Fall 10-16-2021

A method for verifying compliance with the General Data Protection Regulation - a proposal to adapt an Information Security Management System

Helena Pilonas
Instituto Politécnico de Beja, maria.helena.ramalho@gmail.com

Isabel Sofia Sousa Brito
ESTIG – Instituto Politécnico de Beja, isabel.sofia@ipbeja.pt

Um método para a verificação da conformidade com o Regulamento Geral de Proteção de Dados – uma proposta de adaptação de um Sistema de Gestão de Segurança da Informação

A method for verifying compliance with the General Data Protection Regulation - a proposal to adapt an Information Security Management System

Helena Pilonas, Instituto Politécnico de Beja, maria.helena.ramalho@gmail.com

Isabel Sofia Brito, Instituto Politécnico de Beja, isabel.sofia@ipbeja.pt

Resumo

Após a entrada em vigor do Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016 designado por Novo Regulamento Geral de Proteção de Dados, em 25 de maio de 2018, tornou-se emergente proporcionar os requisitos e orientações para estabelecer, implementar, manter e melhorar de forma continua um sistema de gestão de segurança de informação, que preserve a confidencialidade, integridade e disponibilidade da informação. Pretende-se como resultado final deste trabalho, a apresentação de um método para verificação da conformidade do Sistema de Segurança Informação para o cumprimento do novo Regulamento Geral de Proteção de Dados seguindo as linhas das Normas ISO/IEC 27001:2013 (Sistemas de Gestão de Segurança de Informação), ISO/IEC 27002:2013 (Information technology — security techniques — code of practice for information security controls) e consequentemente, a ISO/IEC 27701:2019 (Security techniques – extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – requirements and guidelines).

Palavras-chave: ISO27k; RGPD; SGSI; Privacidade.

Abstract

After the entry into force of Regulation 2016/679 of the European Parliament and of the Council of the European Union, of 27 April 2016, designated as New General Data Protection Regulation, on 25 May 2018, it became emergent to provide the requirements and guidelines for establishing, implementing, maintaining and continuously improving an information security management system that preserves the confidentiality, integrity and availability of information. It is intended as the final result of this work, the presentation of a method for verifying the information security system to comply with the new general data protection regulation following the lines of ISO/IEC 27001:2013 (Security management systems) information), ISO/IEC 27002:2013 (Information technology - security techniques - code of practice for information security controls) and, consequently, ISO/IEC 27701:2019 (Security techniques - extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - requirements and guidelines).

Keywords: ISO27k; GDPR; ISMS; Privacy.

1. INTRODUÇÃO

A implementação de um sistema de segurança para a proteção de dados é essencial para cumprir as disposições do Regulamento Geral de Proteção de Dados (RGPD), para além de outros aspetos,

menos formais, como a confiança na organização. Este trabalho propõe um método para a adaptação e consequente verificação da conformidade com base na Resolução de Conselho de Ministros de n.º 41/2018, 28 de março (RCM2018), de um Sistema de Gestão de Segurança da Informação (SGSI) existente na organização, para o cumprimento do RGPD que preserve a confidencialidade, integridade e disponibilidade da informação e resiliência. O SGSI da organização foi desenvolvido com base na norma ISO/IEC 27001/2:2013, logo faremos uso da ISO/IEC 27701:2019 para apoiar a conformidade com o RGPD, considerando que a ISO/IEC 27701 é uma norma orientada para gestão de informação pessoal, definindo requisitos e fornecendo orientações que ajudam as organizações na gestão da privacidade da informação. A aplicação desta norma, bem como da resolução do conselho de ministros é a novidade desta proposta.

O presente documento está dividido em cinco secções. A segunda secção descreve os elementos considerados no método para que este possa alcançar os objetivos definidos. Assim, o RGPD e a RCM2018 são descritos na secção 2.1, a família ISO 27k é descrita na secção 2.2 e os trabalhos relacionados na secção 2.3. A secção 3 descreve o método, a secção 4 ilustra a aplicação do método através de um estudo de caso e a última secção apresenta as conclusões.

2. ASPETOS BASE DA PROPOSTA

Para o desenvolvimento do método foi analisado o RGPD à luz da RCM2018, tendo em vista a identificação dos aspetos técnicos relevantes para a verificação da conformidade dos SGSI.

A publicação recente da ISO 27701 onde se define requisitos e orientações que apoiam as empresas na gestão da privacidade relacionados com informação de identificação pessoal (do inglês *Personally Identifiable Information* (PII)). Estes requisitos e orientações estão definidas à luz das regulamentações internacionais, permitindo demonstrar aos *stakeholders* a existência de elementos eficazes para apoiar a conformidade com o RGPD e outros regulamentos de privacidade em todo o mundo.

2.1. RGPD e Resolução do Conselho de Ministros.

O novo RGPD, designa que os dados pessoais devem ser tratados de forma que garanta a sua segurança, cujas propriedades básicas são confidencialidade, integridade, disponibilidade e resiliência, adotando as medidas técnicas ou organizativas adequadas, o que exige a implementação de um sistema de gestão de segurança da informação e, a RCM2018, define "orientações técnicas para a Administração Pública, recomendando-as ao sector empresarial do Estado, em matéria de arquitetura de segurança das redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas do RGPD" (Ministros, 2018). Para cumprimento do RGPD e compreendê-lo na íntegra, é obrigatório garantir os seguintes requisitos:

- Registos de tratamento de dados pessoais (Artigo 30º);
- Segurança de dados pessoais (Artigo 32º);
- Notificação de incidentes de violação de dados pessoais (Artigo 33º);
- Avaliações de Impacto sobre a proteção de dados (Artigo 35º);
- Nomeação de um encarregado da proteção de dados (Artigo 37º);
- Incentivar códigos de conduta e processos de certificação (Artigo 42º).

A RCM2018, vem reforçar a entrada em vigor do RGPD para que exista um reforço na proteção judicial dos direitos dos titulares dos dados pessoais, sendo aplicado através da implementação de novas regras e procedimentos do ponto de vista tecnológico.

Segundo a RCM2018, "a relação entre a tecnologia e o Direito está espelhada de modo especial, na proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD), nas medidas adequadas para garantir a segurança do tratamento (artigo 32.º do RGPD), na notificação de violações de dados pessoais às autoridades de controlo (artigo 33.º do RGPD), na comunicação de violação de dados pessoais aos titulares dos dados (artigo 34.º do RGPD) e na avaliação de impacto sobre a proteção de dados pessoais (artigo 35.º do RGPD).

O direito ao apagamento dos dados pessoais e o direito à portabilidade destes consagrados respetivamente nos artigos 17.º e 20.º do RGPD, exigem igualmente a implementação de tecnologias de informação que utilizem formatos interoperáveis, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, e que permitam que estes direitos possam ser efetivamente exercidos." (Ministros, 2018)

Enuncia-se os artigos constantes na RCM2018 referentes ao RGPD, e respetiva definição:

- Artigo 17.º - "Direito ao apagamento dos dados ("Direito a ser esquecido"): 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, …". (Europeia, 2016)
- Artigo 20.º - "Direito de portabilidade dos dados: 1. O titular dos dados tem o direito de receber os dados que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, …". (Europeia, 2016)
- Artigo 25.º - "Proteção de dados desde a conceção e por defeito: 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as

finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, …". (Europeia, 2016)

- Artigo 32.º - "Segurança do tratamento: 1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, …". (Europeia, 2016)
- Artigo 33.º - "Notificação de uma violação de dados pessoais à autoridade de controlo: 1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, ...". (Europeia, 2016)
- Artigo 34.º - "Comunicação de uma violação de dados pessoais ao titular dos dados: 1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada." (Europeia, 2016)
- Artigo 35.º - "Avaliação de impacto sobre a proteção de dados: 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação." (Europeia, 2016)

Consequentemente, estes são os artigos usados na proposta descrita neste artigo.

2.2. Família da ISO 27K

A família de normas ISO/IEC 27000 é um conjunto de várias normas que convergem para um SGSI tendo como objetivo a segurança de dados e dos seus respetivos sistemas de armazenamento eletrónico. "Muitos sistemas de informação não foram projetados para serem seguros. A identificação de controlos a serem implementados requer planeamento cuidadoso e atenção nos detalhes." (ISO, ISO/IEC 27000:2018, 2018)

A ISO 27701 é uma extensão às normas ISO/IEC 27001 e ISO/IEC 27002, e orientada para

gestão de informação pessoal, definindo requisitos e (ISO, ISO/IEC 27000:2018, 2018) fornecendo orientações que ajudam as empresas na gestão de riscos de privacidade relacionados com informação de identificação pessoal (PII). A ISO 27701 promove a criação de sistemas eficazes para apoiar a conformidade com o RGPD e outros regulamentos de privacidade em todo o mundo.

Os benefícios da implementação da ISO 27701 são: suporte para conformidade com o RGPD e outros regulamentos de proteção de dados; aumento da confiança, por parte dos clientes e outros *stakeholders*, na capacidade de gestão da informação pessoal; garantia da proteção adequada dos dados; facilmente integrável com a norma ISO/IEC 27001; transparência nos controlos estabelecidos para a gestão da privacidade; melhoria dos processos internos para evitar quebras de confidencialidade; facilita o estabelecimento de acordos com parceiros de negócios onde o processamento de PII é mutuamente relevante.

2.3. Trabalhos relacionados

Existem vários trabalhos que demonstram a implementação de um SGSI. O trabalho intitulado "Plano de Implementação da Norma ISO/IEC 27001:2013 na organização INEM-Instituto Nacional de Emergência Médica, I. P." apresenta "a preparação para a implementação do Sistema de Gestão de Segurança da Informação (SGSI) baseado nas orientações da família das normas ISO/IEC 27000", com o objetivo de construir o SGSI da instituição. (Correia, 2016)

O trabalho intitulado "Estudo do grau de alinhamento dos STI com a norma ISO 27000", visa "analisar os objetivos de controlo e controlos implementados à segurança da informação" e "são apresentados os principais objetivos, análise dos controlos selecionados e os resultados obtidos no decorrer do trabalho desenvolvido. A base deste estudo assenta nas normas da família ISO 27000, sobretudo na norma ISO 27002:2005 – *Code of practice for information security management*." (Godinho, 2014) A proposta apresentada neste documento difere destes dois trabalhos pois usa o RCM2018 e a ISO 27701 para verificação da conformidade de um SGSI com o RGPD.

3. MÉTODO

Tendo como foco o desenvolvimento de um SGSI, segundo os requisitos da Norma ISO/IEC 27001/2:2013, o objetivo do artigo é a aplicabilidade dos controlos da Norma ISO/IEC 27701:2019 para verificação da conformidade do SGSI com o RGPD.

O método é baseado num processo dividido em três passos, tal e como ilustra a Figura 1 e descrito nas seções seguintes.

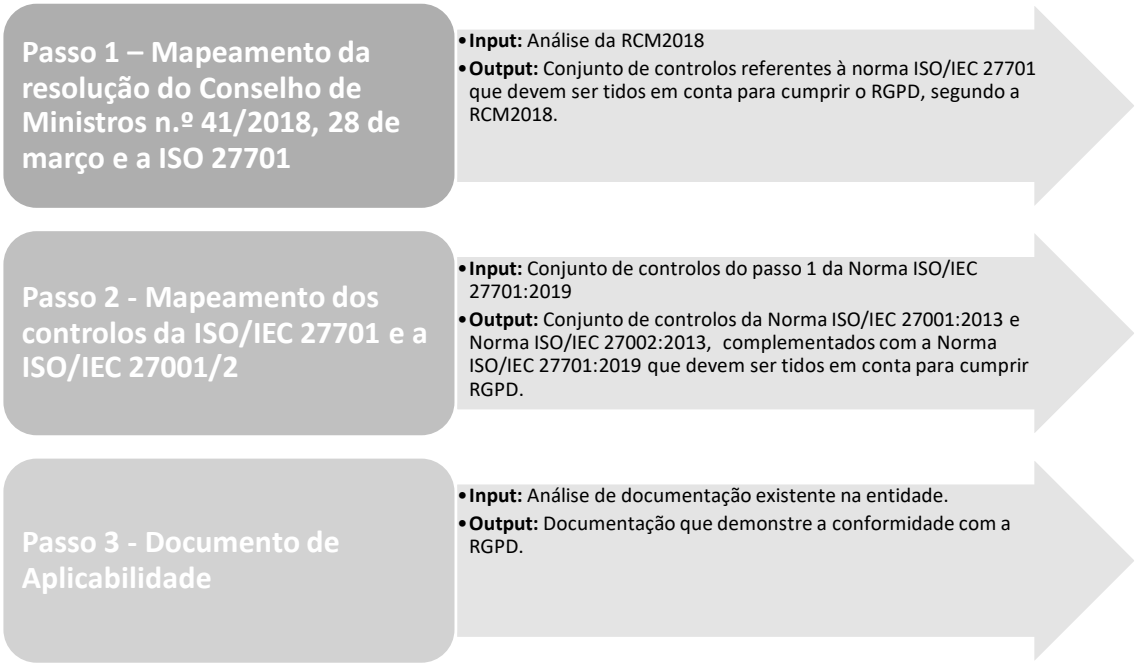

Figura 1 – Diagrama de processos

3.1. Fases do processo

Passo 1 – Mapeamento da RCM2018 e a ISO 27701:2019

Input: RCM2018

Output: Conjunto de controlos referentes à norma ISO/IEC 27701 que devem ser tidos em conta para cumprir o RGPD.

Atividade: identificar quais as regras e procedimentos a efetuar da Norma ISO/IEC 27701:2019 com base na resolução, propõe-se a aplicação de um mapeamento que identifica explicitamente a relação entre a norma ISO/IEC 27701:2019 e a RGPD. O RCM2018 identifica os artigos do RGPD que são usados nesta atividade. Cabe ressalvar que a proposta não é "fechada" e é possível acrescentar outros artigos do RGPD.

O mapeamento está ilustrado na Tabela 1 que é composta por duas colunas, sendo que a primeira coluna mostra as regras e procedimentos identificados na Norma ISO/IEC 27701:2019 e a segunda coluna mostra os artigos que devem ser tidos em conta para que se cumpra os requisitos identificados na RCM2018 e assim, se cumpra o RGPD.

Norma ISO/IEC 27701/2019	RGPD
5.2.1.	(25)(3); (32)(3)
5.2.2.	(35)(9)
5.2.3.	(32)(2)

5.2.4.	(32)(2)
5.4.1.2.	(32)(1)(b); (32)(2)
5.4.1.3.	(32)(1)(b); (32)(2)
6.5.2.1.	(32)(2)
6.5.3.1.	(32)(1)(a)
6.5.3.3.	(32)(1)(a)
6.7.1.1.	(32)(1)(a)
6.9.3.1.	(32)(1)(c)
6.11.1.2.	(32)(1)(a)
6.11.2.1.	(25)(1)
6.11.5.1.	(25)(1)
6.12.1.2.	(32)(1)(b)
6.13.1.1.	(33)(1); (33)(3)(a); (33)(3)(b); (33)(3)(c); (33)(3)(d); (33)(4); (33)(5); (34)(1); (34)(2); (34)(3)(a); (34)(3)(b); (34)(3)(c); (34)(4)
6.13.1.5.	(33)(1); (33)(2); (33)(3)(a); (33)(3)(b); (33)(3)(c); (33)(3)(d); (33)(4); (33)(5); (34)(1); (34)(2)
6.15.1.1.	(32)(1)(b)
6.15.2.1.	(32)(1)(d); (32)(2)
6.15.2.3.	(32)(1)(d); (32)(2)
7.2.1.	(32)(4)
7.2.2.	(17)(3)(a); (17)(3)(b); (17)(3)(c); (17)(3)(d); (17)(3)(e)
7.2.5.	(35)(1); (35)(2); (35)(3)(a); (35)(3)(b); (35)(3)(); (35)(4); (35)(5); (35)(7)(a); (35)(7)(b); (35)(7)(c); (35)(7)(d); (35)(8); (35)(9); (35)(10); (35)(11)
7.3.6.	(17)(1)(a); (17)(1)(b); (17)(1)(c); (17)(1)(d); (17)(1)(d); (17)(1)(f); (17)(2)
7.3.8.	(20)(1); (20)(2); (20)(3); (20)(4)
7.4.2.	(25)(2)
7.4.5.	(32)(1)(a)
8.2.1.	(35)(1)
8.3.1.	(17)(2)

Tabela 1 – Mapeamento RGPD e a ISO 27701 (Fonte: (ISO, ISO/IEC 27701:2019, 2019), (Ministros, 2018))

A Tabela 1 mostra um total de 29 relações entre a norma ISO/IEC 27701:2019 e o RGPD. Cada linha pode ser lida de forma a que para cada procedimento a efetuar na norma ISO/IEC 27701:2019, está relacionado com o(s) artigo(s) mencionado(s) na RCM2018, para que a organização, pública ou privada, tenha em cumprimento o RGPD.

Por exemplo, a linha 2 da Tabela 1, ilustra que para cumprir os requisitos exigidos na RCM2018 referentes ao artigo n.º 35, alínea 9, do RGPD será necessário aplicar o controlo 5.2.2. existente na norma ISO/IEC 27701:2019.

Passo 2 – Mapeamento dos controlos da ISO/IEC 27701 e a ISO/IEC 27001/2

Input: Conjunto de controlos do passo 1 da Norma ISO/IEC 27701:2019.

Output: Conjunto de controlos da Norma ISO/IEC 27001:2013 e Norma ISO/IEC 27002:2013, que devem ser tidos em conta para cumprir o RGPD.

Atividade: Como foi referido anteriormente, a ISO 27701 promove a criação de sistemas eficazes para apoiar a conformidade com o RGPD e outros regulamentos de privacidade em todo o mundo. Sendo a ISO 27701 é uma extensão às normas ISO/IEC 27001/2 e considerando que as organizações já têm um SGSI baseado na ISO/IEC 27001/2 propõe-se a aplicação de um mapeamento que identifica explicitamente a relação entre a norma ISO/IEC 27701:2019 e a ISO/IEC 27001/2:2013. O mapeamento está ilustrado na Tabela 2 e Tabela 3 respetivamente, onde a primeira coluna mostra os procedimentos da Norma ISO/IEC 27701/2019 a serem implementados, para complementar os procedimentos da Norma ISO/IEC 27001:2013 (Tabela 2) e da Norma ISO/IEC 27002:2013 (Tabela 3) que se mostram na segunda coluna.

Norma ISO/IEC 27701/2019		**Norma ISO/IEC 27001:2013**
5.2.1.	**Compreender a organização e seu contexto:** A organização deve determinar o seu papel como controlador de dados de PII – *Personally Identifiable Information* (Informações de Identificação Pessoal) e / ou um processador de dados PII.	**4.1 Compreender a organização e o seu contexto:** A organização deve determinar as questões internas e externas que são relevantes para a sua finalidade e que afetam a sua capacidade para alcançar os resultados pretendido.
5.2.2.	**Compreender as necessidades e expectativas das partes interessadas:** A organização deve incluir entre as suas partes interessadas, as que tenham interesses ou responsabilidades associadas com o processamento de PII, incluindo os diretores PII.	**4.2 Compreender as necessidades e as expectativas das partes interessadas:** Quais as partes interessadas que são relevantes para o sistema de gestão de segurança de informação; os requisitos, destas partes interessadas, relevantes para a segurança da informação.
5.2.3.	**Determinar o escopo do sistema de gestão de segurança da informação:** Ao determinar o alcance dos PIMS, a organização deve incluir o processamento de PII.	**4.3 Determinar o âmbito do sistema de gestão de segurança de informação:** A organização deve determinar os limites e aplicabilidade do SGSI para estabelecer o seu âmbito.
5.2.4.	**Sistema de gestão de segurança da informação:** A organização deve estabelecer, implementar, manter e melhorar continuamente um PIMS de acordo com os requisitos da ISO/IEC 27001:2013.	**4.4 Sistema de gestão de segurança da informação:** A organização deve estabelecer, implementar, manter e

Norma ISO/IEC 27701/2019		Norma ISO/IEC 27001:2013
		melhorar de forma contínua um SGSI de acordo com os requisitos desta Norma.
5.4.1.2.	**Avaliação de riscos de segurança da informação:** A organização deve aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade, no âmbito dos PIMS.	**6.1.2 Avaliação do risco de segurança da informação:** alínea c) 1) identificar os riscos de segurança da informação: aplicando o processo de avaliação do risco de segurança da informação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação; e, identificando os responsáveis pelos riscos.
5.4.1.3.	**Informações sobre o tratamento risco de segurança:** ao avaliar a aplicabilidade dos objetivos de controle e controles da ISO/IEC 27001:2013 Anexo A para o tratamento de riscos, os objetivos e controlos devem ser considerados no contexto de ambos os riscos para a segurança da informação, bem como os riscos relacionados ao tratamento de PII, incluindo riscos para diretores PII.	**6.1.3 Tratamento do risco de segurança da informação:** alínea c) comparar os controlos determinados em 6.1.3.b com os controlos do Anexo A e verificar se não foram omitidos controlos que sejam necessários.

Tabela 2 – Mapeamento dos controlos da ISO/IEC 27701 e a ISO/IEC 27001 (Fonte: (ISO, ISO/IEC 27701:2019, 2019), (ISO, ISO/IEC 27001 - Information Security Management, 2013))

Norma ISO/IEC 27701/2019		Norma ISO/IEC 27002:2013
6.5.2.1.	**Classificação da informação:** O sistema de classificação da informação da organização deve considerar explicitamente as PII como parte do esquema implementado.	**8.2.1 Classificação da informação:** As informações devem ser classificadas em termos de requisitos legais, valor, criticidade e sensibilidade à divulgação ou modificação não autorizada.
6.5.3.1.	**Manuseamento de Multimédia**: a organização deve documentar qualquer uso de multimédia e / ou dispositivos amovíveis para o armazenamento de PII. Sempre que possível, a organização deve usar multimédia física amovível e / ou dispositivos que permitam criptografia ao armazenar PII.	**8.3.1 Manuseamento de Multimédia:** Os procedimentos devem ser implementados para a gestão de multimédia amovível, de acordo com o esquema de classificação adotado pela organização.
6.5.3.3.	**Utilização de Multimédia Removível:** quando um disco removível for utilizado para transferência de informações, o sistema deve estar implementado	**8.3.3 Utilização de Multimédia Removível:** Toda a multimédia que

Norma ISO/IEC 27701/2019		Norma ISO/IEC 27002:2013
	para gravar informações sobre entrada e saída, incluindo o tipo de multimédia utilizado, o remetente / destinatário autorizado, a data e a hora, e o número utilizado.	contém informações deve ser protegida contra acesso não autorizado, uso indevido ou corrupção durante o transporte.
6.7.1.1.	**Política de utilização de controlos criptográficos**: Algumas jurisdições podem exigir a utilização de criptografia para proteger tipos específicos de PII, como dados de saúde, números de registo de residentes, números de passaporte e números de carteira de motorista.	**10.1.1 Política de utilização de controlos criptográficos:** Deve ser implementada uma política sobre a utilização de controlos criptográficos para proteção de informação.
6.9.3.1.	**Cópias de Segurança**: A organização deve ter uma política que atenda aos requisitos de cópia de segurança, recuperação e restauro de PII e quaisquer outros requisitos para o apagamento das PII contidas em informações mantidas por requisitos de cópias de segurança.	**12.3.1 Cópias de Segurança:** Cópias de segurança de informação, software e imagens do sistema devem ser guardadas e testadas regularmente de acordo com uma política de backup implementada.
6.11.1.2.	**Proteger serviços de aplicativos em redes públicas**: a organização deve garantir que as IPI transmitidas por redes de transmissão de dados não confiáveis sejam criptografadas para transmissão.	**14.1.2 Proteger serviços de aplicativos em redes públicas:** As informações envolvidas nos serviços de aplicativos que passam por redes públicas devem ser protegidas contra atividade fraudulenta, disputa de contrato e divulgação e modificação não autorizadas.
6.11.2.1.	**Política de desenvolvimento seguro:** Devem incluir orientações para o processamento das necessidades de PII da organização, com base nos princípios de PII e / ou em qualquer legislação e / ou regulamentação aplicável e nos tipos de processamento realizados pela organização.	**14.2.1 Política de desenvolvimento seguro:** Regras para o desenvolvimento de software e sistemas devem ser estabelecidas e aplicadas dentro da organização.
6.11.3.1.	**Proteção de dados de teste**: não se deve utilizar PII para fins de teste; deve optar-se por PII falsos. Quando a utilização de PII para fins de teste não puder ser evitado, devem ser colocadas em prática medidas técnicas e organizacionais equivalentes às usadas no ambiente de produção para minimizar os riscos.	**14.3.1 Proteção de dados de teste:** Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

Norma ISO/IEC 27701/2019		Norma ISO/IEC 27002:2013
6.12.1.2.	**Segurança nos contratos com os fornecedores:** A organização deve especificar acordos com os fornecedores de modo a especificar se as PII são processadas e quais as medidas técnicas e organizacionais mínimas que o fornecedor precisa adotar para que a organização cumpra as suas obrigações de segurança das informações e proteção de PII.	**15.1.2 Segurança nos contratos com os fornecedores:** Todos os requisitos relevantes de segurança da informação devem ser estabelecidos e acordados com cada fornecedor que pode aceder, processar, armazenar, comunicar ou fornecer componentes de infraestrutura de TI para as informações da organização.
6.13.1.1.	**Responsabilidades e procedimentos:** Como parte do processo geral da gestão de incidentes de segurança da informação, a organização deve estabelecer responsabilidades e procedimentos para a identificação e registo de violações de PII.	**16.1.1 Responsabilidades e procedimentos:** Devem ser estabelecidas responsabilidades e procedimentos de gestão para garantir uma resposta rápida, eficaz e ordenada aos incidentes de segurança da informação.
6.13.1.5.	**Resposta a incidentes de segurança da informação:** Um incidente que envolva PII deve desencadear uma revisão pela organização, como parte do seu processo de gestão de incidentes de segurança da informação, para determinar se ocorreu uma violação envolvendo PII que requer resposta.	**16.1.5 Resposta a incidentes de segurança da informação:** Os incidentes de segurança da informação devem ser tratados de acordo com os procedimentos documentados.
6.15.1.1.	**Identificação da legislação aplicável e requisitos contratuais:** A organização deve identificar possíveis sanções legais (que podem resultar do não cumprimento de algumas obrigações) relacionadas ao processamento de PII, incluindo multas substanciais diretamente da autoridade supervisora local.	**18.1.1 Identificação da legislação aplicável e requisitos contratuais:** Todos os requisitos legais, regulamentares, contratuais e legislativos relevantes e respetiva abordagem da organização para atender a esses requisitos devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação e organização.
6.15.2.1.	**Revisão independente da segurança da informação: A** organização deve disponibilizar aos clientes, antes de celebrar e pela duração de um contrato, evidência independente de que as informações e respetiva segurança é implementada	**18.2.1 Revisão independente da segurança da informação:** A abordagem da organização para realizar a gestão da segurança das informações e respetiva implementação devem ser revistos independentemente, em intervalos

Norma ISO/IEC 27701/2019		Norma ISO/IEC 27002:2013
	e operada de acordo com as políticas e procedimentos da organização.	planeados ou quando ocorram alterações significativas.
6.15.2.3.	**Revisão de conformidade técnica:** Como parte das análises técnicas de conformidade com políticas e padrões de segurança, a organização deve incluir métodos de revisão dessas ferramentas e componentes relacionados ao processamento de PII.	**18.2.3 Revisão de conformidade técnica:** Os sistemas de informação devem ser verificados regularmente quanto à conformidade com as políticas e padrões de segurança da informação da organização.

Tabela 3 – Tabela de relação entre a norma ISO/IEC 27701:2019 e a norma ISO/IEC 27002:2013 (Fonte: (ISO, ISO/IEC 27701:2019, 2019), (ISO, ISO/IEC 27002:2013, 2013))

Por último, existem ainda, controlos novos a aplicar e que não têm correlação com as Norma ISO/IEC 27001:2013 e Norma ISO/IEC 27002:2013, mas que são essenciais para que sejam cumpridos os requisitos exigidos no RGPD. Esses controlos adicionais estão resumidos na Tabela 4. Por exemplo, o artigo n.º 32, alínea 4, da RGPD, será necessário aplicar o controlo 7.2.1. da Norma ISO/IEC 27701:2019.

Norma ISO/IEC 27701/2019	Designação do Controlo
7.2.1.	**Identificar e comunicar a finalidade**: A organização deve identificar e documentar os objetivos específicos para os quais as PII serão processadas.
7.2.2.	**Identificar a base legal:** A organização deve determinar, documentar e cumprir a base legal relevante para o processamento de PII cujos os fins sejam identificados.
7.2.5.	**Avaliação do impacto na privacidade:** A organização deve avaliar a necessidade e implementar, quando apropriado, um impacto na privacidade.
7.3.6.	**Acesso, correção e / ou apagamento:** A organização deve implementar políticas, procedimentos e / ou mecanismos para cumprir as suas obrigações para aceder, corrigir e / ou apagar suas PII.
7.3.8.	**Fornecer cópias das PII processadas**: A organização deve poder fornecer uma cópia das PII processadas quando solicitadas pelo titular da PII.
7.4.2.	**Limite de processamento:** A organização deve limitar o processamento de PII ao adequado, relevante e necessário para os fins identificados.
7.4.5.	**Identificação e apagamento de PII no final do processamento:** A organização deve eliminar as PII ou identifica-las de uma forma que não permita a identificação ou reidentificação de entidades da PII, assim que a PII original não seja mais necessária para o(s) objetivo(s) identificado(s).

Norma ISO/IEC 27701/2019	Designação do Controlo
8.2.1.	**Contrato do cliente:** A organização deve garantir, quando relevante, que o contrato para processar PII cumpra o papel da organização em fornecer assistência às obrigações do cliente (levando em conta a natureza do processamento e as informações disponíveis para a organização).
8.3.1.	**Obrigações dos diretores de PII**: A organização deve fornecer ao cliente os meios para cumprir as suas obrigações relacionadas aos princípios de PII.

Tabela 4 – Controlos adicionais à norma ISO/IEC 27002 existentes na norma ISO/IEC 27701:2019 (Fonte: (ISO, ISO/IEC 27701:2019, 2019), (ISO, ISO/IEC 27002:2013, 2013))

Passo 3

Input: Análise de documentação existente na entidade.

Output: "Documento de aplicabilidade dos controlos da Norma ISO/IEC27701:2019 para verificação da conformidade com o RGPD". Essa documentação demonstra a conformidade com o RGPD indicando evidencias e a classificação.

Atividade: A Declaração de Aplicabilidade é o documento que tem como objetivo ser o elo de ligação entre a avaliação, tratamento de riscos e a implementação do sistema de segurança da informação e é responsável pelo planeamento, implementação, manutenção e melhoria do SGSI, através da documentação de cada controlo aplicável, por exemplo, se está implementado e respetiva medida da segurança.

Neste passo será então demonstrado, se o SGSI está em conformidade com o RGPD seguindo os controlos da ISO27701:2019 e as orientações técnicas da RCM2018.
O documento será composto por:

- Descrição do requisito da Norma ISO/IEC 27701/2019 a que se refere a orientação técnica da RCM2018 e consequente controlo que deve ser executado, referente à ISO/IEC 27001/2013;
- Análise e verificação da aplicabilidade do requisito no sistema de gestão de segurança da informação;
- Demonstração da sua evidencia, ou seja, a existência de uma prova, por exemplo documento interno, log de eventos;
- Realização da sua classificação (implementado, em implementação, a implementar, implementado e sujeito a melhorias).

4. PLANO DE AÇÃO

Nesta secção é apresentado um plano ação tendo em vista a aplicação da proposta a uma organização com base na abordagem *action research*[1]. O plano iniciar-se-á com a análise da organização e a execução da atividade do passo 2 e 3 descrito na seção anterior. Esta análise envolve um dos autores deste trabalho e representantes dos diferentes níveis da organização: Direção; Comité de Segurança da Informação; Gestor de Segurança da Informação; Gestores de negócio; Áreas de Suporte e Colaboradores.

4.1. Organização - Entidade pública

A entidade pública em causa, é um serviço que visa a promoção da melhoria das condições de trabalho. Esta entidade possui o documento de aplicabilidade desde o ano 2018, baseado na ISO/IEC 27001.

4.2. Plano e resultados esperados de cada fase do processo.

Segundo a Figura 1, o trabalho foi realizado em três passos: o primeiro devolve o conjunto de controlos referentes à norma ISO/IEC 27701 que devem ser tidos em conta para cumprir o RGPD, segundo a RCM2018; o segundo passo define o conjunto de controlos da Norma ISO/IEC 27001:2013 e Norma ISO/IEC 27002:2013, complementados com a Norma ISO/IEC 27701:2019, e por último, no terceiro passo, obtém-se o documento de aplicabilidade que irá demonstrar a conformidade do SGSI com o RGPD implementado na entidade, coadjuvado com as especificações técnicas do RCM2018.

Para a elaboração do documento de aplicabilidade, os controlos do passo dois do processo são analisados tendo em vista a verificação da conformidade ou não, com base no conteúdo do SGSI da organização.

Por motivos de espaço, o documento de aplicabilidade é ilustrado usando apenas três controlos. Tabela 5 ilustra a informação, nos termos descritos na fase 3 do processo, sobre a conformidade do controlo 5.2.1. Compreender a organização e seu contexto (ISO 27701).

A Tabela 6 mostra a informação, nos termos descritos na fase 3 do processo, sobre a conformidade e sujeito a melhorias, do controlo 6.5.2.1. Classificação da informação (ISO 27701).

A Tabela 7 mostra a informação, nos termos descritos na fase 3 do processo, sobre a não conformidade do controlo 6.15.2.3. Revisão de conformidade técnica (ISO 27701).

[1] Método de investigação-ação onde o investigador é também colaborador/funcionário na organização.

5.2.1. Compreender a organização e seu contexto: A organização deve determinar o seu papel como controlador de dados de PII – *Personally Identifiable Information* (Informações de Identificação Pessoal) e / ou um processador de dados PII.	
Controlo	deve ser executado, adicionalmente ao controlo 4.1 da norma ISO/IEC 27001:2013 (**Compreender a organização e o seu contexto -** A organização deve determinar as questões internas e externas que são relevantes para a sua finalidade e que afetam a sua capacidade para alcançar o(s) resultado(s) pretendido(s) do seu sistema de gestão de segurança da informação.)
Análise	"Para assegurar a gestão efetiva de Segurança da Informação foi alinhada uma estrutura que se estende pelos níveis estratégico, tático e operacional responsáveis pela orientação, planeamento, implementação, manutenção e melhoria do Sistema de Gestão de Segurança da Informação. Esta estrutura considera a necessidade de descentralizar as responsabilidades da gestão da Segurança da Informação pelas várias divisões da entidade." (Estrutura Organizacional, 2018)
Evidências	Documento Interno, Estrutura Organizacional, 2018
Classificação	Em implementação

Tabela 5 – Controlo em conformidade com o RGPD

6.5.2.1. Classificação da informação: O sistema de classificação da informação da organização deve considerar explicitamente as PII como parte do esquema implementado. Considerar as PII dentro do sistema de classificação geral é essencial para entender os dados processados e armazenados pela organização.	
Controlo	deve ser executado, adicionalmente ao controlo 8.2.1 da norma ISO/IEC 27002:2013 (**Classificação da informação -** As informações devem ser classificadas em termos de requisitos legais, valor, criticidade e sensibilidade à divulgação ou modificação não autorizada.)
Análise	O âmbito da Política de Classificação da Informação aplica-se a todos os colaboradores da entidade (independentemente da sua função, posição hierárquica e vínculo contratual), fornecedores e parceiros, e outros que tenham acesso a informação sensível. As entidades externas com acesso a informação da entidade devem considerar a presente política como recomendação na

	classificação de toda a informação (gerada, processada, transmitida ou arquivada) da sua instituição.
Evidências	Documento Interno, Política de Classificação da Informação, 2018
Classificação	Implementado, sujeito a melhorias

Tabela 6 – Controlo em conformidade mas sujeito a melhorias com o RGPD

6.15.2.3. Revisão de conformidade técnica: Como parte das análises técnicas de conformidade com políticas e padrões de segurança, a organização deve incluir métodos de revisão dessas ferramentas e componentes relacionados ao processamento de PII. Isso pode incluir: i. monitorização contínuo para verificar se apenas o processamento permitido está a ser efetuado; e / ou ii. testes específicos de penetração ou existência de vulnerabilidades.	
Controlo	deve ser executado, adicionalmente ao controlo 18.2.3 da norma ISO/IEC 27002:2013 (**Revisão de conformidade técnica -** Os sistemas de informação devem ser verificados regularmente quanto à conformidade com as políticas e padrões de segurança da informação da organização.)
Análise	Sem evidências
Evidências	Sem evidências
Classificação	Não implementado

Tabela 7 – Controlo em não conformidade com o RGPD

No fim deste processo, os *stakeholders* deverão analisar as conformidades e desenvolver um plano de ação para mitigar os controlos que não estão em conformidade e que, de acordo com o RCM2018 são obrigatórios.

4.3. Recomendações

A proposta é um guia de forma a que a entidade, publica ou privada, possuindo um SGSI, tenha a capacidade para verificar a conformidade para com o RGPD.

Caso não possua no momento um SGSI implementado ou iniciado, tem um método para desenvolver o trabalho, sabendo de antemão quais os controlos mais importantes a apresentar.

Para que a proposta possa ser aplicada é necessário o apoio de alguns setores da entidade: direção, divisão de sistemas de informação e núcleo de proteção de dados pessoais com o objetivo de ter acesso à documentação e processos de negócio. Cabe destacar que no núcleo de proteção de dados tem que existir o encarregado de proteção de dados, do inglês, *Data Protection Officer* (DPO).

Durante a aplicação do processo não foram identificados obstáculos. No entanto, e caso existam, deve por exemplo, procurar o envolvimento da parte da direção na verificação da conformidade da entidade, através da demonstração da possibilidade de eventuais fugas de dados, o que iria gerar uma má imagem que a entidade poderia dar aos seus utentes como consequência e ainda a possibilidade de aplicação de coimas.

5. CONCLUSÃO

O processo e os mapeamentos aqui apresentados são meios que podem coadjuvar uma empresa a garantir a conformidade com o RGPD, em particular se a empresa tiver o documento de aplicabilidade da ISO/EIC 27000. Não obstantes esta condição, acreditamos que os mapeamentos podem ser usados por qualquer empresa, independentemente do seu grau de maturidade com respeito aos controlos de segurança. Com a família da ISO 27k é possível reforçar a segurança dos dados e exigir que as organizações garantam a confidencialidade, integridade e disponibilidade dos dados. Esta família de normas segue o modelo de ciclo de processo *Plan-Do-Check-Act* (PDCA) de melhoria contínua que, por sua vez, promove a resiliência.

Por último, considerando a evolução natural dos SGSI é importante manter altos níveis de desempenho. Neste sentido, propomos que o processo seja aplicado continuamente tendo em vista apoiar a melhoria continua e, consequentemente, a adaptação do SGSI aos novos cenários, nomeadamente ao cenário que se prevê que irá ocorrer na "época" pós-pandemia, com a inclusão, por exemplo do teletrabalho.

REFERÊNCIAS

Correia, C. M. (novembro de 2016). *Plano de Implementação da Norma ISO 27001 no INEM.* Obtido em 1 de novembro de 2019, de https://run.unl.pt/bitstream/10362/19605/1/TGI0069.pdf

Europeia, P. E. (27 de abril de 2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.* Obtido em 9 de novembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Godinho, P. X. (2014). Estudo do grau de alinhamento dos STI com a norma ISO 27000. Beja: Ipbeja.

ISO. (outubro de 2013). *ISO/IEC 27001 - Information Security Management.* Obtido em 9 de novembro de 2019, de https://www.iso.org/standard/54534.html

ISO. (outubro de 2013). *ISO/IEC 27002:2013.* Obtido em 9 de novembro de 2019, de ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls: https://www.iso.org/standard/54533.html

ISO. (fevereiro de 2018). *ISO/IEC 27000:2018.* Obtido em 9 de novembro de 2019, de ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary: https://www.iso.org/standard/73906.html

ISO. (agosto de 2019). *ISO/IEC 27701:2019.* Obtido em 20 de dezembro de 2019, de ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines: https://www.iso.org/standard/71670.html

Magalhães, F., & Pereira, M. (2017). *Regulamento Geral de Proteção de Dados - Manual Prático.* Vida Económica.

Ministros, P. d. (28 de março de 2018). *Resolução do Conselho de Ministros n.º 41/2018.* Obtido em 27 de dezembro de 2019, de DRE: https://dre.pt/home/-/dre/114937034/details/maximized