INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL SUPERIOR
2019/2020

TII

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: IMPACTO NOS SISTEMAS DE INFORMAÇÃO DE RECURSOS HUMANOS DA FORÇA AÉREA

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Pedro José de Sousa Henriques
CAP/TPAA

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: IMPACTO NOS SISTEMAS DE INFORMAÇÃO DE RECURSOS HUMANOS DA FORÇA AÉREA

CAP/TPAA Pedro José de Sousa Henriques

Trabalho de Investigação Individual do CPOS-FA 2019/20

Pedrouços 2020

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: IMPACTO NOS SISTEMAS DE INFORMAÇÃO DE RECURSOS HUMANOS DA FORÇA AÉREA

CAP/TPAA Pedro José de Sousa Henriques

Trabalho de Investigação Individual do CPOS-FA 2019/20

Orientador: TCOR/TPAA Paulo Guilherme Domingos Ferreira Simões
Coorientador: TCOR/TMMA Nuno Alberto Rodrigues Santos Loureiro

Pedrouços 2020

Declaração de compromisso Antiplágio

Eu, **Pedro José de Sousa Henriques**, declaro por minha honra que o documento intitulado **Regulamento Geral de Proteção de Dados: Impacto nos Sistemas de Informação de Recursos Humanos da Força Aérea** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial Superior – Força Aérea 2019/20** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 31** de **janeiro** de **2020**

Pedro José de Sousa Henriques

Agradecimentos

Apesar de este ser um trabalho individual, a sua realização é fruto do contributo, do aconselhamento, da discussão, da orientação e do auxílio de várias pessoas, às quais é de sincera e elementar justiça agradecer nas próximas linhas.

Em primeiro lugar, ao Tenente-Coronel Paulo Simões, na qualidade de orientador deste trabalho, pela disponibilidade, aconselhamento e liberdade de ação que permitiu que esta investigação contribuísse para o meu desenvolvimento académico.

Ao Tenente-Coronel Nuno Loureiro, na qualidade de coorientador, pela preocupação e constante apoio às exigências formais deste Trabalho de Investigação.

A todos os entrevistados que se demonstraram sempre disponíveis e com vontade de contribuir para o enriquecimento deste trabalho através da sua experiência e saber.

Aos camaradas deste Curso de Promoção a Oficial Superior, em especial aos Ninjas, pelo espírito de sã camaradagem e espírito de corpo, característica distinta do nosso grupo.

Às minhas mulheres pela sua compreensão e apoio, particularmente nos dias mais difíceis. Elas são e continuarão a ser o porto de abrigo em dias de tempestade.

A todos, bem hajam.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades, no entanto, não é pelo facto de alguém entregar dados pessoais a uma organização que deixa de ser o proprietário ou titular dos mesmos, e quem os recebe tem o dever de respeitar essa titularidade.

O presente estudo tem como objetivo a proposta de medidas de mitigação dos riscos para os direitos dos titulares dos dados, associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, no âmbito da implementação do RGPD. Através de um raciocínio dedutivo, obtêm-se respostas para uma área de conhecimento científico recente e pouco desenvolvida, baseando-se numa estratégia de investigação qualitativa.

O processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, é caraterizado e verificado quanto à sua conformidade com os princípios fundamentais: a necessidade e a proporcionalidade de processamento e a proteção dos direitos dos titulares dos dados pessoais. Os riscos associados ao processo são avaliados quanto à sua probabilidade e gravidade, e consequentemente, identifica-se um conjunto de medidas mitigadoras dos mesmos.

Palavras-chave

RGPD, Risco, Sistema de Informação, Recursos Humanos, AIPD.

Abstract

New technologies allow private companies and public entities to use personal data on an unprecedented scale in the exercise of their activities, however, it is not because someone delivers personal data to an organization that they are no longer the owner or holder of the data themselves, and whoever receives them has a duty to respect that title.

This study aims to propose risk mitigation measures for the rights of data subjects, associated with the process of managing profiles of access to the personal data of the HR of the FA, present in the SIGDN-RH, within the scope of the implementation of the GDPR. Through deductive reasoning, answers are obtained for a recent and undeveloped area of scientific knowledge, based on a qualitative research strategy.

The process of managing the profiles of access to the personal data of the HR of the FA, present in the SIGDN-RH, is characterized and verified regarding its compliance with the fundamental principles: the need and proportionality of processing and the protection of the rights of the data subjects personal. The risks associated with the process are assessed for their probability and severity, and consequently, a set of mitigating measures is identified.

Keywords

GDPR, Risk, Information System, Human Resources, DPIA.

1. Introdução

A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais, em que a recolha e a partilha dos mesmos registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais e deverá ser reforçada a segurança jurídica e prática para as pessoas singulares, os operadores económicos e as autoridades públicas. (Parlamento Europeu, 2016).

Os Recursos Humanos (RH) de uma organização militar são um pilar essencial na missão confiada às Forças Armadas (FFAA) e à defesa militar da República Portuguesa. Desta forma, devemos confiar-lhes dignidade e condições que legitimem a sua importância e condição, relevantes para o cumprimento da missão incumbida à Força Aérea (FA), sendo importante que estes militares e trabalhadores civis da FA vejam os seus direitos protegidos (Almeida, 2018).

A Lei de Proteção de Dados[1], veio regulamentar na ordem jurídica nacional, o Regulamento Geral de Proteção de Dados[2] (RGPD), o qual, traduz uma mudança concetual associada a questões relacionadas com a segurança dos dados pessoais. Assim, são criados um conjunto de novos direitos para o cidadão, novos procedimentos e novas obrigações para as entidades públicas e privadas. Estando a FA na dependência direta do Estado, através do Ministério da Defesa Nacional (MDN), encontra-se abrangida por este novo regulamento (Almeida, 2018).

Assim, no seguimento da intenção[3] do Chefe de Estado-Maior da Força Aérea (CEMFA) de garantir o exercício dos direitos dos titulares dos dados pessoais à responsabilidade da FA e assegurar que estes dados estão protegidos e os tratamentos cumprem o disposto no RGPD, este trabalho tem como tema fundamental de análise, o impacto da implementação do RGPD nos Sistemas de Informação (SI) de RH da FA.

O estudo exaustivo do impacto da aplicação do RGPD nos SI de RH da FA seria demasiado extenso, atendendo à transversalidade deste novo quadro legal e múltiplas implicações nas mais variadas áreas de gestão de RH da Organização. Além disso, as restrições temporais definidas para esta investigação, permitem apenas o aprofundamento da

[1] Lei n.º 58/2019, de 08 de agosto.
[2] Regulamento (UE) 679/2016, do Parlamento Europeu e do Conselho, de 27 de abril.
[3] Diretiva n.º 12/CEMFA/2018, de 14 de junho.

análise no processo de gestão de acessos aos dados pessoais dos RH da FA, presentes no Sistema Integrado de Gestão da Defesa Nacional – Recursos Humanos (SIGDN-RH).

A presente investigação tem por objeto, o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, no âmbito da avaliação do impacto da implementação do RGPD. Apesar da FA possuir vários sistemas que concorrem para a gestão de RH, além do SIGDN-RH, esta investigação debruça-se apenas neste, por ser a principal base de dados de RH.

Santos (2018) define um SI, como um conjunto de componentes inter-relacionados que recolhe ou retira, processa, armazena e distribui informação para suportar a tomada de decisões, coordenar e controlar processos de trabalho. O SIGDN-RH constitui-se como uma ferramenta tecnológica e um instrumento de gestão integrada da Defesa que potencia a adoção de procedimentos normalizados dentro do MDN e das FFAA, nas áreas de planeamento, gestão administrativa e vencimentos, gestão de carreiras, obtenção e recrutamento de pessoal, formação, justiça e disciplina (Secretaria-Geral do Ministério da Defesa Nacional (SGMDN), 2011). Este SI foi adotado pela FA, em 01 de outubro de 2018, tendo decorrido um processo de migração de informação de RH do Sistema de Informação de Gestão da Área de Pessoal (SIGAP), de cerca de 140 mil militares e trabalhadores civis, que prestam ou prestaram serviço na FA (Coordenador da Área Técnica de Informação de Recursos Humanos (cATIRH), entrevista presencial, 30 de setembro de 2019).

Neste enquadramento, este estudo tem o seguinte objetivo geral (OG): *Propor medidas de mitigação dos riscos para os direitos dos titulares dos dados, associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, no âmbito da implementação do RGPD*, alicerçado nos seguintes objetivos específicos (OE):

OE1 – Caracterizar o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH.

OE2 – Analisar a conformidade com os princípios fundamentais: a necessidade e a proporcionalidade de processamento e a proteção dos direitos dos titulares dos dados pessoais dos RH da FA, presentes no SIGDN-RH.

OE3 – Avaliar os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH.

Estes objetivos refletem-se na seguinte questão central (QC): *De que forma, os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA,*

presentes no SIGDN-RH, podem ser mitigados, respeitando os direitos dos titulares dos dados definidos pelo RGPD?

Decorrente da QC surgem as seguintes questões derivadas (QD):

QD1 – Em que consiste o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?

QD2.1 – Qual o grau de necessidade do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?

QD2.2 – Qual o grau de proporcionalidade do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?

QD2.3 – Qual o grau de proteção dos direitos dos titulares dos dados no processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?

QD3 – Qual a avaliação dos riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?

Estruturalmente, o presente documento encontra-se organizado em cinco capítulos, sendo que o primeiro é a presente introdução. O segundo, tem por objetivo proceder ao enquadramento teórico e concetual que norteou a investigação. O terceiro, é destinado à apresentação da metodologia e método orientadores deste trabalho. O quarto, é dedicado à apresentação dos dados, discussão dos resultados e resposta às questões da investigação. O quinto, e último, tem como propósito efetuar um sumário da investigação, avaliar os resultados obtidos, elencar os contributos para o conhecimento, indicar as limitações identificadas, propor estudos futuros e enumerar algumas recomendações de ordem prática.

2. Enquadramento teórico e concetual

Neste capítulo apresentam-se o estado da arte, os conceitos estruturantes e a metodologia seguida neste estudo.

2.1. Revisão da literatura e conceitos estruturantes

O RGPD entrou em vigor em 25 de maio de 2016, tendo como objetivo o direito à proteção dos dados pessoais das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e sendo aplicável a todos os Estados membros da União Europeia, veio definir um novo quadro legal de proteção de dados pessoais, com aplicabilidade direta na ordem jurídica nacional a partir de 25 de maio de 2018 (Parlamento Europeu, 2016).

A Lei de Proteção de Dados veio assegurar a execução do RGPD, na ordem jurídica nacional, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Como este novo quadro legal tem impacto direto na forma como a FA trata os dados pessoais à sua responsabilidade, obrigando a verificações e alterações nos processos da Organização relacionados com esta matéria, o CEMFA definiu as responsabilidades e as tarefas a desenvolver pelas Unidades, Estabelecimentos e Órgãos (U/E/O) da FA, em matéria de tratamento de dados pessoais, nomeadamente no que respeita à aprovação de regulamentação interna, às alterações aos processos informatizados ou manuais de tratamento de dados pessoais, ao registo das operações efetuadas e às informações a prestar ao titular dos dados pessoais. Também procedeu à nomeação do Encarregado de Proteção de Dados (EPD), ao qual compete, controlar a conformidade do tratamento de dados pessoais com as políticas de proteção de dados da FA e com o RGPD, assim como a realização de Avaliações de Impacto sobre a Proteção de Dados (AIPD), aconselhando a sua realização, quando necessário[4].

2.1.1. Avaliação de Impacto sobre a Proteção de Dados (AIPD)

Apesar de não ser algo de novo[5], o artigo n.º 35.º do RGPD introduz o conceito de AIPD, considerando-a 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-

[4] Diretiva n.º 12/CEMFA/2018, de 14 de junho.

[5] A expressão «Avaliação de Impacto na Privacidade» (AIP) é também frequentemente utilizada noutros contextos como referência ao mesmo conceito (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (GT Art.º 29.º), 2017).

os e determinando as medidas necessárias para fazer face a esses riscos. As AIPD são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento. Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar conformidade (GT Art.º 29.º, 2017).

Ainda que se possa realizar esta avaliação de acordo com várias circunstâncias, existe a obrigação de sua realização, quando o tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis. Uma AIPD também pode ser útil para avaliar o impacto na proteção de dados de um produto tecnológico, como por exemplo, um programa informático, sempre que este seja suscetível de ser utilizado por vários responsáveis pelo tratamento de dados para realizar diferentes operações de tratamento (GT Art.º 29.º, 2017).

2.1.2. Processo de Gestão de Perfis de Acesso

Os perfis de autorização permitem controlar o acesso a todas as funcionalidades disponíveis num SI para cada um dos utilizadores, assim como o acesso aos dados, de acordo com as funções executadas e a respetiva estrutura organizacional em que se insere (SGMDN, 2011). Na área dos Sistemas de Gestão da Segurança da Informação (SGSI), a gestão envolve a supervisão e tomada de decisões necessárias para alcançar os objetivos de negócios por meio da proteção dos ativos de informação da organização (International Organization for Standardization (ISO), 2018a). Sendo um processo, a forma como uma entidade se organiza para a obtenção de um determinado objetivo (Antunes, 2018, p. 98), pode-se considerar, que no âmbito da proteção de dados presentes num SI, um processo de gestão de perfis de acesso se constitui como, um conjunto de regras e procedimentos definidos pela organização para a gestão de autorização e perfis de acesso à informação disponível num SI, com vista à proteção dos direitos dos titulares dos dados. As políticas de controlo de acesso são requisitos de alto nível que especificam como é feita a gestão de acessos, e quem, e em que circunstâncias pode aceder a que informação (Hu & Scarfone, 2012).

2.1.3. Necessidade do processo de gestão de perfis de acesso

De acordo com o RGPD, a necessidade de avaliação de um determinado tratamento de dados advém da sua suscetibilidade de implicar riscos elevados para os direitos e as liberdades das pessoas singulares (GT Art.º 29.º, 2017), sendo assim um requisito essencial de uma AIPD. A necessidade está relacionada com o carácter indispensável ou

imprescindível de uma situação, a qual impõe a implementação ou reformulação de determinadas ações preventivas ou mitigadores de riscos identificados.

2.1.4. Proporcionalidade do processo de gestão de perfis de acesso

Neste âmbito, a proporcionalidade de um processo de gestão de perfis de acesso aos dados, pretende avaliar a adequabilidade face os objetivos definidos pelos vários normativos de gestão de informação e proteção de dados pessoais. De acordo com o RGPD (Parlamento Europeu, 2016), o "tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais". Por exemplo, o tratamento de dados pessoais para fins estatísticos, deverá ficar sujeito à garantia adequada dos direitos e liberdades do titular dos dados, nomeadamente, assegurar a existência de medidas técnicas e organizativas que assegurem, o princípio da minimização dos dados, ou seja, a adequação dos dados pessoais às finalidades para as quais são tratados.

2.1.5. Proteção dos direitos dos titulares dos dados

O titular dos dados é a "pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". Ainda o capítulo III do RGPD, define os seguintes direitos do titular dos dados: Direito à Informação, Acesso aos dados pessoais, Retificação, Apagamento, Limitação do tratamento, Notificação, Portabilidade, Oposição, Não sujeição a decisões automatizadas e Aviso em caso de violação de dados pessoais (Parlamento Europeu, 2016). Assim, a proteção dos direitos dos titulares dos dados deverá garantir a segurança de qualquer informação relativa a uma pessoa singular identificada ou identificável, nomeadamente na defesa dos seus direitos legalmente estabelecidos.

2.1.6. Riscos do processo

O conceito de risco está associado ao efeito de incerteza na consecução dos objetivos (ISO, 2018b), assim como a um cenário que descreve um acontecimento e as respetivas consequências, estimado em termos de gravidade e probabilidade (GT Art.º 29.º, 2017). Sendo um processo, a forma como uma entidade se organiza para a obtenção de um determinado objetivo (Antunes, 2018, p. 98), neste âmbito, os riscos do processo englobam os efeitos, estimados em termos de gravidade e probabilidade, resultantes da aplicação do

conjunto de regras e procedimentos definidos pela organização com vista à gestão de autorização e perfis de acesso aos dados disponíveis num SI.

2.2. **Modelo de análise**

A presente investigação norteou-se pelo modelo de análise refletido no Apêndice A.

3. Metodologia e método

De seguida, apresentam-se a metodologia e o método desta investigação.

3.1. Metodologia

Conforme Santos e Lima (2019), a metodologia da presente investigação segue um percurso constituído por três fases:

- Exploratória, com recurso a análise documental, entrevistas exploratórias, enquadramento concetual, formulação do problema, objetivos e questões;

- Analítica, baseada na recolha, apresentação e análise dos dados das entrevistas realizadas, bem como no aprofundamento da análise documental;

- Conclusiva, com a avaliação e discussão dos resultados, apresentação das conclusões, contributos para o conhecimento, limitações, sugestões para estudos futuros e recomendações.

O presente estudo segue um raciocínio dedutivo, tentando obter respostas para uma área de conhecimento científico recente e pouco desenvolvida, baseado numa estratégia de investigação qualitativa. O raciocínio dedutivo parte da lei geral para o particular, onde se procura raciocinar dedutivamente, partindo da teoria em busca de uma verdade particular (Santos & Lima, 2019, p. 19).

3.2. Método

A este nível, são apresentados os participantes, o procedimento, o instrumento de recolha de dados e as técnicas de tratamento dos dados.

3.2.1. Participantes e procedimentos

Na recolha de informação, utilizou-se uma estratégia qualitativa, suportada em entrevistas semiestruturadas aplicadas a seis entrevistados (Apêndice B), escolhidos por serem interlocutores privilegiados nesta área de atividade e reunirem o conhecimento, a experiência e o entendimento da problemática estudada, fator determinante na recolha dos contributos para a realização deste trabalho.

Foi estabelecido um primeiro contacto com os potenciais participantes a saber da disponibilidade para integrar esta investigação. Após anuência, foi enviado o guião da entrevista semiestruturada por *email*, e, nos casos em que foi possível, agendada a entrevista presencial. Todas as transcrições das entrevistas utilizadas neste trabalho foram devidamente validadas e autorizadas pelos interlocutores.

3.2.2. Instrumentos de recolha de dados

Para além da recolha bibliográfica de artigos e trabalhos científicos sobre a temática, da análise da legislação e dos normativos internos do MDN e da FA, construiu-se um guia de entrevista semiestruturada, adaptado aos diferentes entrevistados (Apêndice B), tendo por base, um conjunto alargado de controlos e questões apresentadas por Saldanha (2019), pela ISO (2013) e pela *Commission Nationale de l'Informatique et des Libertés* (CNIL) (2018a).

3.2.3. Técnica de tratamento de dados

As teorias vão-se evidenciando ao longo da recolha e análise dos dados, em que se procuram padrões e relações do fenómeno analisado (Santos & Lima, 2019, p. 116). Ou seja, as orientações sobre o tratamento de dados neste trabalho, encontram-se centradas na análise de conteúdo (Apêndice C), técnica mais frequente numa abordagem qualitativa, onde se procede a uma comparação sistemática do material com recurso a uma grelha de análise.

Na análise de dados, recorreu-se a uma AIPD, baseada nas orientações da CNIL (2018a) e do GT Art.º 29.º (2017), recorrendo ainda ao *software Privacy Impact Assessment* (PIA), desenvolvido pela CNIL (2019), para possibilitar uma melhor gestão da avaliação, desdobrando passo a passo a metodologia de forma simples e esclarecedora, obtendo um cenário completo dos riscos.

Uma AIPD é um processo contínuo, que apresenta as seguintes quatro fases de execução, das quais, apenas se desenvolveram as três primeiras em consonância com o objetivo geral deste estudo:

1. Definir e descrever o contexto do tratamento de dados pessoais sob consideração;

2. Analisar os controlos que garantem o cumprimento dos princípios fundamentais: necessidade e proporcionalidade de processamento e proteção dos direitos dos titulares de dados;

3. Avaliar os riscos de privacidade associados à segurança dos dados e garantir que eles sejam tratados adequadamente;

4. Documentar formalmente a validação da AIPD em vista dos factos anteriores conhecidos ou decidir revisitar as etapas anteriores.

4. Apresentação dos dados e discussão dos resultados

Neste capítulo são estudadas e respondidas as QD e a QC.

4.1. Processo de Gestão de Perfis de Acesso a dados pessoais no SIGDN-RH

A sociedade moderna depende cada vez mais da utilização de sistemas informáticos, sendo crucial garantir que os dados que estes sistemas tratam e armazenam estejam protegidos contra fugas de informação, garantindo que são utilizados somente para os fins a que se destinam e por quem de direito. Os sistemas de gestão de bases de dados são os principais guardiões de dados, armazenando e gerindo o acesso a estes dados nos sistemas informáticos. É sobre estes que incidem ameaças e riscos no que respeita a fugas de informação (Sobral, 2015). Ainda, a redação do RGPD inicia-se com o esclarecimento de que "a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental", considerando uma violação de dados pessoais, como uma "violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (Parlamento Europeu, 2016).

Uma política de controlo de acesso implementa-se através de mecanismos que tratam do acesso requerido pelo utilizador e a estrutura existente no sistema. Entre estes dois níveis existe um terceiro nível que preenche a lacuna existente entre estes dois níveis, no qual se encontra o modelo de controlo de acesso, que faz a ponte entre a política e o mecanismo de controlo de acesso (Hu & Scarfone, 2012).

De acordo com o RGPD, os Dados Pessoais consistem em qualquer informação relativa a uma pessoa singular identificada ou identificável (Titular dos Dados) (Parlamento Europeu, 2016). Os Dados Pessoais de todos os RH (ou Titulares dos Dados) da FA, disponíveis no SIGDN-RH "estão organizados em infotipos[6] e conjuntos de infotipos, com informação pessoal e organizacional" (A.3.1.1). O acesso aos mesmos através de um perfil de acesso, permite o tratamento de dados pessoais, ou seja, uma ou várias operações efetuadas por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição[7].

[6] Conjunto de informação relacionada entre si sobre o militar ou civil, que é organizada e apresentada num ou vários ecrãs conjugados (SGMDN, 2011).
[7] Diretiva n.º 12/CEMFA/2018, de 14 de junho.

Os perfis de acesso "estão organizados por uma matriz que cruza os perfis de estrutura com os perfis de autorização" (A.2.1.1), ou seja, por "macroprocessos, processos e estrutura organizacional, que depois derivam para os infotipos" (A.2.1.2). A Figura 1 apresenta os vários macroprocessos, relacionados com o ciclo de vida da pessoa na organização.

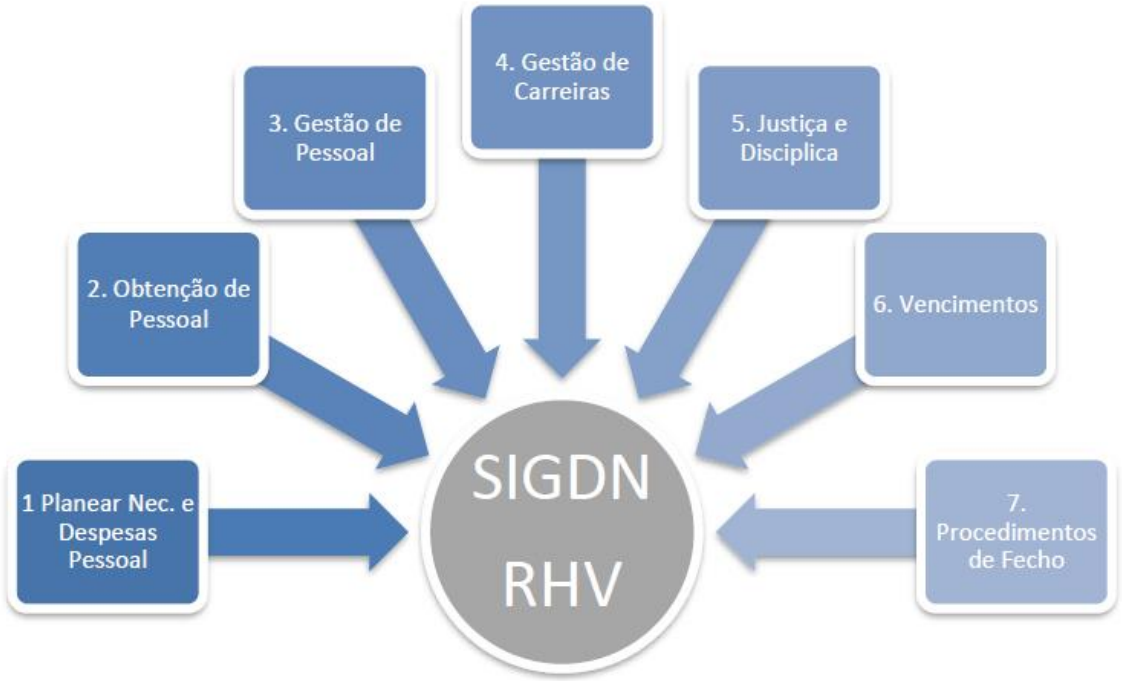

Figura 1 – Macroprocessos SIGDN-RH

(SIGDN/RHV, 2011)

Existe uma estrutura de perfis previamente definida por área funcional e tipo de função" (A.2.1.2). Em 16 de janeiro de 2020, o SIGDN-RH tinha 273 utilizadores da FA, distribuídos de acordo com o Quadro 1.

Quadro 1 – Utilizadores do SIGDN-RH

Tipologia	Total	Tipologia	Total
Áreas de Pessoal	98	JSFA	3
Secretariados	17	Consulta	8
Gestores SIG para Área de RH	9	DP-RD + AD HOC QUERY	2
CRFA	11	SR	3
Formação	1	DP-RPC + AD HOC QUERY	1
SJD	6	Auditoria e contabilidade	7
SDFA	1	Chefia da Repartição de Abonos	3
DP-RC	5	Processadores/Verificadores da RA	10
DP-RCP	10	Chefia de Repartição / Secção SAF	2
DP-RPC	7	Processadores SAF	6
DP-RD	13	Processadores Unidade	48
SAS	0	Repartição de Gestão Orçamental	2

Fonte: Repartição de Dados e Proteção Social, *email*, 16 de janeiro de 2020

"A gestão de acessos ao SIGDN-RH é baseada na ocupação de função/cargo, em consonância com o estabelecido na Diretiva 06/2017 do GEN CEMFA – Gestão Orgânica do SIGDN na FA, que preconiza o modelo de gestão/governação daquele sistema na FA, nomeadamente a gestão de utilizadores (…)" (A.1.1.4), no entanto, "não existe uma lista pré-definida de funções/cargo que podem ter acesso ao SIGDN-RH. A concessão do acesso é avaliada caso a caso, consoante a informação presente no pedido" (A.1.1.5). "O ADIAP é o responsável por efetuar a gestão dos utilizadores das aplicações/módulos da área de Pessoal (…) em estreita coordenação com elementos da área de pessoal com responsabilidades atribuídas nesta matéria" (A.1.2.1).

O processo de criação de perfil de utilizador do SIGDN-RH encontra-se explanado em fluxograma no Apêndice D, o qual resulta das várias entrevistas realizadas[8] e da Diretiva n.º 06/2017, do CEMFA, no entanto, "não existe uma política relativa à criação de novos utilizadores" no SIGDN-RH (C.1.3), uma vez que, a referida Diretiva ainda não foi atualizada, face à entrada em funcionamento do módulo de RH em 2018. Apesar disso, o fluxograma agora apresentado deve ser entendido como a "regra, estando ainda em falta a nomeação dos Delegados de Informação Locais" (A.1.2.11). O processo de pedido de alteração do perfil é igual, no entanto, os cancelamentos de autorização de acesso têm resultado de procedimentos informáticos controlados pela Administração de Sistemas Aplicacionais (C.5.6), assim como de auditorias periódicas de utilizadores, que cessaram as suas funções (A.1.2.8), apesar de estar "determinado que sempre que o utilizador deixe de desempenhar as funções que deram origem ao perfil atribuído, as chefias devem comunicar" (A.1.2.9).

Pelo exposto, e em resposta à QD 1: *Em que consiste o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?*, pode-se afirmar que este processo consiste num mecanismo entre o utilizador e a estrutura de dados do SIGDN-RH, que garante que os Dados Pessoais dos Titulares de Dados da FA, apenas são passíveis de tratamento pelos utilizadores, de acordo com as suas funções e posição na estrutura organizacional da FA. Através de um conjunto de procedimentos refletidos no fluxograma em Apêndice D, pretende-se controlar o acesso a toda a informação e funcionalidades disponíveis no SIGDN-RH, com vista à proteção dos direitos dos titulares dos dados.

[8] Conforme Apêndice C – A.1.2.

4.2. **Conformidade com os princípios fundamentais do RGPD**

Além de uma descrição das operações de tratamento e sua finalidade, uma AIPD inclui uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos (Parlamento Europeu, 2016).

O artigo n.º 5.º do RGPD identifica os seguintes princípios fundamentais: Licitude, Lealdade e Transparência; Propósito Limitado; Minimização dos Dados; Exatidão; Limitação da Conservação; Integridade e Confidencialidade, e por fim, Responsabilidade (Parlamento Europeu, 2016).

4.2.1. Necessidade

Face ao objetivo do tratamento, a necessidade de segurança dos dados, assim como a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, presente no Principio da Integridade e Confidencialidade, são os valores a reter. Adicionalmente, o Princípio da Exatidão exige que os dados sejam exatos e atualizados sempre que necessário, e em caso de inexatidão, prontamente apagados ou retificados (Parlamento Europeu, 2016). A Chefe da Divisão de Comunicações e Sistemas de Informação do Estado-Maior da FA (EMFA) acrescenta que a confidencialidade dos dados pessoais ganhou importância crescente com a aplicação do RGPD, que veio imprimir acrescida relevância à necessidade de proteção dos dados pessoais das pessoas singulares (B.1.3).

Assim, e em resposta à QD 2.1: *Qual o grau de necessidade do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?*, pode-se concluir que existe total necessidade de existência deste processo, por forma a proteger o acesso aos dados pessoais disponíveis no SIGDN-RH, e consequentemente, os direitos das pessoas singulares, cumprir vários princípios fundamentais e reduzir o risco de violação de dados pessoais.

4.2.2. Proporcionalidade

Os dados recolhidos devem ser objeto de um tratamento lícito, leal e transparente, assim como, utilizados apenas para a finalidade determinada, garantindo assim a sua adequabilidade ou minimização (Parlamento Europeu, 2016).

Segundo os vários interlocutores entrevistados, os dados pessoais solicitados no pedido de autorização (Quadro 2) são adequados e proporcionais à finalidade pretendida,

enquadrando-se o tempo de resposta nos requisitos, apesar da FA ser um utilizador recente do sistema, advindo daí algumas necessidades de readaptação[9].

Quadro 2 – Dados solicitados no pedido de acesso

NIP	Nome Completo
Posto/Especialidade	Função
Unidade	Telefone de Serviço
E-Mail	Perfil de Referência*
Identificação do Chefe	Data do Pedido
* User ID e NIP do utilizador com perfil semelhante ao pretendido, caso não exista, indicar módulos e transações necessárias.	

Relativamente à gestão da informação dos utilizadores, fora do SIGDN-RH, a identificação do acesso está integrada com vários dados, inclusive o NIP, e no sistema, apenas está integrado com o posto, nome, função e unidade do utilizador, no entanto, tecnicamente não existe nenhuma ligação ao colaborador de RH (A.3.2).

Pelo exposto, e em resposta à QD 2.2: *Qual o grau de proporcionalidade do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?*, afirma-se que, face aos dados recolhidos, o processo é adequado e proporcional ao objetivo definido para o mesmo.

4.2.3. Proteção dos direitos dos titulares dos dados

O Capítulo III do RGPD identifica os direitos dos titulares dos dados, dividindo-os em cinco secções: Transparência e regras para o exercício dos direitos dos titulares dos dados; Informação e acesso aos dados pessoais; Retificação e apagamento; Direito de oposição e decisões individuais automatizadas; e Limitações.

Não é pelo facto de alguém entregar dados pessoais a uma organização que deixa de ser o proprietário ou titular dos mesmos; e quem os recebe tem o dever de respeitar essa titularidade. No entanto, os direitos não são absolutos e podem estar limitados pela segurança, defesa, justiça, bem-estar social e económico, que constituem a "espinha dorsal" das sociedades democráticas (Antunes, 2018, p. 43 e 51).

[9] Conforme Apêndice C – B.1 e B.2.

A FA encontra-se a desenvolver várias ações conducentes à conformidade com o RGPD, nomeadamente ao nível de políticas e doutrina, definição de procedimentos e responsabilidades para exercício dos direitos dos titulares, revisão e atualização de processos e formação/sensibilização dos utilizadores[10]. É opinião de vários entrevistados, que apesar do RGPD e SIGDN-RH serem recentes, os utilizadores do sistema são os mesmos do anterior, tendo-se mantido o rigor das políticas organizacionais e o nível de consciencialização da sensibilidade e natureza dos dados pessoais[11].

Pela análise efetuada, e em resposta à QD 2.3: *Qual o grau de proteção dos direitos dos titulares dos dados no processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?*, considera-se que, embora não exista um documento que defina os procedimentos para este processo e a FA esteja numa fase de adaptação ao RGPD e SIGDN-RH, os direitos dos titulares dos dados continuam protegidos, atendendo ao nível geral de consciencialização da sensibilidade e natureza dos dados pessoais.

4.3. **Riscos associados ao processo de Gestão de Perfis de Acesso**

O RGPD exige que os responsáveis pelo tratamento apliquem medidas adequadas para assegurar e comprovar a sua conformidade, tendo em conta, a avaliação dos riscos para os direitos e liberdades das pessoas singulares, cuja gravidade e probabilidade podem ser variáveis (Parlamento Europeu, 2016).

Um risco é um cenário que descreve um acontecimento e as respetivas consequências, estimado em termos de probabilidade e gravidade. A probabilidade expressa a possibilidade de ocorrer um risco, estimada em termos do nível de vulnerabilidades dos ativos de suporte e do nível de recursos das fontes de risco para explorá-los. A gravidade representa a magnitude de um risco e depende principalmente da natureza prejudicial dos possíveis impactos sobre os titulares dos dados (Figura 2). Em ambas, os controles existentes, planeados ou adicionais (devidamente justificados) devem ser tidos em consideração (CNIL, 2018b).

[10] Conforme Apêndice C – C.4.1, C.1.12 e C.5.11.
[11] Conforme Apêndice C – C.6.

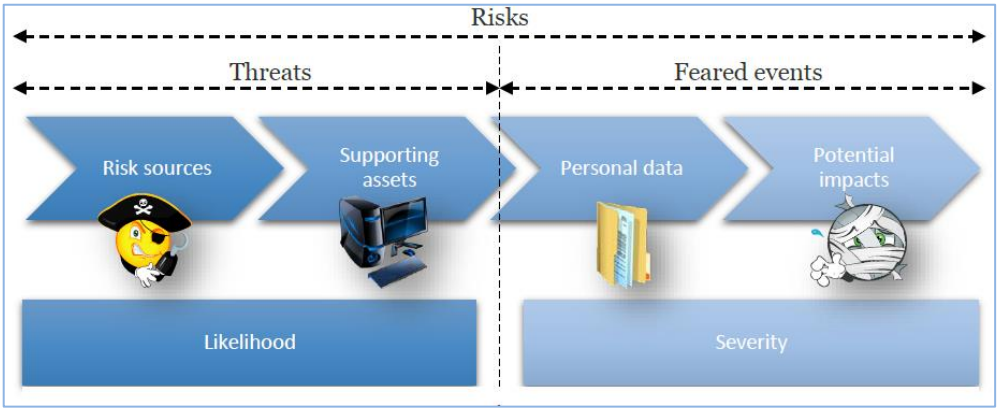

Figura 2 – Componentes do Risco

(CNIL, 2018a)

Uma AIPD ao abrigo do RGPD é um instrumento da organização que visa gerir os riscos para os direitos dos titulares dos dados e, como tal, avalia-os na perspetiva destes últimos (GT Art.º 29.º, 2017). Importa determinar a origem, natureza e particularidade desses riscos, podendo a sua probabilidade e gravidade variar, de acordo com o Quadro 3, por forma a definir uma estratégia de priorização e definição de implementação de controlos mitigatórios (Parlamento Europeu, 2016).

Quadro 3 – Classificação dos Riscos

	Probabilidade
Insignificante	Não parece possível que as fontes de risco selecionadas materializem a ameaça explorando as vulnerabilidades.
Limitada	Parece difícil para as fontes de risco selecionadas materializarem a ameaça explorando as vulnerabilidades.
Significativa	Parece possível que as fontes de risco selecionadas materializem a ameaça explorando as vulnerabilidades.
Máxima	Parece extremamente fácil para as fontes de risco selecionadas materializarem a ameaça, explorando as vulnerabilidades.
Impacto	**Gravidade**
Insignificante	Os titulares dos dados não serão afetados ou poderão encontrar alguns inconvenientes, que serão superados sem qualquer problema.
Limitado	Os titulares de dados podem encontrar inconvenientes significativos, que poderão superar apesar de algumas dificuldades.
Significativo	Os titulares de dados podem encontrar consequências significativas, que devem ser capazes de superar, embora com dificuldades reais e graves.
Máximo	Os titulares dos dados podem encontrar consequências significativas, ou mesmo irreversíveis, que podem não superar.

Fonte: Adaptado a partir de CNIL (2018b)

Por forma a avaliar os riscos de uma forma dinâmica, o *software* PIA e respetiva Base de Conhecimento, desenvolvidos pela CNIL (2019) (2018b), divide os riscos em três categorias: acesso ilegítimo, modificação indesejada e desaparecimento dos dados, possibilitando assim, a introdução das ameaças, fontes de riscos, impactos e controlos de

mitigação, e também estimar a probabilidade e o impacto se os riscos ocorrerem. Tendo por base esta metodologia, assim como a análise documental e conteúdo das entrevistas[12], os Quadros 4, 5 e 6, apresentam as ameaças, fontes de risco do processo e possíveis impactos.

A CNIL (2018b) apresenta várias consequências em caso de ocorrência de um cenário de risco, e no caso de acesso ilegítimo, a consequência pode ser nula, ao nível da alteração da localização do arquivo, redistribuição dos dados e ainda ao nível da hipótese de uso indevido da informação. A modificação indesejada de dados pode originar informação enviesada ou uso incorreto da mesma, originando erros ou mau funcionamento do processo. O desaparecimento de dados, além do referido anteriormente, pode originar um bloqueio do processo ou serviço. Assim, os impactos possíveis podem ser ao nível pessoal, originando violações de dados pessoais, ou ao nível organizacional, prejudicando a eficácia e eficiência dos processos e a qualidade da informação disponível, inclusive noutros sistemas de informação que dependem do SIGDN-RH.

Uma ameaça é um procedimento que compreende uma ou mais ações individuais em dados que suportam ativos, usado intencionalmente ou não, por fontes de risco e pode causar um evento não desejado. Para qualquer das tipologias de risco, as ameaças podem estar ao nível do hardware, software, formas de comunicação digital ou documental e das pessoas (CNIL, 2018b). O Quadro 4 apresenta as várias ameaças identificadas no decorrer da análise de conteúdo das entrevistas[13], interligando-as com os vários riscos, atendendo às diferentes consequências em caso de ocorrência de um cenário de risco, apresentadas pela CNIL (2018b).

Quadro 4 – Ameaças por Risco

Ameaça	Acesso Ilegítimo	Modificação Indesejada	Desaparecimento dos dados
Política desatualizada de gestão de acessos ao SIGDN-RH	**X**	**X**	**X**
Formação/sensibilização do utilizador	**X**	**X**	**X**
Ausência de *Identity Management*	**X**		
Perfil inadequado às funções do utilizador	**X**	**X**	**X**
Ausência de informação de pedidos recusados	**X**		
Forma de comunicação	**X**	**X**	**X**

A Diretiva n.º 06/2017, do CEMFA, ainda não foi atualizada, face à entrada em funcionamento do módulo de RH em 2018, nomeadamente ao nível dos procedimentos para gestão do acesso a toda a informação e funcionalidades disponíveis no SIGDN-RH (C.1.12).

[12] Conforme Apêndice C – C.1, C.2 e C.3.
[13] Conforme Apêndice C – C.1.

Apesar de existir um sistema de autenticação centralizado e de gestão de acessos (Micro Focus iManager), o mesmo não integra o SIGDN-RH, sendo a gestão de acessos feita de forma isolada e diferenciada para cada SI (C.1.1). A formação e sensibilização dos utilizadores é uma necessidade identificada[14] na FA e um fator importante em qualquer processo que envolva intervenção humana. A atribuição de um perfil inadequado às funções do utilizador pode originar um acesso ou alteração de dados, atendendo às múltiplas combinações de roles que o sistema permite, e ao facto da atribuição de perfis não ser automática, existindo o risco da ação humana em dar mais acessos do que a pessoa necessita (C.1.14). A ausência de um arquivo dos pedidos de acesso, com registo do motivo de indeferimento, pode originar uma incorreta análise dos pedidos subsequentes. A forma de comunicação é uma ameaça sempre presente em qualquer situação que envolva transmissão de dados entre diferentes intervenientes ou SI, como acontece no decorrer dos procedimentos do processo em análise, identificados no Apêndice D.

As fontes de risco podem causar um risco de forma deliberada ou acidental, e ser de natureza humana, interna ou externa à organização, ou ainda de natureza não humana (CNIL, 2018b). O Quadro 5 apresenta as várias fontes de risco identificadas[15] no processo em análise.

Quadro 5 – Fontes de Risco

Fonte de Risco	Acesso Ilegítimo	Modificação Indesejada	Desaparecimento dos dados
Utilizador do SIGDN-RH	**X**	**X**	**X**
Concurrent Employement	**X**	**X**	**X**
Entidade/Pessoa externa à FA	**X**	**X**	**X**
Matriz de Perfil de Acesso	**X**	**X**	**X**

A funcionalidade *Concurrent Employment* permite que determinada informação de RH esteja disponível para consulta e alteração por outras entidades do MDN, onde o militar desempenhe funções temporariamente, no entanto, "possibilita a alteração indesejada de dados, não por via do perfil de acesso, mas sim pela forma como a funcionalidade está a ser aplicada, ao nível dos procedimentos" (C.2.4).

O acesso à informação necessária para a correta execução das tarefas do utilizador é garantida através de uma matriz de perfil de acesso "onde estão identificados todos os possíveis perfis, atividades e infotipos que cada utilizador necessita para o desempenho das

[14] Conforme Apêndice C – C.1.15 e C.5.11.
[15] Conforme Apêndice C – C.2.

suas tarefas diárias" (A.2.1.3), "a qual posteriormente tem vindo a ser alvo de correção, manutenção e atualização face a novas necessidades" (C.2.1), logo, consequentemente, a referida matriz pode ser considerada uma fonte de risco, em caso de alguma incorreção.

As pessoas internas (Utilizadores do SIGDN-RH) e externas à FA podem ser consideradas como uma fonte de risco, uma vez que, por insuficiência na sua formação pessoal, as pessoas facilitam perante a exigência do exercício das suas funções (C.1.15).

As conjugações das ameaças com as fontes de risco podem originar um cenário de risco, advindo daí algumas consequências ou impactos. As consequências apresentadas no Quadro 6 em caso de ocorrência de um cenário de risco, decorrem das ameaças e fontes de risco identificadas anteriormente, tendo também por base os vários exemplos apresentados pela CNIL (2018b).

Quadro 6 – Impactos por Risco

Impacto	Acesso Ilegítimo	Modificação Indesejada	Desaparecimento dos dados
Utilização ilegítima de dados pessoais	**X**		
Divulgação de dados pessoais	**X**		
Violação de dados pessoais	**X**	**X**	**X**
Informação incorreta		**X**	**X**
Informação dos sistemas dependentes do SIGDN-RH		**X**	**X**
Ausência de informação relevante			**X**
Impedimento de acesso ao SIGDN-RH			**X**

Tendo por base a classificação de riscos presente no Quadro 3, questionaram-se os principais intervenientes do processo em análise, acerca da sua estimativa de probabilidade e gravidade dos riscos apresentados, tendo-se obtido as respostas constantes no Quadro 7. Importa referir que, de acordo com o conceito de risco e as suas componentes identificadas na Figura 2, a probabilidade foi estimada atendendo às ameaças e fontes de risco identificadas, e a gravidade quanto aos seus impactos.

Quadro 7 – Estimativa de Risco

	Probabilidade		Gravidade	
	cGADIAP, entrevista por *email*, 15 de janeiro de 2020	cRDPS, entrevista por *email*, 17 de janeiro de 2020	cGADIAP, entrevista por *email*, 15 de janeiro de 2020	cRDPS, entrevista por *email*, 17 de janeiro de 2020
Acesso Ilegítimo	3-Significativa	2-Limitada	2-Limitado	1-Insignificante
Modificação Indesejada	3-Significativa	3-Significativa	3-Significativo	2-Limitado
Desaparecimento dos dados	4-Máxima	3-Significativa	3-Significativo	2-Limitado

Assim, e em resposta à QD 3: *Qual a avaliação dos riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?*, os Quadros 4, 5 e 6 apresentam as ameaças, fontes de risco do processo e possíveis impactos dos três principais riscos seguidos pela CNIL, sendo os mesmos, avaliados pelos principais intervenientes do processo, quanto a sua gravidade e probabilidade no Quadro 7.

4.4. Medidas de mitigação dos riscos associados ao processo de Gestão de Perfis de Acesso

Neste capítulo, importa identificar medidas mitigadoras dos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais, demonstrando a conformidade com o RGPD, tendo em conta os direitos e os legítimos interesses dos titulares dos dados.

Na sua análise, Almeida (2018) identificou que a FA pretende adotar, sempre que possível, as medidas de proteção e segurança de dados pessoais sugeridas pelo RGPD, nomeadamente a pseudonimização, a minimização e também a encriptação de dados.

Além destas legalmente previstas, e tendo por base o conhecimento desenvolvido pela CNIL (2018b) e pela ISO (2013) (2018b), assim como a análise das entrevistas[16] realizadas, apresenta-se um conjunto de medidas, algumas já implementadas, adequadas ao tratamento de dados em questão (Quadro 8), assim como uma descrição das mesmas.

Quadro 8 – Medidas mitigadoras

	Medida	Descrição
M1	**Responsabilidades e Procedimentos**	- Desenvolvimento de ações conducentes à conformidade com o RGPD, nomeadamente ao nível de políticas e doutrina; - Definição de procedimentos e responsabilidades para exercício dos direitos dos titulares.
M2	**Controlo de utilizadores ativos**	- Implementação de sistema de *Identity Management*; - Análise periódica dos utilizadores ativos no sistema, e consequente desativação daqueles que já não reúnem condições para tal; - Bloqueio de acesso, após três tentativas de login falhadas.
M3	**Rastreabilidade (Gestão de log)**	- Controlo das ações dos utilizadores em tempo real e diferido; - Registo de logs de tentativas falhadas de login; - Expiração do Login por inexistência de ação.
M4	**Backups de informação**	- Backups totais e parciais, diários e semanais.
M5	**Manutenção do sistema**	- Responsabilidade de manutenção do sistema repartida entre a SGMDN e FA; - Maior autonomia do Ramo para a gestão e criação de utilizadores.
M6	**Segurança de rede interna**	- Regras definidas pelo MDN e FA para utilização de rede interna; - Inclusão de fatores adicionais de autenticação.

[16] Conforme Apêndice C – C.4 e C.5.

M7	**Controlo de acesso físico**	- Espaço físico inserido em infraestruturas militares, com regras de acesso específicas.
M8	**Proteção contra fontes não-humanas de riscos**	- Inspeção periódica de segurança e prevenção de acidentes nas áreas militares.
M9	**Supervisão**	- Nomeação do EPD; - Inspeções periódicas (Conformidade com o RGPD); - Constituição do Grupo Coordenador de Gestão da Informação (GCGI); - Relatório anual da atividade dos utilizadores.
M10	**Revisão e Atualização de Diretivas**	- Revisão e Atualização da Diretiva n.º 06/2017, do CEMFA (Gestão Orgânica do SIGDN na FA); - Definição do fluxo de informação do processo de gestão de perfis de acesso ao SIGDN-RH.
M11	**Delegado de Informação Local**	- Identificação dos Delegados de Informação Local para o SIGDN-RH.
M12	**Formação/Sensibilização**	- Formação/Sensibilização dos utilizadores (inicial e ad-hoc); - Boas práticas na definição de Password.
M13	**Matriz de perfil de acesso**	- Revisão da estrutura de perfis previamente definida por área funcional e tipo de função; - Reestruturação da matriz de perfil.
M14	**Arquivo de pedidos**	- Definição de procedimentos para arquivo de pedidos de acesso que contenham dados pessoais para garantir o seu valor legal, durante o período necessário.
M15	**Sistema de *Provisioning***	- Integração dos dados de RH com os dados do Utilizador (Acessos inerentes à posição).

As descrições sublinhadas no Quadro 8 correspondem às medidas agora sugeridas para implementação futura, enquanto que as restantes já se encontram implementadas na FA. Os parágrafos seguintes justificam as medidas apresentadas no referido Quadro.

A definição de um EPD, constituição de um grupo de monitorização na sua dependência e a definição de papéis, responsabilidades e interações entre os principais intervenientes nesta área (M10, M11), permitem que a organização obtenha a capacidade de gerir e controlar a proteção de dados pessoais na sua posse. Ainda, este grupo deve reunir regularmente, pelo menos uma vez por ano, para definição e revisão de objetivos, assim como inspecionar periodicamente as operações de tratamento de dados pessoais da organização (M9) (CNIL, 2018b).

Os utilizadores deverão seguir as boas práticas da organização no uso de informação restrita para autenticação, por forma a responsabilizar os mesmos pela proteção dos dados de login (ISO, 2013). Também os sistemas de gestão de password devem ser interativos e assegurar a utilização de senhas com qualidade (M12). A realização de sessões de informação e de formação são necessárias para implementação de uma estrutura a vários níveis para gestão do risco, devendo a organização assegurar que aqueles que são

responsabilizados estão aptos para cumprir a sua função atribuindo-lhes autoridade, tempo, formação e treino, recursos e competências suficientes para assumirem a sua responsabilização (M1 e M12) (ISO, 2018b). Os procedimentos para exercício dos direitos dos titulares dos dados devem estar estabelecidos e divulgados, e o processo não deve ser desencorajador nem acarretar custos para as pessoas (M1) (CNIL, 2018b). A recente publicação do Despacho n.º 117/2019, do CEMFA, de 30 de dezembro, veio definir os procedimentos relativos ao exercício dos direitos dos titulares dos dados pessoais, à participação de violações de dados pessoais e aos pedidos de acesso a dados pessoais efetuados por terceiros.

O responsável pela gestão do sistema deve rever regularmente os direitos de acesso dos utilizadores, por forma a limitar o acesso à informação ou recursos de processamento da mesma (M2) (ISO, 2013). Também, os utilizadores apenas devem ter acesso à rede ou aos serviços de rede, para os quais, foi especificamente autorizado o seu uso.

O método de autenticação deve ser adequado ao contexto, nível de risco e robustez esperada. Um forte mecanismo de autenticação requer um mínimo de dois fatores de autenticação separados, entre algo tangível e uma caraterística específica do indivíduo. No caso de uma workstation partilhada, deve ser incluída uma segunda autenticação no sistema de dados pessoais (M6) (CNIL, 2018b).

A gestão do software, hardware e redes de comunicação deve reduzir a possibilidade de afetar adversamente os dados pessoais guardados num sistema informático, devendo ser assinados contratos de tratamento com subcontratantes[17], estabelecendo todos os aspetos estipulados no RGPD, como por exemplo: duração, âmbito, finalidade, instruções de tratamento documentadas, autorização prévia onde um subcontratante está envolvido, fornecimento de qualquer documentação que comprove a conformidade com o RGPD e notificação imediata de qualquer violação de dados (M5) (CNIL, 2018b).

Uma política de controlo de acesso deve ser estabelecida, documentada e revista, com base nos requisitos de negócio e segurança de informação da organização, devendo ser implementado um processo formal de registo e cancelamento do mesmo para definir os direitos de acesso, os quais devem ser restritos e controlados (M10) (ISO, 2013).

A separação entre tarefas e áreas de responsabilidade na gestão dos perfis de utilizador, preferencialmente de forma centralizada, limita o acesso exclusivo a pessoas autorizadas,

[17] Pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do responsável pelo tratamento (Parlamento Europeu, 2016).

aplicando princípios de minimização de dados e privilégios. A gestão de privilégios e tarefas por perfil, deve ser adequada ao requerido e revista regularmente (M2 e M13) (CNIL, 2018b).

Um sistema de *Provisioning* é um automatismo que melhora a "gestão de pessoas versus utilizadores do sistema, ou seja, enquanto uma pessoa estiver associada a uma posição, tem os acessos inerentes à mesma" (C.5.15). O Chefe da Secção de Administração de Sistemas de Informação da Direção de Comunicações e Sistemas de Informação (DCSI) (C.4.9) também identifica a "automatização na atribuição e cessação de acessos", como uma melhoria no processo (M15).

Para garantir a disponibilidade e/ou integridade dos dados pessoais, mantendo a sua confidencialidade, devem ser feitos backups regularmente, com base nos requisitos de integridade definidos pela organização (M4) (CNIL, 2018b).

A rastreabilidade (gestão de logs) garante que as consultas e ações realizadas pelos utilizadores do tratamento de dados sejam registradas e atribuídas, de modo que seja possível fornecer evidências durante as análises periódicas e, se necessário, estabelecer um sistema que detete atividades anormais automaticamente (M3) (CNIL, 2018b).

O controle de acessos a espaços físicos, através da criação de áreas de segurança e regras de acesso às mesmas, limita o risco de acesso de pessoas não autorizadas obterem acesso físico a dados pessoais (M7) (CNIL, 2018b).

Como garantia de cumprimento dos princípios do RGPD e proteção dos direitos dos titulares, e por forma a que os dados pessoais não sejam retidos por mais tempo do que o necessário, devem ser definidos para cada categoria de dados, os tipos, procedimentos e tempos de arquivo, adequados ao objetivo do processamento e/ou requisitos legais. Um período de armazenamento deve ser definido para cada tipo de dados e justificado pelos requisitos legais e/ou necessidades de tratamento (M14) (CNIL, 2018b).

A segurança geográfica e de instalações, assim como as boas práticas de prevenção de acidentes, nas áreas onde os dados pessoais são processados ou armazenados, são importantes para reduzir ou evitar riscos associados a fontes não humanas (M8) (CNIL, 2018b).

A gestão de risco é relevante e transversal à organização, porque permite controlar os riscos que todas as operações de tratamento de dados pessoais representam sobre os direitos e liberdades dos titulares dos dados (CNIL, 2018b).

O Quadro 9 associa as medidas identificadas por risco.

Quadro 9 – Medidas mitigadoras por Risco

	Medida	Acesso Ilegítimo	Modificação Indesejada	Desaparecimento dos dados
M1	Responsabilidades e Procedimentos	**X**		
M2	Controlo de utilizadores ativos	**X**	**X**	**X**
M3	Rastreabilidade (Gestão de log)	**X**	**X**	**X**
M4	Backups de informação		**X**	**X**
M5	Manutenção do sistema		**X**	**X**
M6	Segurança de rede interna	**X**		**X**
M7	Controlo de acesso físico	**X**		**X**
M8	Proteção contra fontes não-humanas de riscos		**X**	**X**
M9	Supervisão	**X**		
M10	Revisão e Atualização de Diretivas	**X**	**X**	
M11	Delegado de Informação Local	**X**		
M12	Formação/Sensibilização	**X**	**X**	**X**
M13	Matriz de perfil de acesso	**X**	**X**	**X**
M14	Arquivo de pedidos	**X**		
M15	Sistema de *Provisioning*	**X**		

Em resposta à QC: *De que forma, os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, podem ser mitigados, respeitando os direitos dos titulares dos dados definidos pelo RGPD?*, apresenta-se um conjunto de medidas mitigadoras por risco, adequadas ao tratamento de dados em questão, conforme se pode verificar nos Quadros 8 e 9.

5. Conclusões

As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais e deverá ser reforçada a segurança jurídica e prática para as pessoas singulares, os operadores económicos e as autoridades públicas. (Parlamento Europeu, 2016).

A Lei de Proteção de Dados veio assegurar a execução do RGPD, na ordem jurídica nacional, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos.

A presente investigação tem por objeto, o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, no âmbito da avaliação do impacto da implementação do RGPD. Apesar da FA possuir outros sistemas que concorrem para a gestão de RH, esta investigação debruça-se apenas neste, por ser a principal base de dados de RH. O SIGDN-RH constitui-se como uma ferramenta tecnológica e um instrumento de gestão integrada da Defesa que potencia a adoção de procedimentos normalizados dentro do MDN e das FFAA. Adotado pela FA em 01 de outubro de 2018, este SI contêm os dados pessoais de cerca de 140 mil militares e trabalhadores civis. O acesso a estes dados pessoais é garantido através de um perfil de acesso, o qual é definido pela área funcional e tipo de função do utilizador.

Metodologicamente, este estudo carateriza-se por um raciocínio dedutivo, alicerçado numa estratégia de investigação qualitativa, baseada na análise documental e no desenvolvimento de entrevistas semiestruturadas e respetiva análise de conteúdo, sob as regras base de uma AIPD. Uma AIPD é um processo concebido para descrever o tratamento, avaliar a sua necessidade e proporcionalidade, 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.

A fim de estudar o OG, e a correspondente QC que norteou esta investigação, foram elencados três OE, operacionalizados em cinco QD.

Neste âmbito, para responder à QD1 e, consequentemente, ao OE1: *Caracterizar o processo de gestão de perfis de acesso aos dados pessoais dos Recursos Humanos da Força Aérea, presentes no SIGDN-RH*, identificou-se um conjunto de procedimentos e responsabilidades, por forma a caraterizar o processo de criação de perfil de utilizador do SIGDN-RH, tendo sido este posteriormente explanado em fluxograma no Apêndice D.

Também se verifica que a Diretiva n.º 06/2017, do CEMFA, (Gestão Orgânica do SIGDN na FA) ainda não foi atualizada, face à entrada em funcionamento do módulo de RH em 2018, e como ainda não existe uma lista pré-definida de funções/cargo que podem ter acesso ao SIGDN-RH, a concessão do acesso é avaliada caso a caso, consoante a informação presente no pedido.

Este processo consiste num mecanismo entre o utilizador e a estrutura de dados do SIGDN-RH, que garante que os Dados Pessoais dos Titulares de Dados da FA, apenas são passíveis de tratamento pelos utilizadores, de acordo com as suas funções e posição na estrutura organizacional da FA. Através de um conjunto de procedimentos refletidos no fluxograma em Apêndice D, pretende-se controlar o acesso a toda a informação e funcionalidades disponíveis no SIGDN-RH, com vista à proteção dos direitos dos titulares dos dados.

A fim de responder às QD2.1 e QD2.2, referentes ao OE2: *Analisar a conformidade com os princípios fundamentais: a necessidade e a proporcionalidade de processamento e a proteção dos direitos dos titulares dos dados pessoais dos RH da FA, presentes no SIGDN-RH*, analisou-se a adequabilidade do processo de gestão de perfis de acesso aos dados, face os objetivos definidos pelos vários normativos de gestão de informação e proteção de dados pessoais. Também, e como requisito essencial de uma AIPD, avaliou-se a necessidade deste tratamento de dados devido à sua suscetibilidade de implicar riscos elevados para os direitos e as liberdades das pessoas singulares. Assim, por forma a proteger o acesso aos dados pessoais disponíveis no SIGDN-RH, e consequentemente, os direitos das pessoas singulares, cumprir os Princípios da Integridade, Confidencialidade e Exatidão, e reduzir o risco de violação de dados pessoais, conclui-se que existe total necessidade de existência deste processo. Segundo os vários interlocutores entrevistados, os dados pessoais solicitados no pedido de autorização (Quadro 2) são adequados e proporcionais à finalidade pretendida, enquadrando-se o tempo de resposta nos requisitos, apesar da FA ser um utilizador recente do sistema, advindo daí algumas necessidades de readaptação.

Relativamente à QD2.3, referente ao OE2, embora não exista um documento que defina os procedimentos para este processo e a FA esteja numa fase de adaptação ao RGPD e SIGDN-RH, os direitos dos titulares dos dados estão protegidos, atendendo ao facto dos utilizadores deste SI serem os mesmos do anterior, tendo-se mantido o rigor das políticas organizacionais e o nível geral de consciencialização da sensibilidade e natureza dos dados pessoais. A recente publicação do Despacho n.º 117/2019, do CEMFA, de 30 de dezembro,

é exemplo deste esforço de adaptação, ao definir procedimentos relativos ao exercício dos direitos e à participação de violações de dados pessoais, por forma a respeitar os direitos dos titulares dos dados, elencados no Capítulo III do RGPD.

A resposta à QD3, e subsequentemente ao OE3: *Avaliar os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos Recursos Humanos da Força Aérea, presentes no SIGDN-RH,* importa reter que um risco, é um cenário que descreve um acontecimento e as respetivas consequências, estimado em termos de probabilidade e gravidade, assim como, uma AIPD ao abrigo do RGPD, é um instrumento da organização que visa gerir os riscos para os direitos dos titulares dos dados e, como tal, avalia-os na perspetiva destes últimos. Tendo por base a metodologia desenvolvida pela CNIL (2018b), assim como a análise documental e conteúdo das entrevistas, foram identificadas as ameaças, fontes de risco do processo e possíveis impactos, conforme se pode verificar na Figura 3, relacionando-os em três categorias de risco: acesso ilegítimo, modificação indesejada e desaparecimento dos dados. Os impactos possíveis podem ser ao nível pessoal, originando violações de dados pessoais, ou ao nível organizacional, prejudicando a eficácia e eficiência dos processos e a qualidade da informação disponível, inclusive noutros sistemas de informação que dependem do SIGDN-RH. Posteriormente, e tendo por base as ameaças, fontes de risco e impactos identificados, questionaram-se os principais intervenientes do processo em análise, acerca da sua estimativa de probabilidade e gravidade dos riscos apresentados, tendo-se obtido as respostas constantes no Quadro 7, realçando-se um nível de probabilidade máxima de desaparecimento de dados e um impacto insignificante em caso de acesso ilegítimo.

Face ao exposto, em resposta à QC, e ao correspondente OG: *Propor medidas de mitigação dos riscos para os direitos dos titulares dos dados, associados ao processo de gestão de perfis de acesso aos dados pessoais dos Recursos Humanos da Força Aérea, presentes no SIGDN-RH, no âmbito da implementação do RGPD*, além das medidas de proteção e segurança de dados pessoais sugeridas pelo RGPD, tendo por base o conhecimento desenvolvido pela CNIL (2018b) e pela ISO (2013) (2018b), assim como a análise das entrevistas realizadas, apresenta-se um conjunto de medidas (Figura 3), algumas já implementadas, adequadas ao tratamento de dados em questão e relacionadas por tipologia de risco. A gestão de risco é relevante e transversal à organização, porque permite controlar os riscos que todas as operações de tratamento de dados pessoais representam sobre os direitos e liberdades dos titulares dos dados (CNIL, 2018b).

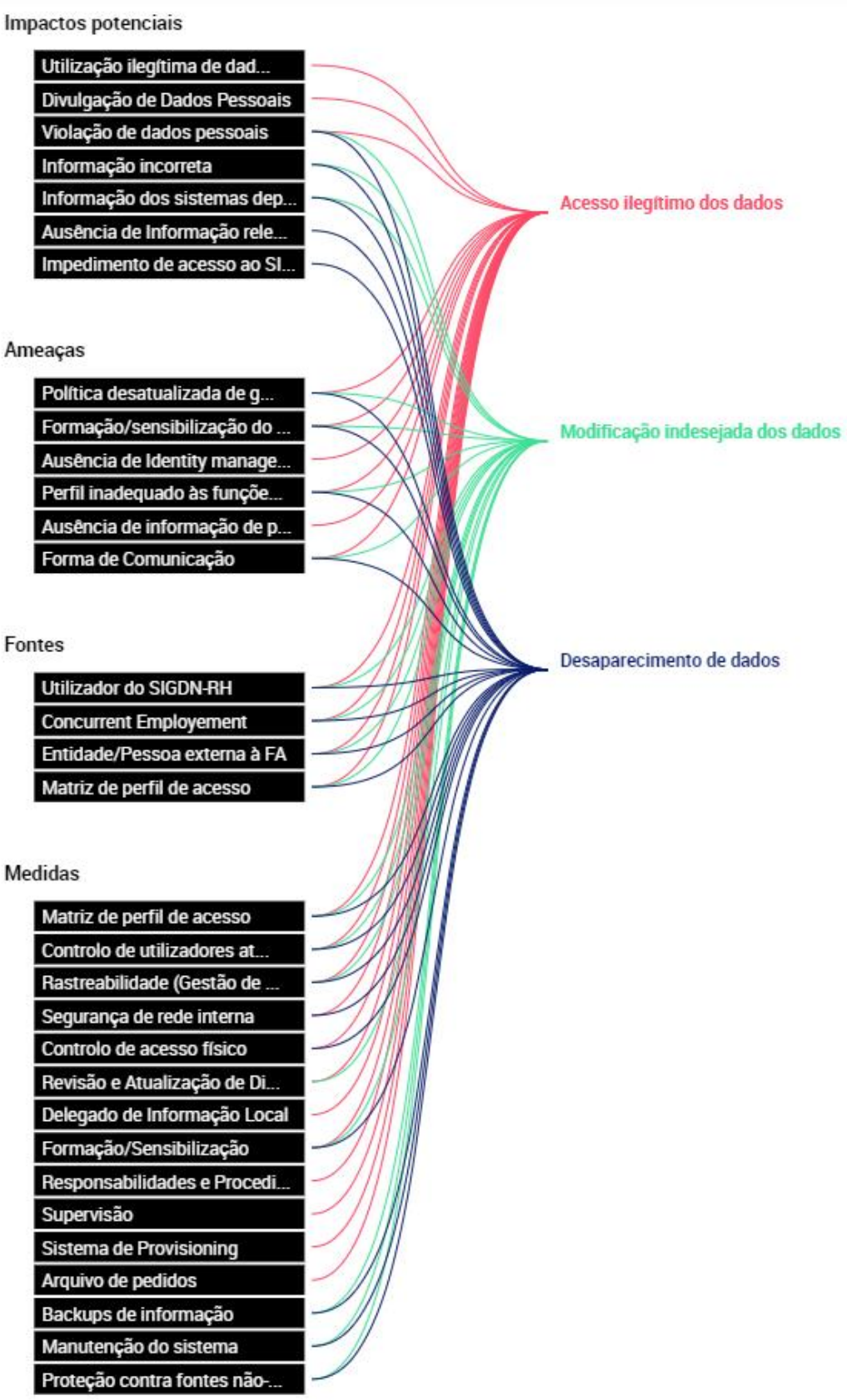

Figura 3 – Visão geral dos riscos

Estas medidas incluem as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais, demonstrando a conformidade com o RGPD, tendo em conta os direitos e os legítimos interesses dos titulares dos dados.

Neste seguimento, têm-se como principais **contributos para o conhecimento** decorrentes da presente investigação, o seguinte:

- Caraterização do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH;

- Verificação da sua conformidade com os princípios fundamentais: a necessidade e a proporcionalidade de processamento e a proteção dos direitos dos titulares dos dados pessoais;

- Avaliação dos riscos associados ao processo, e consequente identificação de medidas mitigadoras dos mesmos.

Durante a realização desta investigação existiram algumas **limitações**, nomeadamente o curto espaço temporal em que a mesma se desenvolveu, não permitindo uma análise mais profunda e, principalmente, uma validação destas medidas junto das entidades responsáveis pela implementação das mesmas.

No que respeita a **estudos futuros**, e atendendo ao facto deste tipo de avaliações de conformidade e análise de risco terem um carácter contínuo, julga-se pertinente efetuar a validação das medidas apresentadas no âmbito desta AIPD, relativamente à viabilidade financeira de implementação das mesmas, e caso necessário, a sua reformulação e adequação, face a novos factos ou condicionalismos. Ainda, atendendo à acrescida relevância relativa à necessidade de proteção dos dados pessoais das pessoas singulares, à transversalidade deste novo quadro legal e múltiplas implicações nas mais variadas áreas de gestão de RH da Organização, importa continuar a desenvolver análises de gestão de risco, por forma a garantir a conformidade com o RGPD.

Decorrente do presente trabalho de investigação, **recomenda-se** a análise das medidas agora apresentadas e consequente implementação ou melhoria das mesmas, priorizando as que contribuem para a diminuição da probabilidade máxima do risco de desaparecimento de dados, conforme estimado pelos intervenientes do processo em análise. Adicionalmente, também se considera que a revisão e atualização da Diretiva n.º 06/2017, do CEMFA (Gestão Orgânica do SIGDN na FA), e consequente definição do fluxo de informação do processo de gestão de perfis de acesso ao SIGDN-RH, é uma medida prioritária face à necessidade de proteger o acesso aos dados pessoais disponíveis no SIGDN-RH, e consequentemente, os

direitos das pessoas singulares, cumprir os vários princípios fundamentais e reduzir o risco de violação de dados pessoais.

Referências Bibliográficas

Almeida, I. F. (2018). *O Regulamento Geral sobre a Proteção de Dados: Impacto na Política da Gestão de Informação da Força Aérea.* Sintra: Academia da Força Aérea.

Antunes, L. (2018). *Pôr em Prática o RGPD - O que muda para nós? E para as Organizações?* Lisboa: FCA.

Commission Nationale de l'Informatique et des Libertés (2018a). *Privacy Impact Assessment (PIA) - Methodology*. França: Autor.

Commission Nationale de l'Informatique et des Libertés (2018b). *Privacy Impact Assessment (PIA) - Knowledge Bases*. França: Autor.

Commission Nationale de l'Informatique et des Libertés (2019). *The open source PIA software helps to carry out data protection impact assesment*. Retirado de https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Despacho n.º 117/2019, do CEMFA, de 30 de dezembro (2019). *Exercício dos direitos dos titulares dos dados pessoais, participação de violação de dados pessoais e acesso a dados pessoais por terceiros*. Lisboa: Força Aérea.

Diretiva n.º 12/CEMFA/2018, de 14 de junho (2018). *Proteção de Dados Pessoais na Força Aérea.* Lisboa: Força Aérea.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (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.

Hu, V. C., & Scarfone, K. (2012). *Guidelines for Access Control System Evaluation Metrics.* U.S. Department of Commerce: National Institute of Standards and Technology.

ISO/IEC 27000. (2018a). *Information technology - Security techniques - Information security management systems - Overview and vocabulary.* Suiça: International Organization for Standardization.

ISO/IEC 27001. (2013). *Information technology - Security techniques - Information security management systems – Requirements.* Suiça: International Organization for Standardization.

ISO 31000. (2018b). *Risk Management-Guidelines.* Suiça: International Organization for Standardization.

Lei n.º 58/2019, de 08 de agosto (2019). *Lei da Proteção de Dados.* Diário da República, 1.ª Série, 151. 3 a 40. Lisboa: Assembleia da República.

Parlamento Europeu. (2016). *Regulamento 2016/679 de 27 de Abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* União Europeia: Jornal Oficial das Comunidades Europeias.

Saldanha, N. (2019). *RGPD - Guia para uma Auditoria de Conformidade - Dados, Privacidade, Implementação, Controlo, Compliance.* Lisboa: FCA.

Santos, L., & Lima, J. (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (2.ª ed., revista e atualizada).* Lisboa: Instituto Universitário Militar.

Santos, V. (2018). *Criatividade em Sistemas de Informação.* Lisboa: FCA.

Secretaria-Geral do Ministério da Defesa Nacional. (2011). *SIGDN Recursos Humanos e Vencimentos. Business Blueprint (Desenho Conceptual).* Lisboa: Autor.

Sobral, L. M. (2015). *Análise do Controlo de Acesso num Sistema de Gestão de Base de Dados.* Beja: Escola Superior de Tecnologia e Gestão.

Apêndice A — Mapa Concetual

Objetivo Geral:	Propor medidas de mitigação dos riscos para os direitos dos titulares dos dados, associados ao processo de gestão de perfis de acesso aos dados pessoais dos Recursos Humanos da Força Aérea, presentes no SIGDN-RH, no âmbito da implementação do RGPD.					
Questão Central	De que forma, os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos Recursos Humanos da Força Aérea, presentes no SIGDN-RH, podem ser mitigados, respeitando os direitos dos titulares dos dados definidos pelo RGPD?					
Objetivos Específicos	**Dimensão**	**Questão Derivada**	**Conceito**	**Indicadores**	**Técnicas de recolha de dados**	**Técnicas de análise de dados**
OE1 Caracterizar o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH.	----------	**QD1** Em que consiste o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?	Processo de gestão de perfis de acesso	Definição do processo de gestão de perfis de acesso	Pesquisa documental Entrevistas semiestruturadas	Análise de Conteúdo
OE2 Analisar a conformidade com os princípios fundamentais: a necessidade e a proporcionalidade de processamento e a proteção dos direitos dos titulares dos dados pessoais dos RH da FA, presentes no SIGDN-RH.	Necessidade	**QD2.1 -** Qual o grau de necessidade do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?	Necessidade do processo de gestão de perfis de acesso	Grau de necessidade do processo de gestão de perfis de acesso	Pesquisa documental Entrevistas semiestruturadas	Análise de Conteúdo
	Proporcionalidade	**QD2.2** Qual o grau de proporcionalidade do processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?	Proporcionalidade do processo de gestão de perfis de acesso	Grau de proporcionalidade do processo de gestão de perfis de acesso		
	Proteção	**QD2.3** Qual o grau de proteção dos direitos dos titulares dos dados no processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?	Proteção dos direitos dos titulares dos dados	Grau de proteção dos direitos dos titulares dos dados		
OE3 Avaliar os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH.	----------	**QD3** Qual a avaliação dos riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH?	Riscos do processo	Probabilidade e gravidade dos riscos associados ao processo de gestão de perfis de acesso	Pesquisa documental Entrevistas semiestruturadas	Análise de Conteúdo

Apêndice B — Guiões das entrevistas semiestruturadas

Preâmbulo de Orientação

Em primeiro lugar gostaria de agradecer o seu tempo e disponibilidade para ajudar neste Trabalho de Investigação subordinado ao Tema "Regulamento Geral de Proteção de Dados: Impacto nos Sistemas de Informação de Recursos Humanos da Força Aérea", o qual tem como objetivo geral, a proposta de medidas de mitigação dos riscos para os direitos dos titulares dos dados, associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH, no âmbito da implementação do Regulamento Geral de Proteção de Dados (RGPD).

No âmbito da proteção de dados presentes num Sistema de Informação (SI), um processo de gestão de perfis de acesso constitui-se como, um conjunto de regras e procedimentos definidos pela organização para a gestão de autorização e perfis de acesso à informação disponível num SI, com vista à proteção dos direitos dos titulares dos dados.

O seu contributo, como interlocutor privilegiado nesta área de atividade, é de sobremaneira relevante para a investigação e as suas respostas às questões seguintes enriquecerão definitivamente o conteúdo deste trabalho.

As questões estão organizadas por várias áreas de interesse, e obedecem a uma metodologia de investigação que implica um foco na resposta. No entanto, agradeço qualquer tipo de contributo extra que entenda dar, mesmo que se desvie do âmbito das perguntas.

Questões

POLÍTICA DE AUTORIZAÇÃO E GESTÃO DE ACESSOS

1. Existe um sistema integrado e centralizado de gestão de acessos e controlo de identidades (Identity Management) na FA?
2. A gestão de acessos ao SIGDN-RH é baseada em políticas predefinidas e/ou em funções/cargos?
3. Existe uma política relativa à criação de novos utilizadores?
4. Existe uma política relativa ao cancelamento e apagamento de utilizadores?
5. Existe um manual de procedimentos que imponha e regule a análise periódica da atividade dos utilizadores do SIGDN-RH?

6. É efetuada uma revisão periódica das autorizações de acesso concedidas ao SIGDN-RH?

7. É efetuada uma revisão anual à atividade dos utilizadores do SIGDN-RH?

8. Os resultados desta revisão são comunicados a outras áreas da organização?

CARACTERIZAÇÃO DE DADOS DO SIGDN-RH

9. Os dados de RH da FA, disponíveis no SIGDN-RH, estão organizados de que forma?

10. Os dados disponíveis no SIGDN-RH estão disponíveis para outros sistemas de informação? Se sim, qual o processo e forma de transmissão desses dados?

11. Os dados disponíveis no SIGDN-RH estão disponíveis para outras entidades? Se sim, para que efeitos e/ou finalidades?

GESTÃO DE AUTORIZAÇÃO DE ACESSO

12. Existe um responsável definido e credenciado para a criação e alteração da estrutura dos perfis de acesso aos dados no SIGDN-RH?

13. Como estão organizados os perfis de acesso aos dados de RH, disponíveis no SIGDN-RH?

14. Quais os requisitos essenciais do utilizador para concessão de acesso aos dados no SIGDN-RH?

15. Quais os procedimentos do processo de autorização de acesso a dados no SIGDN-RH?

16. Os dados pessoais do utilizador, solicitados no pedido de autorização, são adequados e proporcionais à finalidade pretendida?

17. O tempo de resposta a um pedido de autorização de acesso atende os requisitos definidos?

18. Qual o procedimento formal para entrega de password?

19. Existe um registo dos pedidos de autorização que foram recusados? Qual a informação guardada?

20. Quais os procedimentos de alteração do perfil de acesso a dados no SIGDN-RH?

21. Quais os procedimentos de cancelamento da autorização de acesso a dados no SIGDN-RH?

22. Existe um procedimento de comunicação de saída de um utilizador da organização?

23. Existe uma forma de controlar os utilizadores autenticados em tempo real ou diferido?

CARACTERÍSTICAS DE AUTENTICAÇÃO

24. Existe algum mecanismo de segurança quando existam várias tentativas falhadas de login?

25. Existe um registo de logs de tentativas falhadas de login? Se sim, qual a informação guardada?

26. As autorizações de acesso aos dados têm algum período de validade? Se sim, como funciona?

27. A identificação das autorizações de acesso aos dados é integrada com outros dados de identificação do utilizador?

28. De que forma é garantido apenas o acesso apenas à informação que é necessária para a correta execução das tarefas do utilizador?

29. Qual é a forma de autenticação (inclusive política de password) no SIGDN-RH?

30. Esta forma de autenticação pode ser melhorada? De que forma?

31. Após autenticação no sistema, a sessão tem algum período de expiração por inexistência de ação?

32. O utilizador pode alterar a sua password de acesso sempre que assim entender?

RISCOS E OPORTUNIDADES DE MELHORIA

33. Considera que o processo de gestão de perfis de acesso apresenta riscos, como por exemplo: acesso ilegítimo, modificação indesejada ou desaparecimento de dados? Se sim, quais os riscos e medidas mitigadoras possíveis?

34. Quais as oportunidades de melhoria que identifica no processo de gestão de perfis de acesso?

35. Considera que os utilizadores do SIGDN-RH estão sensibilizados para o uso e confidencialidade dos dados pessoais que estão a tratar?

CÓDIGO	ENTREVISTADO	
cDivCSI	Chefe da Divisão de Comunicações e Sistemas de Informação do Estado-Maior da FA (EMFA)	Entrevista por *email*, 29 de novembro de 2019
cGADIAP	Chefe do Gabinete de Administração de Informação da Área de Pessoal do Comando de Pessoal da FA (CPESFA)	Entrevista por *email*, 11 de novembro de 2019
cRDPS	Chefe da Repartição de Dados e Proteção Social da Direção de Pessoal (DP)	Entrevista presencial, 08 de novembro de 2019
cSASI	Chefe da Secção de Administração de Sistemas de Informação da Direção de Comunicações e Sistemas de Informação (DCSI)	Entrevista por *email*, 24 de novembro de 2019)
cATIRH	Coordenador da Área Técnica de Informação de Recursos Humanos da Direção de Serviços dos Sistemas de Informação (DSSI) da SGMDN	Entrevista por email, 15 de novembro de 2019
cAASA	Chefe da Área de Administração de Sistemas Aplicacionais da Direção de Serviços do Centro de Dados da Defesa (DSCDD) da SGMDN	Entrevista presencial, 26 de novembro de 2019

Questão	cDivCSI	cGADIAP	cRDPS	cSASI	cATIRH	cAASA
Política de Autorização e Gestão de Acessos						
1	x	x	x	x		
2	x	x	x			
3	x	x	x			
4	x	x	x			
5	x	x	x			
6	x	x	x			
7	x	x	x			
8	x	x	x			
Caracterização de dados do SIGDN-RH						
9			x			
10			x	x		
11			x			
Gestão de Autorização de Acesso						
12	x	x	x		x	x
13		x	x			
14		x	x		x	x
15		x	x		x	x
16		x	x			
17		x	x			x
18		x	x			x
19		x	x			x
20		x	x			
21		x	x			
22		x	x			
23		x	x		x	x
Características de Autenticação						
24						x
25						x
26		x	x			x
27		x	x			x
28		x	x		x	x
29		x	x		x	x
30		x	x		x	x
31		x	x			x
32		x	x			x
Riscos e Oportunidades de Melhoria						
33	x	x	x	x	x	x
34	x	x	x	x	x	x
35	x	x	x		x	x

Apêndice C — Análise de conteúdo das entrevistas

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
OE1 Identificar o processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH.	Processo de gestão de perfis de acesso	Política de autorização de Gestão de Acessos	cGADIAP	"Existe um sistema de controlo de identidades para os sistemas da FA, para o SIG não existe nenhum sistema de identidades."	1	A.1.1.1
			cRDPS	"Existe um sistema integrado de gestão de acessos para vários áreas e sistemas, exceto para o SIGDN-RH."	1	A.1.1.2
			cSASI	"… não podemos afirmar que temos um IdM (Identity management) integrado e centralizado na FA. Temos sim, um sistema de autenticação centralizado e de gestão de acessos (Micro Focus iManager) mas somente integrado para alguns serviços. (…) a gestão de acessos é feita isoladamente e com diferentes processos em cada SI, de acordo com os critérios dos seus administradores funcionais."	1	A.1.1.3
			cDivCSI	"A gestão de acessos ao SIGDN-RH é baseada na ocupação de função/cargo, em consonância com o estabelecido na Diretiva 06/2017 do GEN CEMFA – Gestão Orgânica do SIGDN na Força Aérea, que preconiza o modelo de gestão/governação daquele sistema na Força Aérea, nomeadamente a gestão de utilizadores, formação, disponibilização de informação, procedimentos de execução, entre outros."	2	A.1.1.4
			cRDPS	"A gestão de acessos é baseada em funções/cargo (..). Não existe uma lista pré-definida de funções/cargo que podem ter acesso ao SIGDN-RH. A concessão do acesso é avaliada caso a caso, consoante a informação presente no pedido."	2	A.1.1.5
			cGADIAP	"Não existe uma politica escrita, a criação de novos utilizadores só se realiza havendo nova necessidade esta é analisada e atribuído perfil com os roles necessários para o desempenho da função. A única "política" escrita é a informação prestada no portal de DFFA ..."	3	A.1.1.6
		Caraterização do Processo de gestão de perfis de acesso	cDivCSI	"O ADIAP é o responsável por efetuar a gestão dos utilizadores das aplicações/módulos da área de Pessoal (…) em estreita coordenação com elementos da área de pessoal com responsabilidades atribuídas nesta matéria"	12	A.1.2.1
			cRDPS	"… os perfis são coordenados entre o Ramo e a SGMDN. A resposta ao pedido inicial cabe à RD."	12	A.1.2.2
			cAASA	"A necessidade é levantada pelo responsável da FA, avaliada pela área funcional, em conjunto connosco é criado o perfil de acesso em SAP, e posteriormente os POC da FA fazem a atribuição do perfil ao utilizador. Em RH, como a implementação do sistema é recente, a responsabilidade de criação da matriz de roles do perfil e consequente atribuição ao utilizador, ainda não foi passada totalmente a responsabilidade do POC da FA, este efetua um pedido de perfil especificando na matriz de roles o que pretende, nós atribuímos os roles ao utilizador em SIGDN-RH, e informamos o POC da criação do utilizador com determinadas autorizações."	12	A.1.2.3

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
			cATIRH	"Depois de testados funcionalmente na ATIRH todos os roles que compõem cada um dos perfis que são pedidos pelas empresas, a tarefa de concessão de acesso aos dados do SIGDN-RH já não é da responsabilidade desta área técnica"	14	A.1.2.4
			cAASA	"Nós estamos envolvidos apenas na parte final do processo, ou seja, implementação do pedido de criação do perfil."	14	A.1.2.5
			cRDPS	"O processo (de alteração de perfil de acesso) é igual ao da criação de um novo utilizador."	20	A.1.2.6
			cGADIAP	"O cancelamento é efetuado sempre que chega ao conhecimento da DP/RD que o militar deixou de desempenhar as funções anteriores, ou após a "auditoria" mensal efetuada com o cruzamento de listas em ficheiros EXCEL."	21	A.1.2.7
			cRDPS	"Nunca houve um pedido de cancelamento. Os cancelamentos têm resultado da análise periódica referida anteriormente."	21	A.1.2.8
			cGADIAP	"… está determinado que sempre que o utilizador deixe de desempenhar as funções que deram origem ao perfil atribuído, as chefias devem comunicar."	22	A.1.2.9
			cRDPS	"… aquando da saída do utilizador da organização, estas pessoas deixam de ter acesso de todo à rede e ao SIGDN-RH."	22	A.1.2.10
			cGADIAP	"De acordo com a Diretiva n.º 06/2017, do CEMFA, a necessidade de acesso ao SIGDN-RH é determinada pela respetiva chefia sendo o correspondente formulário de pedido de acesso, disponibilizado no portal da FA, entregue ao Delegado de Informação Local. Este deverá fazer-me chegar o pedido de acesso, via correio eletrónico, para minha validação. Pode haver a necessidade de apoio da DFFA para verificar se é necessário ter acesso a roles de vencimentos, passando para a área de pessoal que atribui roles de RH, e solicita ao CDD a criação de um utilizador. Após a criação do utilizador, a RDPS é informada por Service Desk, e comunica por mail ao utilizador, o user e password provisória. Importa referir que este fluxo é a regra, estando ainda em falta a nomeação dos Delegados de Informação Locais, pelo que os Chefes estão a enviar os pedidos diretamente para mim."	15	A.1.2.11
			cRDPS	"Em circunstâncias normais, a intenção/pedido chega-nos através do ADIAP, após a sua análise e autorização, com indicação de um perfil de referência. Pode haver o envolvimento da DFFA/SIAFP caso exista a necessidade de atribuição de roles de vencimentos. Uma matriz do perfil é preenchida e enviada por Service Desk para a DSCDD para parametrização em sistema, a qual é devolvida pela mesma via com a confirmação do registo. A RDPS envia por mail para o utilizador, os dados necessários ao primeiro login (User + Password temporária). O sistema obriga a alteração de password após o 1º login."	15	A.1.2.12

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
			cATIRH	"Antes de serem submetidos para acesso na Adm. Sistemas os perfis pedidos pelos ramos são analisados pela ATIRH, especialmente se invocarem novos roles não definidos na matriz em vigor. Após esta validação funcional, os pedidos são autorizados através de processos definidos diretamente entre a Adm. Sistemas e os respetivos POC das empresas ..."	15	A.1.2.13
			cAASA	"Após o pedido da FA, efetuamos uma análise inicial do mesmo, em caso de necessidade, reencaminhamos para a área funcional para análise adicional, posteriormente efetuamos as parametrizações necessárias em SIGDN-RH e informamos o Ramo."	15	A.1.2.14
			cGADIAP	"A password como é provisória é enviada para o mail do utilizador."	18	A.1.2.15
			cGADIAP	"A autenticação no sistema é feito com o utilizador e password, esta password é escolhida pelo utilizador logo após entrar no sistema pela primeira vez com password temporária."	29	A.1.2.16
		Análise periódica de procedimentos	cDivCSI	"A Diretiva 06/2017, já mencionada, prevê a realização de reuniões internas de coordenação, periódicas, bem como a elaboração de um relatório anual de atividades, onde deverão ser incluídas métricas relativas à utilização do sistema e à sua exploração pelos utilizadores. Estas atividades devem ser coordenadas pelo Grupo Coordenador de Gestão da Informação."	5	A.1.3.1
			cGADIAP	"… é realizada uma "auditoria" das autorizações de acesso concedidas, recorrendo ao cruzamento de listagens de excel normalmente uma vez por mês."	5	A.1.3.2
			cRDPS	"… são feitas análises periódicas, no entanto, importa ressalvar que o sistema é recente e não tem havido muitas mudanças até ao momento, pelo que ainda não sentimos muito esta necessidade. Esta análise já era efetuada no sistema anterior."	5	A.1.3.3
			cDivCSI	"Após produção" (de uma revisão anual à atividade dos utilizadores)", os resultados devem ser comunicados às áreas da Organização que são stakeholders do processo."	8	A.1.3.4
	Perfis de acesso ao SIGDN-RH	Estrutura dos perfis de acesso ao SIGDN-RH	cGADIAP	"Estão organizados por uma matriz que cruza os perfis de estrutura com os perfis de autorização."	13	A.2.1.1
			cRDPS	"Os perfis estão organizados por macroprocessos, processos e estrutura organizacional, que depois derivam para os infotipos. Existe uma estrutura de perfis previamente definida por área funcional e tipo de função."	13	A.2.1.2
			cGADIAP	"Foi construída uma matriz onde estão identificados todos os possíveis perfis, atividades e infotipos que cada utilizador necessita para o desempenho das suas tarefas diárias."	28	A.2.1.3
	Dados Pessoais	Caraterização dos dados pessoais disponíveis	cRDPS	"Os dados estão organizados em infotipos e conjuntos de infotipos, com informação pessoal e organizacional."	9	A.3.1.1
			cSASI	"Há um conjunto de dados do SIGDN-RH que foram identificados como sendo o conjunto mínimo de dados pessoais que permitem sustentar os diferentes SI da FA. Nesse sentido, foram	10	A.3.1.2

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
		no SIGDN-RH		produzidos e disponibilizados à FA, pela SGMDN-DSSI, um conjunto de interfaces por webservices que possibilitam esse fluxo de dados."		
		Integração de dados de perfil	cRDPS	"Fora do SIGDN-RH, a identificação do acesso está integrada com vários dados, inclusive o NIP. No sistema, apenas está integrado com o posto, nome, função e unidade do utilizador."	27	A.3.2.1
			cAASA	"Apesar de existir um conjunto de informação de caracterização do utilizador, mas não existe nenhuma ligação à informação do SIGDN-RH. Utilizador SAP é diferente de Colaborador de RH."	27	A.3.2.2
OE2 Analisar a conformidade com os princípios fundamentais: a necessidade e a proporcionalidade de processamento e a proteção dos direitos dos titulares dos dados pessoais dos RH da FA, presentes no SIGDN-RH.	Necessidade	Grau de necessidade do processo de gestão de perfis de acesso	cGADIAP	"São."	16	B.1.1
			cRDPS	"Sim."	16	B.1.2
			cDivCSI	".. a confidencialidade dos dados pessoais (...) ganhou importância crescente com a aplicação do Regulamento 679/2016 da Comissão Europeia, o Regulamento Geral sobre a Proteção de Dados (RGPD), que veio imprimir acrescida relevância à necessidade de proteção dos dados pessoais das pessoas singulares."	35	B.1.3
	Proporcionalidade	Grau de proporcionalidade do processo de gestão de perfis de acesso	cGADIAP	"São."	16	B.2.1
			cRDPS	"Sim."	16	B.2.2
			cGADIAP	"… o tempo de resposta está dentro dos requisitos."	17	B.2.3
			cRDPS	"… consideramos que seja um processo rápido e não temos detetado reclamações inerentes ao processo."	17	B.2.4
			cAASA	"Depende da complexidade do pedido, no entanto, apesar da FA ser um utilizador recente do sistema, advindo daí algumas necessidades de (re)adaptação, considero que sim."	17	B.2.5
	Proteção	Grau de proteção dos direitos dos titulares dos dados	cATIRH	"Os utilizadores de SIGDN-RH serão exatamente os mesmos que operavam com os sistemas legados de gestão de pessoal e, nessa circunstância, o nível de consciencialização da sensibilidade e natureza dos dados pessoais não defere em função da ferramenta de gestão utilizada. Tanto quanto me é dado a perceber, as empresas e nomeadamente os Ramos têm tido, desde sempre, uma política de algum rigor sobre esta matéria, embora se admita a existência de uma ou outra falha mais pontual."	35	B.3.1

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
OE3 Avaliar os riscos associados ao processo de gestão de perfis de acesso aos dados pessoais dos RH da FA, presentes no SIGDN-RH.	Ameaças	Ameaças ao processo	cSASI	"… não podemos afirmar que temos um IdM (Identity management) integrado e centralizado na FA. Temos sim, um sistema de autenticação centralizado e de gestão de acessos (Micro Focus iManager) mas somente integrado para alguns serviços. (…) a gestão de acessos é feita isoladamente e com diferentes processos em cada SI, de acordo com os critérios dos seus administradores funcionais."	1	C.1.1
			cGADIAP	"Não existe uma politica escrita, a criação de novos utilizadores só se realiza havendo nova necessidade esta é analisada e atribuído perfil com os roles necessários para o desempenho da função. A única "política" escrita é a informação prestada no portal de DFFA ..."	3	C.1.2
			cRDPS	"Não existe uma política relativa à criação de novos utilizadores."	3	C.1.3
			cRDPS	"Não existe uma política …" (Relativamente a uma política relativa ao cancelamento e apagamento de utilizadores)	4	C.1.4
			cRDPS	"… o processo não está claro quando o perfil requerido abrange roles de vencimentos e de RH, pelo que todos os pedidos exclusivos de RH não necessitam de transitar pela DFFA."	34	C.1.5
			cGADIAP	"Ainda não se completou um ano em produtivo, pelo que não foi feita nenhuma análise." (Relativa à atividade dos utilizadores do SIGDN-RH)	7	C.1.6
			cSASI	"Há um conjunto de dados do SIGDN-RH que foram identificados como sendo o conjunto mínimo de dados pessoais que permitem sustentar os diferentes SI da FA. Nesse sentido, foram produzidos e disponibilizados à FA, pela SGMDN-DSSI, um conjunto de interfaces por webservices que possibilitam esse fluxo de dados."	10	C.1.7
			cAASA	"A nossa rede tem um grau de classificação de "Não classificado". Todos os dados não têm uma marca de credenciação de informação."	12	C.1.8
			cRDPS	".. Apenas é guardado o pedido. Não é registado o motivo da recusa, apesar da maioria ser recusada por não desempenhar funções na área de pessoal."	19	C.1.9
			cAASA	"… a informação é guardada no Service Desk, no entanto, como o campo é descritivo, não podemos garantir sempre o registo do motivo de recusa."	19	C.1.10
			cGADIAP	"... este fluxo é a regra, estando ainda em falta a nomeação dos Delegados de Informação Locais, pelo que os Chefes estão a enviar os pedidos diretamente para mim."	15	C.1.11
			cDivCSI	"… este processo carece de revisão e atualização, de forma a mitigar os riscos apresentados. Pese embora a diretiva existente remonte a 2017, existe a necessidade de revisitar os procedimentos definidos e balizar os acessos de forma adequada."	33	C.1.12
			cSASI	"Considero que atualmente, não existindo um modelo de governance único, transversal e integrado sobre a gestão de acessos dos SI da FA, que os riscos elencados são reais."	33	C.1.13

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
			cAASA	"É um POC que faz a atribuição das autorizações. ...existe o risco da ação humana em dar mais acessos do que a pessoa necessita."	33	C.1.14
			cAASA	"… por insuficiência na sua formação pessoal, as pessoas facilitam perante a exigência do exercício das suas funções."	35	C.1.15
	Fontes de Risco	Fontes de Risco do Processo	cRDPS	"Aquando da implementação, foi criada uma matriz com todos os possíveis perfis, atividades e infotipos que cada utilizador, a qual posteriormente tem vindo a ser alvo de correção, manutenção e atualização face a novas necessidades."	28	C.2.1
			cATIRH	"O acesso à informação que é necessária para a correta execução das tarefas do utilizador "depende da forma com cada entidade interpreta as inúmeras combinações que a matriz de perfis oferece para a criação de acessos ao sistema. ...serão milhões as combinações possíveis para se formar o perfil de acesso de um utilizador."	28	C.2.2
			cRDPS	"… alguns infotipos pré-definidos estão disponíveis para outras entidades por força do "Concurrent Employment". A alteração de um dado do militar por outra entidade tem reflexo na FA, e vice-versa."	11	C.2.3
			cRDPS	"… o Concurrent Employment possibilita a alteração indesejada de dados, não por via do perfil de acesso, mas sim pela forma como a funcionalidade está a ser aplicada, ao nível dos procedimentos, originando alguns problemas. Temos receio que haja pessoas a alterar dados de militares da FA, que não estejam sensibilizadas nem preparadas para as implicações que daí possam advir, como já aconteceu, inclusive há poucos dias."	33	C.2.4
			cGADIAP	"Como qualquer sistema contém sempre riscos, essencialmente muitas vezes por descuido do utilizador."	33	C.2.5
			cAASA	"… por insuficiência na sua formação pessoal, as pessoas facilitam perante a exigência do exercício das suas funções."	35	C.2.6
			cATIRH	"A pouca familiarização com o novo sistema e a manutenção de processos ainda utilizados nos sistemas legados, leva algumas empresas mais que outras, a segmentarem em demasia os perfis dos seus utilizadores, não aproveitando plenamente uma das idiossincrasias deste sistema que é a integração dos seus processos."	34	C.2.7
			cRDPS	"A RDPS não tem esta capacidade." (forma de controlar os utilizadores autenticados em tempo real ou diferido)	23	C.2.8
			cAASA	"Neste momento, temos apenas um fator de autenticação (User e password)…"	30	C.2.9
	Impactos	Impactos de risco do processo	cATIRH	"... os POC funcionais das empresas têm que ter uma ideia muito clara dos acessos que pretendem dar a cada utilizador, avaliando as suas atividades e interpretar quais os roles necessários para o desempenho das mesmas, ao mesmo tempo que terão que perceber se a	28	C.3.1

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
				natureza desses roles não darão acesso aos utilizadores a informação desnecessária ao seu desempenho."		
			cAASA	"Como qualquer sistema, se o perfil do utilizador permitir apagar dados, existe sempre o risco de modificação ou desaparecimento de dados."	33	C.3.2
			cSASI	"Há um conjunto de dados do SIGDN-RH que foram identificados como sendo o conjunto mínimo de dados pessoais que permitem sustentar os diferentes SI da FA. Nesse sentido, foram produzidos e disponibilizados à FA, pela SGMDN-DSSI, um conjunto de interfaces por webservices que possibilitam esse fluxo de dados."	10	C.3.3
	Oportunidades de melhoria	Oportunidades de melhoria do processo de gestão de perfis de acesso	cDivCSI	"… ao nível de políticas e doutrina, encontra-se em curso o desenvolvimento de uma política de gestão de utilizadores única, para todos os sistemas de informação explorados pelos utilizadores na Organização."	34	C.4.1
			cRDPS	"Podem haver funcionalidades no sistema que não estejam disponíveis para a FA, mas apenas na SGMDN."	23	C.4.2
			cRDPS	"A RDPS necessita do apoio da DSCDD para qualquer alteração de perfil de utilizador em SIGDN-RH. No entanto, o ADIAF consegue fazer alterações de roles da área deles."	26	C.4.3
			cGADIAP	"… maior autonomia do Ramo para a gestão e criação de utilizadores."	34	C.4.4
			cAASA	"… no futuro, prevê-se que o processo de atribuição de perfis passe a ser gerido pelo Ramo, em conjunto com a ATIRH."	28	C.4.5
			cGADIAP	"Por exemplo através de CMD (chave móvel digital)." (Melhoria da forma de autenticação)	30	C.4.6
			cRDPS	"… reconhecimento automático do acesso por via do posto de trabalho, com um sistema integrado e centralizado de identificação única."	30	C.4.7
			cGADIAP	"… obrigar a uma password com características mais robustas utilizando letras números e caracteres especiais." "… acesso através de cartão de cidadão ou “militar desde que já tivesse microchip”, e ainda a chave móvel digital."	33	C.4.8
			cSASI	"... automatização na atribuição e cessação de acessos tendo como critério, por exemplo, a posição ocupada na organização; o refactoring de SI legados; conhecimento exato dos fluxos de dados de pessoal, onde são obtidos, usados e retidos; e a adição de accountability."	34	C.4.9
			cATIRH	"A gestão das autorizações torna-se tanto mais fácil e eficiente quanto menos diferenciadora for a sua estrutura." "Em suma deveriam haver menos perfis de utilizadores e as tarefas deveriam estar o mais concentradas possível num número restrito de pessoas."	34	C.4.10
	Medidas mitigadoras	Medidas mitigadoras	cDivCSI	"Importa referir que se pretende que este relatório seja desenvolvido no início de 2020, tendo particular atenção ao facto de o Módulo SIGDN-RHV ter entrado em exploração no início de	8	C.5.1

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
		dos riscos associados ao processo de gestão de perfis de acesso		2019, podendo assim efetuar-se um balanço e aferir alguns indicadores relativos à exploração específica deste módulo com dados referentes ao primeiro ano de utilização."		
			cRDPS	"O SIGDN-RH não permite que dois utilizadores alterem em simultâneo dos dados da mesma pessoa."	23	C.5.2
			cAASA	"… ao final de três tentativas de login) o utilizador fica bloqueado."	24	C.5.3
			cAASA	"… guardamos o nome da máquina/posto de trabalho e User ID." (Registo de Logs de tentativas falhadas de login)	25	C.5.4
			cRDPS	"As autorizações não têm um período de validade, no entanto, após um mês sem efetuar login, o User passa para o estado "Expirado". Este automatismo pode ser considerado um prazo de validade. A reativação destes utilizadores necessita de uma ação da DSCDD."	26	C.5.5
			cAASA	"Mensalmente, nós corremos um procedimento para desativar utilizadores que nos últimos 90 dias (ou 30, no caso de login inicial) não tenham feito login …"	26	C.5.6
			cAASA	"O SAP funciona como uma base de dados negada, ou seja, quando é criado um utilizador, este não tem acesso a nada. Em RH, o acesso à informação necessária é garantido através de dois mecanismos, essencialmente um perfil técnico de autorização (matriz de atividades) e um perfil de estrutura, os quais formam um role composto para atribuir ao utilizador."	28	C.5.7
			cAASA	"Além dos requisitos inerentes ao RGPD, existe a Resolução do Conselho de Ministros n.º 41/2018 que complementa o RGPD, e nesta perspetiva, pode ser melhorada adicionando fatores de autenticação nas máquinas."	30	C.5.8
			cAASA	"… uma hora de inatividade." (período de expiração por inexistência de ação).	31	C.5.9
			cAASA	"Sim." (O utilizador pode alterar a sua password de acesso sempre que assim entender.)	32	C.5.10
			cDivCSI	"No âmbito das ações conducentes à conformidade da Força Aérea com o RGPD, estão já a ser desenvolvidas ações de formação/sensibilização dos utilizadores, a três níveis: Palestras (...), módulo específico de 10 horas de formação (...) e Formação ad-hoc ..."	35	C.5.11
			cDivCSI	(A revisão e atualização do processo) "... deverá ser efetuada pelas entidades responsáveis na Força Aérea, mas envolvendo também elementos da equipa SIGDN, uma vez que poderá ser necessária intervenção sobre o sistema, e não apenas na delimitação funcional de perfis."	33	C.5.12
			cSASI	"... instalação e exploração de um IdM, fully cappable em todas as suas dimensões. Todavia, são conhecidas outras medidas mitigadoras, como por exemplo: encriptação, pseudonimização e minimização dos dados; técnicas capazes de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos serviços de tratamento; intrusion detection systems (IDS); e capacidade de tracking e logging das ações sobre os dados."	33	C.5.13

Objetivo Específico	Variável	Informação pretendida	Entrevistado	Excertos das Entrevistas	Questão	Codificação
			cAASA	"É possível saber os utilizadores em tempo real, login time, logout time e transações efetuadas. Isto além da capacidade da ATIRH conseguir auditar as alterações efetuadas em SIGDN-RH por pessoa e IT."	23	C.5.14
			cAASA	"… automatismos que os sistemas de provisioning proporcionam na gestão de pessoas versus utilizadores do sistema, ou seja, enquanto uma pessoa estiver associada a uma posição, tem os acessos inerentes à mesma."	34	C.5.15
			cAASA	"Pode ser melhorado pela utilização de sistemas de Provisioning, para uma gestão automática de todas as tarefas por posição que pode ser atribuída a um utilizador. Este sistema é um ad-on do SAP e requere uma tipificação exaustiva de tarefas por posição da organização, com uma baixa volatilidade."	33	C.5.16
				"... os vários tipos de backups que temos apenas permitem a reposição total do sistema, por forma a que se possa recuperar ou consultar qualquer tipo de dado."		
	Sensibilização dos utilizadores	Grau de sensibilização dos utilizadores	cDivCSI	"À semelhança dos utilizadores de todos os Sistemas de Informação que se encontram em exploração na Força Aérea, os utilizadores do SIGDN-RH deverão estar sensibilizados para as questões relacionadas com a confidencialidade dos dados pessoais, pelo que o requisito é transversal. Este assunto ganhou importância crescente com a aplicação do Regulamento 679/2016 da Comissão Europeia, o Regulamento Geral sobre a Proteção de Dados (RGPD), que veio imprimir acrescida relevância à necessidade de proteção dos dados pessoais das pessoas singulares."	35	C.6.1
			cGADIAP	"Considero que de um modo geral estão sensibilizados."	35	C.6.2
			cRDPS	"... como o universo de utilizadores é inferior, mas coincidente com o que tinha acesso ao SIGAP, considero que já estavam sensibilizados no anterior sistema. Esta sensibilização tem vindo a ser contínua junto de todos aqueles que pretendem ter acesso aos dados pessoais no SIGDN-RH."	35	C.6.3
			cATIRH	"Os utilizadores de SIGDN-RH serão exatamente os mesmos que operavam com os sistemas legados de gestão de pessoal e, nessa circunstância, o nível de consciencialização da sensibilidade e natureza dos dados pessoais não defere em função da ferramenta de gestão utilizada. Tanto quanto me é dado a perceber, as empresas e nomeadamente os Ramos têm tido, desde sempre, uma política de algum rigor sobre esta matéria, embora se admita a existência de uma ou outra falha mais pontual."	35	C.6.4

Apêndice D — Processo de Criação de Perfil de Utilizador do SIGDN- RH

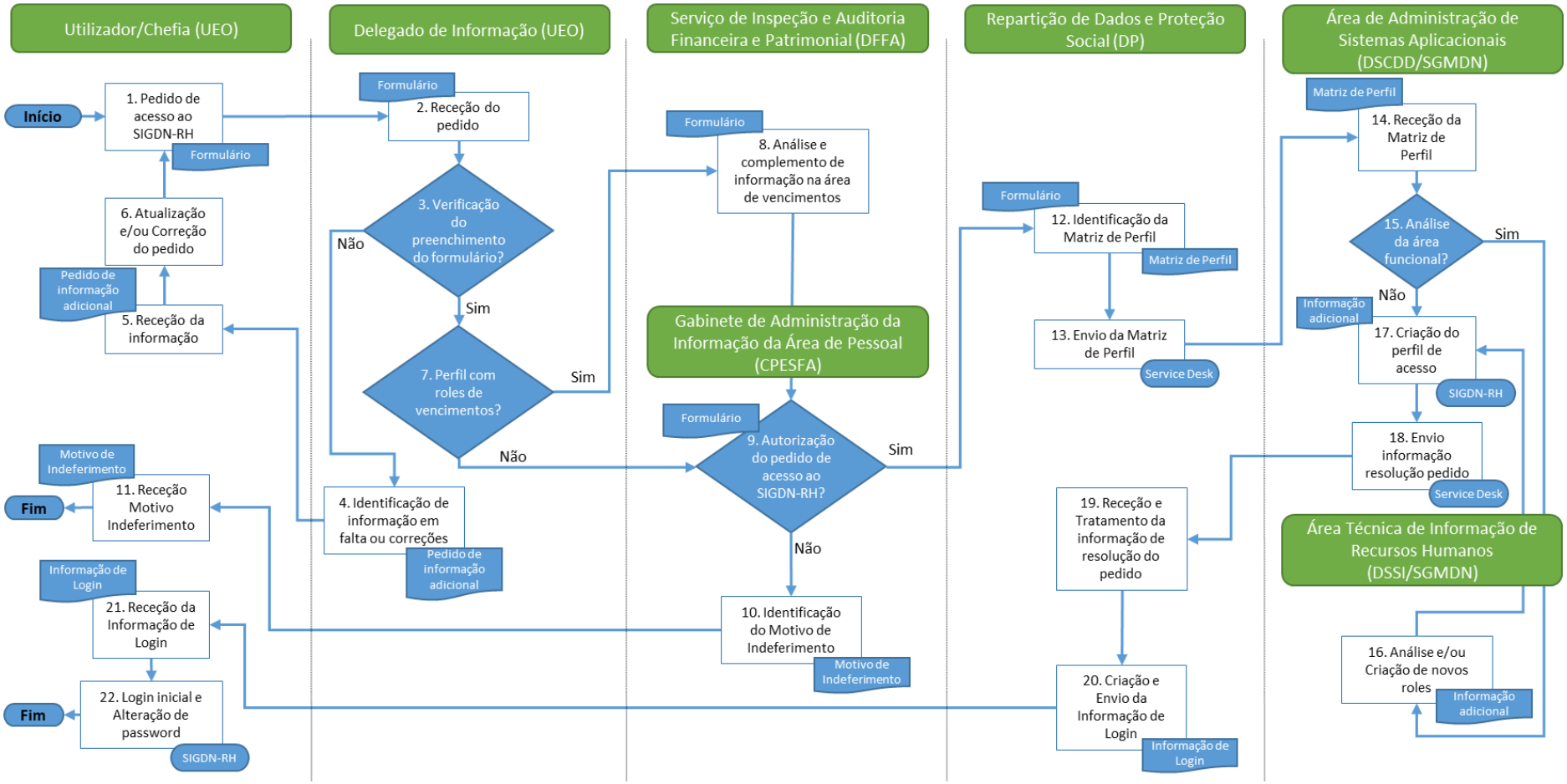

Figura 4 – Fluxograma de Criação de Perfil de Utilizador do SIGDN-RH