Association for Information Systems
AIS Electronic Library (AISeL)

CAPSI 2019 Proceedings | Portugal (CAPSI)

10-2019

Integrated Information Security and Privacy Management System

Ekaterina Volchkova

Follow this and additional works at: https://aisel.aisnet.org/capsi2019

This material is brought to you by the Portugal (CAPSI) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CAPSI 2019 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Sistema de Gestão Integrada de Privacidade e Segurança da Informação

Integrated Information Security and Privacy Management System

Volchkova, Gfi Portugal, Portugal, ekaterina.volchkova@gfi.world

Resumo

A complexidade dos processos de tratamento de dados pessoais nas entidades do Serviço Nacional de Saúde (SNS) cria desafios na adoção de normas de privacidade e segurança da informação. A necessidade de obter resultados práticos no curto prazo, devido à aplicação do Regulamento Geral Sobre a Proteção de Dados (RGPD), levou as organizações a procurarem novas abordagens para ultrapassar a escassez de competências e recursos disponíveis.

A abordagem aqui proposta consiste na implementação do Sistema de Gestão Integrada de Privacidade e Segurança da Informação (SGISIP). Assim, no decurso de 2017, e no âmbito de uma tese de mestrado, foi definida uma *framework* genérica a utilizar pelas entidades do setor da saúde para orientar a implementação do SGISIP.

O presente artigo visa dar breve descrição do trabalho desenvolvido, e dos controlos que foram adicionados ao Anexo A da norma ISO/IEC 27001:2013 para dar resposta efetiva aos requisitos do RGPD.

Palavras-chave: Privacidade; Proteção de Dados; Segurança da Informação; RGPD; GDPR.

Abstract

The complexity of the personal data processing in the entities of the National Health Service (NHS) creates challenges in the adoption of privacy and information security standards. The need for practical results in the short term due to the application of the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS Directive) leads organizations to seek new approaches to overcome the lack of competencies and available resources.

The proposed approach consists of implementation of the Integrated Information Security and Privacy Management System (IISPMS). The master´s thesis which results are described in this article was developed in 2017 with the objective of defining a generic framework to be used by health sector entities to guide the implementation of the IISPMS.

This article aims to describe the project and the controls that have been added to Annex A of ISO/IEC 27001:2013 to meet the requirements of the GDPR.

Keywords: *Privacy; Data Protection; Information Security; GDPR.*

1. INTRODUÇÃO

Embora o Regulamento Geral Sobre a Proteção de Dados (RGPD) foque-se na proteção de dados pessoais, a sua aplicação resulta na transformação transversal da paisagem digital em toda a Europa, e até mesmo ao nível mundial, virando as empresas para as atitudes mais pró-ativas em relação à

segurança da informação e incentivando-as a investir na "aplicação das medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco" (n.º 1 do artigo 32.º do RGPD).

O RGPD não contem o requisito explícito para a implementação do Sistema de Gestão de Segurança da Informação (SGSI), contudo, a abordagem descrita nos seus artigos 24.º e 32.º corresponde ao ciclo da gestão do risco para estabelecimento, monitorização, manutenção e melhoria do SGSI que está subjacente ao conjunto das normas ISO/IEC 27k.

Diversas organizações nacionais e europeias seguiram esta lógica disponibilizando as recomendações específicas para endereçar os requisitos do RGPD através da implementação da norma ISO/IEC 27001:2013.

No entanto, analisando o alinhamento proposto pela Agência Europeia para a Segurança das Redes e da Informação ENISA (ENISA, 2016) e Confederação da Indústria Dinamarquesa CID (Mortensen, 2016) entre os requisitos do RGPD e controlos do Anexo A da norma ISO/IEC 27001:2013, consideramos que esta abordagem é limitada apenas ao campo de implementação de controlos e não prevê os mecanismos que permitam sustentar e melhorar os controlos implementados e ajudar as organizações ao cumprimento – ininterrupto – das obrigações de responsável pelo tratamento ou subcontratante, especialmente no que diz respeito à obrigação de assegurar e poder comprovar a qualquer momento que o tratamento é realizado em conformidade com o RGPD.

Do nosso ponto de vista, para além da implementação dos controlos de privacidade e segurança da informação propriamente ditos, é crucial, para efeitos de comprovação da conformidade com o RGPD, a implementação de um Sistema de Gestão Integrada de Segurança da Informação e Privacidade (SGISIP) com especial enfoque no estabelecimento das práticas de avaliação e tratamento de riscos de privacidade e segurança da informação, avaliação do desempenho e da eficácia do SGISIP, bem como o tratamento de não conformidades e melhoria contínua.

Adicionalmente, os controlos de segurança da informação (Anexo A da norma ISO/IEC 27001:2013) devem ser complementados com os controlos de privacidade para garantir o cumprimento das obrigações que vão para além do campo de segurança da informação, tais como o cumprimento dos direitos de titulares de dados (o direito de acesso do titular dos dados, direito de retificação, direito ao apagamento dos dados, direito à limitação do tratamento e outros). Outro grupo de requisitos do RGPD, que devem ser incorporados dentro do SGISIP, abrange as questões da licitude e lealdade do tratamento.

2. OBJETIVOS DO PROJETO

Limitando o âmbito do trabalho ao setor da saúde em Portugal, foi estabelecido como principal objetivo a definição de uma *framework* genérica para o SGISIP nas entidades do Serviço Nacional

de Saúde (SNS), alinhada com os requisitos e controlos da norma ISO 27001 e com os requisitos do RGPD. Adicionalmente foi decidido incluir na *framework* os controlos específicos para cumprir os requisitos da Diretiva SRI para os prestadores de serviços essenciais do setor da saúde.

3. DESCRIÇÃO DO PROJETO

Depois da exclusão dos artigos relacionados com o âmbito da aplicação da legislação, definições e diversos aspetos da implementação, todos os requisitos do RGPD e da Diretiva SRI foram listados e analisados na perspetiva da sua aplicabilidade para o setor da saúde português.

A seguir foram definidos os controlos de segurança da informação e privacidade necessários para garantir o cumprimento dos requisitos do RGPD e da Diretiva SRI identificados anteriormente.

O consecutivo mapeamento com os controlos do Anexo A da norma ISO 27001 permitiu dividir todos os controlos a seguinte maneira:

A – Controlos de Segurança da Informação - 149 no total – foram divididos em duas categorias:

- 114 controlos do Anexo A da norma ISO/IEC 27001:2013 que, dependendo do tipo de controlo, correspondem na integra aos controlos originais da norma ou necessitam alguma atualização devido à inclusão dos requisitos da proteção de dados e privacidade. Embora a descrição detalhada destes controlos fique fora do âmbito do presente artigo, no capítulo 5 podem ser encontradas as referências às alterações mais significativas que devem ser tidas em conta;

- 35 novos controlos de segurança da informação que foram acrescentados aos já existentes no Anexo A da norma ISO/IEC 27001:2013, por forma a assegurar o cumprimento dos requisitos do RGPD e da Diretiva SRI. Os mesmos estão consolidados no capítulo 5 do presente artigo.

B – Controlos de Privacidade foram introduzidos para guiar as unidades clínicas e operacionais das entidades do SNS no processo da implementação do SGISIP, garantindo o cumprimento dos requisitos do RGPD e da Diretiva SRI nas três vertentes:

- **B1 – Licitude de Tratamento** é uma categoria de controlos que devem ser escolhidos em função do fundamento jurídico para tratamento a fim de assegurar a sua licitude de acordo com o RGPD (27 controlos);

- **B2 – Privacidade de Operações** é uma categoria de controlos necessários para garantir cumprimento dos direitos de titulares de dados de acordo com o RGPD (9 controlos).

- **B3 – Proteção Específica dos Dados Pessoais** é uma categoria de controlos composta pela lista das situações que exigem a proteção específica de acordo com o RGPD (10 controlos).

Os controlos de privacidade estão consolidados no capítulo 6 do presente artigo.

A figura 1 visualmente representa a estrutura de sub-categorias de controlos de segurança da informação e privacidade descritos nos capítulos 5 e 6 do presente artigo.

4. ASPETOS PRÁTICOS NA IMPLEMENTAÇÃO DO SGISIP

Previamente à descrição dos controlos de privacidade sugeridos para adicionar ao Anexo A da norma ISO/IEC 27001:2013, consideramos importante comentar alguns aspetos relevantes da implementação do SGISIP numa perspetiva de adequação ao RGPD.

O corpo principal da norma ISO/IEC 27001:2013 contem uma lista de requisitos necessários para estabelecer, implementar, manter e melhorar de forma contínua o Sistema de Gestão de Segurança da Informação (SGSI). O Sistema de Gestão Integrada de Segurança da Informação e Privacidade (SGISIP) deve também cumprir com os mesmos, no entanto, os requisitos devem ser devidamente atualizados a fim de abranger, para alem da vertente de Segurança da Informação, a dimensão de Privacidade e Proteção de Dados.

Quanto a implementação do SGISIP é importante considerar os seguintes aspetos:

Contexto da organização

Na fase da análise do contexto interno e externo para estabelecer o âmbito do SGISIP a organização deve determinar os seus limites e aplicabilidade, considerando, para além das questões referidas no requisito 4.3 da norma ISO/IEC 27001:2013, os seguintes pontos:

- as categorias dos dados pessoais tratados pela organização, bem como a natureza, o âmbito, o contexto e as finalidades do tratamento a que os dados pessoais se destinam;
- os serviços, prestados pela organização, que são essenciais para a manutenção de atividades societais e económicas cruciais, de acordo com a Diretiva SRI.

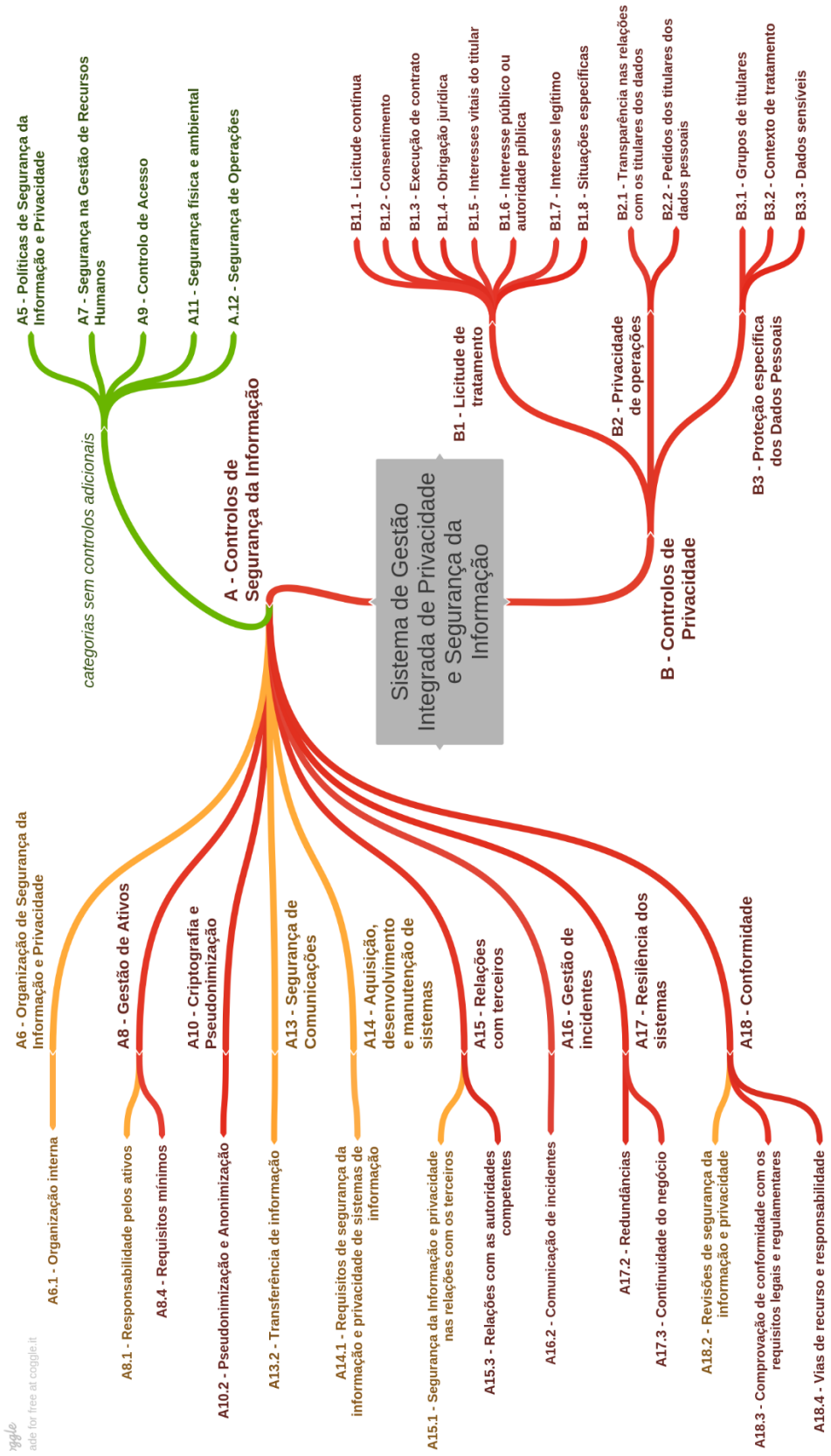

Figura 1 – *Mindmap* de controlos adicionais relativos ao Anexo A da Norma ISO/IEC 27001:2013

LEGENDAS:
- Novas categorias dos controlos
- Categorias dos controlos existentes na norma ISO/IEC 27001:2013 que foram alargadas por novos controlos
- Categorias dos controlos existentes na norma ISO/IEC 27001:2013 que não foram alargadas por controlos adicionais

Liderança

Quanto a definição de funções, responsabilidades e autoridades na organização (requisito 5.3 do corpo da norma ISO/IEC 27001:2013) as entidades do SNS, de acordo com o n.º 1 do artigo 37.º do RGPD, têm obrigação de nomear o Encarregado da Proteção de Dados (EPD), que na prática frequentemente tem alocação parcial e não dispõe independência e recursos necessários para desempenhar as suas funções com sucesso. É crucial definir e formalizar as funções do EPD, garantindo a segregação de funções com áreas jurídica e de segurança da informação.

Deve ser claro para todas as partes envolvidas que garantir o tratamento lícito, leal e transparente em relação ao titular dos dados, é da responsabilidade direta do negócio e inconformidade com o RGPD não pode ser incumbida ao EPD.

Planeamento e Operação

Nas fases de planeamento e operação do SGISIP, para além das atividades abrangidas pelo processo da gestão de risco de segurança da informação (pts. 6 e 8 do corpo da norma ISO/IEC 27001:2013), o mesmo deve prever a identificação dos riscos para os direitos e liberdades das pessoas singulares antes de iniciar um certo tipo de tratamento, em particular, caso utilize novas tecnologias, avaliando o impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

É crucial garantir alinhamento da metodologia da Avaliação de Impacto da Proteção de Dados (AIPD) com a metodologia da Gestão de Risco de Segurança da Informação, bem como com o processo de gestão de risco empresarial para poder comunicar efetivamente com todas as linhas de gestão utilizando a mesma linguagem e escalas de risco.

O processo da AIPD deve prever as atividades necessárias para efetuar a consulta a autoridade de controlo antes de proceder ao tratamento dos dados pessoais, quando a avaliação de impacto sobre a proteção de dados indicar que desse tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

Suporte

O desafio, no âmbito de segurança de informação e privacidade nas entidades do SNS, passa pela complexidade dos processos internos de tratamento de dados pessoais quando colocado num contexto de transparência, interoperabilidade e portabilidade dos dados e informação entre as entidades do setor da saúde, bem como pela necessidade de obter resultados práticos no curto prazo em situação de escassez das capacidades e recursos disponíveis.

Entendemos que melhores resultados podem ser alcançados através da integração dos processos da gestão de privacidade com processos de gestão de segurança da informação e outros processos já

existentes na organização (gestão de serviços IT, gestão de fornecedores, gestão de risco geral e risco clínico, etc.).

Uma transformação de cultura empresarial desta amplitude exige implementação de um programa robusto de gestão de mudança com múltiplos canais de comunicação. O aspeto importante a controlar é a coerência das mensagens no âmbito da privacidade divulgadas em diversas ocasiões e pelos vários departamentos envolvidos neste processo (legal, segurança da informação, privacidade, recursos humanos, etc.).

Avaliação de desempenho (9) e Melhoria contínua (10)

Finalmente é necessário sublinhar a importância que ganham os processos de gestão documental (7.5), avaliação de desempenho (9) e melhoria contínua (10) para demonstrar e poder comprovar a conformidade com o RGPD em qualquer momento. Neste contexto torna-se indispensável a implementação das ferramentas GRC para gestão de risco e conformidade (*Governace, Risk & Compliance*) que, ao contrário dos processos implementados com base nos formulários em excel, permitem garantir automatização e agilização dos processos, libertando simultaneamente recursos competentes para outras atividades de valor acrescentado. A escolha de ferramenta apropriada e adaptação dos processos estandardizados à realidade da organização diminui resistência organizacional e contribui para adotação duradoura dos processos de gestão de risco e melhoria contínua.

5. CONTROLOS DE SEGURANÇA DA INFORMAÇÃO A INTEGRAR NO SGISIP

Segue descrição de controlos de segurança da informação a adicionar ao Anexo A da norma ISO/IEC 27001:2013 a fim de garantir gestão integrada de Segurança da Informação e Privacidade.

A.6 - Organização de Segurança da Informação e Privacidade

A sub-categoria A.6.1 (Organização interna) foi alargada por forma a prever o necessário controlo de garantia de comunicação eficaz com titulares de dados:

- Controlo A.6.1.6 - Contacto com titulares dos dados pessoais.

Estabelecer e manter os canais de comunicação apropriados com os titulares dos dados pessoais facilita o cumprimento das várias obrigações impostas pelo RGPD, tais como comunicação de violações de dados pessoais, avaliação de impacto da proteção de dados, resposta aos pedidos de titulares. Por outro lado, a comunicação eficaz com titulares de dados pode ter impacto positivo na mitigação de riscos de litigância.

A.8 - Gestão de Ativos

A categoria A.8 (Gestão de ativos) foi alargada pelos controlos específicos para gestão do ciclo de vida:

- Controlo A.8.1.5 - Ciclo de vida dos dados pessoais;
- Controlo A.8.1.6 - Ciclo de vida da informação destinada ao público.

A implementação destes controlos visa garantir o cumprimento dos princípios relativos ao tratamento de dados pessoais ao longo do ciclo de vida da informação, endereçando também as questões relevantes para divulgação de conteúdos da informação destinados ao público no contexto de transparência na Administração Pública.

Os requisitos do RGPD impactam consideravelmente a abordagem para definição de esquemas de classificação da informação e escolha de medidas de segurança por classe de dados, levando à necessidade de ter em consideração a facilidade de identificação de pessoas singulares diretamente por referência a um identificador ou indiretamente através da análise de combinações de dados pessoais.

Para endereçar os requisitos do artigo 25.º do RGPD (Proteção de dados desde a conceção e por defeito) foi adicionado um novo grupo de controlos (A.8.4) para definição de requisitos mínimos (técnicos e organizativos) de segurança da informação e privacidade, consoante o tipo da tecnologia utilizada para o seu tratamento:

- Controlo A.8.4.1 - Requisitos mínimos para as várias categorias dos ativos;
- Controlo A.8.4.2 - Requisitos mínimos para integração dos sistemas.

A implementação destes controlos visa garantir a mitigação dos riscos associados à utilização das novas soluções tecnológicas para o tratamento dos dados pessoais, bem como à integração das diversas soluções tecnológicas entre si e/ou com sistemas legados na organização.

A.10 - Criptografia e Pseudonimização

No contexto do RGPD os controlos criptográficos previstos na norma ISO/IEC 27001:2013 devem ser complementados por controlos específicos para assegurar a utilização adequada e eficaz de pseudonimização e anonimização, garantindo que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

- Controlo A.10.2.1 - Política sobre a Pseudonimização e Anonimização.

A implementação adequada deste controlo permitirá as organizações efetuar operações de tratamento críticos reduzindo ou evitando (no caso de anonimização) os riscos para os titulares de dados.

A.13 - Segurança de Comunicações

Para além dos controlos já previstos na norma ISO/IEC 27001:2013 para transferências da informação, o RGPD introduz um novo controlo que pode ser aplicável às entidades do grupo(s) empresarial(ais) envolvidos numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o cumprimento das regras internas de proteção de dados:

- A.13.2.5 - Regras vinculativas aplicáveis às empresas.

A.14 - Aquisição, desenvolvimento e manutenção de sistemas

Como já referido, os princípios de engenharia de sistemas seguros (controlo A.14.2.5 da norma ISO/IEC 27001:2013) devem prever a segurança da informação e proteção de dados desde a conceção e por defeito.

Os requisitos para os sistemas da informação devem incluir, para alem dos referidos no controlo A.14.1.1 do anexo A da norma ISO/IEC 27001:2013, os de interoperabilidade, privacidade e proteção dos dados pessoais, bem como os referentes à tomada das decisões automatizadas. Tendo em consideração que o tratamento de dados pessoais pode ser efetuado por meios automatizados ou não automatizados, os mesmos requisitos devem ser definidos para novos processos de negócio ou para melhorias nos já existentes:

- Controlo A.14.1.4 - Especificação e análise de requisitos para os processos de negócio.

Por sua vez, é necessário acompanhar fatos novos relevantes e a evolução das tecnologias da informação, das comunicações e das práticas comerciais, na medida em que tenham incidência na segurança das redes e informação e na proteção de dados pessoais:

- Controlo A.14.1.5 - Levantamento dos progressos técnicos mais recentes.

O especial enfoque deve ser dado às novas ameaças cibernéticas, as vulnerabilidades que podem ser exploradas por elas e as possíveis medidas tecnológicas para o tratamento do risco associado.

A.15 - Relações com terceiros

A respetiva categoria de controlos da norma ISO/IEC 27001:2013 é aplicável no contexto da relação da organização com os seus fornecedores. No entanto, controlos semelhantes devem ser implementados para relações com qualquer parte envolvida no tratamento de dados pessoais da responsabilidade da organização.

Assim, o âmbito da política de segurança da informação para as relações com fornecedores (controlo A.15.1.1 do anexo A da norma ISO/IEC 27001:2013) deve ser alargado para incluir, para além dos fornecedores, todas as partes interessadas, nomeadamente, os responsáveis conjuntos pelo tratamento, os responsáveis pelo tratamento que delegam à organização o tratamento dos dados

pessoais por sua conta, bem como os subcontratantes que efetuam o tratamento dos dados pessoais por conta da organização e as autoridades de controlo que dispõem dos poderes de investigação.

Adicionalmente sugerimos implementar mecanismos de verificação de credenciais e referências de todos os potenciais subcontratantes, de acordo com as leis, regulamentações e códigos de ética relevantes, e de forma proporcional aos requisitos do negócio, à classificação da informação que será acedida e aos riscos percecionados:

- Controlo A.15.1.4 - Verificação de credenciais e referências dos subcontratantes.

A monitorização dos serviços de fornecedores (controlo A.15.2.1 do anexo A da norma ISO/IEC 27001:2013) deve também abranger a verificação do cumprimento pelos seus subcontratantes das obrigações contratuais e instruções documentadas, garantindo que os subcontratantes que efetuam o tratamento dos dados pessoais por conta da organização cumpram os requisitos do RGPD.

De igual forma, as relações com as autoridades competentes devem ser reguladas internamente, a fim de garantir o cumprimento dos procedimentos estabelecidos por lei no que respeita ao exercício dos seus poderes de investigação e de correção destes, bem como dos poderes consultivos e de autorização. Neste sentido foi introduzida uma nova sub-categoria (A.15.3 - Relações com as autoridades competentes) que engloba os seguintes controlos:

- Controlo A.15.3.1 - Cooperação com as autoridades competentes (autoridades de controlo);
- Controlo A.15.3.2 - Retificação, apagamento e limitação do tratamento de dados pessoais imposta pela autoridade de controlo;
- Controlo A.15.3.3 - Suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais por pedido da autoridade de controlo competente;
- Controlo A.15.3.4 - Consulta prévia;
- Controlo A.15.3.5 - Autorização da autoridade de controlo para transferência de informação;
- Controlo A.15.3.6 - Autorização da autoridade de controlo para estabelecimento de acordos administrativos, regras vinculativas e cláusulas contratuais.

A.16 - Gestão de incidentes de segurança da informação e privacidade

Face aos requisitos impostos pelo RGPD e Diretiva SRI, as entidades do SNS têm obrigação de comunicar os incidentes de cibersegurança para o Centro Nacional de Ciber Segurança (CNCS) e violações de dados pessoais para a Comissão Nacional de Proteção de Dados (CNPD) e titulares de dados.

Neste sentido, para garantir a notificação atempada às partes interessadas dos incidentes de segurança da informação e de violações de dados pessoais relevantes foi criada sub-categoria que abrange os seguintes controlos:

- Controlo A.16.2.1 - Notificação de violação de dados pessoais à autoridade de controlo;
- Controlo A.16.2.2 - Comunicação de violação de dados pessoais ao responsável pelo tratamento;
- Controlo A.16.2.3 - Comunicação de violação de dados pessoais aos titulares dos dados;
- Controlo A.16.2.4 - Notificação dos incidentes com um impacto importante na continuidade dos serviços essenciais às autoridades competentes ou as CSIRT;
- Controlo A.16.2.5 - Comunicação por subcontratantes de incidentes com impacto importante na continuidade dos serviços ao prestador de serviço essencial;
- Controlo A.16.2.6 - Notificação obrigatória centralizada dos incidentes de cibersegurança às autoridades competentes ou às CSIRT;
- Controlo A.16.2.7 - Comunicação de atividades ilícitas e crimes públicos.

A implementação destes controlos permite garantir que eventos e incidentes de segurança da informação e privacidade são reportados ao longo da cadeia de fornecimento e, justificando-se, para as autoridades competentes através dos canais de comunicação apropriados e o mais rapidamente possível.

A.17 - Resiliência dos sistemas e dos serviços de tratamento

A norma ISO/IEC 27001:2013 endereça apenas os aspetos de segurança da informação na gestão da continuidade do negócio, mas não impõe obrigações explícitas de garantir a continuidade de negócio.

No entanto, de acordo com o artigo 32.º do RGPD, o responsável pelo tratamento, em função do risco para os direitos e liberdades das pessoas singulares, deve implementar medidas técnicas e organizativas para assegurar a disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, bem como a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico. Já a Diretiva SRI preve que os operadores de serviços essenciais tomem as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.

Assim, torna-se essencial a implementação de controlos para garantir a recuperação célere de incidentes disruptivos quando surgem, garantindo a disponibilidade e o acesso aos sistemas, informação e dados pessoais de forma atempada:

- Controlo A.17.3.1 - Gestão da continuidade operacional;
- Controlo A.17.3.2 - Exercícios relativos a planos de contingência.

A.18 – Conformidade

Quando a organização atua como subcontratante é recomendável implementar controlo específico que permita facilitar a realização de auditorias de segurança da informação e privacidade, garantindo o seguimento atempado dos pedidos dos clientes da organização:

- Controlo A.18.2.4 - Auditorias e inspeções conduzidas pelos clientes.

Um dos conceitos importantes do RGPD é a responsabilização da organização não só por garantir conformidade com o Regulamento mas, igualmente, por comprová-lo. A fim de poder demonstrar o cumprimento das obrigações do responsável pelo tratamento, de acordo com a legislação aplicável, devem ser implementados os controlos da nova sub-categoria A18.3 (Comprovação de conformidade com os requisitos legais e regulamentares):

- Controlo A.18.3.1 - Adesão a um código de conduta;
- Controlo A.18.3.2 - Certificação em matéria de proteção de dados, selos e marcas de proteção de dados.

Em organizações do setor da saúde é crucial definir e implementar procedimentos para garantir o tratamento adequado das reclamações e uma representação adequada nos eventuais processos judiciais, a fim de minimizar os prejuízos associados às queixas de titulares de dados. Tais controlos foram agrupados na sub-categoria A.18.4 (Vias de recurso e responsabilidade):

- Controlo A.18.4.1 - Reclamações dos titulares dos dados pessoais contra a organização;
- Controlo A.18.4.2 - Reclamação contra a autoridade competente;
- Controlo A.18.4.3 - Queixa contra prestador de serviços digitais junto da entidade competente;
- Controlo A.18.4.4 - Ação judicial efetiva contra autoridade de controlo;
- Controlo A.18.4.5 - Ação judicial contra a organização;
- Controlo A.18.4.6 - Reclamação de parte da indemnização paga, atendendo à corresponsabilidade pelo dano;

- Controlo A.18.4.7 - Resposta à reclamação de parte da indemnização paga, atendendo à corresponsabilidade pelo dano.

6. CONTROLOS DE PRIVACIDADE A INTEGRAR NO SGISIP

De seguida são descritos os controlos de privacidade que, visando garantir a gestão integrada de Segurança da Informação e Privacidade e o cumprimento dos requisitos do RGPD. A consolidação no Anexo B, como proposto, complementam os controlos de segurança da informação definidos no Anexo A da norma ISO/IEC 27001:2013.

B.1 - Licitude de tratamento

A licitude de tratamento é um dos princípios relativos ao tratamento de dados pessoais consagrados pelo RGPD. Os controlos da **sub-categoria B.1.1 (Licitude contínua)** são obrigatórios independentemente do fundamento inicial para o tratamento de dados e permitem manter a licitude ao longo do ciclo da vida dos dados pessoais:

- Controlo B.1.1.1 - Registo das atividades de tratamento;
- Controlo B.1.1.2 - Tratamento posterior dos dados pessoais para outros fins;
- Controlo B.1.1.3 - Apagamento dos dados pessoais para garantir a licitude de tratamento.

Seguem elencados os controlos que devem ser implementados atento ao fundamento para tratamento de dados pessoais, tais controlos foram divididos em 6 sub-categorias, correspondentes às situações definidas como licitas para tratamento de dados pessoais no n.º 1 do artigo 6.º do RGPD:

Sub-Categoria B.1.2 – Consentimento:

- Controlo B.1.2.1 - Consentimento para tratamento dos dados pessoais;
- Controlo B.1.2.2 - Consentimento para tratamento dos dados pessoais para efeitos de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos;
- Controlo B.1.2.3 - Consentimento para tratamento dos dados pessoais de crianças em relação aos serviços da sociedade da informação.

Sub-Categoria B.1.3 - Execução de contrato:

- Controlo B.1.3.1 - Tratamento dos dados pessoais necessário para a formalização de um contrato;
- Controlo B.1.3.2 - Tratamento dos dados pessoais no âmbito de contrato formalizado.

Sub-Categoria B.1.4 - Obrigação jurídica

- Controlo B.1.4.1 - Tratamento dos dados pessoais de acordo com uma obrigação jurídica;
- Controlo B.1.4.2 - Tratamento dos dados pessoais necessário à declaração, ao exercício ou à defesa de um direito num processo judicial.

Sub-Categoria B.1.5 - Interesses vitais do titular:

- Controlo B.1.5.1 - Tratamento dos dados pessoais para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.

Sub-Categoria B.1.6 - Interesse público ou autoridade pública

- Controlo B.1.6.1 - Tratamento dos dados pessoais necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
- Controlo B.1.6.2 - Tratamento dos dados pessoais por motivo de interesse público no domínio da saúde pública.

Sub-Categoria B.1.7 - Interesse legítimo

- Controlo B.1.7.1 - Tratamento dos dados pessoais dos clientes;
- Controlo B.1.7.2 - Tratamento dos dados pessoais dos titulares dos dados que estão ao serviço do responsável pelo tratamento;
- Controlo B.1.7.3 - Tratamento dos dados pessoais para efeitos de comercialização direta;
- Controlo B.1.7.4 - Tratamento dos dados pessoais para assegurar a segurança da rede e das informações;
- Controlo B.1.7.5 - Tratamento dos dados pessoais no âmbito do grupo de empresas;
- Controlo B.1.7.6 - Indicação de eventuais atos criminosos ou ameaças à segurança pública a autoridades competentes;
- Controlo B.1.7.7 - Tratamento de dados pessoais necessário à prevenção e controlo da fraude;
- Controlo B.1.7.8 - Transferências não repetitivas.

Igualmente, na sub-categoria **B.1.8 (Situações específicas)** são agrupados controlos que possibilitem a implementação correta e segura dos procedimentos para garantir a legalidade e lealdade do tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) relativo às situações específicas de tratamento:

- Controlo B.1.8.1 - Tratamento dos dados pessoais para fins jornalísticos e para fins de expressão académica, artística ou literária;

- Controlo B.1.8.2 - Disponibilização do acesso do público aos documentos oficiais a divulgar;
- Controlo B.1.8.3 - Tratamento dos dados pessoais no contexto laboral;
- Controlo B.1.8.4 - Arquivo de interesse público;
- Controlo B.1.8.5 - Investigação científica ou histórica;
- Controlo B.1.8.6 - Fins estatísticos.

B.2 - Privacidade de operações

Ao nível operacional, deve ser garantida a transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados através da implementação dos controlos da sub-categoria **B.2.1 (Transparência nas relações com os titulares dos dados)**:

- Controlo B.2.1.1 - Recolha dos dados pessoais junto do titular;
- Controlo B.2.1.2 - Recolha dos dados pessoais a partir de outra fonte;
- Controlo B.2.1.3 - Decisões automatizadas.

A implementação destes controlos visa facultar ao titular dos dados toda a informação exigida pelo RGPD quanto os dados pessoais, bem como permitir o exercício dos direitos relativos às decisões individuais automatizadas - incluindo definição de perfis - nomeadamente, o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão.

A subcategoria **B.2.2 (Pedidos dos titulares de dados pessoais)** reúne os controlos para garantir que os titulares dos dados pessoais usufruam de controlo efetivo sobre os mesmos, assegurando a resposta atempada aos seus pedidos:

- Controlo B.2.2.1 - Resposta aos pedidos dos titulares dos dados pessoais;
- Controlo B.2.2.2 - Disponibilização de acesso do titular aos seus dados pessoais;
- Controlo B.2.2.3 - Retificação dos dados pessoais;
- Controlo B.2.2.4 - Apagamento dos dados pessoais a pedido do titular dos dados;
- Controlo B.2.2.5 - Limitação do tratamento dos dados pessoais a pedido do titular dos dados;
- Controlo B.2.2.6 - Portabilidade dos dados pessoais.

B.3 - Proteção específica

Especial cuidado deve ser garantido no tratamento de dados das pessoas singulares vulneráveis. Os controlos agrupados na sub-categoria **B.3.1 (Grupos de titulares)** garantem a proteção de dados específica dos direitos e liberdades de titulares vulneráveis:

- Controlo B.3.1.1 - Proteção especial das crianças quanto aos seus dados pessoais;
- Controlo B.3.1.2 - Proteção especial dos colaboradores quanto aos seus dados pessoais;
- Controlo B.3.1.3 - Proteção especial dos doentes quanto aos seus dados pessoais.

Igualmente deve ser garantida a proteção específica dos dados pessoais quando o contexto do seu tratamento possa implicar riscos significativos para os direitos e liberdades fundamentais. Na sub-categoria **B.3.2 (Contexto de tratamento)** encontram-se listados os controlos relevantes no contexto do SNS (não exaustivo):

- Controlo B.3.2.1 - Tratamento dos dados pessoais em grande escala;
- Controlo B.3.2.2 - Intercâmbio de dados pessoais com os registos nacionais e internacionais.

Por último, a sub-categoria **B.3.3 (Dados sensíveis)** é composta por controlos dedicados à proteção das categorias especiais dos dados pessoais que sejam, pela sua natureza e sensibilidade do ponto de vista dos direitos e liberdades fundamentais:

- Controlo B.3.3.1 - Tratamento de categorias especiais dos dados pessoais;
- Controlo B.3.3.2 - Tratamento dos dados biométricos;
- Controlo B.3.3.3 - Tratamento dos dados pessoais relativos à saúde;
- Controlo B.3.3.4 - Tratamento dos dados genéticos;
- Controlo B.3.3.5 - Tratamento dos dados da localização ou deslocações do titular dos dados.

7. CONCLUSÕES

Visando contribuir para o processo de operacionalização da aplicação do RGPD junto das entidades do setor da Saúde em Portugal, o projeto de desenvolvimento acima descrito, alcançou a framework aplicável a todas as organizações do setor da saúde, independentemente da sua natureza, dimensão ou tipologia. A adoção da gestão integrada de Segurança da Informação e Privacidade permite sustentar e melhorar os controlos implementados e ajudar as organizações a cumprir ininterruptamente com as obrigações de conformidade com o RGPD.

Ao contrário do alinhamento entre os requisitos do RGPD e controlos do Anexo A da norma ISO/IEC 27001:2013, a abordagem proposta não é limitada apenas pelo campo de implementação

de controlos, prevendo também mecanismos que permitem definir o âmbito da implementação dos mesmos. Para este efeito os controlos do anexo B - descritos no capítulo 6 - podem ser utilizados como *check-list* para identificação das principais áreas de tratamento dos dados pessoais na organização.

A aplicabilidade dos resultados deste projeto, com o atual grau de aprofundamento, possibilita orientar o processo da implementação do SGISIP ou atualização do SGSI de acordo com os requisitos relevantes do RGPD e da Diretiva SRI, incluindo a implementação ou atualização dos controlos de segurança da informação e privacidade. Como fontes adicionais da informação recomendamos a utilização das normas ISO/IEC 27002:2013 e ISO/IEC 27799:2016, bem como das recomendações para segurança de tratamento dos dados pessoais da ENISA (ENISA, 2016) e dos *guidelines* para preparação ao RGPD da Confederação da Indústria Dinamarquesa (Mortensen, 2016).

No entanto, para a maioria das empresas o desafio não é apenas saber o que há a fazer, mas também como fazê-lo de forma adequada ao seu contexto empresarial (ENISA, 2015, p. 19). Assim, é crucial complementar os controlos de segurança da informação e privacidade acima identificados com *guidelines* de implementação especificamente definidos para o seu setor, por forma a facilitar a sua adoção e dinamizar a partilha de boas práticas e recursos.

A esta realidade não é estranho o SNS, devendo complementar com *guidelines* de implementação especificamente definidos para setor da saúde nacional os controlos de segurança da informação e privacidade acima identificados, de forma transversal.

Neste sentido é fundamental que os Serviços Partilhados do Ministério da Saúde (SPMS) continuem a desempenhar o papel de coordenação, fomentando boas práticas de Segurança da Informação e Privacidade nas entidades do SNS de uma forma estruturada, coerente e sistémica.

Para dar continuidade ao projeto, os resultados deverão servir como *input* para projetos posteriores no âmbito da gestão de segurança da informação e privacidade nas entidades do SNS, bem como para definição do modelo da avaliação do nível de conformidade transversalmente ao SNS.

Consideramos importante que estes projetos, ao nível organizacional ou transversalmente ao SNS, alcancem na próxima fase os seguintes objetivos específicos:

OBJ.01 – Definir os métodos de avaliação necessários para medir o desempenho e o sucesso:

- Método de avaliação da maturidade do SGISIP;
- Método de avaliação da eficácia e eficiência do Programa da implementação do SGISIP.

OBJ.02 – Definir o *Roadmap* para o Programa da implementação do SGISIP, tendo em conta a especificidade do setor da saúde em Portugal:

- identificando um conjunto de passos, com especial ênfase nas fases iniciais do processo;
- determinando os critérios de seleção das medidas de melhoria contínua a implementar;
- incluindo as recomendações para definição do plano da gestão de mudança.

OBJ.03 – Mapear os requisitos do sistema de gestão e os controlos de segurança da informação e privacidade com as boas práticas de governança e gestão de serviços TIC mais conhecidas e implementadas em Portugal (por exemplo, COBIT5, ITIL e ISO/IEC 20000-1:2011). Permitindo assim facilitar o alinhamento do SGISIP com outras *frameworks* de governança e gestão já existentes, em fase de implementação ou em planeamento nas entidades do SNS, bem como para garantir a máxima integração possível dos processos e procedimentos e a minimização dos recursos necessários para operacionalização conjunta das diferentes *frameworks*.

REFERÊNCIAS

DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Retirado de http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT

ENISA – European Union Agency for Network and Information Security (2016). Guidelines for SMEs on the security of personal data processing. Retirado de https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA – European Union Agency for Network and Information Security (2016). Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures. Retirado de https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

ENISA – European Union Agency for Network and Information Security (2015). Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Retirado de https://www.enisa.europa.eu/publications/standardisation-for-smes

Mortensen, H. (2016). GUIDELINE General Data Protection Regulation – Implementation in Danish companies. The Danish ICT and Electronics Federation, DI Digital. Retirado de https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen_engelsk.pdf

NP ISO/IEC 27001:2013, Tecnologia de Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO 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). Retirado de http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

Volchkova E. (2017) Sistema de Gestão Integrada de Segurança da Informação e Privacidade. Alinhamento com o Regulamento Geral sobre a Proteção de Dados. Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Gestão de Informação, especialização em Gestão de Sistemas e Tecnologias de Informação. Pode ser consultado através de link https://run.unl.pt/handle/10362/31313