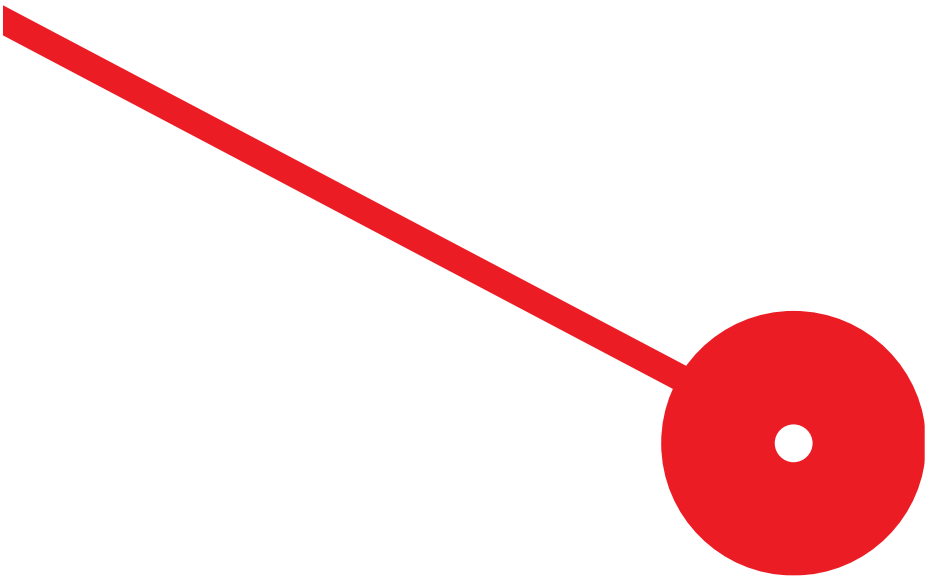
M

MESTRADO
Informação Empresarial

Estágio: Avaliações de Impacto sobre Proteção de Dados e de Segurança da Informação

Raúl Manuel do Novo Catarino Jaques

10/**2022**



Raúl Jaques. Estágio: Avaliações de Impacto sobre Proteção de Dados e de Segurança da Informação
10/**2022**

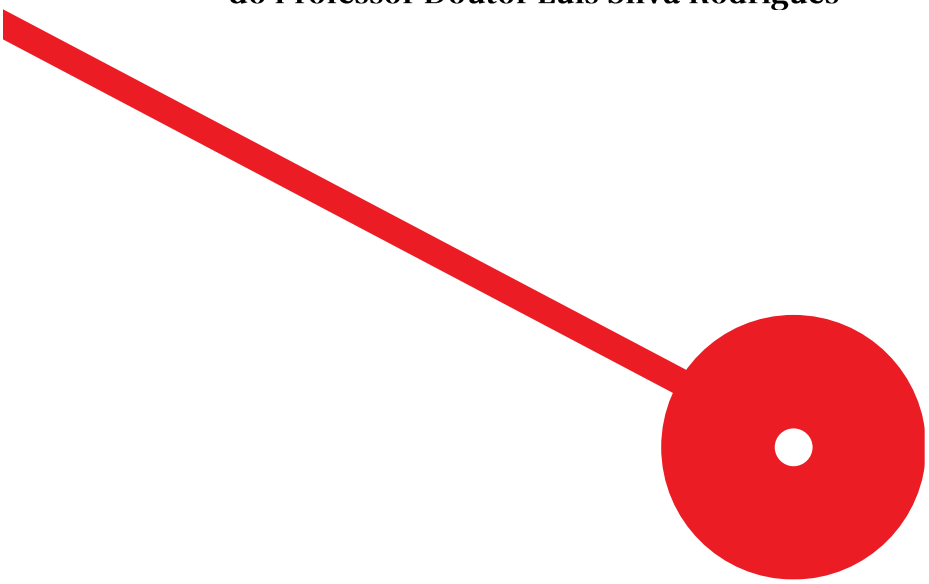
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO
Informação Empresarial

Estágio: Avaliações de Impacto sobre Proteção de Dados e de Segurança da Informação

Raúl Manuel do Novo Catarino Jaques

Relatório de Estágio apresentado ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Informação Empresarial, sob orientação do Professor Doutor Luís Silva Rodrigues



Raúl Jaques. Estágio: Avaliações de Impacto sobre Proteção de Dados e de Segurança da Informação
10/2022

Resumo:

Em 2016, a União Europeia criou o Regulamento Geral sobre a Proteção de Dados (RGPD), com aplicação obrigatória em toda a União Europeia a partir de 25 de maio de 2018, tendo gerado um forte debate em torno da proteção de dados, em particular os dados pessoais. Ao se considerarem medidas impostas por lei como o Direito de Acesso, o Direito ao Apagamento de Dados e o Direito de Retificação dos dados pessoais, torna-se necessária a existência de mecanismos que assegurem a conformidade dos Sistemas de Informação (SI) perante tais imposições.

De modo a assegurar que as organizações sigam as diretrizes do RGPD é encorajada a realização de Avaliações de Impacto sobre a Proteção de Dados de modo a serem visíveis as mudanças nas necessidades de segurança dos SI das organizações.

No âmbito do Mestrado em Informação Empresarial foi realizado um estágio do qual resultou o presente relatório. O estágio foi realizado durante cerca de seis meses e meio, no edifício central da Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A., inserido na Divisão de Proteção de Dados e Gestão de Risco Empresarial. Tendo como foco a proteção dos dados pessoais usados nas atividades da organização foram definidos dois objetivos principais. Por um lado, analisar e avaliar as práticas e os mecanismos de segurança de cada SI utilizados dentro da organização e, por outro lado, verificar o nível de conformidade da implementação das diretrizes do RGPD.

Durante este estágio foram avaliados oito SI, alguns interligados, mas todos com processos e finalidades diferentes, concluiu-se que, de uma forma geral, se verifica um aumento no nível de segurança dos SI, e que, apesar de serem necessárias alguns ajustes, também existe um elevado nível de conformidade quanto à aplicação das diretrizes do RGPD.

Palavras chave: Dados Pessoais; RGPD; Avaliações de Conformidade de Segurança.

Abstract:

In 2016, the European Union created the General Data Protection Regulation (GDPR), with mandatory application throughout the European Union starting 25 May 2018, it generated a strong debate around data protection, in particular personal data. When considering measures imposed by law such as the Right of Access, the Right to Erase Data and the Right to Rectify Personal Data, it is necessary to have mechanisms that ensure the compliance of the Information Systems (IS) with such rules.

In order to ensure that organizations follow the guidelines of the RGPD, it is encouraged to carry out Impact Assessments on Data Protection (AIPD) in order to know what changes are needed in the organization's IS.

Within the scope of the Master in Business Information, an internship was carried out for which this document serves as a report. The internship was carried out for about six and a half months, in the headquarters of Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A., inserted in the Data Protection and Business Risk Management Division. Focusing on the protection of personal data used in the organization's activities, two objectives were defined. On the one hand, analyze and evaluate the practices and security mechanisms of each IS used within the organization and, on the other hand, verify the level of compliance of the implementation of the GDPR guidelines.

During the internship eight IS were evaluated, some interconnected, but all with different processes and purposes. It was concluded that overall there is an increase in the security level of the IS, and that, although some adjustments are necessary, there is also a high level of compliance with GDPR guidelines.

Key words: Personal Data; GDPR; IADP; Security Compliance Evaluation.

Índice Geral

Índice de Figuras

Índice de Tabelas

Lista de Siglas e Acrónimos

3PL	Portaria Principal do Porto de Leixões
AEPD	Autoridade Europeia para a Proteção de Dados
AIPD	Avaliação de Impacto sobre a Proteção de Dados
APDL	Administração dos Portos de Douro, Leixões e Viana de Castelo
CA	Conselho de Administração
CCTV	Closed Circuit TV
CdE	Conselho da Europa
CEDH	Convenção Europeia dos Direitos do Homem
CEE	Comunidade Económica Europeia
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
CUP	Cartão Único Portuário
DOPS	Divisão de Operações Portuárias e Segurança
DRH	Divisão de Recursos Humanos
DSI	Direção de Sistemas de Informação
DvIP	Divisão de Informação e Processos
DvPDGRE	Departamento de Proteção de Dados e Gestão de Risco Empresarial
DvST	Divisão de Sistemas e Tecnologia
ENISA	European Union Agency for Cybersecurity
EPD	Encarregada de Proteção de Dados
GESDOC	Gestão Documental
IP	Protocolo Internet
JUL	Janela Única Logística
JUP	Janela Única Portuária
NATO	North Atlantic Treaty Organization
PEX	Portal Executivo
RFID	Radio Frequency Identification
RGPD	Regulamento Geral de Proteção de Dados
SI	Sistema de Informação
VGM	Verified Gross Mass

CAPÍTULO - INTRODUÇÃO

1.1 Contextualização do Estágio

O presente relatório de estágio, constitui um requisito para a conclusão do Mestrado em Informação Empresarial, no Instituto Superior de Contabilidade e Administração do Porto. O estágio realizou-se na Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A., também conhecida por APDL, inserido na Divisão de Proteção de Dados e Gestão de Risco Empresarial (DvPDGRE), e supervisionado pela Dra. Teresa Silva, chefe da divisão e Encarregada de Proteção de Dados (EPD) da organização.

De modo a poder realizar este estágio, tornou-se necessária a obtenção de conhecimentos sobre conceitos como Privacidade, Dados Pessoais e Cibersegurança. Numa perspetiva mais técnica foi também necessário conhecer as especificidades do RGPD, bem como para que servem e como são realizadas as Avaliações de Impacto sobre a Proteção de Dados (AIPD) e Avaliações de Conformidade. O levantamento da literatura existente, e posterior análise, foi o primeiro objetivo deste estágio.

A APDL, que tem por finalidade a administração dos portos do Douro, Leixões e Viana do Castelo, visando a sua exploração económica, conservação e desenvolvimento, necessita de inúmeros SI diferentes, todos com funções diversas, mas alguns interligados, de modo a concretizar esta finalidade.

Estes SI requerem avaliações periódicas de modo a ser analisado o seu nível de segurança da informação e o nível de conformidade para com as diretrizes do RGPD, sendo estes os dois objetivos principais do estágio. Por um lado, analisar o nível de segurança de cada SI usado na organização, comparando com as medidas de segurança apresentadas na Diretiva (EU) 2016/1148 (EU,2016) e também no RGPD, e se existe uma evolução das práticas adequadas quanto à segurança dos mesmos, usando para tal a realização de avaliações de conformidade para cada SI e uma consequente comparação com as avaliações anteriores do mesmo. E por outro, verificar a implementação e do nível de conformidade dos SI perante as diretrizes do RGPD.

1.2 Estrutura do Documento

Para além da Introdução que constitui o presente capítulo, este documento é consituido por vários capítulos. No capítulo II inicia-se com uma apresentação da organização, sendo explicadas as suas áreas de atuação e os serviços que presta, e do departamento onde o estágio decorreu. Em seguida são apresentados de forma detalhada os objetivos do estágio e as atividades planeadas.

No terceiro capítulo, é apresentado um enquadramento teórico sobre a temática da proteção de dados, mais concretamente a evolução das empresas em matéria de conformidade com o RGPD e a aplicação das AIPD como instrumento de análise de risco, referindo alguns conceitos como privacidade, tratamento de dados, responsáveis pelo tratamento de dados pessoais, encarregado de proteção de dados e direitos do titular dos dados.

O capítulo IV reserva-se à apresentação das tarefas desenvolvidas durante o estágio e a descrição dos resultados obtidos.

Para finalizar, o capítulo V, apresenta uma síntese do documento e de toda a experiência, onde são descritas as limitações do projeto e considerações para projetos futuros.

2.1 Apresentação do Local de Estágio

Como referido anteriormente, o estágio foi realizado na APDL. A APDL é uma sociedade anónima de capitais exclusivamente públicos, que tem por objeto a administração dos portos do Douro e Leixões, visando a sua exploração económica, conservação e desenvolvimento. De acordo com informação apresentada no website da organização (https://www.apdl.pt), a sua missão é a seguinte:

> *Prestar serviços de reconhecido valor aos clientes e utilizadores do sistema de portos do Norte de Portugal, nas vertentes comercial, logística e turística através de uma adequada oferta de infraestruturas, de uma elevada eficiência operacional, de sistemas tecnológicos e de práticas inovadoras, de recursos humanos qualificados e motivados, de uma prática de sustentabilidade e de segurança, ordenando e desenvolvendo o espaço portuário e assegurando a adequada integração urbana, envolvendo as comunidades portuárias.*

Uma vez que opera e gere áreas portuárias, a APDL é caracterizada perante a Lei e os órgãos competentes como um operador de infraestruturas críticas pois opera um "sistema situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções" (Lei 46/2018, 2018, artigo 3º, alínea d). Possuindo estas características mostra-se necessário um acompanhamento sério e minucioso quanto à segurança dos SI usados dentro da organização

Perante o conjunto de áreas de atuação que a organização apresenta, são de salientar, no âmbito deste estágio, as seguintes:

- Assegurar o normal funcionamento dos portos em todas as suas vertentes;
- Atribuir licenças e/ou concessões;
- Licenciar o exercício da atividade portuária e a concessão de serviços públicos portuários; e
- Expropriar servidões administrativas.

Em mais pormenor, de todos os diferentes serviços prestados pela organização, no âmbito deste estágio, são de destacar os seguintes: Gestão de postos de acostagem; Controlo de tráfego marítimo; Controlo de acessos à área portuária; Sistemas de segurança; Atribuição de licenças; e Atribuição de concessões. Esta informação foi recolhida junto da tutora de estágio através de documentos internos da organização, e também através do website da organização (https://www.apdl.pt)

Considerando o enquadramento legal em vigor, visto tratar-se de uma infraestrutura crítica na perspetiva da Lei mostra-se necessário um acompanhamento sério e minucioso quanto à segurança dos SI usados dentro da organização. De modo a gerir esta necessidade de segurança foi criada a DvPDGRE, departamento onde se realizou o estágio. Na Figura 1 é possível constatar o posicionamento desta divisão no organigrama da APDL.

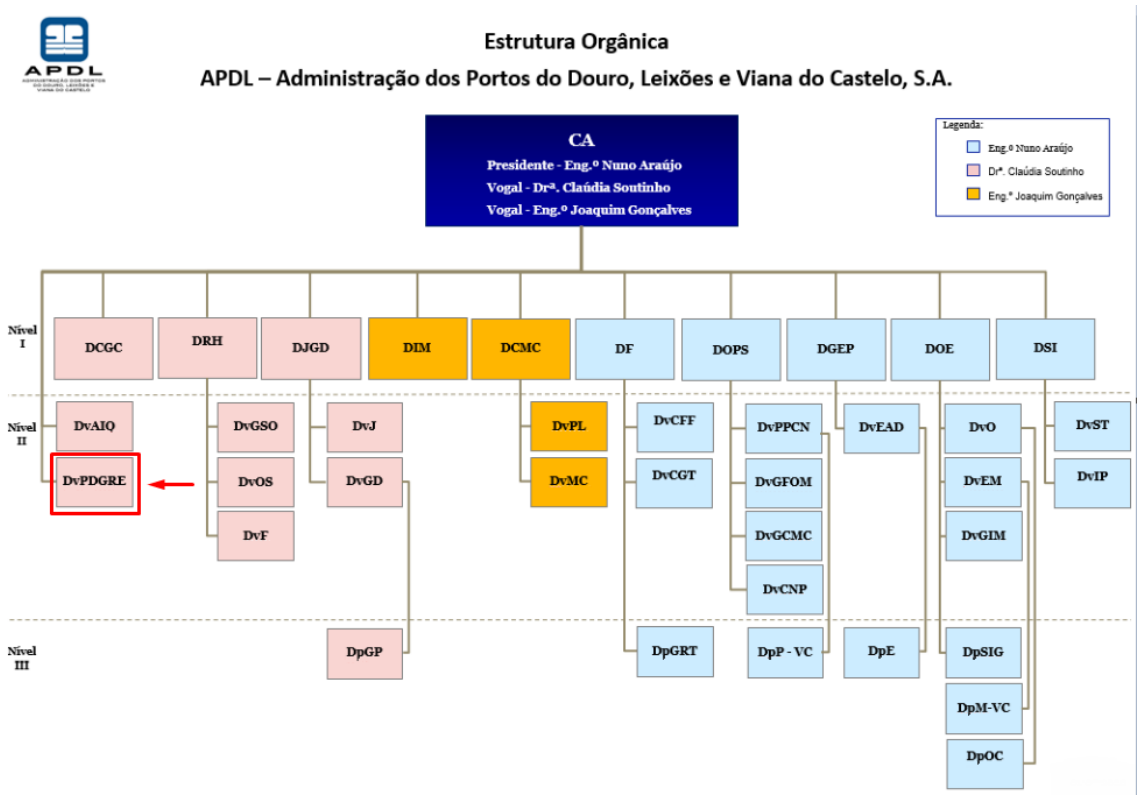


Figura 1 *- Estrutura Orgânica da Organização*

Fonte*: APDL (2022)*

A DvPDGRE, liderada pela tutora do estágio, a Dra. Teresa Silva (EPD), tem como tarefas:

- Garantir, junto da Direção de Sistemas de Informação (DSI), da Divisão de Recursos Humanos (DRH) e demais unidades orgânicas, a segurança e confidencialidade de informações;
- Informar e aconselhar o Conselho de Administração (CA) sobre as respetivas obrigações nos termos do RGPD;
- Controlar o cumprimento, por parte de todos os serviços, da legislação relacionada com a Proteção de Dados, nomeadamente com avaliações, atividades de sensibilização e formação do pessoal, implicando-os nas operações de tratamento;
- Atuar como ponto de contacto para pedidos de pessoas singulares relativamente ao tratamento dos seus dados pessoais e ao exercício dos seus direitos; e
- Assegurar a confidencialidade dos dados pessoais (sejam de clientes ou de colaboradores) e controlar estritamente o acesso, a transmissão e o uso desses dados.

2.2 Objetivos do Estágio

Para que o estagiário desenvolvesse uma aprendizagem básica acerca do trabalho realizado pela Divisão, foi determinado que o primeiro objetivo do estágio seria o levantamento e, consequente, compreensão da literatura existente referente aos conceitos nucleares das atividades da Divisão. Com esse intuito, seriam recolhidas todas as leis e legislações que guiam o trabalho realizado na Divisão, entre outras o RGPD.

Foram ainda estabelecidos dois objetivos para o estágio que seriam realizados, em paralelo, durante as sessões de avaliação. Um destes objetivos foi o de analisar se existe uma evolução das práticas de segurança dos SI, tanto a nível técnico como a nível de recursos humanos, dentro da organização. Para tal, considerou-se que com a realização de Avaliações de Conformidade de Segurança para cada SI, usando os requisitos do RGPD e da legislação conexa como referência, e uma consequente comparação com as avaliações anteriores do mesmo, seria possível determinar se de facto existe uma melhoria das práticas e da segurança dos SI. Com o outro objetivo, pretendia-se verificar a implementação das diretrizes do RGPD de modo a assegurar que os dados pessoais utilizados dentro da organização estão devidamente protegidos. Para tal considerou-se

necessário realizar AIPD, com recurso a documentos especializados, de modo a medir o grau de segurança de cada SI no âmbito da Proteção de Dados. Dependendo do grau de segurança atingido seria ou não necessário identificar oportunidades de melhoria ou potenciais riscos.

A realização das AIPD apresentavam um nível de dificuldade acrescido uma vez que os SI utilizados no seio da organização estão maioritariamente interligados, passando informação entre eles. Esta interligação dificulta as avaliações e o grau de segurança pois existem SI em fases diferentes do seu ciclo de vida, uns ainda em fase de teste e desenvolvimento, enquanto outros estão em *phasing out* (descontinuação do sistema).

Durante o planeamento do estágio ficou estabelecido que seriam avaliados os seguintes SI:

- Portaria Principal do Porto de Leixões (3PL)
- Sistema de Controlo de Acessos Físicos
- PowerBI
- Cartão Único Portuário (CUP)
- Portal Executivo (PEX)
- Ferramenta de Combate a Ciberameaças
- Gestão Documental (GESDOC)
- Closed Circuit TV (CCTV)

O sistema 3PL é usado para gerir as entradas e saídas do Porto de Leixões. O Sistema de Controlo de Acessos Físicos, tal como diz o nome, é responsável pela gestão dos acessos físicos das áreas geridas pela APDL. O sistema PowerBI tem como objetivo reunir e tratar informação de modo a apresentá-la num formato simples e intuitivo ao utilizador para que este possa criar *dashboards* e relatórios. O sistema CUP, em sintonia com o Sistema de Controlos de Acesso Físico, serve de plataforma para a criação dos cartões de acesso. O sistema PEX é a aplicação responsável pela gestão dos assuntos a ser tratados pelo Conselho de Administração da organização. A Ferramenta de Combate a Ciberameaças é um sistema de monitorização da rede interna. A aplicação GESDOC é o sistema de

gestão documental usado pela organização. E, o sistema CCTV tem como finalidade a proteção da área administrada pela APDL através da gravação de imagens.

2.3 Atividades Planeadas

De modo a contextualizar o estagiário sobre o trabalho realizado na DvPDGRE, ficou estabelecido que, as primeiras semanas do estágio, seriam dedicadas à consolidação de conhecimentos sobre o RGPD, leis e legislação relevantes para a atividade da Divisão, consubstanciada numa revisão da literatura sobre os conceitos necessários para a realização do estágio.

Durante esta preparação para o trabalho a ser realizado durante o estágio, também deveriam ser estudados os SI que iriam ser alvo das avaliações, de modo a que o estagiário formasse uma ideia da informação que iria necessitar durante o estágio.

Aquando do planeamento do estágio ficou ainda estabelecido que na avaliação de cada um dos SI fossem realizadas as seguintes etapas:

- Estudo prévio do SI e a sua funcionalidade;
- Revisão dos documentos já preenchidos de relevância a cada SI;
- Preparação dos instrumentos de base à avaliação;
- Realização da sessão de avaliação do SI;
- Apreciação do SI e definição dos pontos críticos; e
- Elaboração de relatórios.

As três primeiras etapas, ou seja, o estudo prévio do SI, a revisão dos documentos já preenchidos, e a preparação dos instrumentos de base à avaliação, não tinham um prazo pré-estabelecido para serem realizadas, sendo apenas necessário que o estagiário demonstrasse os conhecimentos necessários aquando das avaliações. Os documentos referentes a avaliações passadas, seriam fornecidos pela tutora do estágio de modo a minimizar a necessidade de acesso a qualquer outro tipo de SI ou plataforma usada pela empresa

No que se refere às últimas três etapas, nomeadamente a realização das sessões de avaliação dos SI, a apreciação dos SI e definição dos pontos críticos, e a elaboração dos

relatórios, para estas foram definidos prazos concretos. Este conjunto de etapas, deveriam ser realizadas para cada SI com uma duração de cerca de uma semana, sendo que em casos especiais de elevada complexidade e interligação de sistemas, esta duração poderia ser alargada.

A sessão de avaliação de cada SI seria agendada de acordo com a disponibilidade dos membros da Divisão juntamente com a disponibilidade do Responsável pelo SI em questão. De um modo geral, as sessões seriam realizadas em formato online na plataforma Microsoft Teams©, tendo uma duração prevista de duas horas, mas sem limite definido, respeitando, no entanto, os horários dos colaboradores.

Inicialmente, previa-se que as sessões começassem por uma breve apresentação da finalidade do SI, realizada pelo seu responsável, de modo a contextualizar todos os presentes sobre o que iria ser discutido, seguida de demonstração do sistema. Durante estas sessões previa-se ainda o preenchimento de documentos de apoio ao registo das avaliações em curso e, complementarmente, a utilização da plataforma Tekprivacy©. Esta plataforma é uma solução que agiliza o processo de avaliação dos SI, sendo que tem como objetivo promover soluções especializadas quanto ao tratamento de informação e dados pessoais tendo em conta a natureza das atividades da organização

Após cada sessão, com recurso aos documentos preenchidos e às plataformas de suporte, seguir-se-ia a etapa de definição dos pontos críticos de cada SI de forma a identificar potenciais riscos ou falhas existentes no SI e, consequentemente, identificar possíveis oportunidades de melhoria. No decurso desta etapa seria necessário a elaboração de relatórios individuais a cada SI, não só pelas diferentes especificidades de cada SI usado dentro da organização, mas também por ser uma boa prática organizacional, tendo assim registo de todas as ocorrências durante o processo. Para cada relatório, primeiramente, seria elaborado um rascunho no qual a informação é verificada pelos colaboradores envolvidos no processo. Uma vez verificado o rascunho será então transformado num documento oficial que será partilhado com o responsável de cada SI, de modo a que este ofereça um último parecer sobre toda a avaliação antes da mesma ser apresentada à direção como um serviço concluído.

Concluída a avaliação de cada SI, seriam agendadas reuniões com membros da direção da organização com a finalidade de apresentar cada relatório informando assim a situação

atual de cada SI, bem como oportunidades de melhoria ou potenciais riscos que apresentem.

3.1 Privacidade

Antes de se apresentar uma exposição sobre a proteção de dados pessoais deve-se entender que esta necessidade de proteção resulta também da preocupação com proteção da privacidade do indivíduo.

O direito à privacidade foi autonomizado pela primeira vez em 1890, quando Samuel Warren e Louis Brandeis publicaram, na Harvard Law Review, um artigo sob o título "The Right to Privacy" (Castro, 2005, p. 17). O debate sobre a privacidade colocou em evidência que a ocorrência de alterações sociais, políticas e económicas, com a divulgação de fotografias e documentos que originavam uma violação à vida privada das pessoas e lesionava o senso da pessoa sobre a sua independência, individualidade, dignidade e honra (Figueiredo, 2020).

Nos dias de hoje, o direito à privacidade é tomado como um direito fundamental pelo nosso ordenamento jurídico.

3.2 Dados Pessoais

Segundo Magalhães e Pereira (2018, p.19), e dada a necessidade de definir claramente o que são estes dados pessoais dos quais falamos em proteger, considera-se dados pessoais todos e quaisquer dados relativos a pessoas singulares, como nome, morada, e-mail, idade, estado civil, dados de localização, genéticos, fisiológicos, económicos, culturais ou sociais. Dado o mundo altamente digital em que vivemos este conceito foi alargado para também incluir "endereços IP (Protocolo Internet).

Alguns exemplos de dados que não são considerados pessoais são: o número de registo de empresa, um endereço de correio eletrónico genérico como, por exemplo info@empresa.com, ou seja, qualquer tipo de dados que não identifiquem uma pessoa singular.

Validando esta interpretação do conceito, no artigo 4º, número 1 do RGPD, são classificados como dados pessoais, toda a informação relativa a uma pessoa singular identificada ou identificável, sendo essa pessoa singular designada por "titular dos dados". Em certas situações e processos existe a necessidade, ou precaução, de

descaracterizar e, ou, codificar dados pessoais, criando assim dados pseudonimizados (artigo 4º, número 5 do RGPD) uma vez que não identificam diretamente um titular dos mesmos. Este tipo de dados tem a particularidade de, com recurso a programas ou chaves específicas (identificadores), ser possível reidentificar a pessoa singular a quem esses dados pertencem. É de notar que estes tipos de dados continuam abrigados pelo RGPD como sendo dados pessoais.

Apenas numa situação de anonimização irreversível, ou seja, caso se verifique a não existência de qualquer tipo de identificador, é que há a transformação dos dados pessoais para dados não pessoais pois foram verdadeiramente anonimizados. Dados não pessoais não estão salvaguardados pelo RGPD.

3.3 Recolha e Tratamento de Dados Pessoais

O facto de vivermos numa época avassaladoramente digital resulta no constante tráfego de informação pelos meios binários, fenómeno que se mostra como um catalisador para acelerar o processo de recolha de dados, não só os pessoais.

A recolha de dados por si só raramente representa valor às organizações, sendo que na maioria dos casos estes dados precisam de ser tratados.

Suportado pelo artigo 4º, número 2, do RGPD, Magalhães e Pereira (2018, p.19), descrevem tratamento de dados como a operação ou um conjunto de operações efetuadas sobre dados pessoais, ou sobre conjuntos de dados pessoais, por meios automatizados ou não. Determinado pelo RGPD, sempre que uma organização trata dados pessoais, é necessário nomear um Responsável pelo Tratamento.

Segundo o artigo 4º do RGPD, e, novamente, mencionado por Magalhães e Pereira (2018), um responsável pelo tratamento de dados trata-se de uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-membro, o Responsável pelo Tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-membro.

O Responsável pelo Tratamento pode subcontratar serviços de tratamento de dados pessoais a outras organizações. De acordo com o RGPD essas empresas são designadas

por Subcontratantes e o RGPD exige que exista um Acordo de Proteção de Dados Pessoais entre as partes, onde o Responsável pelo Tratamento coloca todas as condições, controlos e medidas que o Subcontratante deve implementar no decurso das suas atividades em nome do Responsável pelo Tratamento.

Será agora pertinente apresentar um diagrama que represente todos os intervenientes e autoridades de controlo no espaço dos dados pessoais, como apresentado na Figura 2. As definições dos mesmos são referenciadas pelo artigo 4º do RGPD e por Martins (2020):

- Encarregado de Proteção de Dados – Orienta o subcontratado e o responsável pelo tratamento e é o principal ponto de contacto com os titulares dos dados pessoais e as autoridades de supervisão;
- Subcontratado – Uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento deles, e de acordo com as regras definidas pelo mesmo;
- Responsável pelo Tratamento – Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais;
- Titulares dos Dados – Pessoal singular que dá o consentimento para o tratamento dos seus dados pessoais.

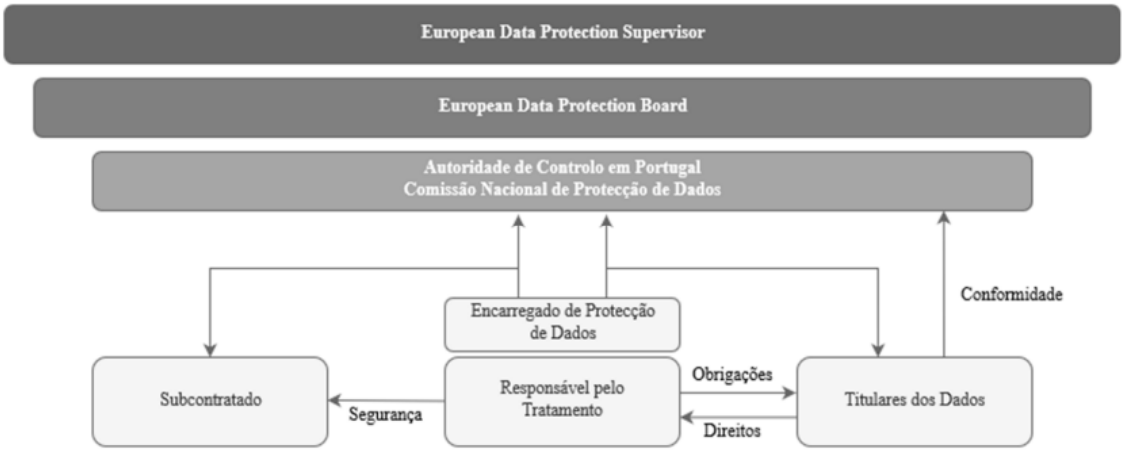


***Figura 2** - Autoridades de Controlo*

***Fonte**: Martins (2020)*

3.4 Regulamento Geral de Proteção de Dados – RGPD

A nível europeu, o primeiro passo em prol da proteção de dados foi quando, em 1950, o Conselho da Europa (CdE), adotou a Convenção Europeia dos Direitos do Homem (CEDH), onde, sob o artigo 8º, "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência".

Alguns anos mais tarde, em 1957, através do Tratado de Roma, cria-se a Comunidade Económica Europeia (CEE), uma organização internacional com a finalidade de estabelecer um mercado comum europeu. Existindo um mercado comum mostra-se necessária a existência de legislação para que todos os países envolvidos na comunidade possuam os mesmos direitos e deveres, sendo um dos temas englobados nesta legislação o tratamento de dados.

Já em 1981 foi aprovada a convenção número 108 pelo CdE, onde seriam estabelecidas medidas e níveis de proteção das pessoas quanto ao tratamento automatizado de dados pessoais. Segundo Saldanha (2019, p.11), estas medidas surgem devido à necessidade de adequar a proteção dos direitos individuais a estas novas realidades, entenda-se o avanço nas tecnologias de informação.

A nível nacional, o tema da proteção de dados começou por ser vagamente abordado na Constituição de 1976, onde se estabeleciam os direitos de conhecimento, tanto sobre a existência de registos como as suas finalidades, e também o poder de exigir a retificação e atualização dos seus dados.

Dada esta falta de harmonia entre o plano europeu e o plano nacional de cada estado-membro, em 1995, é aprovada a diretiva 95/46/CE (PE, 1995) relativa à proteção de indivíduos singulares referente ao tratamento de dados pessoais, e à livre circulação destes mesmos dados. É neste momento histórico que se nota uma maior consciencialização para a proteção de dados e uma mudança de mentalidade referente a este assunto. Como resultado desta diretiva surgiu, em Portugal, a Lei 67/98 de 26 de outubro (AR, 1998) (Lei da Proteção de dados) que transpõe para a ordem jurídica interna esta aprovação europeia.

Em 2009, com a entrada em vigor o Tratado de Lisboa (EU, 2007), a proteção de dados é consagrada como um direito fundamental. Poucos anos depois, em 2011, a Autoridade

Europeia para a Proteção de Dados (AEPD) emite um parecer onde declara a necessidade de legislação referente à proteção de dados, e onde refere sugestões de melhoria.

O último passo na história do RGPD, decorreu entre 2014 e 2016, uma vez que foi durante este período que o Parlamento Europeu, com o objetivo de fornecer aos cidadãos e residentes na União Europeia formas de controlar os seus dados pessoais, definiu e aprovou o atual RGPD. A Lei 58/2019 (AR, 2019), que entrou em vigor em 8 de agosto de 2019, assegura o seu cumprimento na ordem jurídica nacional. Este novo regulamento colocou às organizações novos obstáculos e desafios, os quais estas têm a responsabilidade de resolver.

Reiterando o que foi dito anteriormente, a junção de uma sociedade de informação com um acelerado desenvolvimento tecnológico, gera mercados altamente complexos e dinâmicos. Este fator de mudança constante, gera um sentimento de insegurança nas transações e relações digitais que decorrem diariamente (Magalhães, 2017). Adicionalmente, segundo vários autores (Moreira, 2018; Martins, 2020), o direito à proteção de dados aparece também devido ao conflito de interesses entre o cidadão e o Estado.

Com a crescente relevância desta temática, e o facto de resultar em ideias tão dissonantes, compete aos órgãos responsáveis estabelecer leis e regulamentos de modo que todos os participantes tenham conhecimento dos seus direitos e deveres. Alguns desses direitos assegurados aos titulares dos dados no RGPD são:

- Direito de Acesso;
- Direito de Retificação;
- Direito ao Apagamento de Dados (“direito de ser esquecido”);
- Direito à Limitação do Tratamento;
- Direito de Portabilidade dos Dados; e
- Direito/Dever à Informação.

Segundo o RGPD, explicado pelo Direito de Acesso, o titular tem o direito de saber se os seus dados pessoais estão a ser objeto de tratamento, qual o destino dos mesmos (caso sejam enviados para outras entidades), bem como o Direito de Aceder aos dados e

informações que a organização possua sobre o mesmo. Este Direito de Acesso deve ser gratuito, exceto no caso de requisições excessivas onde uma taxa de acesso poderá ser cobrada (Magalhães & Pereira, 2018; Regulamento (UE) 2016/679, 2016).

O regulamento menciona também que o titular dos dados tem o Direito de obter a Retificação dos seus dados caso estes estejam incorretos, incompletos ou desatualizados (UE, 2016).

O Direito ao Apagamento dos Dados, um aspeto recente na temática do RGPD, confere ao titular dos mesmos o direito de solicitar a uma organização a eliminação dos seus dados. Esta eliminação só ocorre, caso uma das seguintes situações se verifique (Magalhães & Pereira, 2018):

- Os dados recolhidos mostram-se desnecessários para as finalidades descritas;
- Os dados pessoais tenham sido tratados de forma ilícita;
- O titular opõe-se ao tratamento dos seus dados para a criação de listas de profiling;
- Caso não exista fundamento legal para o tratamento dos dados pessoais, e o titular retire o seu consentimento.

Em qualquer um destes casos, torna-se responsabilidade da organização criar mecanismos e protocolos que garantam que os dados mencionados sejam eliminados de forma permanente e segura dos seus registos e sistemas. Na eventualidade dos dados pessoais terem sido partilhados com outras entidades, é competência da organização informar os restantes responsáveis da solicitação de eliminação de dados (Magalhães & Pereira, 2018).

Juntamente com o Direito do Apagamento de Dados, mas numa medida menos drástica, o novo RGPD introduziu o direito à limitação do tratamento de dados pessoais. Este direito concede ao titular o direito de exigir a limitação de tratamento nas seguintes situações:

- Vontade do titular de contestar a exatidão dos dados pessoais;
- O titular, face a tratamento ilícito dos seus dados, se opor à eliminação dos mesmos, e optar por limitar a sua utilização;

- Caso o titular se oponha ao tratamento dos seus dados pessoais, até se apurar se os motivos legítimos da organização prevalecem sobre os do titular;
- Quando se verificar que a perante a organização os dados não são necessários, mas o titular os solicitar para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Tendo em conta o mundo altamente digital no qual vivemos, o RGPD confere ao titular o Direito de Solicitar à organização os seus dados pessoais, em domínio completo, e a sua transferência para outra entidade à sua escolha (Direito de Portabilidade de Dados). A execução deste direito apenas é possível quando se verificar que é tecnicamente possível tal transferência.

Traduzido pelo Direito/dever à informação, a nova versão do regulamento assegura também que, caso solicitado, deve ser fornecido ao titular um conjunto de informações, no formato à escolha do titular, caso a recolha dos dados tenha sido realizada na presença do titular ou caso tal não se verifique.

Também importante, o conceito de consentimento é um dos pilares do RGPD. Não só este deve ser dado de livre vontade por parte do titular dos dados, como também lhe deve ser explicada a finalidade do tratamento da informação do mesmo. Esta explicação deve ser feita de modo a não haver qualquer erro ou equívoco. A conceção ou revogação do consentimento devem ser de igual facilidade para o titular dos dados. O consentimento deverá ser livre, específico, informado e inequívoco.

Em suma, o RGPD mudou o paradigma da Proteção de Dados. Ao orientar as organizações sobre a melhor forma de assegurar a sua inviolabilidade, através da autorresponsabilização do Responsável pelo Tratamento e a necessidade da demonstração da conformidade das empresas, o RGPD foca-se em salvaguardar os dados pessoais dos titulares.

Um incentivo para as organizações implementarem as diretrizes do RGPD são as coimas, que podem ser de um montante exorbitante de acordo com a gravidade da violação de dados, podendo colocar em risco a saúde financeira da mesma.

3.5 Cibersegurança

Devido aos frequentes avanços tecnológicos, novas ameaças e perigos vão surgindo. À medida que mais e mais dados são introduzidos em serviços na internet, a segurança dos mesmos torna-se cada vez mais fraca, por outras palavras, existe uma relação de proporcionalidade inversa entre a quantidade de dados e a segurança dos mesmos.

Paralelo a este contínuo enfraquecimento de segurança têm vindo a ser criadas leis e normas num esforço de colmatar possíveis debilidades dos SI. Este objetivo é incutido a entidades como o Centro Nacional de Cibersegurança (CNCS) e a Comissão Nacional de Proteção de Dados (CNPD), assim como entidades internacionais, como a *European Union Agency for Cybersecurity* (ENISA) e a *North Atlantic Treaty Organization* (NATO). No âmbito deste estágio o foco será apenas no plano nacional.

Procedendo a Diretiva (EU) 2016/1148 (EU, 2016), do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, a Assembleia da República Portuguesa criou a Lei 46/2018 (AR, 2018), aprovada a 13 de agosto de 2018, de modo a estabelecer o regime jurídico da segurança do ciberespaço.

Complementar a esta lei, foi aprovado o Decreto-Lei 65/2021 (DR, 2021), de 30 de julho de 2021, que procede à regulamentação da lei supramencionada, e à execução das obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, permitindo assim a implementação de um quadro nacional de certificação de cibersegurança. Para tal, este Decreto-Lei estabelece os requisitos de segurança das redes e dos SI que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais.

Deste modo, e no âmbito deste estágio, é pertinente referir alguns dos artigos presentes no Decreto-Lei supramencionado, tais como: o artigo 5º, no qual se refere a necessidade de as entidades designarem um responsável de segurança que tem como tarefas gerir as medidas de segurança adotadas e, em caso de incidente, notificar as entidades devidas; o artigo 9º, que encaminha as entidades a implementar medidas para o cumprimento dos requisitos de segurança; e também o artigo 10º, que impõe a realização de análises de risco em relação a todos os ativos de modo a que se assegure o normal funcionamento dos SI.

Um aspeto de muita relevância no âmbito da segurança dos SI é a taxonomia de incidentes e de efeitos, por outras palavras a causa de um incidente e o resultado desse incidente. Nessa ótica é de importância referir o artigo 16º do Decreto-Lei 65/2021, de 30 de julho de 2021, que elenca os possíveis cenários de incidentes e efeitos (DR, 2021, pp.17-18).

3.6 Avaliação de Impacto sobre a Proteção de Dados - AIPD

A AIPD é uma das novidades trazidas pelo RGPD que consiste numa avaliação focada em detetar possíveis ameaças à proteção de dados, e, caso as detete, reduzir o seu impacto.

Uma AIPD pode ser entendida como um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento, e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais, avaliando-os e determinando as medidas necessárias para fazer face a esses riscos (Magalhães e Pereira, 2019).

Segundo Fazendeiro (2017), este tipo de avaliações, da competência do Responsável pelo Tratamento de dados, devem ser realizadas antes de serem iniciadas as operações de tratamento de dados que utilizem novas tecnologias e que possam implicar elevado risco para os direitos e liberdades dos titulares dos dados.

De acordo com o artigo 35º, número 7 do RGPD, estas avaliações devem conter descrições sistemáticas das operações de tratamento previstas, aliadas das suas finalidades e os porquês desses mesmos tratamentos. Deve também ser analisado, tendo como medida os objetivos definidos, a necessidade e a proporcionalidade das operações de tratamento, bem como avaliar os riscos para os titulares dos dados e as medidas para combater esses possíveis riscos. Estas avaliações devem ser feitas com regularidade pois têm o objetivo de a qualquer momento detetar possíveis riscos quanto à segurança dos dados dos titulares, e devem ser realizadas pelo responsável pelo tratamento dos dados.

De maneira a preencher estes requisitos, uma AIPD apresenta as seguintes etapas (RGPD, artigo 35º, nº7):

- Descrição dos dados pessoais recolhidos pelo SI;
- Descrição das operações de tratamento previstas, e as suas finalidades;
- Avaliação da necessidade e proporcionalidade das operações de tratamento;
- Avaliar os riscos para os titulares dos dados, e as suas liberdades

- Descrição das medidas previstas que mitiguem esses riscos, e/ou demonstrem conformidade com o presente regulamento;
- Elaboração de um relatório de apreciação global do SI.

3.7 Avaliação de Conformidade de Segurança de Sistemas de Informação

No contexto das tecnologias da informação e comunicação, uma Avaliação de Conformidade de Segurança é revisão dos registos e da atividade de um SI para verificar a adequação dos controlos do sistema, garantir a conformidade com a política de segurança e com os procedimentos de exploração estabelecidos, detetar eventuais intrusões e recomendar as modificações apropriadas no controlo, na política de segurança e nos procedimentos (APDSI, s.d.).

Segundo Saldanha (2019), uma Avaliação de Conformidade de Segurança necessita de cinco etapas essenciais de modo a corresponder aos requisitos do RGPD. Essas etapas são:

- Recolha dos dados gerais da organização;
- Análise do tratamento efetuado aos dados;
- Verificação de cumprimento dos princípios do regulamento;
- Existência de cometimento dos titulares dos dados; e
- Verificação dos requisitos de conservação dos dados.

Nestas avaliações é necessária a realização de relatórios, não só como requisito do RGPD, mas também como elemento de suporte numa eventual fiscalização da CNPD, e estes relatórios são de caráter confidencial e de uso exclusivo interno da organização.

As avaliações de conformidade devem ser feitas com regularidade sendo que, apesar de não ser explícito em qualquer documento um número específico de avaliações por período de tempo, o popularmente aconselhável serão duas ou três avaliações anuais. A quantidade de avaliações é impactada, por exemplo, pela dimensão da empresa, o nível de risco previsto, entre outras.

CAPÍTULO IV – DESCRIÇÃO DAS ATIVIDADES DESENVOLVIDAS E APRESENTAÇÃO DOS RESULTADOS

4.1 Síntese das atividades realizadas

De acordo com os objetivos do estágio, e as atividades planeadas, o primeiro foco deste estágio foi o estudo e compreensão das leis, normas e toda a literatura relevante para as atividades do mesmo. Com este propósito, desde a data de início do estágio, 11 de novembro, até depois de dado o início das avaliações aos SI, foram fornecidos documentos ao estagiário para que este pudesse atingir este objetivo.

Entre documentos internos e legislação em vigor, foram diversos os documentos fornecidos pelos colaboradores da DvPDGRE. Para além destes, foi realizada uma revisão de literatura abrangente, abordando conceitos como o RGPD, cibersegurança e as AIPD.

Em seguida, no que respeita aos dois principais objetivos do estágio, as avaliações dos SI dividiram-se em duas vertentes, por um lado avaliar o nível de conformidade de segurança do SI, em comparação com os requisitos do RGPD e a legislação conexa e, por outro, avaliar a implementação das diretrizes do RGPD de modo a assegurar que os dados pessoais usados dentro da organização estão devidamente protegidos. No total foram avaliados oito SI, nomeadamente: Portaria Principal do Porto de Leixões (3PL); Sistema de Controlo de Acessos Físicos; PowerBI; Cartão Único Portuário (CUP); Portal Executivo (PEX); Ferramenta de Combate a Ciberameaças; Gestão Documental (GESDOC); e *Closed Circuit* TV (CCTV).

Para ambos os tipos de avaliações foram observados e analisados os seguintes elementos: Gestão de Perfis, Gestão de *Logs*, Interconexão de Sistemas, Base de Dados, Acesso a Dados, Arquitetura Geral do Sistema, e Menus de Opções e Funcionalidades. No entanto, foram ainda observados elementos exclusivos de cada tipo de avaliação. Nas Avaliações de Conformidade de Segurança foram observados as Medidas de Segurança existentes nos SI, e nas AIPD foram observados os Dados Pessoais Recolhidos.

A Gestão de Perfis alude à funcionalidade de criar perfis de utilizadores individuais, ou de grupos de perfis, de modo a facilitar o controlo sobre que colaborador, ou tipo/grupo de colaboradores, tem acesso a determinados dados ou funcionalidades do SI em si. A

existência desta opção no SI ajuda no objetivo da proteção de informação, pois apenas utilizadores com perfis específicos têm acesso a certo tipo de informação, limitando o acesso indevido a dados.

A Gestão de *Logs* refere-se à capacidade de ter acesso a um histórico de ações realizadas no SI, onde, por norma, é possível saber quem foi o utilizador que realizou a ação, que ação decorreu, e a que momento aconteceu. A existência desta funcionalidade num SI apresenta-se como uma mais-valia em termos de segurança, e em termos de responsabilidade dos colaboradores.

Como descrito na ISO 7498 (ISO, 1994), Interconexão de Sistemas é descrita como um conjunto de um ou mais computadores, o *software* associado, periféricos, terminais, operadores, processos físicos e meios de transferência de informações que formam um todo autônomo capaz de realizar processamento de informações e/ou transferência de informações.

Específico às AIPD, uma Base de Dados representa uma coleção de dados organizada de acordo com uma estrutura concetual que descreve as características desses dados, sendo estes destinados a um ou vários domínios de aplicação (APDSI, s.d.). Bastante interligado a este conceito, por Acesso a Dados entende-se a possibilidade de ler, escrever, modificar ou apagar dados (APDSI, s.d).

Entende-se por Arquitetura Geral do SI as principais propriedades físicas, estilo, estrutura, interações e finalidade de um sistema (Hatley et al, 2000).

O elemento de Menus de Opções e Funcionalidades alude à disposição visual da informação durante a utilização do SI, e de que forma as suas funcionalidades estão organizadas e apresentadas no SI.

Específico às Avaliações de Conformidade de Segurança, a observação das Medidas de Segurança é feita com a intenção de verificar o nível de proteção que o SI possui contra acessos indevidos, combatido, por exemplo, através do uso de palavras-passe complexas, ou ataques externos, combatido, por exemplo, por *firewalls*.

Quanto aos Dados Pessoais Recolhidos, trata-se, simplesmente, da avaliação sobre que dados pessoais são solicitados aos clientes ou colaboradores, qual a finalidade com que são pedidos, e de que maneira são tratados para atingir essa finalidade.

Relativamente ao trabalho realizado, na sessão de avaliação de cada SI, participaram o estagiário, os elementos do DvDPGRE e o Responsável do SI em avaliação. Cada sessão de avaliação, iniciava-se por uma breve apresentação da finalidade do SI, feita pelo Responsável do mesmo, de modo a contextualizar todos os presentes sobre o que iria ser falado.

Em seguida, o Responsável do SI partilhava a tela do seu computador, através da plataforma Microsoft Teams©, de modo a que os restantes participantes pudessem ver a utilização do sistema. Primeiramente, era solicitado ao Responsável do SI que percorresse os menus de forma a se perceber a configuração visual do SI (Arquitetura Geral do Sistema), e que opções de navegação existem dentro do mesmo (Menus de Opções e Funcionalidades).

Durante esta apresentação, era ainda pedido ao Responsável do SI que apresentasse os tipos de perfis de utilizador existentes e como a sua gestão era realizada. Em alguns SI esta gestão é feita através da definição de grupos de perfis, noutros a gestão é feita individualmente para cada colaborador. Através da Gestão de Perfis era também avaliada a questão do Acesso a Dados, nomeadamente quais os utilizadores com acesso a dados específicos, se existiam utilizadores com acesso indevido a dados pessoais, e se seria necessário refazer níveis de permissões ou criar novos parâmetros.

No que se refere à Gestão de *Logs*, era verificado se esta funcionalidade existia no SI e se esta se encontrava ativa. Caso ambas as situações se verificassem, era avaliado com que qualidade e grau de pormenor era executada essa gestão.

Face à frequente Interconexão dos Sistemas, constatou-se que vários SI partilham Bases de Dados. Por esta razão, realizou-se a avaliação destes dois elementos em simultâneo. Aquando da verificação, se um SI entra em contacto direto com outro, era realizada uma avaliação dessa ligação (que informação é transmitida e como), assim como a Base de Dados que partilhavam. É de notar que, aquando da avaliação de cada um dos SI interligados, a Base de Dados voltava a ser avaliada, resultando numa avaliação mais meticulosa.

O penúltimo elemento a ser avaliado neste processo eram as Medidas de Segurança existentes no SI, como, por exemplo, a utilização de *passwords* complexas, o seu tempo de "vida" até o utilizador ser obrigado a mudar a mesma e, caso o SI operasse em conexão com outros, que mecanismos de segurança estão ativos na eventualidade de um ataque

malicioso através de outro SI. Por questões de segurança da organização, esta parte dos relatórios de avaliação não será apresentada neste relatório de estágio.

No final, após avaliados os elementos dos SI, era pedido ao Responsável que efetuasse um *test run* ao uso da aplicação, por outras palavras, que mostrasse com uma demonstração prática, passo por passo, como o SI funciona, explicando que Dados Pessoais necessita para realizar a sua tarefa, como são tratados e com que finalidade, de modo a ser avaliado o nível de proteção de Dados Pessoais presente, e que melhorias se podem ou devem fazer ao SI.

Realizadas estas avaliações, e preenchidos os documentos de suporte, era também perguntado ao Responsável se este tem alguma ideia de melhoria para o SI, dado o seu uso diário do mesmo.

Terminada a sessão de avaliação do SI, na organização, é mantido um diálogo constante entre a DvPDGRE e o Responsável do SI de modo a mitigar qualquer erro ou lacuna presente no relatório da sessão, podendo então oficializar o fim da avaliação ao SI em questão.

As sessões de avaliação dos SI realizaram-se entre 14 de fevereiro e 23 de maio de 2022, maioritariamente durante a manhã dos dias agendados, e sempre através da plataforma Microsoft Teams©. Em todas as sessões foi também utilizada a plataforma Tekprivacy©, para a validação e revisão do formulário AIPD SI, e o questionário de controlos gerais de SI.

A avaliação do sistema 3PL realizou-se no dia 14 de fevereiro de 2022 pelas 10 horas da manhã, sendo que participou como Responsável do SI a chefia da Divisão de Informação e Processos (DvIP).

A avaliação do sistema de Controlo de Acessos Físicos realizou-se no dia 21 de fevereiro de 2022 pelas 10 horas da manhã. Na sessão para além do Responsável do SI, a chefia da DSI, participou também a Direção de Operações Portuárias e Segurança (DOPS), uma vez que a sua atividade envolve Tratamentos de Dados deste SI.

A avaliação do sistema PowerBI realizou-se no dia 28 de fevereiro de 2022 pelas 14 horas e 30 minutos, tendo participado como Responsável pelo SI a chefia da DSI.

A avaliação do sistema CUP realizou-se no dia 17 de março de 2022 pelas 09 horas e 30 minutos da manhã. Uma vez que este SI funciona paralelamente ao SI de Controlo de

Acessos Físicos, também esta sessão foi realizada com a participação de um elemento da DOPS, assim como a chefia da DvIP, Responsável pelo SI.

A avaliação do sistema PEX realizou-se no dia 29 de março de 2022 pelas 11 horas da manhã, sendo que participou como Responsável do SI a chefia da DSI.

A avaliação do sistema de Combate a Ciberameaças realizou-se no dia 19 de abril de 2022 pelas 09 horas e 30 minutos da manhã, sendo que o Responsável pelo SI participante foi a chefia da Divisão de Sistemas e Tecnologia (DvST).

A avaliação do sistema GESDOC realizou-se no dia 28 de abril de 2022 pelas 08 horas e 30 minutos da manhãs, com a chefia da DS, o Responsável do SI.

A avaliação do sistema CCTV realizou-se no dia 23 de maio de 2022 pelas 09 horas e 30 minutos da manhã, sendo que o Responsável pelo SI é a chefia da DOPS.

4.2 Avaliação dos Sistemas de Informação

Nas secções seguintes serão apresentados os principais aspetos que emergem dos diferentes relatórios de avaliação, gerados durante o estágio, dos oito SI avaliados (3PL; Sistema de Controlo de Acessos Físicos; PowerBI; CUP; PEX; Ferramenta de Combate a Ciberameaças; GESDOC; CCTV). Serão abordados os seguintes aspetos: Breve Descrição do SI, Elementos Observados; Observações e Não Conformidades; Proposta de Implementação de Melhorias e Apreciação Global. É importante referir que relativamente aos Elementos Observados, reiterando o que foi dito anteriormente, durante as sessões foram avaliadas as Medidas de Segurança, Subcontratantes e Base de Dados de cada SI, contudo por questões de confidencialidade estes aspetos não serão apresentados neste relatório de estágio.

4.2.1 Sistema 3PL

Esta secção apresenta a informação mais relevante resultante da avaliação do sistema 3PL. A avaliação centrou-se no tratamento dos dados pessoais da 3PL e na camada aplicacional. Os requisitos relativos a base de dados e redes foram remetidos para análise posterior com a DvST.

Breve Descrição do SI

O Sistema 3PL é o SI utilizado para gerir as entradas e saídas do Porto de Leixões, sendo o seu processo o seguinte.

Aquando da chegada do condutor do veículo de carga ao portão do Porto de Leixões, este tem de se identificar através da apresentação do seu cartão de motorista. Este cartão de motorista dá acesso, no sistema 3PL, aos seguintes dados pessoais: nome, empresa, número de identificação (Cartão de Cidadão ou carta de condução), número RFID (*Radio Frequency Identification)* do cartão do motorista. É também possível, através do sistema de *log*, perceber os movimentos do camião (entradas e saídas do porto de Leixões), e, por conseguinte, o rastreamento dos motoristas nas entradas e saídas.

Caso seja uma primeira vez do motorista no porto de Leixões, ou se o veículo tenha passagens esporádicas no porto de Leixões, poderá ser gerado um PIN temporário, aleatório, que permitirá que o motorista possa entrar credenciado no porto.

O camião, caso traga um contentor, terá de passar por uma báscula, para pesagem e obtenção de um certificado VGM (*Verified Gross Mass)*. Nesse sistema é apresentado o cartão do motorista.

No processo de atendimento do camião, este passa por um equipamento designado por canópia, onde são registadas várias imagens do veículo com o propósito de reconhecer a sua matrícula. Nesse processo é também registada a imagem do motorista (de perfil). Caso traga um contentor, o camião terá de passar por uma báscula, para pesagem e obtenção de um certificado VGM. Nesse sistema é apresentado o cartão do motorista.

Elementos Observados

Durante a avaliação do sistema foram observados os seguintes elementos:

- Gestão de Perfis;
- Gestão de *Logs*;
- Interconexão de sistemas;
- Base de Dados;
- Acesso a Dados;
- Medidas de Segurança.

Durante a avaliação da Gestão de Perfis verificou-se que cada utilizador pertence a um grupo, facilitando a gestão de acessos de cada colaborador. Referente à Gestão de *Logs* não se encontrou nenhuma não conformidade.

O sistema 3PL relaciona-se com vários outros sistemas e através de diversos mecanismos de interconexão. Os sistemas com que se relaciona a 3PL são:

- CUP – para validação do cartão de motorista/credencial ativa, sistema que também foi avaliado;
- Sistema de Controlo de Acessos Físicos, sistema que também foi avaliado;
- APP Motorista – para validações relacionadas com pesagens;
- JUP (Janela Única Portuária) – Processo Veículo;

Também foram avaliadas a Base de Dados, Acesso a Dados e Medidas de Segurança deste SI, no entanto não serão apresentadas por razões de confidencialidade.

Os elementos de Arquitetura Geral do Sistema, Menus de Opções e Funcionalidades de Dados Pessoais Recolhidos não foram avaliados neste SI por motivos que dizem respeito à direção do DvPDGRE.

Observações e Não Conformidades Encontradas

No decorrer da avaliação foram registadas uma não conformidade e uma observação. A não conformidade refere-se ao processo de rastreamento de atividade dos utilizadores, onde algumas entradas e saídas de sessão não ficavam registadas no sistema, assim como alguns acessos de leitura sobre dados pessoais. A observação registada deveu-se ao facto de perante mudanças na organização ser dispensável um utilizador específico ainda ter acesso de *admin* ao sistema.

A tabela 1 apresenta a informação sobre as Observações encontradas na avaliação do sistema 3PL.

Tabela 1 – Observações e Não Conformidades do sistema 3PL

Tipo*	Descrição	Utilizadores	Medidas a aplicar
NC	*Log* incompleto		Melhorar o processo de rastreamento de atividade dos utilizadores, permitindo o registo das atividades de acesso a dados pessoais (*read*), bem como as entradas e saídas de sessão.
OBS	Acesso *Admin*	/*confidencial*/	Avaliar a necessidade do acesso deste utilizador a contas SYS e SYSTEM.

*NC – Não Conformidade | OBS – Observação

Propostas de Implementação de Melhorias

Terminada a avaliação foram apresentas propostas de melhoria que, estando este SI em fase de descontinuação, serão implementadas na próxima versão do mesmo. As propostas de melhoria são as seguintes:

- Avaliar a oportunidade e custo/benefício da melhoria do processo de rastreamento da atividade dos utilizadores, permitindo o registo das atividades de acesso a dados pessoais (*read*/leitura), bem como as entradas e saídas de sessão.
- Formalizar um documento de arquitetura de sistemas 3PL.
- Criar um Aviso de Privacidade para este sistema.
- Melhorar o processo de ofuscamento da cara do motorista no processo OCR do contentor, na canópia.
- Replicar propostas de melhoria na JUL (Janela Única Logística).
- Realização de testes periódicos de recuperação de dados, a partir dos backups.

- Limpeza regular do ficheiro de *log*. Sugere-se de 2 em 2 anos.
- Avaliar a necessidade de criação de Acordos de Proteção de Dados, com potenciais responsáveis conjuntos: Alfândega e Operadores portuários.
- Avaliações de conformidade das bases de dados e restantes aplicações com que a 3PL se relaciona.

De todas as propostas de implementação de melhorias, sobre o âmbito da proteção de dados pessoais, será importante realçar as seguintes: a melhoria do processo de rastreamento da atividade dos utilizadores; a criação de um aviso de privacidade para o sistema; melhorar o processo de ofuscamento do motorista; avaliar a necessidade de criação de Acordos de Proteção de Dados, com potenciais responsáveis conjuntos; e a realização de avaliações de conformidade aos sistemas interligados à 3PL.

Apreciação Global

Aquando da sua criação, há quase década e meia, o tema da proteção de dados pessoais cingia-se apenas ao nível de segurança da informação, explicando em parte o porquê deste sistema não ter apresentado grandes evidências de cuidados referentes à proteção de dados pessoais.

Dito isto, a aplicação encontra-se em fase de descontinuação e será substituída por um novo sistema, sendo que todas as melhorias encontradas nesta avaliação serão idealizadas para integração no novo projeto.

4.2.2 Sistema de Controlo de Acessos Físicos

Esta secção apresenta a avaliação do sistema de Controlo de Acessos Físicos, no âmbito do controlo de acessos de pessoas a áreas sob a jurisdição da APDL. A sessão centrou-se nos tratamentos de dados pessoais relativos ao Controlo de Acessos de pessoas. Os requisitos relativos a base de dados e redes foram remetidos para uma análise posterior com a DvST. Será de notar que as funcionalidades deste SI estão em processo de migração para um novo SI.

Breve Descrição do SI

Este SI é a plataforma responsável pela gestão dos acessos físicos, sendo que esses acessos são controlados por cartões ou credenciais. Os utilizadores que querem entrar nas instalações no Porto de Leixões podem fazê-lo por uma de duas formas: ou apresentam um cartão da APDL ou possuem uma credencial válida de visitante no SI.

Quem entra na instalação deve apresentar um documento de identificação para que o segurança privado possa validar se pode entrar mediante a apresentação do cartão ou da visualização de uma credencial válida.

O pedido de criação de um cartão chega à DOPS - via email ou via aplicação CUP. A DOPS, após apreciação do pedido, emite o cartão e o mesmo só é entregue ao próprio titular contra apresentação do cartão de cidadão. O titular assina um documento em como recebeu o cartão, termos de aceitação e aviso de privacidade.

No processo de aceitação de um pedido de visita sem cartão, mas com emissão de uma credencial no sistema, o requerente é avisado com uma notificação, se o pedido foi efetuado via CUP. Caso contrário o requerente será avisado, por uma via informal, pela pessoa que criou o pedido no sistema.

Elementos Observados

Durante a avaliação a este sistema foram observados os seguintes elementos:

- Gestão de Perfis;
- Gestão de *Logs*;
- Interconexão de Sistemas;
- Base de Dados;
- Acesso a Dados;
- Arquitetura Geral;
- Menus de opções e funcionalidades;
- Medidas de Segurança.

Durante a avaliação da Gestão de Perfis verificou-se que existia um perfil de administrador desnecessário, e vários perfis com acessos desnecessário. Referente à Gestão de *Logs* não se encontrou nenhuma não conformidade.

Quanto à Interconexão de Sistemas, este SI relaciona-se com outros SI tais como o CUP e a 3PL.

Existe também uma plataforma de *streaming* de dados, que, entre outros, é usada pela JUL com o objetivo de sincronização de tabelas entre bases de dados distintas. Esta plataforma é usada para fazer as leituras ou inserções necessárias aos processos de sincronização que venham a existir.

É de notar que existem organizações externas que possuem determinados níveis de acesso ao sistema, de modo a poderem realizar as suas atividades, tais como, aprovação de pedidos de visita ou introdução de elementos para finalidades de segurança.

Destes elementos é de notar que a Arquitetura Geral se encontrava desatualizada, as funcionalidades de Envio de emails e a Criação de cartões encontram-se desativadas, e a funcionalidade de Biometria não está a ser usada.

Apesar de alguns elementos se encontrarem desativados, ou no caso da criação de cartões até migrados para outro sistema, uma vez que o SI vai ser descontinuado, esta avaliação teve mais focada na recolha de informação sobre este tipo de sistema do que na correção do mesmo, tendo sido por essa razão avaliados elementos desativados.

Novamente, as questões de Base de Dados, Acesso a Dados e Medidas de Segurança não serão apresentadas por razões de confidencialidade. O elemento de Dados Pessoais Recolhidos não foi avaliado pois esta atividade foi migrada para outro SI.

Devido á particularidade deste SI, foram avaliados também os seguintes elementos:

- Dados pessoais recolhidos durante o pedido de acesso ao porto;
- Troca de emails dentro do sistema;
- Consultar pedidos de entrada no porto;
- Criação de cartões;
- Biometria.

Os elementos Troca de emails dentro do SI, Consulta de pedidos de entrada no porto, e a Criação de cartões foram avaliados pois, durante estas ações no SI podem ser visíveis Dados Pessoais, alusivo aos Dados Pessoais Recolhidos. Também foi avaliada a funcionalidade de Biometria incluída no SI pois para esta ser utilizada necessita de Dados Pessoais dos colaboradores.

A tabela 2 elenca todos os dados recolhidos durante o processo de criação do cartão de acessos, assim como as finalidades para as quais esses dados são recolhidos. Perante o âmbito do estágio e o conceito da proteção de dados pessoais são de realçar os seguintes dados: Nome, Carta de condução, Fotografia do titular do cartão, Número mecanográfico, NIF, Endereço email, Número Telemóvel, Número Telefone, e Morada.

Tabela 2 - Dados Pessoais Recolhidos pelo sistema Controlo de Acessos Físicos

Elemento	Finalidade
Nome	Identificação da pessoa que vai entrar
Carta de condução	Exigido pelo SEF e interconexão com a 3PL
Empresa	Identificação da pessoa
Número do cartão de visitante	Emissão de cartão unívoco
Nacionalidade	Exigido pelo SEF
Matrícula da viatura	Identificação da pessoa que vai entrar
Número do cartão de identificação	Identificação da pessoa que vai entrar
Validade do cartão de identificação	Identificação da pessoa que vai entrar
Fotografia do titular do cartão	Emissão do cartão
Número mecanográfico	Para emissão cartão colaborador
NIF – Número de Identificação Fiscal	Faturação
Cargo	Para colocação no cartão de visita
Endereço de email	Contacto
Telemóvel	Contacto
Nome abreviado	Identificação da pessoa que vai entrar
Sexo	Identificação da pessoa que vai entrar
Data de nascimento	Exigido pelo SEF
Título Académico	Para colocação no cartão de visita
Estado civil	Identificação da pessoa que vai entrar
Morada	Faturação
Telefone	Contacto
Telefone profissional	Contacto
Extensão do telefone	Contacto
Data de emissão do Cartão de Cidadão	Identificação da pessoa que vai entrar
Entidade emissora	Identificação da pessoa que vai entrar

Elemento	Finalidade
Local de emissão	Identificação da pessoa que vai entrar

Observações e Não Conformidades Encontradas

Durante a avaliação, e como descrito na tabela, foram registadas três não conformidades no sistema, assim como uma observação. A observação registada refere-se ao facto de a funcionalidade de pesquisa no sistema não se encontrar operacional, sendo assim recomendado uma atualização do sistema.

Em termos de não conformidades é descrito que existia um perfil específico de um colaborador com acessos de administrador apesar de este já não possuir atividades neste sistema, esse perfil foi removido. Numa situação semelhante foram encontrados mais perfis com acessos não necessários face às suas atividades, os quais ficaram ao encargo do Responsável do sistema rever. Para finalizar, de acordo com o RGPD, aquando do pedido da criação do cartão, ao solicitar dados pessoais deve ser enviado um documento de sensibilização ao requerente, processo que não se verificava totalmente.

A tabela 3 apresenta a informação sobre as Observações e Não Conformidades encontradas na avaliação do sistema de Controlo de Acessos Físicos.

Tabela 3 - Observações e Não Conformidades do Sistema de Controlo de Acessos Físicos

Tipo*	Descrição	Utilizadores	Medidas a aplicar
NC	Perfil excessivo de administrador	/*confidencial*/	Retirado o perfil
NC	Utilizadores com acesso não necessário		Rever perfis e/ou eliminar utilizadores
NC	Email a solicitar a criação de cartões com cópias de cartão de cidadão anexadas		Sensibilizar requerentes
OBS	As consultas no sistema não funcionam		Atualização do software

*NC – Não Conformidade | OBS – Observação

Propostas de Implementação de Melhoria

Realizada a avaliação ao sistema seguem-se as seguintes propostas de implementação de melhorias:

- Atualização de desenho da arquitetura global desta aplicação e ligação a restantes sistemas de informação.
- Melhoria global do acesso a informação de gestão. Por exemplo: ter lista de

utilizadores com o respetivo perfil associado; saber, perfil a perfil, quais os utilizadores e quais as opções de menu a que acedem.

- Realizar ações de sensibilização dos requerentes para não enviarem cópias de cartão de cidadão em anexo a emails.
- Implementar *logs* de acordo com a RCM 41/2018, e avaliar custo/benefício desta implementação, uma vez que o sistema está a ser descontinuado, relembrando que o rastreio das atividades dos utilizadores é um requisito obrigatório.
- Elaboração de termos de adesão e direito de informação, dando deles conhecimento quer aos requerentes e titulares.
- Eliminar os utilizadores que não necessitam de ter acesso ao portal.
- Formalizar os gestores de perfis do portal e os procedimentos para a criação de perfis e utilizadores.
- Realização de testes periódicos de recuperação de dados, a partir dos backups.
- Avaliar a necessidade de criação de Acordos de Proteção de Dados, com potenciais responsáveis conjuntos (Operadores portuários).

Apreciação Global

O sistema já existe desde o ano de 2010, não tendo na sua génese a pretensão de cumprir com o preceituado na legislação de Proteção de Dados.

Tornam-se evidentes as suas falhas ao nível de conformidade para com o RGPD, designadamente nas vertentes: rastreamento das atividades dos utilizadores, na forma intrincada de gerir os perfis dos utilizadores, bem como na falta de ferramentas de *reporting*/visualização que permitam uma resposta célere a eventuais pedidos de exercício de direitos dos titulares ou na averiguação de um eventual *databreach*.

O direito de informação dos titulares não foi ainda contemplado neste sistema, sendo apenas assegurado no processo de entrega de cartões.

O princípio da exatidão não parece estar a ser conseguido, pois detetaram-se falhas na sincronização de informação entre o sistema CUP e o sistema avaliado (dados pessoais

que não foram sincronizados), bem como muitos problemas nas consultas a dados pessoais e bugs.

Uma vez que nos parece que este sistema não irá evoluir ou ser atualizado, e estando em curso atividades de migração para um novo sistema, parece-nos que essa transição dever-se-á efetuar o mais breve possível, sugerindo a criação de um *roadmap* e planeamento efetivo dessas tarefas.

Haverá que contemplar nesta mudança as seguintes cautelas:

- Histórico de dados pessoais: o que vai acontecer;
- Desativação do sistema e acessos ao mesmo;
- Eliminação dos dados: prazo de preservação máximo.

4.2.3 Sistema PowerBI

Este secção representa a avaliação da aplicação Power BI, da empresa Microsoft. O foco desta avaliação centrou-se no uso da plataforma, em particular na implementação, pela DSI, de dashboards e indicadores. Foram também abordados alguns requisitos técnicos relacionados gestão de perfis, mecanismos de *logs* e segurança da plataforma.

Breve Descrição do SI

O objetivo do Power BI é fornecer visualizações interativas e recursos de *business intelligence* com uma *interface* simples para que os usuários finais criem os seus próprios relatórios e dashboards.

Elementos Observados

No decorrer da avaliação a este sistema foram observados os seguintes elementos:

- Gestão de Perfis;
- Gestão de *Logs*;
- Interconexão de sistemas;
- Base de Dados;
- Acesso a Dados;
- Medidas de Segurança;
- Dados pessoais recolhidos.

Relativamente à Gestão de Perfis e Acesso a Dados, a plataforma PowerBI dispõe de um sistema de licenças onde está atribuído uma licença de gestor da plataforma a um colaborador específico, e, para cada *workspace* necessário à atividade da organização, podem ser atribuídos quantos perfis de *admin* quanto o necessário para a organização. Qualquer outro utilizador apenas terá acesso aos *workspaces* necessário para as suas atividades, sendo que todos os utilizadores são nomeados de modo a poder ser feito um rastreamento.

No que diz respeito à Gestão de *Logs*, *a* funcionalidade não se encontrava ativada, apresentando-se como uma não conformidade.

Este sistema apresenta bastantes interconexões, especialmente na vertente de Base de Dados, no entanto por questões de segurança e confidencialidade não se podem mencionar.

Quanto aos Dados Pessoais Recolhidos existem alguns utilizados neste sistema. Incentivado ainda mais devido à pandemia do Covid-19, foram criadas listagens extensas com a informação dos pilotos e tripulações que interajam com a área portuária supervisionada pela APDL. Numa abordagem mais empresarial também são processados nomes e emails de empresas unipessoais. E por fim, também são processados nomes e números de motoristas, assim como siglas de colaboradores internos de outras organizações.

As Medidas de Segurança também foram avaliadas, mas não serão apresentadas por razões de confidencialidade. Os elementos de Arquitetura Geral do Sistema e Menus de Opções e Funcionalidades não foram avaliados neste SI por motivos que dizem respeito à direção do DvPDGRE.

Devido á particularidade deste SI, também foram avaliados os Acessos de externos ao SI, sendo que estes não se verificam. Apenas colaboradores da APDL possuem acesso a este SI.

Observações e Não Conformidades Encontradas

Durante esta avaliação apenas uma não conformidade foi encontrada, referente à Gestão de *Logs*, que surgiu devido à falta de conhecimento técnico da parte do Responsável pelo SI. Uma vez que se trata de uma aplicação gerida completamente por outra organização, nomeadamente a Microsoft, qualquer impossibilidade de conformidade estará ao cuidado da mesma.

Propostas de Implementação de Melhorias

De acordo com a não conformidade e as observações registadas, seguem então as propostas de implementação de melhorias para este SI:

- Segregar dados pessoais dos dados gerais;
- Identificar as empresas unipessoais nas listagens, pois neste momento não existe diferença entre um perfil pessoal ou de uma empresa;
- Elaborar e aprovar Política de extração e tratamentos de dados – procedimentos para solicitar, arquivar e utilizar dados.
- Reforçar sempre que possível os contratos com os subcontratantes: Microsoft, entre outros.
- Ativar a funcionalidade dos *logs* de modo a poder ser feito um controlo mais efetivo das ações realizadas no sistema;
- Tal como nos outros sistemas, fazer a "revisão e limpeza" das permissões e acessos, e fazer isto o mais regularmente possível para facilitar o processo;
- Avaliar a opção para gerar relatórios de "Uso e *Performance*", para cada *workspace*, relacionados com os relatórios e documentos utilizados dentro do mesmo, o que se calhar seria um bom mecanismo para uma melhor movimentação e acompanhamento da informação e agilizar processos;
- Relacionado com a *data protection*, o PowerBi tem uma opção de *sensitivity labels* que permite atribuir *labels* de modo a definir e proteger conteúdos, mesmo fora do PowerBI. Avaliar a utilização destes *labels* (que pode ser gerida pelos *admins* e podem ser dadas exceções aos utilizadores).

Apreciação Global

O sistema PowerBI, fortemente dependente da implementação de controlos da Microsoft, pareceu, para já, estar a ser gerido de acordo com as melhores práticas relativas a gestão de acessos e proteção de dados pessoais.

No entanto, dado que é um sistema *user-fiendly*, terá uma adesão de cada vez mais utilizadores internos. Isto poderá provocar uma explosão de tratamentos de dados pessoais, que carecerão de regras formais, quanto ao uso dos *workspaces* e disponibilização da informação.

É um SI crítico para produção e informação para gestão, e como tal deverá ser regulado, inclusive com perfis de acesso bem definidos e regras para a disponibilização e distribuição da informação.

4.2.4 Sistema CUP – Cartão Único Portuário

Esta secção representa a avaliação do sistema CUP, em particular a gestão dos perfis de acesso a dados pessoais, e *logs*. A avaliação centrou-se nos tratamentos de dados pessoais do CUP e na camada aplicacional. Os requisitos relativos a base de dados e redes foram remetidos para análise posterior com a DvST. A aplicação CUP está em processo de descontinuação até à entrada em produção de uma nova versão deste SI.

Breve Descrição do SI

Tal como descrito durante a avaliação do Sistema de Controlo de Acessos Físicos, este SI, o CUP, serve de plataforma para a criação dos cartões e credenciais que permitem o acesso das áreas reguladas pela APDL.

Os pedidos de acesso requerem a escolha de qual porto se deseja aceder, a que instalação em específico, e o tipo/razão do acesso. Os pedidos de acesso à zona portuária podem ser pontuais ou por vários dias. É durante a criação destes pedidos de acesso que são recolhidos os dados pessoais mencionados no Sistema de Controlo de Acessos Físicos.

Uma vez que o sistema vai ser descontínuado, e não irá haver transições literais de informação, a avaliação a este sistema decorreu com uma perspetiva diferente, onde o foco foi analisar o sistema antigo com o objetivo de gerar ideias e metodologias para ajudar na criação do novo sistema, em vez de resolver não conformidades existentes.

Elementos Observados

Durante a avaliação deste SI foram observados os seguintes elementos:

- Gestão de Perfis;
- Gestão de *Logs*;
- Interconexão de sistemas;
- Base de Dados;
- Medidas de Segurança;
- Dados Pessoais Recolhidos;

Referente à Gestão de Perfis foi encontrada uma não conformidade, e alguns erros de baixo impacto. Quanto à Gestão de *Logs* não foram encontradas quaisquer não conformidades.

Tal como mencionado no Sistema de Controlo de Acessos Físicos, aquando da criação do cartão portuário são Recolhidos Dados Pessoais, e esses dados podem ser acedidos no também no CUP.

Durante a avaliação deste SI também foram observados os elementos de Base de Dados, Medidas de Segurança, sendo que por questões de confidencialidade, estes elementos não serão apresentados.

Os elementos de Acessos a Dados, Arquitetura Geral do Sistema, e Menus de Opções e Funcionalidades não foram avaliados neste SI por motivos que dizem respeito à direção do DvPDGRE.

Devido á utilização deste SI por outras entidades que não a APDL, foram avaliados também os seguintes elementos:

- Acessos Externos;
- Processo CUP;
- Autorização do pedido de acesso;
- Processo de recuperação da password.

Uma vez que várias organizações fazem parte do ecosistema do Porto de Leixões é expectável que também necessitem de acesso à plataforma responsável pelos acessos a

essa área. Estas organizações possuem Perfis de Acesso individuais de modo a haver um rastreamento de segurança. Os pedidos são feitos pelas empresas no CUP (portal externo) e enviados para aprovação à APDL e aos restantes concessionários de modo a poderem ter acessos às instalações.

O Processo de Recuperação de Passwords é feito através de pedido à chefia do SI.

Observações e Não Conformidades Encontradas

Durante a avaliação do sistema foram registadas seis não conformidades e quatro observações. Em termos de observações verificou-se que existe muita depêndencia do fornecedor quando é necessário realizar atividades básicas de gestão, esta dependência atrasa processos e causa falhas de segurança quanto à proteção de dados. As restantes três observações enquandram-se no âmbito da Gestão de Perfis onde, a criação de perfis de utilizadores apresenta erros, deve ser avaliada a necessidade de existirem perfis não nominais (empresas), e devem ser formalizados os tipos de acessos dos "super-users" que, imitando o acesso de administradores, devem ser devidamente registados e supervisionados.

As não conformidades estas podem ser divididas em quatro aspetos. Primeiramente, durante o envio de emails, dois erros graves foram observados sendo que estes permitiam acesso excessivo a Dados Pessoais, e poderiam permitir acessos antes de haver uma credenciação efetiva. De seguida, em termos de acessos, verificou-se que existia um perfil desconhecido com acessos excessivos, e que devido à necessidade de elementos da segurança terem um cartão de acesso, o processo implementado aquando do despedimento ou mudança desses elementos deveria ser melhorado, pois utilizadores que já não necessitem de acesso não o devem ter.

Para finalizar, devido à Resolução do Conselho de Ministros n.º 41/2018, que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais, é obrigatório o uso de passwords complexas. E por último, existia informação inconsistente entre vários écrans/menus.

A tabela 4 apresenta a informação sobre as Observações e Não Conformidades encontradas na avaliação do sistema CUP.

Tabela 4 - Observações e Não Conformidades do sistema CUP

Tipo*	Descrição	Utilizadores	Medidas a aplicar
NC	Passwords não são complexas.		Implementação da RCM 41/2018.
NC	Perfis não nominais: /*confidencial*/		GRAVE. Como os acessos poderão ser do exterior, quando um elemento sai da empresa, continua a aceder aos dados
NC	/*confidencial*/		GRAVE. Apenas permitir o acesso a dados pessoais após credenciação efetiva.
NC	Emails enviados permitem acesso excessivo a dados pessoais		GRAVE. Implementar o princípio "Need to know".
NC	Não se sabe quem tem acesso à função /*confidencial*/		GRAVE. Solicitar informação ao fornecedor.
NC	Informação inconsistente entre vários écrans		Avaliar custo/beneficio destas correções.
OBS	Muita dependência do fornecedor para atividades básicas de gestão		Acordo de proteção de dados; acordos de níveis de serviço e qualidade do produto.
OBS	Perfis não nominais: empresas		Avaliar a necessidade de dar acessos individuais, tal como na JUP.
OBS	Acessos a tudo /*confidencial*/		Formalizar este tipo de acessos de "super-users".
OBS	A criação de utilizadores apresenta erros quando se tenta criar um utilizador		Corrigir *bugs*.

*NC – Não Conformidade | OBS – Observação

Propostas de Implementação de Melhorias

Não fazendo sentido implementar melhorias num sistema que irá ser descontinuado em breve, seguem propostas de melhoria a serem acauteladas no futuro sistema:

- Implementar o conceito "Need to know", com particular relevância no acesso a certos dados pessoais: NIF, CC, data de nascimento, por exemplo.
- Sempre que um requerente registar um pedido de acesso, o sistema deveria enviar um email aos titulares de dados do pedido (assegurar o direito de informação).
- Avaliar a implementação de cada um dos direitos dos titulares, em particular os direitos ao apagamento e retificação.
- Atender à problemática dos emails não nominais (por exemplo da segurança

privada), em particular no desligamento de um elemento da segurança, pois o acesso via portal continuará a ficar disponível.

- Atender às falhas de segurança quando são enviados links via email, que dão acesso a dados pessoais sem a devida credenciação.
- Assim que o novo sistema entre em produção, deve-se proceder à atualização dos registos de tratamentos de dados pessoais na plataforma de suporte às avaliações de conformidade e de impacto sobre a proteção de dados.
- Eficaz e efetiva gestão de perfis e gestão de *logs*.

Apreciação Global

Sendo este um sistema em fase de descontinuação, não é razoável que as melhorias apresentadas anteriormente sejam realizadas neste sistema, mas sim no novo. Deve o novo sistema atender às melhorias atrás elencadas, resolver erros já conhecidos e encaminhados aos departamentos devidos, bem como proporcionar à organização uma ferramenta ágil e eficaz na gestão da segurança dos acessos portuários.

4.2.5 Sistema PEX – Portal Executivo

Esta secção retratra a avaliação do sistema PEX. Procurou-se nesta avaliação apreciar em particular: a gestão dos perfis, a gestão de *logs* e a interconexão com outros sistemas.

Breve Descrição do SI

Esta aplicação congrega todas as propostas de assuntos que têm de ser aprovadas pelo Conselho de Administração (CA), em sede de reunião do conselho. Algumas das propostas poderão ficar na alçada de aprovação de um único Administrador.

As propostas em PEX são criadas pelos proponentes, tipicamente a primeira linha de dirigentes, e são encaminhadas para aprovação pelo Administrador do respetivo Pelouro. As propostas são selecionadas para uma reunião do CA, e essa reunião culmina com a aprovação ou rejeição das propostas. Nessa sequência são criadas deliberações do CA, que são enviadas por email aos dirigentes, para conhecimento.

Elementos Observados

Durante a avaliação do sistema, foram observados os seguintes elementos:

- Gestão de Perfis;
- Gestão de *Logs*;
- Interconexão de Sistemas;
- Medidas de Segurança.

Este sistema apresenta um total de cinco tipos de perfis, sendo eles os seguintes: Conselho de Administração, Vogais, Secretários, Grupo para os assuntos confidenciais, e Proponentes.

O perfil "Conselho de Administração" está reservado para os três elementos do CA da organização, nomeadamente o presidente e dois vogais, no entanto os vogais também usufruem de um perfil próprio. As/Os secretários de cada membro do CA também têm o seu perfil de modo a facilitar as suas tarefas dentro do SI.

Para finalizar, existem dois perfis situacionais, um deles é atribuido aos colaboradores para quem é pertinente terem acesso a assuntos confidenciais, e o outro é o perfil dado aos proponentes dos assuntos introduzidos no sistema.

Relativamente à Interconexão de Sistemas, este SI relaciona-se com o sistema GESDOC, bidireccionalmente, através do qual envia emails no final de cada sessão de conselho. Para este SI também foram avaliadas as Medidas de Segurança, no entanto, por questões de confidencialidade, não serão apresentadas.

Elementos como Base de Dados, Acesso a Dados e Dados Pessoais Recolhidos não foram avaliados uma vez que o SI não apresenta estas características. Por motivos que dizem respeito à direção do DvPDGRE, os elementos de Arquitetura Geral do Sistema, e Menus de Opções e Funcionalidades não foram avaliados.

Observações e Não Conformidades Encontradas

Durante a avaliação do sistema foram registadas uma não conformidade e quatro observações. Como não conformidade foi verificado que a funcionalidade "campo confidencial", que tem como objetivo ocultar informações de utilizadores que não a necessitem, não estava disponível, o que causou vários fugas de informação.

Referente a observações, ficou registado que o documento de suporte à avaliação (AIPD SI) se encontrava incompleto, pelo que deveria ser revisto e completado. A funcionalidade de *logs* não estava a atuar como o esperado, assim como a função de atualização do sistema, sendo que para ambos os casos deve ser contactado o fornecedor. Tal como em outros sistemas, deve ser feito um teste contra acessos maliciosos na ligação entre o sistema PEX e o sistema GESDOC.

A tabela 5 apresenta a informação sobre as Observações e Não Conformidades encontradas na avaliação do sistema PEX.

Tabela 5 - Observações e Não Conformidades do sistema PEX

Tipo*	Descrição	Utilizadores	Medidas a aplicar
NC	Campo Confidencial: não estava a funcionar		Implementar a funcionalidade. Tem sido o motivo de vários *databreaches* de dados pessoais
OBS	O *webservice* de ligação ao GESDOC deve ser testado contra acessos maliciosos		Testar o *webservice*.
OBS	Desenvolvimentos *hardcoded* em *sharepoint* dificulta a atualização do software		Avaliar com o fornecedor o custo/benefício de atualização do software.
OBS	Não foi possível verificar *logs* do sistema		Avaliar com *fornecedor*
OBS	AIPD SI incompleta		Completar AIPD SI na plataforma Tekprivacy

*NC – Não Conformidade | OBS – Observação

Propostas de Implementação de Melhorias

Realizada a avaliação ao sistema seguem-se as seguintes propostas de implementação de melhorias:

- Avaliar a possibilidade da delegação de ações entre propotentes, na eventual falha de um deles.
- Classificação da informação confidencial, pois a mesma ainda não estava a funcionar.
- Evitar a inclusão de linhas de *software hardcoded*.
- Na proposta colocar no despacho/circulação as interações posteriores decorrentes da votação.
- Colocação de um Aviso de Privacidade em cada email enviado.

Apreciação Global

Este sistema, que já existe desde o ano de 2010, onde em certas atividades não era notada a necessidade de proteção dos dados, e a proteção de dados não era um tema em cima da mesa, apesar de ter como prevista a funcionalidade de marcação de propostas como "confidenciais", entretanto ficou inativa. Posto isto, esta aplicação encontra-se também em fase de descontinuação, para "renascer" numa nova aplicação.

Apesar destas condicionantes, o sistema possui mecanismos de restrição de acessos indevidos dos utilizadores (perfis de utilizadores), possui mecanismos de rastreamento das atividades dos utilizadores (*logs*), mas apenas nas propostas. Também incorpora medidas de segurança lógicas importantes: rede interna restrita, *backups* e sistemas ativos de avaliação de ataques cibernéticos.

4.2.6 Sistema Ferramenta de Combate a Ciberameaças

Esta secção apresenta a avaliação da Ferramenta de Combate a Ciberameaças, que incidiu em particular na Gestão dos Perfis, e na Gestão de *Logs*.

Breve Descrição do SI

Este SI, cujo nome foi adaptado por questões de confidencialidade, tem como objetivo a monitorização da rede interna da APDL, e para tal necessita de recolher Dados Pessoais.

Elementos Observados

Durante a avaliação deste SI foram observados os seguintes elementos:

- Gestão de Perfis;
- Gestão de *Logs;*
- Interconexão de sistemas;
- Base de Dados;
- Dados Pessoais Recolhidos;
- Medidas de Segurança.

A plataforma permite a implementação de Perfis de utilizadores, mas a DSI optou por não utilizar esta funcionalidade, tendo apenas 3 utilizadores nomeados. A etiqueta "admin", que dá acesso a informação dos utilizadores, é utilizado por um colaborador específico. Existe também uma função na aplicação que permite a desativação de utilizadores.

Referente aos *logs*, apenas existe rastreamento de atividades do sistema em si, e não das atividades que este vai captando durante o seu processo, sendo que estes *logs* não estão encriptados e são limpos após 90 dias. O sistema também permite a exportação dos *logs* para um ficheiro em formato *csv*.

Existe ligação a fontes externas grátis, chamados *data lakes*, vulgarmente traduzido para "lagos de informação", onde o sistema poderá ir buscar informação para gestão de incidentes, usufruindo assim de acontecimentos passados, mesmo que em outras organizações.

Os Dados Pessoais Recolhidos por esta plataforma são os seguintes: Informação do Utilizador, IP de rede, MacAdress, e Serviços onde o utilizador se ligou. É de notar que não são transferidos dados pessoais.

Durante a avaliação deste SI também foram obervados os elementos de Medidas de Segurança e Base de Dados, no entanto, por questões de confidencialidade, não serão apresentadas.

Referente ao Acesso a Dados, tendo em conta a atividade específica do SI, foi determinado que a avaliação desta vertente do SI não faria sentido. Os elementos de Arquitetura Geral do Sistema e Menus de Opções e Funcionalidades não foram avaliados uma vez que este SI é fornecido por outra entidade, e estas características são completamente da sua autoria e manutenção.

Devido á particularidade deste SI, foram avaliados também os seguintes elementos:

- Componentes da Plataforma;
- Monitorização Específica;
- Processo de análise de incidências.

A plataforma é composta por 2 componentes – um para deteção de eventos, e outra para bloqueios. Por questões de segurança o nome de ambos os componentes foram ocultados. Durante o processo de análise de incidentes, o sistema consegue realizar procuras por máquina e por utilizador, existindo um sistema de *tags*, que permite a aplicação de filtros. Este sistema também permite a monitorização específica sobre um PC, existindo um procedimento informal para a execução deste processo. Quanto ao Processo de análise de incidências, a avaliação do mesmo é confidencial.

Observações e Não Conformidades Encontradas

Durante a avaliação deste sistema apenas foi registada um não conformidade, sendo esta o facto de na gestão de perfis não ser possível segregar funções entre utilizadores. Como observações foi anotado que deveria ser formalizado o processo para a monitorização de equipamentos específicos, pois um processo não formalizado pode ser explorado tornando-se um risco para a organização, e também devem ser formalizadas as responsabilidades da equipa de colaboradores que utiliza o sistema, pelas mesmas razões

A tabela 6 apresenta a informação sobre as Observações e Não Conformidades encontradas na avaliação do sistema de Combate a Ciberameaças.

Tabela 6 - Observações e Não Conformidades do sistema de Combate a Ciberameaças

Tipo*	Descrição	Utilizadores	Medidas a aplicar
OBS	Responsabilidades		Equipa SOC (formalizar responsabilidades)
OBS	Procedimentos		Formalizar procedimento para a monitorização a equipamentos específicos.
NC	Gestão de perfis		Implementar uma gestão de perfis que permita a correta segregação de funções.

*NC – Não Conformidade | OBS – Observação

Propostas de Implementação de Melhorias

De acordo com as não conformidades e as observações registadas, seguem então as propostas de implementação de melhorias para este SI:

- Formalizar as responsabilidades da equipa SOC da APDL.
- Definição de um procedimento específico para o processo de análise e diagnóstico, que assegure a operacionalidade da equipa na resposta aos incidentes.
- Formalizar uma Política de Uso Aceitável dos Ativos Informáticos da APDL.
- Avaliar o risco efetivo das ligações à *cloud* a partir da ferramenta de combate a ciberameaças (*data lakes*).
- Implementar uma gestão de perfis que permita a correta segregação de funções.

Apreciação Global

Tratando-se de uma solução de deteção e resposta a ameaças de Cibersegurança no âmbito da Lei 46/2018 (artigo 14º), que visa monitorizar, detetar, alarmar, e/ou bloquear autonomamente ameaças em todas as redes e sub-redes da APDL, com origem em máquinas, equipamentos, ou credenciais a que estas se ligam, sendo que não é efetuado um profiling ao utilizador, mas sim comparada a atuação do tráfego com os perfis de risco conhecidos ou anormais.

Posto isto, e uma vez que foram atualizados e distribuídos os documentos de suporte das avaliações referentes à proteção de dados, com as devidas recomendações, parece que o sistema estará a ser bem gerido no sentido de assegurar cada vez mais o conceito de proteção de dados pessoais. Os técnicos estão conscientes da temática da proteção de

dados pessoais, bem como a implementam no seu trabalho diário de combate às ciberameaças.

Foi recomendada a reavaliação interna do custo/benefício na aplicação destas tecnologias e plataformas de combate a ciberameaças, face ao baixo orçamento em Cibersegurança, argumentado pelos elementos da DSI presentes na avaliação.

4.2.7 Sistema GESDOC – Gestão Documental

Esta secção representa a avaliação do sistema GESDOC, onde o seu foco foi avaliar os Perfis e a sua Gestão e as Interconexões do Sistema.

Breve Descrição do Sistema

Este é o sistema de gestão documental da APDL e é regulado pelo Regulamento de Tramitação Documental. É um sistema que permite o *upload* de ficheiros externos, bem como a criação de documentos dentro do próprio SI.

Este sistema apresenta as seguintes caracteristicas:

- Captura todos os emails empresariais;
- O sistema de gestão do correio eletrónico da APDL reencaminha automaticamente os emails.
- Tem uma app exposta para o exterior (iportaldoclight) para a submissão de candidaturas espontâneas de candidatos.
- Interage diretamente com o sistema ERP (*Enterprise Resource Planning*), ao nível da criação automática de entidades, no processo de faturação e pedidos de compra.
- Cada documento em GESDOC tem metadados, o documento e um esquema cronológico. Os documentos associam-se entre si e residem numa determinada pasta (cada documento está numa pasta). A cada documento está associado um determinado *workflow*. Esses *workflows* geram tarefas. Também permite a assinatura digital de documentos PDF.

Elementos Observados

Durante a sessão foram avaliados os seguintes elementos:

- Gestão de Perfis;
- Interconexão de sistemas;
- Medidas de Segurança.

Referente á Gestão de Perfis, os utilizadores pertencem a grupos, e as permissões são definidas ao nível dos grupos, mas os utilizadores poderão ter permissões individuais, sendo eles os seguintes:

- Leitor: ler os seus documentos
- Leitor absoluto: ler todos os documentos de uma determinada pasta.
- Editor: ler e editar os seus documentos
- Editor absoluto: ler e editar todos os documentos da pasta
- Administrador: consegue ler e editar tudo
- Coordenador
- Subcoordenador: não está em uso
- Navegador: ver estruturas de pastas
- *Superuser*: Existem 2 *superuser*, mas apenas a um consegue aceder às pastas da DRH.

Quanto á Interconexão de Sistemas, o sistema GESDOC encontra-se interligado com o seguintes SI:

- ERP – serviço de faturação
- PEX – deliberações de conselho
- SIG – documentos
- Portal do GESDOC

- Sistema de Impressão (*workflow* de conferência de faturas de fornecedores e alguns tipos de documentos específicos)

Para este SI também foram avaliadas as Medidas de Segurança, no entanto, por questões de confidencialidade, não serão apresentadas.

Devido á atividade específica deste SI, também foi avaliado o elemento Mapa de Ações. Durante a avaliação desta funcionalidade verificou-se que existem duas características do sistema que apresentam dados pessoais, sendo elas:

- *Contacts* - Portal de entidades do GESDOC (contem dados pessoais);
- *Logs* - Os administradores e superusers conseguem aceder ao *log* das atividades de todos os utilizadores, sendo que estes contém os seguintes dados: IP, utilizador, evento, data e o documento envolvido.

Os seguintes elementos não foram avaliados por motivos que dizem respeito á direção do DvPDGRE:

- Gestão de *Logs*;
- Base de Dados;
- Acesso a Dados;
- Arquitetura Geral do Sistema;
- Menu de Opções e Funcionalidades;
- Dados Pessoais Recolhidos.

Observações e Não Conformidades Encontradas

Como resultado da avaliação deste SI surgiram três não conformidades e três observações. Começando pelas não conformidades: o portal que suporta a aplicação apresenta uma má gestão das passwords, causando conflito com a Resolução do Conselho de Ministros 41/2018; O sistema não apresenta uma distinção clara entre documentos com e sem dados pessoais, o que facilita o acesso indevido esses dados; e, o portal de entidades integrado no sistema permite acessos indiscriminados a dados pessoais, pelo que o sistema deve permitir reestruturar os privilégios de acesso de determinados utilizadores.

Relativamente às observações, registou-se que: existem mais requisitos obrigatórios da RCM 41/2018 que não estão a ser cumpridos; perante o fluxo cronológico das atividades, uma tentativa de reversão apaga comentários feitos anteriormente; e, durante pesquisas no portal de entidades (CONTACTS) deveria ser possível excluir determinadas entidades das pesquisas tendo em conta o nível de acesso do utilizador a realizar a pesquisa.

A tabela 7 apresenta a informação sobre as Observações e Não Conformidades encontradas na avaliação do sistema GESDOC.

Tabela 7 - Observações e Não Conformidades do sistema GESDOC

Tipo*	Descrição	Utilizadores	Medidas a aplicar
NC	Portal do GESDOC – visualização de password		Gestão de passwords em conformidade com a RCM 41/2018
NC	Identificação de documentos com dados pessoais		Marcar documentos com dados pessoais.
NC	CONTACTS – acesso a dados pessoais		Permitir refinar os privilégios de acesso a dados pessoais de determinados utilizadores.
OBS	Reversão de fluxos apaga os comentários no fluxo cronológico		Rever esta gestão pois corremos o risco de a empresa estar a laborar em cima de um despacho que depois é eliminado.
OBS	Requisitos obrigatórios da RCM 41/2018 não estão a ser cumpridos		Forçar a sua implementação junto do fornecedor.
OBS	Acesso a entidades CONTACTS		Permitir excluir determinadas entidades nas pesquisas

*NC – Não Conformidade | OBS – Observação

Propostas de Implementação de Melhorias

Realizada a avaliação ao sistema seguem-se as seguintes propostas de implementação de melhorias:

- Implementação das alterações decorrentes da nova macroestrutura, revisão decorrente da nova versão do Regulamento de Tramitação Documental;
- Implementação da funcionalidade “Confidencial”.
- Uso da *webapp* GESDOC.
- Restringir a consulta e edição dos utilizadores apenas a algumas tipologias de entidades.
- Fazer o levantamento, por perfis, do *CONTACTS*.

- Revisão do processo de reversão de fluxo, pois apaga o comentário no esquema cronológico.
- Aplicar a RCM 41/2018 na gestão de *log*.
- Nem todos os requisitos obrigatórios da RCM 41/2018 não estão a ser cumpridos pelo fornecedor.
- Marcação dos documentos que contêm dados pessoais e desses os que contêm categorias especiais de dados pessoais.

Apreciação Global

Este sistema, que já existe desde o ano de 2012, de acordo com informação da DSI, será substituído por outra plataforma no médio prazo.

Apesar desta condicionante, o sistema possui mecanismos de restrição de acessos indevidos dos utilizadores (perfis de utilizadores), possui mecanismos de rastreamento das atividades dos utilizadores (logs), bem como incorpora medidas de segurança lógicas importantes: separação dos ambientes de qualidade e produção, sistema de ficheiros encriptado, rastreamento das atividades dos utilizadores.

Por ser um SI que acomoda todos os tipos de dados pessoais, inclusive categorias especiais de dados pessoais, haverá que ter uma atenção em contínuo sobre aos acessos à informação. Sugere-se uma postura mais interventiva da DSI junto do fornecedor para que as solicitações de melhorias ao produto sejam incorporadas.

4.2.8 Sistema CCTV – Closed Circuit TV

Esta secção representa a avaliação do sistema CCTV. Os pontos de foco da avaliação foram os Perfis de Acesso, a localização das camaras, máscaras de privacidade, e a gravação das imagens.

Breve Descrição do Sistema

O sistema CCTV tem como finalidade a proteção de pessoas e bens da área portuária de Leixões, usando como recurso a gravação de imagens.

A categoria de dados pessoais tratados neste sistema são então as imagens captadas pelo mesmo, sendo que estas são conservadas por trinta dias. É também de notar que este sistema não apresenta interconexões com outros SI usados no âmbito da organização.

Elementos Observados

Devido á especificidade deste SI, durante a avaliação do sistema CCTV, foram observados os seguintes elementos:

- Gestão de Perfis;
- Medidas de Segurança;

Por razões de segurança e confidencialidade, a avaliação da Gestão de Perfis e das Medidas de Segurança não serão apresentadas.

Por motivos que dizem respeito à direção do DvPDGRE os seguintes elementos não foram avaliados:

- Gestão de *Logs*;
- Interconexão de Sistemas;
- Base de Dados;
- Acesso a Dados;
- Arquitetura Geral do Sistema;
- Menus de Opções e Funcionalidades;
- Dados Pessoais Recolhidos.

Tendo em conta as características do SI, foi determinado que seria pertinente avaliar os seguintes elementos:

- Validação de Requisitos;
- Forma de exercício do direito de acesso;
- Comunicação das imagens.

Durante a observação da Validação de Requisitos, de acordo com os regulamentos, foram registadas as seguintes respostas:

O sistema não tem a funcionalidade de transmitir imagens para o exterior do local de instalação, e, relativo as medidas e limites de tratamento das imagens, não existe a opção de recolha de som, e a gestão de logs é sofisticada e pormenorizada.

A recolha de imagens deve confinar-se à propriedade do responsável, não podendo abranger imagens da via pública ou de propriedades limítrofes, sendo que o sistema se encontra não conforme, pois vê-se , mesmo que muito tênue, um pouco da área adjacente em algumas câmaras.

No caso de existirem terminais de pagamento ATM, as câmaras não podem estar direcionadas de modo a captar a digitação dos códigos. Neste caso existem câmaras que permitem visualizar parcialmente o terminal ATM, no entanto não se consegue visualizar a digitação dos códigos.

Não podem as câmaras incidir regularmente sobre os trabalhadores durante a atividade laboral, nem as imagens podem ser utilizadas para o controlo da atividade dos trabalhadores, seja para aferir a produtividade seja para efeitos de responsabilização disciplinar, pelo que por norma não existem trabalhadores da APDL no local, apenas trabalhadores dos operadores portuàrios, bem como prestadores de serviço. Em ambos os casos estes trabalhadores não têm responsabilidades para com a APDL.

Encontra-se em conformidade o requisito em que apenas a recolha de imagens nos locais declarados está abrangida pela presente autorização, não podendo, em circunstância alguma, serem recolhidas imagens de acesso ou interior de instalações sanitárias, acesso e interiores de vestiários, áreas de descanso ou outras áreas destinadas aos trabalhadores, zonas de fabrico, zonas de espera, salas de reuniões e auditórios.

Segundo o RGPD, um titular tem o direito de aceder aos seus dados. Deste modo, o requerente deve solicitar de forma escrita ao encarregado da proteção de dados o acesso aos mesmos. Tal deve ser feito na seguinte morada: Avenida da Liberdade - Leça da Palmeira 4450-718 Leça da Palmeira.

Referente à Comunicação de Imagens, as imagens recolhidas são de uso exclusivo de segurança do espaço, sendo que só podem ser transmitidas nos termos da Lei processual penal. Detetada a eventual infração penal, o responsável deverá, juntamente com a participação, enviar à autoridade judiciária ou ao órgão de polícia criminal competentes as imagens recolhidas.

Noutras situações em que as autoridades solicitem acesso às imagens, tal só poderá ocorrer, no âmbito de processo judicial devidamente identificado, em cumprimento de despacho fundamentado da autoridade judiciária competente. Esta situação encontra-se em conformidade.

Ao disponibilizar as imagens ao titular dos dados, o responsável deve adotar as medidas técnicas necessárias para ocultar as imagens de terceiros que possam ter sido abrangidos pela gravação, o que se mantém conforme.

De modo a garantir o direito de informação consagrado no artigo 10.º da LPD, deverão ser afixados em locais bem visíveis avisos informativos sendo que existe sinalização nas entradas, bem como é acessível a política de privacidade no site da APDL.

De acordo com os artigos 32º, 33º, 34º do RGPD, o responsável deve também adotar as seguintes medidas de segurança:

- Pseudonimização, para tal são aplicadas as máscaras no sistema visual;
- Cifragem, que por razões de performance ainda não se aplicam, no entanto no arquivo as imagens só são acedíveis via perfis específicos;
- Confidencialidade, assegurado através do uso de perfis;
- Integridade, aspeto que ficou para avaliação do DSI;
- Disponibilidade, onde apesar de todo o sistema se encontrar operacional, deve ser explorada a possibilidade de gravação em locais alternativos aquando da falha do principal, bem como no caso dos servidores usado para armazenar as filmagens;
- Resiliência, mais um aspeto a ser avaliado pelo DSI;
- Restabelecimento da disponibilidade e o acesso aos dados atempadamente, onde, apesar de não existirem backups de vídeo, existem vários arquivadores de vídeo para assegurar redundância.

Observações e Não Conformidades Encontradas

Devido à extrema sensibilidade deste SI, esta secção é confidencial.

Proposta de Implementação de Melhorias

De acordo com as não conformidades e as observações registadas, seguem então as propostas de implementação de melhorias para este SI:

- Realização de testes programados para apreciar a utilidade das medidas técnicas e organizativas, como por exemplo: desativar um servidor /arquivador para avaliar a resiliência do sistema global.
- Rpa.3pl: avaliar a necessidade de existir este perfil
- CCTV.4: revisão integral deste perfil
- CCTV.6: desativar assim que oportuno
- CCTV.7: avaliar a continuidade de dois utilizadores específicos neste perfil.

Apreciação Global

O sistema permite a correta e devida gestão dos equipamentos (câmaras), por aplicação de máscaras de privacidade e gestão dos acessos dos utilizadores, incluindo o rastreio de todas as suas atividades, estando então a ser bem gerido e com a preocupação de proteção de dados e privacidade em todas as fases: instalação, parametrização, gravação e acessos.

Os perfis de utilização encontrados parecem ser os necessários e suficientes à correta segregação de funções e aplicação do princípio "need to know", mas estão a necessitar de uma revisão integral, uma vez que este é um sistema muito complexo.

4.3 Análise do Resultados Obtidos

Uma vez realizadas todas as avaliações, é notório o nível de complexidade, não só de cada SI individualmente, mas também pela ligações entre eles. Torna-se também evidente que a organização, em termos informáticos e de sistemas, está em processo de remodelação e em evolução, refletida na quantidade de SI que se encontram em fase de descontinuação ou de migração de processos (3PL, Sistema de Controlo de Acessos Físicos e CUP). Como consequência, algumas avaliações foram de certo modo incomums pois quaisquer propostas de melhoria ou não conformidades encontradas, seriam tratadas

como parte do planeamento do SI previsto. Deste modo, o resultado destas avaliações poderá ser de certa maneira redundante.

Sem dúvida o SI mais preocupante é o CUP, pois apresenta o maior número de não conformidades para ambos os tipos de avaliação. No entanto, esta situação poderá ser explicada pelo facto de este SI estar em processo de migração para um novo SI, levando a que estas não conformidades não fossem resolvidas atenpadamente.

O SI com menos problemas encontrados foi o PowerBI, que apenas apresentou uma não conformidade perante a Avaliação de Conformidade de Segurança (Gestão de *Logs* não ativada). Esta não conformidade, que surgiu devido à falta de conhecimento técnico da parte do Responsável pelo SI, foi imediatamente corrigida, deixando o SI sem qualquer não conformidade ou observação registada.

De todas as não conformidades, a que mais vezes se verificou foi a existência de utilizadores com perfis e acessos desnecessários, não conformidade da vertente das AIPD, sendo que todas estas não conformidades foram corrigidas imediatamente. Quanto às observações, a situação que mais se repetiu foram problemas com os *logs* dos SI, seja por *logs* incompletos, ou por falhas no acesso a essa funcionalidade, que por sua vez encaixa na vertente das Avaliações de Conformidade de Segurança.

Dito isto, de um modo geral, através dos resultados das AIPD, todos os SI apresentaram um bom nível de proteção de dados pessoais, e com os resultados das Avaliações de Conformidade de Segurança, os SI também apresentam mecanismos de segurança necessários para assegurar o normal funcionamento do SI e a proteção do mesmo.

CAPÍTULO V – CONCLUSÃO

A proteção de dados pessoais é um tema cada vez mais importante e em evolução, sendo alvo de um debate aceso devido às elevadas coimas associadas à não implementação do RGPD. Constata-se que ainda não existe um consenso sobre qual será o melhor caminho a percorrer rumo à conformidade dos SI. Face as mudanças tecnológicas diárias que se assiste hoje em dia, estas preocupações deverão ser contínuas no tempo. Considerando este contexto, o trabalho realizado neste estágio é de elevada importância, não só pela sensibilização inevitável do público com quem a organização coopera e serve, mas também pelo exemplo que demonstra aos seus parceiros de negócio.

A existência de departamentos especializados para a proteção de dados no seio das organizações é algo muito recente, mas que produz resultados muito benéficos para as mesmas. A APDL ao apresentar uma divisão dedicada para este efeito demonstra preocupação e atenção para com as necessidades do mundo empresarial e com os deveres que tem para com os seus colaboradores, clientes e parceiros. Com cada vez mais questões a serem levantadas diariamente sobre o que acontece os dados pessoais e o constante ajuste do RGPD para colmatar quaisquer lacunas na legislação referente a este assunto, este estágio apresentou-se como uma excelente oportunidade para abordar e consolidar vários conceitos num contexto organizacional.

De acordo com os objetivos estabelecidos no início deste estágio, a análise das práticas de segurança dos SI e a verificação da implementação das diretrizes do RGPD, ambos foram alcançados. Através das avaliações realizadas foi possível determinar o nível de segurança, assim como o nível de conformidade do RGPD, de cada SI perante os requisitos impostos pelas autoridades dos espaços respetivos.

Em função dos resultados alcançados é legítimo afirmar que o problema que mais vezes se repete nos SI avaliados é a gestão insuficiente dos perfis, situação que, ao possibilitar acessos indevidos ao SI e às informações que este contém, pode causar graves danos à organização. Apesar disto, todos os SI apresentam resultados convincentes.

Da parte da organização, ao aceitar o estágio está a possibilitar a estimulação da criatividade e inovação no espaço profissional, uma vez que jovens formados podem trazer ideias e metodologias novas para um ambiente que por outro lado poderia ficar estagnado.

Em termos de limitações do estágio, o facto de vários sistema se encontrarem em fase de descontinuação tornou algumas das avaliações pouco produtivas, pois dependendo do novo sistema algumas propostas de melhoria podem não se aplicar ao mesmo. Devido ao começo tardio do estágio, e a política de agendamento das avaliações da organização, o número de avaliações realizadas tornou-se mais limitado do que seria esperado, tendo sido feitas apenas um total de oito avaliações.

Analisando os resultados obtidos é notório o esforço feito em prol da segurança do sistemas e da proteção de dados pessoais, não só pelo departamento em que se realizou o estágio, mas também por todos os departamentos presentes na organização. É também de valor referir que, apesar das constantes mudanças nas leis e regulamentos, tanto europeus como nacionais, a APDL atinge, e supera, os níveis esperados de segurança dos SI.

A nível pessoal, ao ter tido a possibilidade de realizar este estágio estive numa posição privilegiada tanto em termos de recursos, oportunidades e informação disponível para realizar e observar avaliações de conformidade a um alto nível, bem como experienciar o que é necessário para uma organização desta dimensão estar em conformidade com as leis, normas e regulamentos.

APDL, S.A.. https://www.apdl.pt

APDSI. (s.d.) Acesso Dados. https://apdsi.pt/glossario/a/acesso-dados/

APDSI. (s.d) Base de Dados. https://apdsi.pt/glossario/b/base-de-dados/

APDSI (2014). O Tratamento de Dados Pessoais em Portugal - Breve Guia Prático. Lisboa: APDSI, p.8.

APDSI & CNPD. (2016). Conferência sobre "O Novo Regulamento Europeu de Proteção de Dados". Lisboa: APDSI & CNPD, p.1.

Assembleia da República (1976). Constituição da República Portuguesa. https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

Assembleia da República (2018). Lei n.º 46/2018 Segurança do Ciberespaço. Diário da República, Série I, N. 155. Assembleia da República https://dre.pt/dre/detalhe/lei/46-2018-116029384

Assembleia da República (2018). Lei n.º 58/2019 Proteção Dados Pessoais. Diário da República, Série I, N. 151. Assembleia da República https://dre.pt/dre/detalhe/lei/46-2018-116029384

Assembleia da República (2018). Lei n.º 67/1998 Proteção Dados Pessoais. Diário da República, Série I, N. 247. Assembleia da República https://dre.pt/dre/detalhe/lei/46-2018-116029384

Barros, B. M. C. de, Barros, C. T. L., & Oliveira, R. S. de. (2017). O direito à privacidade: Uma reflexão acerca do anteprojeto de proteção de dados pessoais. Revista Videre, 9(17), 13–27. https://doi.org/10.30612/videre.v9i17.6029

Borges Fortes, V., & Oro Boff, S. (2014). A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: Perspectivas de construção de um marco regulatório para o Brasil. Seqüência: Estudos Jurídicos e Políticos, 35(68), 109. https://doi.org/10.5007/2177-7055.2013v35n68p109

Castro, C. S. (2005). Direito da Informática, Privacidade e Dados Pessoais. Almedina.

Presidência do Conselho de Ministros (2021). Decreto Lei n.º 65/2021 Segurança do Ciberespaço. Diário da República: I série, No 147. https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988

Dewey, J. (2020). A educação é um processo social, é desenvolvimento. 117.

Diogo, S. A. (2021). O papel da Auditoria Interna no Regime Geral de Proteção de Dados enquanto terceira linha de defesa. 119.

Fazendeiro, A. (2017). Regulamento Geral Sobre a Proteção de Dados. Almedina.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dado, (2017). Orientações sobre os Encarregados da Proteção de Dados. União Europeia. Bruxelas.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dado, (2017). Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. União Europeia. Bruxelas

Hatley, D. J., & Hruschka, P. & Pirbhai I. (2000). Process for System Architecture and Requirements Engineering. 65.

ISO/IEC 7498-1:1994(en), Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model—Part 1. (sem data). Obtido 26 de outubro de 2022, de https://www.iso.org/obp/ui/#iso:std:iso-iec:7498:-1:ed-1:v2:en

Machado, F. R. S. (2020). RGPD (Regulamento geral de proteção de dados): Conhecimento e impacto nas organizações. 89. Dissertação de Mestrado em Auditoria. Instituto Superior de Contabilidade e Administração do Porto.

Magalhães, F. (2018). Formação - Regulamento Geral de Proteção de Dados. Portugal: Ordem dos Contabilistas Certificados.

Magalhães, F. M., & Pereira, M. L. (2018). Regulamento Geral de Proteção de Dados: Manual Prático (2.a Edição). Porto: Vida Económica.

Magalhães, M. M. R. (2017). Modelo Integrado de Gestão do Risco para o Sector Público Português Estudo de Caso: O Município da Maia. Projeto de Mestrado em Auditoria. Instituto Superior de Contabilidade e Administração do Porto.

Mamede, H. S. (2015). Revista de Ciências da Computação, nº10. Notas leitura / Recensão crítica [de] Protection of Personal Data.

Martins, J. P. F. (2020). A Auditoria Interna e o Regulamento Geral Sobre a Proteção de Dados Estudo de Caso: O Município de Vila Nova de Gaia. 304.

Millage, A. (2019). GDPR Is Just the Beginning. Internal Audit, The Institute of Internal Auditors, 7, abril.

Moreira, T. F. M. (2018). O Impacto do Regulamento Geral da Proteção de Dados Pessoais nas Organizações: Um Novo Paradigma. Dissertação de Mestrado em Solicitadoria. Instituto Superior de Contabilidade e Administração de Coimbra.

Oliveira, J. P. C. P. M. (2020). O acesso à informação na Administração pública, no contexto do regime geral de proteção de dados pessoais e das tecnologias de informação. Relatório de Estágio em Direito e Prática Jurídica. Especialidade em Direito Administrativo e Administração Pública. Faculdade de Direito Universidade de Lisboa.

Parlamento Europeu e do Conselho (1995). Diretiva 95/46/CE Protecção de Dados Pessoais. Jornal Oficial das Comunidades Europeias, Série I, N. 281 https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:31995L0046

Pedroso, L. M. R. (2021). Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD. Dissertação de Mestrado em Gestão de Sistemas e Tecnologias de Informação. 220. Instituto Universitário Atlântica.

Rebelo, M. P. (2019). Os desafios do RGPD perante as novas tecnologias blockchain Universitat de Barcelona. 15.

Saldanha, N. (2019). RGPD - Guia para uma Auditoria de Conformidade—Dados, Privacidade, Implementação, Controlo, Compliance (1.a Edição). Lisboa: FCA – Editora de Informática. Lda.

Santos, A. F. da C. (2017). As Diretivas Comunitárias de Proteção de Dados Pessoais e a sua Aplicação em Portugal: Barreiras e Facilitadores. Dissertação de Mestrado em Gestão e Políticas Públicas. Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa.

Silva, G. C. (2019). RGPD aplicado nas PME portuguesas. Dissertação de Mestrado em Gestão de Informação. Instituto Superior de Estatística e Gestão de Informação.

Silva, M. T. (2021). A Auditoria e a Proteção de Dados dos Consumidores de Alojamento Local. Dissertação de Mestrado em Auditoria. Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa.

Regulamento Geral de Proteção de Dados (2016) da União Europeia. http://www.privacy-regulationúmeroeu/pt/4.htm

União Europeia (2007). Tratado de Lisboa. Jornal Oficial da União Europeia, Série I, N. 306. União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12007L/TXT&from=PT

União Europeia. (s.d.) European Data Protection Supervisor https://edps.europa.eu/about-edps_en

Vaz, A. R. (2018). O Regulamento Geral de Proteção de Dados: Desafios e Impactos. Dissertação de Mestrado em Ciências Jurídico-Forenses. Faculdade de Direito da Universidade de Coimbra.

Veiga, A. S. P. G. (2020). Proteção de Dados: O Direito à Privacidade na Era do Digital. Dissertação de Mestrado em Direito. Universidade Autónoma de Lisboa.

Vieira, T. (2007). O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação de Mestrado em Direito. Universidade de Brasília.

Zanini, L. E. de A. (2015). O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. Revista de Doutrina da 4a Região, Porto Alegre, número 64, 2.