NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

# Sistema de Gestão Integrada de Privacidade e Segurança da Informação.

*Alinhamento com o Regulamento Geral sobre a Proteção de Dados*

Ekaterina Volchkova

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Gestão de Informação

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

**NOVA Information Management School**
**Instituto Superior de Estatística e Gestão de Informação**
Universidade Nova de Lisboa

# SISTEMA DE GESTÃO INTEGRADA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

*Alinhamento com o Regulamento Geral sobre a Proteção de Dados*

de

Ekaterina Volchkova

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Gestão de Informação, especialização em Gestão de Sistemas e Tecnologias de Informação

**Orientador:** Miguel de Castro Neto

Lisboa, Novembro 2017

# RESUMO

O setor da saúde é geralmente caraterizado pelo elevado número de processos que envolvem o tratamento de dados pessoais, bem como pelo recurso a soluções tecnológicas de várias gerações, muitas vezes incompatíveis entre si e com diferentes níveis de segurança. Neste contexto, cuja vulnerabilidade é agravada pelas últimas tendências para interoperabilidade dos sistemas e para o incremento de transparência nos dados da saúde, o processo da preparação para a aplicação simultânea dos requisitos do Regulamento Geral de Proteção de Dados (internacionalmente designado GDPR - acrónimo de General Data Protection Regulation) e da nova Diretiva de Segurança das Redes e da Informação (Diretiva SRI) – já apartir de maio 2018 - torna-se ainda mais desafiante.

As condições a que se encontra sujeito o tratamento de dados pessoais em Portugal, bem como os requisitos mínimos para o nível de adequação e cumprimento das respetivas regras do GDPR e da Diretiva SRI, foram divulgadas junto das entidades integrantes do Serviço Nacional de Saúde (SNS) pela Serviços Partilhados do Ministério da Saúde, E.P.E. (SPMS) através do "Guia de Privacidade da Informação do Setor da Saúde em Portugal" (Guia) onde foram também consolidadas algumas boas práticas e ações especificamente dirigidas aos diferentes perfis de intervenientes e de Entidades.

O Guia estabelece que as organizações do Ministério da Saúde (MS) e do SNS devem operar de acordo com os princípios e práticas gerais de boas práticas de segurança da informação (ex. ISO 27001), mesmo que não possuam uma certificação. Por outras palavras, para além da implementação dos controlos de privacidade e segurança da informação propriamente ditos, é necessário implementar um **Sistema de Gestão Integrada de Segurança da Informação e Privacidade (SGISIP)** que deverá garantir o cumprimento de obrigações que vão para além do campo de segurança da informação, obrigações tais como a garantia de direitos dos titulares de dados e as questões da licitude e lealdade do tratamento.

No intuito de aprofundar a definição do SGISIP para o setor da saúde e facilitar a sua implementação, foi decidido resumir o âmbito do presente trabalho ao desenvolvimento de uma *framework* genérica que possa ser utilizada pelas entidades deste setor para conduzir o processo de preparação para a aplicação do GDPR. O resultado do presente trabalho deverá ser encarado como crucial para a preparação de um sistema de avaliação tripartido do nível de cumprimento - do GDPR, da norma ISO/IEC 27001:2013, bem como dos requisitos do Guia da SPMS - e, consequentemente, no desencadear do desenvolvimento do *roadmap* da implementação do SGISIP.

A abordagem proposta não é limitada apenas ao campo da implementação de controlos. Adicionalmente, permite estabelecer mecanismos que possibilitam definir o âmbito da implementação dos mesmos, bem como sustentar e melhorar os controlos implementados, ajudando as organizações a cumprir **ininterruptamente** com as obrigações inerentes a 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 GDPR.

# PALAVRAS-CHAVE

Privacidade, Proteção de Dados, Segurança da Informação, GDPR.

# ABSTRACT

The health sector is generally characterized by the high number of processes that involve the personal data processing, as well as the use of technology solutions of various generations that are often incompatible with each other and support different levels of security. In this context, highly vulnerable and compounded by the latest trends in system interoperability and transparency of health data, the preparation process for the simultaneous application in May 2018 of the requirements of the General Data Protection Regulation (GDPR) and the new Directive for Network and Information Security (NIS Directive) becomes even more challenging.

The conditions to which the processing of personal data is subject in Portugal, as well as the minimum requirements for the level of adequacy and compliance with the respective GDPR and NIS Directive rules, were disclosed to public entities that are part of the National Health Service (NHS) by the Shared Services of the Ministry of Health (SSMH) through the "Information Privacy Guide for the Health Sector in Portugal" (the Guide), which also consolidated some good practices and actions specifically addressed to the different profiles of stakeholders and Entities.

In addition, the Guide establishes that organizations of the Ministry of Health (MH) and the NHS must operate in accordance with the general principles and good information security practices (eg ISO 27001), even if they do not have a certification. In other words, in addition to the implementation of the privacy and information security controls themselves, it is necessary to implement an Integrated Information Security and Privacy Management System (IISPMS), which should ensure compliance with obligations that go beyond the security field, such as the fulfilment of the rights of data subjects and questions of lawfulness and fair treatment.

In order to deepen the definition of the IISPMS for the health sector and to facilitate its implementation, it was decided to summarize the scope of the present work to the development of a generic framework that can be subsequently used by the Entities of the Health sector in Portugal to guide them through the process of preparation for GDPR application. The results of this work could be used for evaluating of the level of compliance with the requirements of the GDPR, ISO/IEC 27001: 2013 and ones of the SSMH Guide, as well as for the consecutive development of the IISPMS implementation roadmap.

The proposed approach is not limited only by the field of controls´ implementation, but additionally provides mechanisms to define the scope of implementation, as well as sustain and improve the controls implemented and help organizations to comply **uninterruptedly** with responsibilities of data controller or data processor, in particular with regard to the obligation to ensure and to be able to demonstrate **at any time** that processing is performed in accordance with the GDPR.

# KEYWORDS

Privacy, Data Protection, Information Security, GDPR.

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABELAS

# LISTA DE ABREVIATURAS

| | |
|---|---|
| **AMA** | Agência Para a Modernização Administrativa |
| **APCIBER** | Associação para a Promoção da Cibersegurança e Proteção de Dados |
| **API** | Application Program Interface |
| **APP** | Aplicação |
| **CID** | Confederação da Indústria Dinamarquesa |
| **CIO** | Chief Information Officer |
| **CISO** | Chief Information Security Officer |
| **DPO** | Data Protection Officer |
| **eHealth** | utilização de tecnologias de informação e comunicação (TIC) no setor da saúde |
| **ENESIS** | Estratégia Nacional para o Ecossistema de Informação de Saúde |
| **ENISA** | Agência Europeia para a Segurança das Redes e da Informação |
| **eSIS** | ecoSistema de Informação da Saúde |
| **GDPR** | General Data Protection Regulation |
| **INFARMED** | Autoridade Nacional do Medicamento e Produtos de Saúde, I. P. |
| **IT** | Information Technology |
| **MS** | Ministério da Saúde |
| **PDS** | Plataforma de Dados da Saúde |
| **PMEs** | Pequenas e Médias Empresas |
| **PPP** | Parceria Público Privada |
| **RIS** | Rede da Informação da Saúde |
| **SGISIP** | Sistema de Gestão Integrada de Segurança da Informação e privacidade |
| **SGSI** | Sistema de Gestão de Segurança da Informação |
| **SNS** | Serviço Nacional de Saúde |
| **SPMS** | Serviços Partilhados do Ministério da Saúde, E.P.E. |
| **TIC** | Tecnologias de Informação e Comunicação |
| **UE** | União Europea |

# 1. ENQUADRAMENTO

O objetivo deste capítulo é efetuar um enquadramento geral ao tema do projeto e salientar a pertinência do desenvolvimento deste trabalho no contexto do setor da Saúde em Portugal.

## 1.1. PROTEÇÃO DE DADOS NO CONTEXTO DO MERCADO ÚNICO DIGITAL

A comunicação da Comissão Europeia sobre a Estratégia para o mercado único digital na europa (2015) refere que a transformação digital em todas as áreas da nossa vida está a ocorrer:

> a uma escala e a um ritmo tais que abrem imensas oportunidades para a inovação, o crescimento e o emprego. Todavia, colocam também questões políticas que constituem grandes desafios para as autoridades públicas e que exigem uma ação coordenada da União Europea (UE). … Por essa razão a Comissão Europeia estabeleceu como uma das suas prioridades-chave a criação de um Mercado Único Digital. (p. 3)
>
> O Mercado Único Digital é um mercado em que é assegurada a livre circulação de mercadorias, pessoas, serviços e capitais e em que os cidadãos e as empresas podem beneficiar de um acesso sem descontinuidades a atividades em linha e desenvolver essas atividades em condições de concorrência leal e com um elevado nível de proteção dos consumidores e dos seus dados pessoais, independentemente da sua nacionalidade ou local de residência. (p. 3)

De acordo com a Estratégia para o mercado único digital na europa (2015) "no que se refere aos dados pessoais e à privacidade, a UE está empenhada em manter os mais elevados níveis de proteção garantidos pelos artigos 7.º e 8.º da Carta dos Direitos Fundamentais" (p. 15).

Por sua vez a entrada em vigor do Regulamento Geral de Proteção de Dados (General Data Protection Regulatuion ou GDPR) "traz novas obrigações, de impacto considerável, para as organizações públicas e privadas" (APDSI, 2016, para. 2).

## 1.2. PROTEÇÃO DE DADOS NO SETOR DA SAÚDE

De acordo com o relatório da IBM X-Force® Research (2016) "2016 Cyber Security Intelligence Index" a saúde tornou-se em 2015 o setor mais atacado ao nível de graves violações de dados e ciberataques, ultrapassando o setor financeiro e indústria (p. 9). Cinco das oito maiores violações de segurança no setor da saúde desde o início de 2010 – entenda-se, aquelas com mais de um milhão de registos alegadamente comprometidos - ocorreram durante os primeiros seis meses de 2015. De fato, mais de 100 milhões de registos de saúde foram comprometidos em 2015. (p. 6)

O mesmo relatório (IBM X-Force® Research, 2016, p. 6) sublinha que, tendo em conta a abundância de informações exploráveis, os registos de saúde eletrônicos atingem um elevado valor no mercado negro, uma vez que normalmente contêm dados de cartão de crédito, endereços de e-mail, números

de segurança social, informações sobre o emprego e registos de histórico médico - muitos dos quais permanecerão válidos por anos, senão décadas. O cibercrime utiliza esses dados para lançar ataques de phishing, cometer fraudes e roubar identidades (IBM X-Force® Research, 2016, p. 6) que permitem a sua utilização no acesso a tratamento médico, aquisição de medicamentos prescritos para venda ou consumo pessoal e requerer reembolsos junto do setor dos seguros por meio de faturas médicas fraudulentas (IBM X-Force® Research, 2015, p. 11).

Conforme outro relatório da IBM X-Force® Research (2015) "Security trends in the healthcare industry" a perspetiva de altos rendimentos é um dos fatores que atrai o cibercrime para o setor da saúde, identificando ainda a facilidade de exploração dos diversos vetores de ataque devido a utilização generalizada de sistemas obsoletos e tecnologias desactualizadas (p. 3), bem como os processos arcáicos sem atualizar práticas de segurança implementadas durante anos (p. 15). A migração para processos, sistemas e tecnologias mais seguros exige tempo e dinheiro, e a falta de financiamento pode ser um dos obstáculos fundamentais para melhorar a postura de segurança do setor de saúde (p. 14).

Por outro lado, o aumento do fluxo de informação em cada hospital – bem como na rede hospitalar - acarreta riscos que precisam ser endereçados (ENISA, 2016, p. 6). Os riscos incluem possíveis danos à segurança do paciente ou perda de informações pessoais de saúde, as quais podem ser causados por ações mal-intencionadas, mas também por erros humanos, falhas de sistemas ou de terceiros e fenômenos naturais. À medida que a superfície de ataque aumenta com a introdução de novos dispositivos médicos conectados, computação em nuvem e aplicações móveis, o potencial de ataque cresce exponencialmente. (p. 6)

Neste contexto a cibersegurança de dispositivos médicos torna-se cada vez mais uma preocupação para os prestadores de cuidados de saúde, fabricantes de dispositivos, reguladores e pacientes (Symantec, 2016, para. 1). Esses dispositivos tendem a ter baixa maturidade de segurança, vulnerabilidades significativas e uma alta suscetibilidade geral às ameaças cibernéticas, especialmente ao nível de proteção de dados sensíveis de saúde neles contidos. (para. 1)

No entanto a transformação digital e adesão do setor da saúde aos registos eletrónicos de saúde, e consequente intercâmbio de informação de saúde aumentam o risco de acesso inadequado a informações de saúde identificáveis, mas pode ajudar a melhorar a qualidade dos cuidados de saúde, reduzir os custos e prevenir erros médicos (*U.S. Department of health and human services*, sem data, p. D-2). A privacidade e a segurança absolutas e isentas de riscos não poderão ser atingidas. Assim, os benefícios para pacientes e utentes deverão garantir um equilibrio face aos riscos presentes. O desenvolvimento de normas de privacidade comuns que são seguidas pela indústria de cuidados de saúde podem fornecer esse equilíbrio. (p. D-2)

Neste contexto, o propósito da privacidade é - observando critérios de razoabilidade - assegurar que a informação confidencial seja utilizada e compartilhada apenas quando necessário ou exigido por lei, por exemplo, para aplicação da lei, saúde pública e supervisão dos cuidados de saúde (*U.S. Department of health and human services*, sem data, p. D-3). É da responsabilidade das organizações assegurar cuidados de saúde adequados, sem usar abusivamente os dados ou correr o risco de exposição de dados a entidades ou indivíduos não autorizados a ter acesso a esta informação (p. D-4).

## 1.3. PROTEÇÃO DE DADOS NO SETOR DA SAÚDE EM PORTUGAL

O parágrafo de enquadramento do Relatório final *Think tank* "*eHealth* em Portugal: Visão 2020" (ISCSP, 2015) constata que:

> Hoje em dia é consensual que a utilização de tecnologias de informação e comunicação (TIC) na saúde, designada por *eHealth*, pode trazer inúmeros benefícios ao setor da Saúde. Em Portugal, tem-se assistido a diversas iniciativas neste domínio, mas verifica-se a inexistência de uma visão comum a nível nacional, partilhada pelos diversos atores que garanta o alinhamento de estratégias e ações com a política de saúde expressa no Plano Nacional de Saúde, e a articulação e cooperação entre os diversos intervenientes no desenvolvimento e adoção de e-health. (p. 3)

### 1.3.1. eHealth em Portugal - principais prioridades

Em julho de 2016 a Serviços Partilhados do Ministério da Saúde, E.P.E. (SPMS) promoveu "uma reunião de trabalho com a finalidade de debater a elaboração do Plano Setorial do Ministério da Saúde para a "Estratégia TIC 2020"" (SPMS, 2016, para. 1). De acordo com a notícia publicada no site da SPMS:

> O Plano Setorial TIC 2020 do Ministério da Saúde integra-se na "Estratégia TIC 2020 para a Transformação Eletrónica na Administração Pública, em fase de preparação e sob a coordenação da AMA – Agência Para a Modernização Administrativa, com o propósito de alavancar a interoperabilidade, a eficiência e a eficácia dos serviços públicos. (Para. 3)
>
> Com a elaboração deste Plano (…) pretende-se promover a coordenação e alinhamento da estratégia TIC do Ministério da Saúde com as políticas e estratégias da Saúde e, também, alinhar as estratégias das TIC do Ministério da Saúde com as da Administração Pública. (Para. 4)
>
> Neste contexto, a SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. (doravante designada por SPMS) desempenha um papel estruturante, tendo iniciado os trabalhos no último trimestre de 2015, através da realização do workshop "Think Tank eHealth em Portugal Visão 2020" e com o fórum "Boas práticas no eSIS", que decorreu a 29 de junho no "eHealth Summer Week". (Para. 5)

*Think tank "eHealth em Portugal*: Visão 2020" foi uma iniciativa da SPMS que visou criar um espaço de reflexão e debate alargado tendo em vista a definição da Estratégia Nacional de eHealth para o período 2016-2020, com base na metodologia da Organização Mundial de Saúde "National eHealth Strategy Toolkit" (ISCSP, 2015, p. 3). A sessão decorreu no dia 21 de setembro de 2015 e contou com a participação de 40 profissionais (…) que, ao longo do dia, foram divididos em grupos de trabalho e efetuaram um conjunto de debates, destacando-se os temas sobre o estádio de maturidade de eHealth em Portugal; objetivos e desafios para os quais o eHealth deve ter maior impacto; fatores críticos de sucesso e áreas prioritárias de atuação. (p. 3)

Na **Tabela 1-1** apresenta-se a consolidação da informação sobre as principais prioridades para o eHealth em Portugal e barreiras associadas que foram identificadas pelos participantes com maior frequência, tendo-se procedido ao seu agrupamento em duas vertentes distintas:

- GOVERNAÇÃO e GESTÃO (Liderança e Governação, Estratégia e Investimento, Recursos Humanos);
- TECNOLOGIAS (Sistemas, Aplicações e Infraestruturas, Normas e Interoperabilidade).

**Tabela 1-1** – Prioridades para o *eHealth* em Portugal e barreiras associadas

| | Prioridades | Barreiras |
|---|---|---|
| GOVERNAÇÃO e GESTÃO | • Contribuir para que os cidadãos adquiram um papel mais ativo e responsável;<br>• Garantir que utentes das zonas mais remotas têm as mesmas condições de acessibilidade;<br>• Focalizar ações nas populações mais idosas e com mobilidade reduzida;<br>• Melhorar condições de acessibilidade e de inclusão;<br>• Construir uma estrutura de liderança transversal;<br>• Apoiar a realização de experiências lideradas regionalmente e a cooperação entre as administrações públicas os níveis regional e nacional e sector privado;<br>• Desenvolver mecanismos de monitorização e benchmarking;<br>• Disponibilizar aos utentes acessos a custo reduzido;<br>• Investir em literacia eHealth para profissionais de saúde e cidadãos e promover a adoção das TIC;<br>• Reforçar competências de governação, gestão e operação de tecnologias e sistemas de informação, promovendo decisões mais informadas e seguras para o doente;<br>• Otimizar a utilização de recursos internos, nomeadamente no domínio e partilha do conhecimento | • Inexistência de uma estrutura de governação de iniciativas nacionais de eHealth;<br>• Falta de resiliência e continuidade de políticas para conduzir uma estratégia de longo prazo de eHealth, a desenvolver em vários anos;<br>• Desajuste entre instâncias de poder e serviços, com incapacidade de alinhamento entre atividades;<br>• Assimetrias ao nível dos conhecimentos e instrumentos essenciais para uma adequada governança e gestão;<br>• Baixa literacia pública para a saúde e para o eHealth;<br>• Resistência à utilização das TIC e falta de informação/formação por parte dos profissionais de saúde e do cidadão;<br>• Escassez de recursos humanos;<br>• Escassez de recursos financeiros. |
| TECNOLOGIAS | • **Centrar serviços no utente (por exemplo, o processo clínico centrado no cidadão, com possibilidade de acesso pelos profissionais de saúde com quem se relaciona);**<br>• **Fomentar a telemedicina;**<br>• **Apostar na desmaterialização e simplificação administrativa;**<br>• Reforçar canais de comunicação entre os profissionais de saúde;<br>• **Alterar formas de armazenamento de dados e gerar conhecimento a partir de dados existentes;**<br>• **Garantir segurança e privacidade;**<br>• **Preservar a informação clínica e administrativa;**<br>• **Promover a disponibilização e acesso a plataformas mobile;**<br>• **Melhorar os serviços TI, alinhando com boas práticas de ITSM e tornando-os disponíveis 24 horas / dia;**<br>• Promover a qualidade (robustez, atualidade e usabilidade) dos sistemas e tecnologias;<br>• **Fomentar a interoperabilidade entre os vários níveis de cuidados e incluindo os sectores privado e social;**<br>• Estabelecer na arquitetura nacional níveis de interoperabilidade que permitam desenvolver o eHealth de forma coerente e efetiva;<br>• **Apostar numa lógica de informação registada apenas uma vez;**<br>• Utilizar normas com enquadramento nacional e internacional;<br>• Fomentar a utilização de normas abertas;<br>• **Reutilizar serviços.** | • Diferenças tecnológicas acentuadas e falta de Interoperabilidade, especialmente entre setor público e privado;<br>• Deficiências tecnológicas nas soluções atuais e base instalada obsoleta;<br>• Constrangimentos de acesso à rede de dados e/ou Internet, especialmente em algumas zonas do interior do país;<br>• Existência de uma percentagem relevante de pessoas sem computador ou smartphones. |

Consideramos que, em geral, as prioridades na vertente de GOVERNAÇÃO e GESTÃO são alinhadas com os objetivos do Programa do XXI Governo Constitucional (2015) na área da Saúde, nomeadamente no que toca a redução de desigualdades no acesso à saúde (p. 94) e reforço do poder do cidadão através de uma maior disponibilidade, acessibilidade, comodidade, celeridade e humanização dos serviços (p. 95), bem como a melhoria na governação do SNS (p. 99), na gestão dos recursos humanos e na motivação dos profissionais de Saúde (p.98).

A análise de prioridades na vertente de TECNOLOGIAS também revela uma forte aposta na transformação digital do setor da saúde e interoperabilidade da informação em consonância com os objetivos do Programa do XXI Governo Constitucional (2015) na área da Saúde relacionados com a melhoria da gestão dos hospitais, da circulação de informação clínica e da articulação com outros níveis de cuidados e outros agentes do setor (p. 97).

A Resolução do Conselho de Ministros n.º 62/2016 constata que:

> este esforço tem vindo já a ser concretizado pela área do Governo responsável pela saúde, através da promoção do reforço do Sistema de Informação da Saúde, fazendo uso da disponibilização de múltiplas plataformas de serviços digitais que permitem o acesso e partilha de informação e a simplificação e desmaterialização de diversos processos e documentos, como sejam a prescrição e dispensa eletrónica de medicamentos, a desmaterialização dos processos associados aos certificados de óbito e baixas médicas e muitos outros, bem como a disponibilização de dados e serviços através da Plataforma de Dados de Saúde e portais conexos e, ainda, a disponibilização pública através de dados abertos no Portal do SNS e no Portal dados.gov.pt.

No entanto, os profissionais da saúde que participaram no evento Think tank "eHealth em Portugal: Visão 2020" destacaram adicionalmente e na vertente de TECNOLOGIAS a importancia de garantir segurança da informação, privacidade e proteção da informação clínica e administrativa (ISCSP, 2015, p. 25).

Esta preocupação foi endereçada na Estratégia Nacional para o Ecossistema de Informação de Saúde 2020 (ENESIS 2020), aprovada através da Resolução de Conselho de Ministros n.º 62/2016 de 15 de setembro de 2016 que prevê, entre outras medidas, a definição de uma arquitetura de referência dos Sistemas de Informação de Saúde, em alinhamento com a arquitetura de referência TIC da Administração Pública, com as orientações da AMA – Agência para a Modernização Administrativa, I. P. (doravante designada por AMA), e do Conselho para as Tecnologias de Informação e Comunicação, e contemplando a elaboração de guias para os diversos intervenientes do setor da saúde, com particular destaque para questões emergentes, nomeadamente:

- Requisitos de segurança e usabilidade;
- Adoção de novos mecanismos de proteção de dados pessoais;
- Uso de APPs em dispositivos móveis, e de APIs para partilha de dados de saúde;
- Uso de dispositivos de saúde com recurso a sistemas de informação — alinhado com o INFARMED — Autoridade Nacional do Medicamento e Produtos de Saúde, I. P.;
- Robótica, domótica com aplicação na saúde e integração de ambientes de vida assistida.

Referir ainda que a ENESIS 2020 reconhece a **melhoria da gestão dos riscos e de segurança da informação, bem como a atualização tecnológica do parque informático e dos sistemas legados**, como dois dos principais desafios que se colocam ao desenvolvimento do ecoSistema de Informação da Saúde (eSIS) e, ao nível estratégico, devem ser entendidos e acompanhados no seguinte contexto:

- Aumento significativo do uso pessoal, autónomo e participado dos cidadãos de sistemas de informação;
- Importância do acesso omni-canal, seja através de computadores, telemóveis ou outros aparelhos pessoais, recorrendo a sites online, soluções de mobilidade e APPs para conhecimento e orientação diagnóstica e monitorização de sinais vitais;
- Ubiquidade crescente de aparelhos de uso corrente (como por exemplo carros, relógios, balanças, etc.) com capacidade de computação, e outras formas de informatizados com impacto na saúde direta dos indivíduos e das populações.

Neste contexto, entre os princípios e objetivos estratégicos estabelecidos pela ENESIS 2020, entendemos de relevo os quatro que se destacam infra, uma vez que o cumprimento dos mesmos pode estar sujeito a constrangimentos, tais como requisitos de segurança da informação, privacidade e proteção de dados:

- Princípio da transparência e dos dados abertos, nomeadamente através da sua disponibilização na plataforma dados.gov, da gestão proativa do valor dos dados em saúde, para ensino e investigação, e promoção de uma nova economia do conhecimento baseada na informação de saúde (ponto 3.4);
- Princípio da centralidade no cidadão, através do desenho de serviços e sistemas adequados a eventos de vida ou percursos clínicos e incorporando requisitos de usabilidade e de respeito pelo comportamento humano (ponto 3.5);
- Princípio da portabilidade dos dados e informação de saúde, útil na definição da utilização de *APPs* e de outras formas de interligação, nos objetos da vida comum, de sistemas de informação com impacto na saúde — implicando a adoção do conceito de Saúde Móvel/*mHealth*, e a aceitação do racional «Móvel à partida» no pensamento dos conceitos informacionais, arquiteturas de sistemas e no design e *revamping* de soluções informativas concretas (ponto 3.6);
- Promoção da interoperabilidade legal, organizacional, semântica e técnica específica da saúde em alinhamento com iniciativas em curso, no âmbito da Plataforma de Interoperabilidade da Administração Pública promovida pela AMA, bem como as emanadas pela UE no que diz respeito à área do eHealth/uso de Sistemas Informação em Saúde, garantindo a progressiva adoção dos adequados standards internacionais do setor (ponto 3.7).

Atento ainda ao contexto de informação sensível da saúde, a privacidade dos dados pode constituir uma barreira condicionante à implementação das iniciativas que suportam os princípios acima identificados, em primeiro lugar daquelas que são vistas como imprescindíveis para o sucesso da ENESIS 2020, como o Registo de Saúde Eletrónico, as Plataformas de Partilha de Dados de Saúde e o Acesso dos Cidadãos aos seus dados de saúde e a conhecer quem os consulta.

Em linha com este entendimento surge o Despacho n.º 913-A/2017 de 18 de Janeiro 2017 do Gabinete do Secretário de Estado da Saúde refere que:

> os dados produzidos, pelos serviços e organismos integrados, respetivamente, na administração direta e indireta do Estado, no âmbito do Ministério da Saúde, e das entidades do setor público empresarial, da área da saúde, são um bem público transversal que deve ser devidamente salvaguardado, e cuja disponibilização deve estar circunscrita à prossecução do interesse público e obedecer, de forma estrita, aos princípios da legalidade, da transparência e da proporcionalidade. (para. 4)

Neste contexto e, "considerando as preocupações crescentes com a proteção de dados" o Despacho n.º 913-A/2017 determina que deve ser assegurada:

> a adoção de mecanismos legais adequados à especificidade da informação gerada, no seio das entidades do Serviço Nacional de Saúde e do Ministério da Saúde, para que os mesmos sejam tratados e disponibilizados de forma legítima, com os princípios e regras legalmente definidos, designadamente no 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). (para. 3)

Assim, o Despacho determina que:

> os serviços e organismos integrados na administração direta e indireta do Estado, no âmbito do Ministério da Saúde, e das entidades do setor público empresarial, da área da saúde, não podem ceder a entidades terceiras, a título gratuito ou oneroso, qualquer informação de saúde, sem prévia autorização do membro do Governo responsável pela área da saúde, com a salvaguarda da informação a fornecer a entidades judiciais e administrativas, nos termos legalmente previstos. (ponto 1)

Embora fiquem excecionados da obrigação acima referida os dados transferidos para outras entidades - devidamente justificados e fundamentados - no âmbito de protocolos de investigação ou de realização de estudos promovidos pelos próprios serviços abrangidos pelo despacho, a implementação efetiva do mesmo pode por em causa o sucesso da ENESIS 2020.

Este exemplo particular de desalinhamento entre atos legislativos nacionais ilustra a necessidade eminente da criação em Portugal de uma estratégia de gestão da privacidade na saúde que permitirá equilibrar as medidas, destinadas a cumprimento dos novos requisitos regulamentares no âmbito de privacidade e proteção de dados, com as outras, mais focadas na transformação digital do setor da saúde e "promoção de uma nova economia do conhecimento baseada na informação de saúde" (ENESIS 2020, ponto 3.4).

Todavia, criar um equilíbrio entre o respeito pela privacidade individual e disponibilização da informação de saúde de alta qualidade pode, apesar da sua importância, ser uma tarefa difícil e a enfrentar na conceção do registo de utentes. A luta pela interconexão transfronteiriça e pela interoperabilidade dos registos de utentes é acompanhada por novos riscos de segurança relacionados com a privacidade. (Zaletel, Kralj, 2015, p. 67)

### 1.3.2. Conjuntura atual dos sistemas de informação da saúde

Em Portugal, a origem destes riscos pode ser encontrada na conjuntura atual dos sistemas de informação da saúde que apresenta vários desafios em matéria de protecção da privacidade. Esta conjuntura no contexto nacional foi recentemente descrita por Secundino Domingos Marques Lopes na sua tese "Privacidade dos dados em ambientes de interoperabilidade – a área da saúde" apresentada à Universidade de Évora para obtenção do Grau de Doutor em Gestão (Marques Lopes, 2016). Pretendemos destacar algumas conclusões desse trabalho:

> Na área da saúde, o número de processos que envolvem dados pessoais é, comparando com outras áreas, muito elevado, e as organizações continuam a instalar soluções tecnológicas que aumentam a sua disponibilidade e consequentemente a sua maior exposição, sendo que gradualmente esta exposição ultrapassa os limites "geográficos" das organizações (Marques Lopes, 2016). Por defeito, estes processos não são documentados nem conhecidos, com base numa norma ou padrão estruturado, nem foram sujeitos uma análise prévia de impacto sobre a privacidade, prospetora dos riscos existentes. Nem tão pouco se encontram definidos de forma clara os objetivos associados à recolha de dados, as limitações à sua utilização, o tempo máximo de retenção, e os procedimentos para eliminar dados. (p. 262).
>
> Os sistemas atuais foram desenvolvidos com o pressuposto de que tanto os dados como os mecanismos de segurança vão estar apenas sob a gestão e o controlo de uma organização. As situações que contemplam a partilha de dados, especialmente entre organizações, obrigaram a que este pressuposto fosse invariavelmente questionado. Atendendo a que os sistemas não consideram a privacidade dos dados como um requisito de primeira ordem, traduzido em mecanismos de segurança ajustáveis à sensibilidade dos dados, faz com que um contexto de partilha de dados seja ainda mais complexo. Na sua maioria, os sistemas controlam os dados na ótica do conjunto de registos e não na ótica do elemento de dados o mais granular possível. (p. 260)
>
> No geral, as organizações na área da saúde apresentam, em relação às questões da privacidade, uma visão "insuficiente" e por vezes "distorcida" do problema, que resulta de uma preparação pouco qualificada. Em cada classe profissional existe uma noção muito própria destas questões, que resulta da sua atividade profissional e do conhecimento dos riscos associados à utilização dos dados. (p. 259)

Embora "a preocupação com os dados e com a sua proteção está a surgir nas organizações da área da saúde" (Marques Lopes, 2016), o autor afirma que:

Contudo, a preparação existente não é a suficiente face aos requisitos complexos da proteção de dados e dos ambientes de partilha de dados. As iniciativas estruturadas de partilha de dados entre serviços de várias instituições, apesar de existir uma unanimidade em relação às vantagens que apresentam, colocam numa fase inicial muitas questões aos responsáveis pela sua implementação. As questões técnicas de interoperabilidade são nesta fase as mais fáceis de ultrapassar. O mesmo não se consegue com a proteção de dados. A inversão desta situação só será possível se os profissionais apostarem numa maior experiência nas questões de interoperabilidade, e em projetos que envolvam a disponibilidade de dados a outras organizações. Por acréscimo ganha-se experiência na proteção de dados. Esta experiência vai permitir uma atuação proativa em relação às questões da privacidade dos dados, e fomentar uma visão estratégica para o seu desenvolvimento, em detrimento de soluções pontuais sem continuidade. (p. 234)

Esta evolução vai contribuir para que a experiência atual em proteção de dados, não se limite às tecnologias de segurança, e evolua para a perspetiva dos dados. É necessário um processo de mudança, suportado por profissionais com especialização em proteção e privacidade dos dados, capazes de desenvolver ao nível local um programa contínuo de proteção de dados, e interagir com profissionais de outras organizações no alinhamento de princípios e medidas, reunidas num programa alargado, aceite e aplicado às situações de partilha de dados sob a forma de um padrão. (p. 235)

Tal como aconteceu com outras iniciativas de colaboração (por exemplo, a implementação da Rede da Informação da Saúde – RIS), em que o seu sucesso apenas aconteceu porque existia uma equipa coordenadora da iniciativa, com conhecimento e capacidade de influenciar o rumo dos SI ao nível local, o desenvolvimento de um plano comum a todas as organizações, que participam na PDS (Plataforma de Dados da Saúde), para a proteção da privacidade dos dados, depende da criação de uma equipa permanente ao nível do Ministério da Saúde ou da SPMS. A sua experiência em projetos de interoperabilidade, em segurança, e em proteção de dados, são determinantes para que um processo orientado à proteção da privacidade dos dados se inicie com a solidez necessária. A prioridade deve ser a definição dos princípios e das orientações necessárias à implementação de medidas de proteção para os dados, e claro a sua privacidade. (p. 235)

### 1.3.3. Iniciativas em curso na área de Segurança e Proteção de Dados

Partindo deste princípio, a SPMS lançou um conjunto de iniciativas na área de segurança e privacidade com os seguintes objetivos (SPMS, sem data):

- Fomentar práticas de sensibilização para a Segurança e Privacidade da Informação dirigidas a todas as partes interessadas do Ministério da Saúde de uma forma estruturada, coerente e sistémica.
- Reforçar práticas de divulgação e sensibilização para as boas práticas de Segurança e Privacidade da Informação promovidas pela SPMS para o eSIS (ENESIS 2020 – Estratégia Nacional Ecossistema de Informação de Saúde).

- Dinamizar o conhecimento e formação na área da Segurança da Informação, sensibilizando e capacitando Conselhos Diretivos / de Administração para a temática da Privacidade da Informação, bem como consciencializando os profissionais de saúde e TIC para estes temas.

No âmbito da privacidade foi disponibilizado pela SPMS um "Guia de Privacidade da Informação do Setor da Saúde em Portugal" (SPMS, 2017), doravante designado pelo Guia, "de forma a dar a conhecer, às entidades públicas integrantes do SNS, as condições a que se encontra sujeito o tratamento de dados pessoais em Portugal" (p. 8), permitindo-lhes, por um lado, conhecer as regras e impacto que o novo Regulamento Geral sobre a Proteção de Dados ("GDPR") e a Diretiva de Segurança das Redes e da Informação ("Diretiva SRI") terá nas suas organizações (p. 8) e, por outro lado, realizar uma avaliação do "nível atual de cumprimento, definindo as estratégias de resposta às situações de desalinhamento identificadas e implementando as soluções de acordo com as suas necessidades e possibilidades" (p. 4). De acordo com o Guia (SPMS, 2017), este impacto revelar-se-á nos tratamentos atuais e futuros a diferentes níveis, conforme consolidado na **Tabela 1-2** que mapeia as obrigações a cumprir pelas Entidades (p. 32) com algumas boas práticas que deverão ser implementadas pelas Entidades públicas integrantes do SNS até 25 de maio de 2018 (p. 33).

**Tabela 1-2** – Impacto do GDPR e da Diretiva SRI nas Entidades do setor da saúde.

| NÍVEL | IMPACTO | OBRIGAÇÕES |
|---|---|---|
| **Governança das matérias de dados pessoais** | Maior responsabilização das Entidades na verificação do cumprimento do GDPR e da existência de documentação que evidencie tal cumprimento | • Tratar os dados recolhidos para finalidades determinadas, explícitas e legítimas<br>• Obter o consentimento dos titulares para finalidades de tratamento específicas<br>• Conservar os dados apenas pelo período necessário<br>• Efetuar registos das atividades de tratamento de dados<br>• Realizar auditorias de conformidade e adotar políticas |
| **Sistemas de Informação** | Reforço das medidas de segurança e da interoperabilidade dos sistemas | • Implementar os princípios de "privacy by design" e o "privacy by default"<br>• Implementar as adequadas medidas de segurança<br>• Realizar "privacy impact assessments" |

| NÍVEL | IMPACTO | OBRIGAÇÕES |
|---|---|---|
| **Relacionamento com terceiros e prestadores de serviços** | Maior responsabilização na escolha de terceiros e necessidade de celebração de contratos com conteúdos específicos (v.g. limitação do tratamento à execução do contrato e respeito pelas instruções do responsável, indicação das medidas de segurança, entre outros aspetos) | • Celebrar contratos escritos com os prestadores de serviços<br>• Adoção de cuidados na escolha de prestadores de serviços |
| **Gestão de recursos humanos** | Formação e sensibilização de todos aqueles que intervêm no ciclo de vida do tratamento de dados | • |
| **Gestão da relação com utentes** | Reforço do direito dos titulares dos dados e a capacidade da organização em garantir o seu cumprimento | • Prestar informação aos titulares dos dados<br>• Garantir os direitos de acesso, retificação, apagamento e oposição<br>• Assegurar os direitos de apagamento, limitação do tratamento e portabilidade dos dados |
| **Relação com a Comissão Nacional da Proteção de Dados (CNPD)** | Documentação de evidências do cumprimento do GDPR e interação em caso de ocorrência de violações de dados pessoais | • Designar o Data Privacy Officer<br>• Notificar violações de dados e de incidentes de segurança<br>• Pedir, nos casos aplicáveis, consulta prévia à CNPD para os tratamentos de dados |

Assim, e com vista a responder aos desafios decorrentes, foram consolidadas no Guia algumas boas práticas e ações especificamente dirigidas aos diferentes perfis de intervenientes (gestores hospitalares, profissionais de saúde e profissionais de tecnologias de informação) e de Entidades (SPSM, hospitais, centros hospitalares, centros de saúde e parcerias público privadas – PPPs).

Por sua vez, o Despacho n.º 3156/2017 – Diário da República n.º 74/2017, Série II, aprova o quadro de indicadores de acompanhamento e avaliação da ENESIS 2020, que, para o programa 3.2 "Adoção de novos mecanismos de proteção de dados pessoais" na linha estratégica 3 "Arquitetura de Referência eSIS", defina que todas as instituições abrangidas no âmbito da estratégia devem adotar o Guia acima mencionado no decurso de 2018.

## 1.4. PROBLEMÁTICA E MOTIVAÇÃO

Embora o Despacho n.º 3156/2017 não clarifique como será medido o nível da adoção do Guia, o desafio colocado às entidades do setor da saúde afigura-se-nos enorme, especialmente se for tido em conta que em Portugal - e de acordo com o Manuel Melo, presidente da APCIBER – Associação para a Promoção da Cibersegurança e Proteção de Dados - "nem sequer o atual quadro jurídico está a ser cumprido" e que "muitos gestores não têm noção das práticas ilícitas existentes nas suas empresas" (Business Analytics Portugal, 2017, para. 3).

O desafio passa também pela complexidade dos processos internos de tratamento de dados pessoais nas entidades do MS/SNS 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 devido a aplicação das regras do GDPR já a partir de maio 2018.

Assim, é importante salientar as **barreiras à adoção de normas de privacidade e segurança da informação** nas Pequenas e Médias Empresas (PMEs) reveladas pela Agência Europeia para a Segurança das Redes e da Informação (ENISA, 2015), que compreendem:

- Falta de conhecimento e envolvimento da gestão de topo (p. 13-14);
- Escassez das capacidades e recursos disponíveis (p. 15-16);
- Ineficácia de processos da gestão do risco de segurança da informação (p. 17);
- Falta de diretrizes de implementação adequadas com etapas detalhadas que especificam como aplicar cada requisito de segurança e privacidade de informação, traduzindo-os para controlos tecnológicos e organizacionais específicos (p. 18-19).

No mesmo documento (ENISA, 2015) a ENISA definiu várias recomendações destinadas às administrações públicas da União Europeia (EU) e dos Estados-Membros, às organizacões de standartização internacionais e europeias, às associações profissionais, industriais e de pequenas empresas e outras partes interessadas, a saber:

- **Aumentar o conhecimento e o envolvimento** – tornar as PMEs mais familiarizadas com as normas que podem aplicar, bem como dos benefícios que podem obter através da sua implementação (p. 21-22);
- **Impulsionar a adoção e o cumprimento** – fornecer mecanismos para promover a adoção padronizada pelas PMEs por meio da certificação e conformidade regulatória (p. 23-25);
- **Facilitar a implementação –** tornar as normas mais facilmente implementáveis pelas PMEs adaptando-se às suas características específicas (p. 26-28);
- **Aumentar as capacidades** – aumentar as capacidades de cibersegurança nas PMEs, a fim de as preparar para a adoção normal (p. 29);
- **Promover a cooperação** – criar uma estratégia comum entre as partes interessadas no sentido de uma estratégia global para melhorar a segurança da informação e a normalização da privacidade para as PMEs (p. 30).

Podemos constatar que durante o último ano diversas organizações nacionais e europeias seguiram estas recomendações para efetivamente e eficientemente apoiar as empresas afetadas a lidar com as barreiras identificadas ao processo de adoção das normas e preparação para a aplicação dos requisitos do GDPR.

A título de exemplo, o Guia da SPMS (SPMS, 2017), descrito no parágrafo anterior, endereça a barreira relacionada com falta de conhecimento sobre o novo regulamento e envolvimento da gestão hospitalar no processo de preparação para a sua aplicação, por forma a garantir que o tratamento de dados pessoais é efetuado em consonância com as novas regras.

Como parte do seu apoio contínuo à implementação da política da União Europeia (UE) e, mais especificamente, no intuito de ajudar as PMEs a ultrapassar a terceira barreira acima identificada, a ENISA publicou em Dezembro 2016 um estudo (ENISA, 2016) para apoiar as PMEs na adoção das medidas de segurança para a protecção de dados pessoais, seguindo uma abordagem centrada na gestão dos riscos. Estas medidas podem ser adoptadas pelas PMEs, a fim de cumprir o GDPR.

Em particular, os objectivos do estudo (ENISA, 2016) consistiam em facilitar às PMEs a compreensão do contexto da operação de tratamento de dados pessoais e subsequentemente avaliar os riscos de segurança associados. Com base nisso, o estudo também propõe possíveis medidas de segurança organizacionais e técnicas para a proteção de dados pessoais, que sejam adequadas ao risco apresentado. Na tentativa de facilitar ainda mais este procedimento, também está incluído um mapeamento do grupo de medidas proposto com os controlos de segurança da norma ISO/IEC 27001: 2013 (Anexo A).

Similarmente, para facilitar a preparação para o novo quadro regulamentar, a Confederação da Indústria Dinamarquesa (CID) recomenda as empresas a isolar os requisitos relevantes no âmbito de privacidade, traduzi-los em controlos e combinar estes controlos com os controlos de segurança da informação da norma ISO/IEC 27002:2013 que descreve com mais detalhe os controlos listados no Anexo A da norma ISO/IEC 27001: 2013 (Mortensen, 2016). Adicionalmente, a CID sublinha que as normas de segurança devem ser lidas como uma inspiração para trabalhar com a segurança da informação na empresa em geral - e não apenas para criar conformidade com o GDPR.

Este alinhamento com a norma ISO/IEC 27001:2013 é lógico, tendo em conta que é a *framework* no âmbito de segurança de informação mais conhecido, especialmente na Europa, e os resultados expressos face à norma podem ser facilmente interpretados por outros atores internos e externos, como auditores, clientes, governo, etc. (Toreon, sem data).

Por exemplo, de acordo com os resultados da investigação desenvolvida pela ENISA (ENISA, 2012) para derivar uma lista restrita das principais normas de segurança da rede e da informação e boas práticas relevantes para os fornecedores dos serviços de telecomunicações na União Europeia, a norma ISO/IEC 27001:2013 é considerada a melhor e a mais comum prática implementada sendo que é ainda utilizada como um modelo de referência muitas vezes exigido pelos clientes (p.4).

No nosso entender, é exatamente pela mesma razão, que o Guia da SPMS, descrito no parágrafo 1.3.3 do presente documento, inclui o requisito REQ.PRO.03 na dimensão de PROCESSOS que estabelece que as organizações do MS/SNS devam “operar de acordo com os princípios e práticas gerais de boas práticas de segurança da informação (ex. ISO 27001), mesmo que não tenham uma certificação” (p. 54, requisito REQ.PRO.03).

Embora o GDPR foque-se na proteção de dados pessoais, a sua aplicação, sem dúvida, resultará 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, incluindo, consoante o que for adequado (n.º 1 do artigo 32.º do GDPR):

a) A pseudonimização e a cifragem dos dados pessoais;
b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento."

Adicionalmente, o n.º 1 do artigo 24.º do GDPR define que:

> tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

Embora, os artigos 24.º e 32.º, bem como o GDPR em geral, não exigem explicitamente a implementação do Sistema de Gestão de Segurança da Informação (SGSI), a abordagem descrita nos mesmos 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.

Genericamente, os requisitos do GDPR estão alinhados com os objetivos do SGSI definidos na norma ISO/IEC 27001:2013 da seguinte maneira:

"O sistema de gestão de segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão do risco e dá confiança às partes interessadas de que os riscos são geridos adequadamente" (NP ISO/IEC 27001:2013, p. 5).

Analisando o alinhamento proposto pela ENISA (ENISA, 2016) e CID (Mortensen, 2016) entre os requisitos do GDPR 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 GDPR.

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 GDPR, 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 GDPR, que devem ser incorporados dentro do SGISIP, abrange as questões da licitude e lealdade do tratamento.

Considerando todas as razões acima descritas e no intuito de facilitar o cumprimento do novo regulamento, foi decidido resumir o âmbito do presente trabalho ao desenvolvimento de uma *framework* genérica para o Sistema de Gestão Integrada de Segurança da Informação e Privacidade (SGISIP) no setor da saúde com o objetivo de definir uma lista de requisitos do sistema de gestão e controlos de segurança da informação e privacidade mapeados com requisitos e controlos do GDPR, da norma ISO/IEC 27001:2013 e do Guia da SPMS (SPMS, 2017).

No entanto, embora o seu âmbito seja limitado, o presente trabalho é desenvolvido com o intuito de contribuir para o processo geral de preparação à aplicação do GDPR do ponto de vista operacional nas Entidades do setor da Saúde em Portugal. A lista de requisitos do sistema de gestão e controlos de segurança da informação e privacidade a desenvolver no âmbito do projeto terá certamente aplicabilidade tambem ao nível da avaliação do cumprimento do GDPR, da norma ISO/IEC 27001:2013 e dos requisitos do Guia da SPMS, bem como para o consequente desenvolvimento da *roadmap* de implementação do SGISIP e a definição dos controlos a implementar.

O âmbito e os objetivos específicos do projeto são estabelecidos no próximo capítulo.

# 2. DESCRIÇÃO DO PROJETO

O presente capítulo é dedicado à definição dos objetivos do projeto a desenvolver, bem como a descrição das atividades específicas realizadas a fim de garantir o desenvolvimento de um conjunto de conteúdos (entregáveis) necessários para atingir os objetivos estabelecidos.

## 2.1. PROPÓSITO DO PROJETO

Respondendo aos desafios descritos no parágrafo 1.4 do presente documento, o projeto proposto definirá uma *framework* genérica para o **Sistema de Gestão Integrada de Segurança da Informação e Privacidade (SGISIP)** nas entidades do MS/SNS, alinhada com os requisitos e controlos da norma ISO/IEC 27001:2013 e com os requisitos do GDPR. Adicionalmente serão incluídos na *framework* os controlos específicos para cumprir os requisitos da Diretiva SRI para os prestadores de serviços essenciais do setor da saúde.

A *framework* abrangerá o tratamento de dados pessoais efetuado no contexto das atividades de uma entidade da saúde nacional. Assim, são retirados do âmbito, como não relevantes, os requisitos do artigo 27º do GDPR relacionados com designação dos representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União.

## 2.2. OBJETIVOS DO PROJETO

**OBJ.01** – Consolidar os requisitos do GDPR e da Diretiva SRI aplicáveis às entidades do setor da saúde em Portugal;

**OBJ.02** – Definir a lista dos requisitos do SGISIP e dos controlos de segurança da informação e privacidade necessários para cumprir com os requisitos identificados, mapeando-os com os requisitos aplicáveis do GDPR e da Diretiva SRI, bem como com os requisitos e controlos da norma ISO/IEC 27001:2013;

**OBJ.03** – Mapear os requisitos e recomendações do Guia da SPMS com os requisitos do SGISIP e com os controlos de segurança da informação e privacidade definidos supra (objetivo OBJ.02).

## 2.3. ATIVIDADES DO PROJETO

Neste capítulo são descritas as atividades do projeto desenvolvidas a fim de alcançar os objetivos acima definidos.

### 2.3.1. CONSOLIDAÇÃO DOS REQUISITOS DO GDPR E DA DIRETIVA SRI APLICÁVEIS ÀS ENTIDADES DO SETOR DA SAÚDE EM PORTUGAL

NOTA: A atividade corresponde ao objetívo específico OBJ.01.

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

É importante mencionar que o setor da saúde é um dos setores mais afetados pelo GDPR devido à natureza sensível dos dados tratados, a regularidade e volume das operações de tratamento. Atento isso, face à diversidade das finalidades do tratamento, bem como ao extenso universo de requisitos aplicáveis, excluiremos da análise posterior apenas os seguintes:

- As fundações, associações ou outros organismos sem fins lucrativos que prossigam os fins políticos, filosóficos, religiosos ou sindicais (artigo 9.2d do GDPR);
- A proteção dos dados das igrejas e associações religiosas (artigo 91 do GDPR);
- As operações de tratamento de dados pessoais relacionados com condenações penais e infrações (artigo 10 do GDPR);
- Aos representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União (artigo 27 do GDPR).

Assim, num universo de 298 requisitos do GDPR, foram – para efeitos do presente trabalho - considerados aplicáveis às entidades do setor da saúde 287 requisitos aos quais foram acrescentados os 25 requisitos da Diretiva SRI (dos 36 possíveis).

As listas detalhadas dos requisitos do GDPR e da Diretiva SRI considerados encontram-se na **Tabela 2-3** e na **Tabela 2-4** respetivamente.

### 2.3.2. DEFINIÇÃO DA LISTA DOS REQUISITOS DO SGISIP E DOS CONTROLOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

NOTA: A atividade corresponde ao objetívo específico OBJ.02.

Nesta etapa foram definidos os requisitos do SGISIP e controlos de segurança da informação e privacidade necessários para garantir o cumprimento dos requisitos do GDPR e da Diretiva SRI acima identificados.

O consecutivo mapeamento com os requisitos e controlos da norma ISO/IEC 27001:2013 permitiu definir 3 componentes do SGISIP visualmente representados na **Figura 2-1** – *Mindmap* do Sistema de Gestão Integrada de Segurança da Informação e Privacidade**Figura 2-1**, nomeadamente:

- **Requisitos do SGISIP** descritos no parágrafo 2.3.2.1;
- **A – Controlos de Segurança da Informação e Privacidade** descritos no parágrafo 2.3.2.2;
- **B – Âmbito do SGISIP** descrito no parágrafo 2.3.2.3.

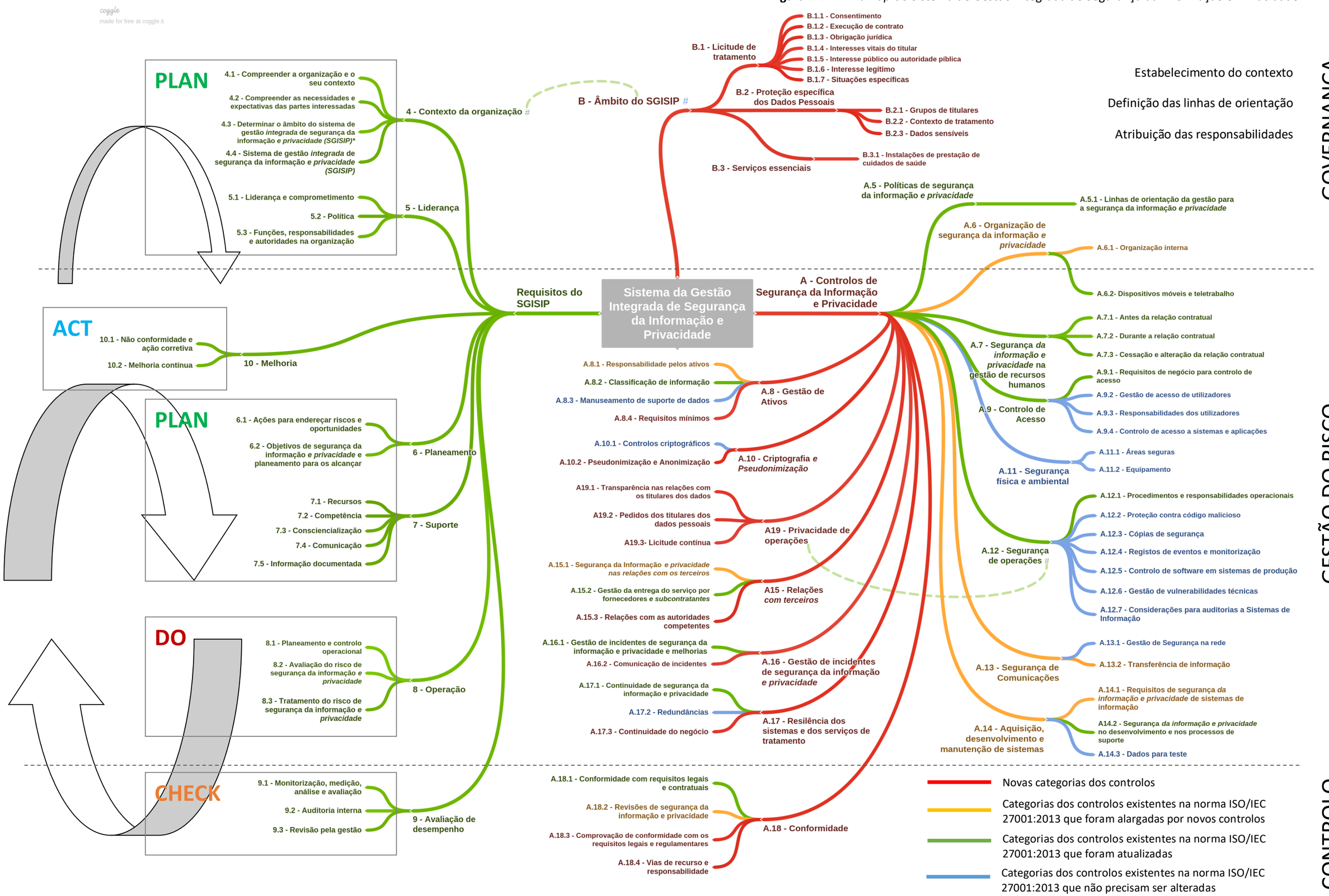
Paralelamente foi efetuado o mapeamento dos requisitos do GDPR e da Diretiva SRI com os requisitos do SGISIP e controlos de segurança da informação e privacidade acima identificados. O resultado deste trabalho encontra-se na **Tabela 2-3** para o GDPR e na **Tabela 2-4** para a Diretiva SRI.

#### 2.3.2.1. REQUISITOS DO SGISIP

Os Requisitos do SGISIP são necessários para estabelecer, implementar, manter e melhorar de forma contínua um Sistema de Gestão Integrada de Segurança da Informação e Privacidade. Estes requisitos correspondem aos requisitos do corpo principal da norma ISO/IEC 27001:2013 e devem ser devidamente atualizados, tendo em consideração os respetivos requisitos do GDPR e da Diretiva SRI, a fim de abranger, para alem da vertente de Segurança da informação, a dimensão de Privacidade e Proteção de Dados dentro da organização e, sendo o caso, também ao nível empresarial.

Os requisitos do SGISIP são consolidados no ANEXO A do presente documento.

**Figura 2-1** – *Mindmap* do Sistema de Gestão Integrada de Segurança da Informação e Privacidade



#### 2.3.2.2. CONTROLOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A consolidação dos Controlos de Segurança da Informação e Privacidade é efetuada numa lista abrangente de objetivos de controlo e controlos que devem ser usados no contexto do Tratamento do Risco de Segurança da Informação e Privacidade (sub-cláusula 6.1.3 dos Requisitos do SGISIP). Estes controlos - 161 no total - foram divididos em três categorias:

- 75 dos 114 controlos da norma ISO/IEC 27001:2013 que não precisam qualquer atualização significativa devido à inclusão dos requisitos da proteção de dados e privacidade, correspondendo na integra aos controlos do Anexo A da norma;

- 39 dos 114 controlos da norma ISO/IEC 27001:2013 necessitam atualização devido à inclusão dos requisitos da proteção de dados e privacidade. A descrição dos mesmos conforme a norma ISO/IEC 27001:2013 deve ser consolidada para assim assegurar o cumprimento dos requisitos do GDPR e da Diretiva SRI a fim de abranger, para além da vertente de Segurança da informação, a dimensão de Privacidade e Proteção de Dados dentro da organização, sendo aplicável ao nível empresarial também;

- 47 novos controlos que foram acrescentados aos já existentes na norma ISO/IEC 27001:2013, por forma a assegurar o cumprimento dos requisitos do GDPR e da Diretiva SRI. Os mesmos estão consolidados na **Tabela 2-1** seguindo a estrutura do Anexo A da norma ISO/IEC 27001:2013, onde se efetuaram as necessárias atualizações de modo a abranger, para além da vertente de Segurança da informação, a dimensão de Privacidade e Proteção de Dados dentro da organização, sendo aplicável ao nível empresarial também.

A lista completa dos Controlos de Segurança da Informação e Privacidade pode ser encontrada no ANEXO B do presente documento.

**Tabela 2-1** – Controlos de Segurança da Informação e Privacidade acrescentados ao Anexo A da norma ISO/IEC 27001:2013 para garantir o cumprimento dos requisitos do GDPR e da Diretiva SRI

| | | |
|---|---|---|
| **A.6 - ORGANIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** <br> *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | |
| SUB-CATEGORIA ALARGADA | **A.6.1 - ORGANIZAÇÃO INTERNA** | |
| **A.6.1.6p** | **Contacto com titulares dos dados pessoais** | ***Controlo novo (CN)*** <br> Devem ser estabelecidos e mantidos os canais de comunicação apropriados com os titulares dos dados pessoais |
| **A.8 - GESTÃO DE ATIVOS** | | |
| SUB-CATEGORIA ALARGADA | **A.8.1 - RESPONSABILIDADE PELOS ATIVOS** | |
| **A.8.1.5p** | **Ciclo de vida dos dados pessoais** | ***Controlo novo (CN)*** <br> Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para gestão do ciclo de vida dos dados pessoais, assegurando o cumprimento dos princípios relativos ao tratamento de dados pessoais |
| **A.8.1.6p** | **Ciclo de vida da informação destinada ao público** | ***Controlo novo (CN)*** <br> Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para gestão dos conteúdos da informação destinados ao público |
| NOVA SUB-CATEGORIA | **A.8.4 - REQUISITOS MÍNIMOS** <br> Objetivo: Garantir a segurança da informação e privacidade consoante o tipo da tecnologia utilizada para o seu tratamento. | |
| **A.8.4.1p** | **Definir os requisitos mínimos para as várias categorias dos ativos** | ***Controlo novo (CN)*** <br> Deve ser definido e aprovado um conjunto de requisitos mínimos (técnicos e organizativos) para garantir a mitigação dos riscos associados à utilização das novas soluções tecnológicas para o tratamento dos dados pessoais, respeitando, em especial, os princípios da segurança da informação e proteção de dados desde a conceção e por defeito. |
| **A.8.4.2p** | **Definir os requisitos mínimos para integração dos sistemas** | ***Controlo novo (CN)*** <br> Deve ser definido e aprovado um conjunto de requisitos mínimos (técnicos e organizativos) para garantir a mitigação dos riscos associados à integração das diversas soluções tecnológicas entre si e/ou com sistemas obsoletos em explotação na organização |

| | | |
|---|---|---|
| **A.10 - CRIPTOGRAFIA *E PSEUDONIMIZAÇÃO**** | | |
| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | |
| **NOVA SUB-CATEGORIA** | **A.10.2 - PSEUDONIMIZAÇÃO E ANONIMIZAÇÃO**<br>Objetivo: Assegurar a utilização adequada e eficaz de pseudonimização e anonimização para reduzir os riscos para os titulares de dados. | |
| **A.10.2.1p** | **Política sobre a Pseudonimização e Anonimização** | ***Controlo novo (CN)***<br>Deve ser desenvolvida e implementada uma política sobre a pseudonimização e anonimização para reduzir os riscos para os titulares de dados em questão garantindo que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. |
| **A.13 - SEGURANÇA DE COMUNICAÇÕES** | | |
| **SUB-CATEGORIA ALARGADA** | **A.13.2 - TRANSFERÊNCIA DE INFORMAÇÃO** | |
| **A.13.2.5p** | **Regras vinculativas aplicáveis às empresas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido, autorizado pela autoridade de controlo competente e implementado um conjunto das regras internas de proteção de dados juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento |
| **A.14 - AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS** | | |
| **SUB-CATEGORIA ALARGADA** | **A.14.1 - REQUISITOS DE SEGURANÇA *DA INFORMAÇÃO E PRIVACIDADE** DE SISTEMAS DE INFORMAÇÃO** | |
| **A.14.1.4p** | **Especificação e análise de requisitos para os processos de negócio** | ***Controlo novo (CN)***<br>Os requisitos relacionados com a segurança da informação, interoperabilidade, privacidade e proteção dos dados pessoais, bem como os requisitos para a tomada das decisões automatizadas devem ser incluídos nos requisitos para novos processos de negócio ou para melhorias nos processos de negócio existentes |

| | | |
|---|---|---|
| **A.14.1.5p** | **Levantamento dos progressos técnicos mais recentes** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para acompanhar fatos novos relevantes e a evolução a nível 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, com especial enfoque nas 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**** <br>*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | |
| **SUB-CATEGORIA ALARGADA** | **A.15.1 - SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE NAS RELAÇÕES COM OS TERCEIROS**** <br>*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | |
| **A.15.1.4p** | **Verificação de credenciais e referências dos subcontratantes** | ***Controlo novo (CN)***<br><br>Devem ser realizadas verificações 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 de negócio, à classificação da informação que será acedida e aos riscos percecionados. |
| **NOVA SUB-CATEGORIA** | **A.15.3 - RELAÇÕES COM AS AUTORIDADES COMPETENTES**<br><br>Objetivo: Garantir o cumprimento dos procedimentos estabelecidos por lei no que respeita a exercício pelas autoridades competentes dos seus poderes de investigação e de correção, bem como dos poderes consultivos e de autorização. | |
| **A.15.3.1p** | **Cooperação com as autoridades competentes (autoridades de controlo)** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para facilitar a realização das auditorias e garantir o seguimento atempado dos pedidos das autoridades competentes efetuados na prossecução das suas atribuições e poderes de investigação |
| **A.15.3.2p** | **Retificação, apagamento e limitação do tratamento de dados pessoais imposta pela autoridade de controlo** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a retificação, apagamento e/ou limitação temporária ou definitiva do tratamento de dados pessoais, ou mesmo a sua proibição, exigida pela autoridade de controlo competente |

| | | |
|---|---|---|
| **A.15.3.3p** | **Suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais por pedido da autoridade de controlo competente** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais na sequência de um pedido da autoridade de controlo competente |
| **A.15.3.4p** | **Consulta prévia** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para realização da consulta a autoridade de controlo antes de proceder ao tratamento dos dados pessoais |
| **A.15.3.5p** | **Autorização da autoridade de controlo para transferência de informação** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para obtenção da autorização da entidade de controlo para transferência de dados pessoais para um país terceiro ou organização internacional |
| **A.15.3.6p** | **Autorização da autoridade de controlo para estabelecimento de acordos administrativos, regras vinculativas e cláusulas contratuais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para obtenção da autorização por parte da entidade de controlo para estabelecimento de acordos administrativos, regras vinculativas aplicáveis às empresas e as cláusulas contratuais |
| **A.16 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** <br>*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | |
| **NOVA SUB-CATEGORIA** | **A.16.2 - Comunicação de incidentes**<br>Objetivo: Garantir a notificação atempada às partes interessadas dos incidentes de segurança da informação e de violações de dados pessoais relevantes. | |
| **A.16.2.1p** | **Notificação de violação de dados pessoais à autoridade de controlo** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação dos incidentes de privacidade (violações de dados pessoais) à autoridade de controlo competente sem demora injustificada |
| **A.16.2.2p** | **Comunicação de violação de dados pessoais ao responsável pelo tratamento** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação dos incidentes de privacidade (violações de dados pessoais) aos respetivos responsáveis pelo tratamento |

| | | |
|---|---|---|
| **A.16.2.3p** | **Comunicação de violação de dados pessoais aos titulares dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação dos incidentes de privacidade (violações de dados pessoais) aos respetivos titulares dos dados |
| **A.16.2.4p** | **Notificação dos incidentes com um impacto importante na continuidade dos serviços essenciais às autoridades competentes ou as CSIRT** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação obrigatória ou voluntária dos incidentes com um impacto importante na continuidade dos serviços essenciais às autoridades competentes ou às CSIRT sem demora injustificada |
| **A.16.2.5p** | **Comunicação por subcontratantes de incidentes com impacto importante na continuidade dos serviços ao prestador de serviço essencial** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir que os subcontratantes informam sem demora injustificada os prestadores de serviços essenciais sobre os incidentes com um impacto importante na continuidade dos serviços prestados |
| **A.16.2.6p** | **Notificação obrigatória centralizada dos incidentes de cibersegurança às autoridades competentes ou às CSIRT** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação sem demora injustificada dos incidentes de cibersegurança às autoridades competentes ou às CSIRT |
| **A.16.2.7p** | **Comunicação de atividades ilícitas e crimes públicos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para efetuar a comunicação às autoridades criminais/judiciais de atividades ilícitas e crimes públicos identificadas no âmbito da resposta a incidentes de segurança da informação e privacidade, bem como para entrega de evidências recolhidas |
| **A.17 - *RESILIÊNCIA DOS SISTEMAS E DOS SERVIÇOS DE TRATAMENTO**** <br>*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | |
| **NOVA SUB-CATEGORIA** | **A.17.3 - CONTINUIDADE DO NEGÓCIO**<br>Objetivo: Garantir a recuperação célere de incidentes disruptivos quando surgem, garantindo a disponibilidade e o acesso aos sistemas, informação e dados pessoais de forma atempada. | |
| **A.17.3.1p** | **Gestão da continuidade operacional** | ***Controlo novo (CN)***<br>A organização deve desenvolver e implementar a estratégia de continuidade do serviço e os planos de contingência, bem como as capacidades de recuperação de desastres |

| | | |
|---|---|---|
| **A.17.3.2p** | **Exercícios relativos a planos de contingência** | ***Controlo novo (CN)***<br>A organização deve definir e testar os seus planos de contingência para garantir que eles sejam eficientes, eficazes e consistentes com os objetivos de continuidade de negócio da organização |
| **A.18 - Conformidade** | | |
| **SUB-CATEGORIA ALARGADA** | **A.18.2 - REVISÕES DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** <br>*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | |
| **A.18.2.4p** | **Auditorias e inspeções conduzidas pelos clientes** | ***Controlo novo (CN)***<br>A organização deve desenvolver e implementar um conjunto de normas e procedimentos apropriados para facilitar a realização de auditorias de segurança da informação e privacidade e garantir o seguimento atempado dos pedidos dos seus clientes |
| **NOVA SUB-CATEGORIA** | **A.18.3 - COMPROVAÇÃO DE CONFORMIDADE COM OS REQUISITOS LEGAIS E REGULAMENTARES**<br>Objetivo: Demonstrar o cumprimento das obrigações do responsável pelo tratamento de acordo com a legislação aplicável. | |
| **A.18.3.1p** | **Adesão a um código de conduta** | ***Controlo novo (CN)***<br>A organização deve recorrer a um código de conduta em matéria de proteção de dados, aprovado nos termos do artigo 40º do GDPR, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos |
| **A.18.3.2p** | **Certificação em matéria de proteção de dados, selos e marcas de proteção de dados** | ***Controlo novo (CN)***<br>A organização deve recorrer a um procedimento de certificação em matéria de proteção de dados, aprovado nos termos do artigo n. 42.o do GDPR, para demonstrar o cumprimento do GDPR, em especial no que respeita à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos. |
| **NOVA SUB-CATEGORIA** | **A.18.4 - VIAS DE RECURSO E RESPONSABILIDADE**<br>Objetivo: Garantir o tratamento adequado das reclamações e uma representação adequada nos eventuais processos judiciais a fim de minimizar os prejuízos associados. | |
| **A.18.4.1p** | **Reclamações dos titulares dos dados pessoais contra a organização** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para recolha e tratamento de reclamações de titulares dos dados pessoais |

| | | |
|---|---|---|
| **A.18.4.2p** | **Reclamação contra a autoridade competente** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para avaliar a fiabilidade e eventualmente apresentar uma reclamação à autoridade competente a fim de minimizar os danos associados à aplicação inadequada das disposições do GDPR e da Diretiva SRI ou quebra do sigilo comercial |
| **A.18.4.3p** | **Queixa contra prestador de serviços digitais junto da entidade competente** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para avaliar a fiabilidade e eventualmente apresentar uma queixa à autoridade competente contra um prestador de serviços digitais que não cumpra os requisitos estabelecidos na Diretiva SRI, especialmente na sequência de um incidente |
| **A.18.4.4p** | **Ação judicial efetiva contra autoridade de controlo** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para avaliar a fiabilidade e eventualmente intentar um processo judicial contra a autoridade de controlo competente a fim de minimizar os danos associados à aplicação inadequada das disposições do GDPR e da Diretiva SRI ou quebra do sigilo comercial |
| **A.18.4.5p** | **Ação judicial contra a organização** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para responder às ações judiciais intentadas contra a organização, alegando a violação das disposições do GDPR |
| **A.18.4.6p** | **Reclamação de parte da indemnização paga, atendendo à corresponsabilidade pelo dano** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para reclamar perante outros responsáveis conjuntos pelo tratamento e/ou subcontratantes de parte da indemnização paga na sequência de uma ação judicial |
| **A.18.4.7p** | **Resposta à reclamação de parte da indemnização paga, atendendo à corresponsabilidade pelo dano** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para responder às reclamações de outros responsáveis conjuntos pelo tratamento e/ou subcontratantes de parte da indemnização paga na sequência de uma ação judicial |
| **A.19 - PRIVACIDADE DE OPERAÇÕES** | | **NOVA CATEGORIA** |
| **NOVA SUB-CATEGORIA** | **A.19.1 - TRANSPARÊNCIA NAS RELAÇÕES COM OS TITULARES DOS DADOS**<br>Objetivo: Garantir a transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. | |

| | | |
|---|---|---|
| **A.19.1.1p** | **Recolha dos dados pessoais junto do titular** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para facultar ao titular dos dados toda a informação exigida pelo GDPR aquando a recolha dos dados pessoais - incluindo as categorias especiais de dados pessoais - junto do titular dos mesmos |
| **A.19.1.2p** | **Recolha dos dados pessoais a partir de outra fonte** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para facultar ao titular dos dados toda a informação exigida pelo GDPR quando os dados pessoais - incluindo as categorias especiais de dados pessoais - não forem recolhidos junto do titular |
| **A.19.1.3p** | **Decisões automatizadas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados que vise permitir o exercício dos direitos dos titulares dos dados 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 |
| **NOVA SUB-CATEGORIA** | **A.19.2 - PEDIDOS DOS TITULARES DOS DADOS PESSOAIS**<br>Objetivo: Garantir que os titulares dos dados pessoais usufruam de controlo efetivo sobre os mesmos, assegurando a resposta atempada aos seus pedidos. | |
| **A.19.2.1p** | **Resposta aos pedidos dos titulares dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para – no sentido de dar resposta a pedido de titulares dos dados - garantir o cumprimento dos direitos e liberdades de terceiros, observando também o segredo comercial ou a propriedade intelectual e, em particular, os direitos de autor que protejam o software |
| **A.19.2.2p** | **Disponibilização de acesso do titular aos seus dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para - na sequência de um pedido do titular dos dados - facultar a este o acesso aos mesmos, bem como às informações adicionais, de acordo com os requisitos do GDPR |
| **A.19.2.3p** | **Retificação dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados que permitam a retificação dos dados pessoais inexatos, na sequencia de um pedido do seu titular e sem demora injustificada |

| | | |
|---|---|---|
| **A.19.2.4p** | **Apagamento dos dados pessoais a pedido do titular dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o apagamento, sem demora injustificada, dos dados pessoais na sequência de um pedido do seu titular e que manifeste oposição ao tratamento |
| **A.19.2.5p** | **Limitação do tratamento dos dados pessoais a pedido do titular dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a limitação do tratamento dos dados pessoais na sequência de um pedido do seu titular e que manifeste oposição ao tratamento, embora parcial |
| **A.19.2.6p** | **Portabilidade dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para - a pedido do titular dos dados - garantir a transferência dos dados pessoais para si ou a outro responsável pelo tratamento |
| **NOVA SUB-CATEGORIA** | **A.19.3 - LICITUDE CONTÍNUA**<br>Objetivo: Manter a licitude de tratamento ao longo do ciclo da vida dos dados pessoais. | |
| **A.19.3.1p** | **Registo das atividades de tratamento** | ***Controlo novo (CN)***<br>Deve ser criado e devidamente mantido (revisto e atualizado) um registo de todas as atividades de tratamento efetuadas pela organização na qualidade de responsável pelo tratamento e/ou na qualidade de subcontratante sob a responsabilidade de um ou vários responsáveis pelo tratamento ou ainda, se aplicável, os seus representantes |
| **A.19.3.2p** | **Tratamento posterior dos dados pessoais para outros fins** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos |
| **A.19.3.3p** | **Apagamento dos dados pessoais para garantir a licitude de tratamento** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o apagamento, sem demora injustificada, dos dados pessoais para garantir a licitude de tratamento, bem como o cumprimento das obrigações jurídicas |

### 2.3.2.3. ÂMBITO DO SGISIP

O Âmbito do SGISIP pode ser definido utilizando a lista dos controlos apresentados na **Tabela 2-2** do presente documento. Todos os controlos deste anexo são novos e foram introduzidos para guiar as unidades clínicas e operacionais das entidades do MS/SNS no processo da implementação do SGISIP, garantindo o cumprimento dos requisitos do GDPR e da Diretiva SRI nas três vertentes:

- **B1 – Licitude de Tratamento** é uma categoria de controlos composta pela lista de tipos de operações de tratamento lícitas de acordo com o GDPR (24 controlos);
- **B2 – Proteção Específica** é uma categoria de controlos composta pela lista das situações que exigem a proteção específica de acordo com o GDPR (8 controlos);
- **B3 - Serviços essenciais** é uma categoria de controlos prevista e que deverá ser definida de acordo com a lista dos serviços essenciais a adotar e publicar pelo Estado Português até 9 de maio de 2018 para dar cumprimento à Diretiva SRI (a quantidade de controlos será definida após a publicação da respetiva lista).

**Tabela 2-2** – Âmbito do Sistema de Gestão Integrada de Segurança da Informação e Privacidade

| **B.1 - LICITUDE DE TRATAMENTO** | | **NOVA CATEGORIA** |
|---|---|---|
| **NOVA SUB-CATEGORIA** | **B.1.1 – CONSENTIMENTO**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para a obtenção do consentimento informado. | |
| **B.1.1.1** | **Consentimento para tratamento dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a obtenção, registo e cancelamento do consentimento do titular de dados pessoais (incluindo as categorias especiais de dados pessoais) para uma ou mais finalidades específicas de tratamento |
| **B.1.1.2** | **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 novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a obtenção, registo e cancelamento do consentimento do titular de dados pessoais (incluindo as categorias especiais de dados pessoais) para os efeitos de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos |

| | | |
|---|---|---|
| **B.1.1.3** | **Consentimento para tratamento dos dados pessoais de crianças em relação aos serviços da sociedade da informação** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a obtenção, registo e cancelamento do consentimento ou autorização dos titulares das responsabilidades parentais da criança para tratamento dos dados pessoais da mesma (incluindo as categorias especiais de dados pessoais) |
| **NOVA SUB-CATEGORIA** | **B.1.2 - EXECUÇÃO DE CONTRATO**<br>Objetivo: Garantir a licitude de tratamento através da execução de contratos | |
| **B.1.2.1** | **Tratamento dos dados pessoais necessário para a formalização de um contrato** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a recolha dos dados pessoais a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar e consequente formalização das relações contratuais em que o titular dos dados seja parte. |
| **B.1.2.2** | **Tratamento dos dados pessoais no âmbito de contrato formalizado** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir o tratamento dos dados pessoais no âmbito da execução de um contrato em cujo titular dos dados pessoais seja parte contratante, observando os requisitos contratuais e legislação aplicável |
| **NOVA SUB-CATEGORIA** | **B.1.3 - OBRIGAÇÃO JURÍDICA**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessários para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito | |
| **B.1.3.1** | **Tratamento dos dados pessoais de acordo com uma obrigação jurídica** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito |
| **B.1.3.2** | **Tratamento dos dados pessoais necessário à declaração, ao exercício ou à defesa de um direito num processo judicial** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário à declaração, ao exercício ou à defesa de um direito num processo judicial |
| **NOVA SUB-CATEGORIA** | **B.1.4 - INTERESSES VITAIS DO TITULAR**<br>Objetivo: Garantir a proteção dos dados pessoais cujo tratamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular | |

| | | |
|---|---|---|
| **B.1.4.1** | **Tratamento dos dados pessoais para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento de dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento |
| **NOVA SUB-CATEGORIA** | **B.1.5 - INTERESSE PÚBLICO OU AUTORIDADE PÚBLICA**<br><br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito decorrente do direito da União ou de um Estado-Membro | |
| **B.1.5.1** | **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 novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o exercício das funções de interesse público ou prerrogativas de autoridade pública |
| **B.1.5.2** | **Tratamento dos dados pessoais por motivo de interesse público no domínio da saúde pública** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o exercício das funções de interesse público no domínio da saúde pública com base no direito da União ou dos Estados Membros |
| **NOVA SUB-CATEGORIA** | **B.1.6 - INTERESSE LEGÍTIMO**<br><br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para proteger os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros | |
| **B.1.6.1** | **Tratamento dos dados pessoais dos clientes** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais dos clientes da organização em casos quando as relações contratuais não são devidamente formalizadas |
| **B.1.6.2** | **Tratamento dos dados pessoais dos titulares dos dados que estão ao serviço do responsável pelo tratamento** | ***Controlo novo (CN)***<br><br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais dos titulares dos dados que prestam serviços ao responsável pelo tratamento independentemente da existência da remuneração |

| | | |
|---|---|---|
| **B.1.6.3** | **Tratamento dos dados pessoais para efeitos de comercialização direta** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para efeitos de comercialização direta |
| **B.1.6.4** | **Tratamento dos dados pessoais para assegurar a segurança da rede e das informações** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir o tratamento dos dados pessoais na medida estritamente necessária e proporcionada para garantir a segurança das redes e das informações |
| **B.1.6.5** | **Tratamento dos dados pessoais no âmbito do grupo de empresas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais no âmbito do grupo de empresas |
| **B.1.6.6** | **Indicação de eventuais atos criminosos ou ameaças à segurança pública a autoridades competentes** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a indicação pelo responsável pelo tratamento a uma autoridade competente de eventuais atos criminosos ou ameaças à segurança pública e à transmissão dos dados pessoais pertinentes |
| **B.1.6.7** | **Tratamento de dados pessoais necessário à prevenção e controlo da fraude** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para efeitos de controlo e prevenção de fraudes e da evasão fiscal de acordo com a legislação aplicável |
| **B.1.6.8** | **Transferências não repetitivas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para transferências que possam ser classificadas como não repetitivas e que apenas digam respeito a um número limitado de titulares de dados |
| **NOVA SUB-CATEGORIA** | **B.1.7 - SITUAÇÕES ESPECÍFICAS**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para garantir a legalidade e lealdade do tratamento relativo as situações específicas de tratamento | |
| **B.1.7.1** | **Tratamento dos dados pessoais para fins jornalísticos e para fins de expressão académica, artística ou literária** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) para fins jornalísticos e para fins de expressão académica, artística ou literária |

| | | |
|---|---|---|
| **B.1.7.2** | **Disponibilização do acesso do público aos documentos oficiais a divulgar** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a divulgação segura dos documentos oficiais na posse de uma autoridade pública ou de um organismo público |
| **B.1.7.3** | **Tratamento dos dados pessoais no contexto laboral** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais dos trabalhadores no contexto laboral |
| **B.1.7.4** | **Arquivo de interesse público** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para fins de arquivo de interesse público |
| **B.1.7.5** | **Investigação científica ou histórica** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para fins de investigação científica ou histórica |
| **B.1.7.6** | **Fins estatísticos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para fins estatísticos |
| **B.2 - PROTEÇÃO ESPECÍFICA** | | **NOVA CATEGORIA** |
| **NOVA SUB-CATEGORIA** | **B.2.1 - GRUPOS DE TITULARES**<br>Objetivo: Garantir a proteção específica dos direitos e liberdades das pessoas singulares vulneráveis | |
| **B.2.1.1** | **Proteção especial das crianças quanto aos seus dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção especial das crianças, nomeadamente em casos da utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como da recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças |
| **NOVA SUB-CATEGORIA** | **B.2.2 - CONTEXTO DE TRATAMENTO**<br>Objetivo: Garantir a proteção específica dos dados pessoais quando o contexto do seu tratamento poderá implicar riscos significativos para os direitos e liberdades fundamentais | |

| | | |
|---|---|---|
| **B.2.2.1** | **Tratamento dos dados pessoais em grande escala** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados sensíveis cujo tratamento seja realizado em grande escala, bem como quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala |
| **B.2.2.2** | **Intercâmbio de dados pessoais com os registos nacionais e internacionais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados pessoais partilhados com outras organizações através de plataformas de interoperabilidade |
| **NOVA SUB-CATEGORIA** | **B.2.3 - DADOS SENSÍVEIS**<br>Objetivo: Garantir a proteção específica das categorias especiais dos dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais | |
| **B.2.3.1** | **Tratamento de categorias especiais dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados sensíveis |
| **B.2.3.2** | **Tratamento dos dados biométricos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados biométricos quando forem processados por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular |
| **B.2.3.3** | **Tratamento dos dados pessoais relativos à saúde** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados pessoais relativos ao estado de saúde dos titulares dos dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro |
| **B.2.3.4** | **Tratamento dos dados genéticos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados genéticos de acordo com a legislação aplicável |

| | | |
|---|---|---|
| **B.2.3.5** | **Tratamento dos dados da localização ou deslocações do titular dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados da localização ou deslocações do titular dos dados de acordo com a legislação aplicável |
| **B.3 - SERVIÇOS ESSENCIAIS** | | **NOVA CATEGORIA** |
| **NOVA SUB-CATEGORIA** | **B.3.1 - Instalações de prestação de cuidados de saúde**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para prestação dos serviços essenciais no setor da saúde | |
| **B.3.1.x** | A lista dos controlos deve ser definida de acordo com a lista dos serviços essenciais definida por cada Estado-Membro. | |

### 2.3.2.4. MAPEAMENTO DOS REQUISITOS DO GDPR E DA DIRETIVA SRI COM OS REQUISITOS E CONTROLOS DO SGISIP

Em paralelo com a definição da lista dos requisitos e controlos do SGISIP foi efetuado o mapeamento dos mesmos com os requisitos do GDPR e da Diretiva SRI aplicáveis ao setor da saúde em Portugal (parágrafo 2.3.1). O resultado deste trabalho é consolidado na **Tabela 2-3** para o GDPR e na **Tabela 2-4** para a Diretiva SRI.

**Tabela 2-3** – Requisitos do GDPR aplicáveis ao setor da saúde em Portugal

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| **Capítulo II – Princípios** | | | |
| 5 - Princípios relativos ao tratamento de dados pessoais | 1 | a | 5.1, 5.2, A.5.1.1, A.8.1.5p |
| | | b | 5.1, 5.2, A.5.1.1, A.8.1.5p |
| | | c | 5.1, 5.2, A.5.1.1, A.8.1.1, A.8.1.5p, A.19.3.1p, A.19.3.2p, A.19.3.3p |
| | | d | 5.1, 5.2, A.5.1.1, A.8.1.5p |
| | | e | 5.1, 5.2, A.5.1.1, A.8.1.5p, B.1.7.4, B.1.7.5, B.1.7.6 |
| | | f | 5.1, 5.2, 6.1.3, 8.3, A.5.1.1, A.8.1.5p, A.9.1.1, A.10.1.1, A.10.1.2, A.10.2.1p |
| | 2 | - | A.18.1.1 |
| 6 - Licitude do tratamento | 1 | a | 5.2, A.5.1.1, A.19.3.1p, B.1.1.1, B.1.1.2, B.1.1.3, B.1.4.1 |
| | | b | 5.2, A.5.1.1, A.19.3.1p, B.1.2.1, B.1.2.2 |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| | | c | 5.2, A.5.1.1, A.19.3.1p, B.1.3.1 |
| | | d | 5.2, A.5.1.1, A.19.3.1p, B.1.4.1 |
| | | e | 5.2, A.5.1.1, A.19.3.1p, B.1.5.1 |
| | | f | 5.2, A.5.1.1, A.19.3.1p, B.1.6.1, B.1.6.2, B.1.6.3, B.2.1.1 |
| | 4 | - | 5.2, A.5.1.1, A.10.2.1p, A.14.3.1, A.19.3.2p |
| 7 - Condições aplicáveis ao consentimento | 1 | - | 5.2, 7.5.1, 7.5.3, 8.1, 8.2, A.5.1.1, A.19.3.1p |
| | 2 | - | 5.2, A.5.1.1, B.1.1.1, B.1.1.2, B.1.1.3 |
| | 3 | - | 5.2, A.5.1.1, A.19.2.4p |
| | 4 | - | 5.2, A.5.1.1, B.1.1.1, B.1.1.2, B.1.1.3, B.1.2.1, B.1.2.2 |
| 8 - Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação | 1 | - | 5.2, A.5.1.1, B.1.1.3, B.2.1.1 |
| | 2 | - | 5.2, A.5.1.1, B.1.1.3, B.2.1.1 |
| 9 - Tratamento de categorias especiais de dados pessoais | 1 | - | 5.2, A.5.1.1, B.1.1.1, B.1.1.2, B.1.1.3, B.1.2.1, B.1.2.2, B.1.4.1, B.1.5.1, B.1.5.2, B.1.7.1, B.2.3.1, B.2.3.2, B.2.3.3, B.2.3.4 |
| | 2 | a | 5.2, A.5.1.1, A.19.3.1p, B.1.1.1, B.1.1.2, B.1.1.3, B.2.3.1 |
| | | b | 5.2, A.5.1.1, A.19.3.1p, B.1.7.3, B.2.3.1 |
| | | c | 5.2, A.5.1.1, A.19.3.1p, B.1.4.1, B.2.3.1 |
| | | e | 5.2, A.5.1.1, A.19.1.2p, A.19.3.1p, B.1.7.1, B.2.3.1 |
| | | f | 5.2, A.5.1.1, A.19.3.1p, B.2.3.1 |
| | | g | 5.2, A.5.1.1, A.19.3.1p, B.1.5.1, B.2.3.1 |
| | | h | 5.2, A.5.1.1, A.19.3.1p, B.1.2.1, B.1.2.2, B.1.5.1, B.1.6.1, B.1.7.3, B.2.3.1, B.2.3.3 |
| | | i | 5.2, A.5.1.1, A.7.1.2, A.9.1.1, A.13.2.4, A.19.3.1p, B.1.5.1, B.1.5.2, B.2.3.1, B.2.3.3 |
| | | j | 5.2, A.5.1.1, A.19.3.1p, B.1.5.1, B.1.7.4, B.1.7.5, B.1.7.6, B.2.3.1 |
| | 3 | - | 5.2, A.5.1.1, A.7.1.2, A.9.1.1, A.13.2.4, B.1.2.1, B.1.2.2, B.2.3.1 |
| 11 - Tratamento que não exige identificação | 1 | - | 5.2, A.5.1.1, B.1.7.4, B.1.7.5, B.1.7.6 |
| | 2 | - | 5.2, 7.5.3, 8.1, 8.2, A.5.1.1, A.10.2.1p, B.1.7.4, B.1.7.5, B.1.7.6 |
| **Capítulo III - Direitos do titular dos dados** | | | |
| ***Secção 1 - Transparência e regras para o exercício dos direitos dos titulares dos dados*** | | | |
| 12 - Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados | 1 | - | 7.4, A.8.1.6p, A.19.1.1p, A.19.1.2p, A.19.2.1p, B.2.1.1 |
| | 2 | - | 7.4, 7.5.3, 8.1, 8.2, A.19.2.1p |
| | 3 | - | 7.4, A.19.2.1p |
| | 4 | - | 7.4, A.19.2.1p |
| | 5 | - | 7.4, 7.5.3, 8.1, 8.2, A.8.1.6p, A.19.1.1p, A.19.1.2p, A.19.2.1p |
| | 6 | - | 7.4, A.19.2.1p |
| | 7 | - | 7.4, A.19.1.1p, A.19.1.2p |
| ***Secção 2 - Informação e acesso aos dados pessoais*** | | | |
| 13 - Informações a facultar quando os | 1 | - | 7.4, A.8.1.6p, A.19.1.1p |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| dados pessoais são recolhidos junto do titular | 2 | - | 7.4, A.8.1.6p, A.8.4.2p, A.9.1.1, A.14.1.1, A.14.1.4p, A.19.1.1p |
| | 3 | - | 7.4, A.8.1.6p, A.19.1.1p |
| | 4 | - | 7.4, A.8.1.6p, A.19.1.1p |
| 14 - Informações a facultar quando os dados pessoais não são recolhidos junto do titular | 1 | - | 7.4, A.8.1.6p, A.19.1.2p |
| | 2 | - | 7.4, A.8.1.6p, A.8.4.2p, A.9.1.1, A.14.1.1, A.14.1.4p, A.19.1.2p |
| | 3 | - | 7.4, A.8.1.6p, A.19.1.2p |
| | 4 | - | 7.4, A.8.1.6p, A.19.1.2p |
| | 5 | - | 7.4, A.7.1.2, A.8.1.6p, A.13.2.4, A.19.1.2p |
| 15 - Direito de acesso do titular dos dados | 1 | - | A.9.1.1, A.19.2.2p |
| | 2 | - | A.19.2.2p |
| | 3 | - | A.9.1.1, A.14.1.1, A.14.1.4p, A.19.2.2p |
| | 4 | - | A.19.2.2p |
| ***Secção 3 - Retificação e apagamento*** | | | |
| 16 - Direito de retificação | - | - | A.19.2.3p |
| 17 - Direito ao apagamento dos dados («direito a ser esquecido») | 1 | - | A.19.2.4p, A.19.3.3p |
| | 2 | - | 7.4, A.19.2.4p, A.19.3.3p |
| | 3 | - | A.19.2.4p, A.19.3.3p, B.1.5.2, B.2.3.3 |
| 18 - Direito à limitação do tratamento | 1 | a | A.19.2.3p, A.19.2.5p |
| | | b | A.19.2.5p, A.19.3.3p |
| | | c | A.19.2.5p, A.19.3.3p |
| | | d | A.19.2.4p, A.19.2.5p |
| | 2 | - | A.19.2.5p |
| | 3 | - | A.19.2.5p |
| 19 - Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento | - | - | 7.4, A.19.2.3p, A.19.2.4p, A.19.2.5p, A.19.3.3p |
| 20 - Direito de portabilidade dos dados | 1 | - | A.8.4.2p, A.14.1.1, A.14.1.4p, A.19.2.6p |
| | 2 | - | A.8.4.2p, A.14.1.1, A.14.1.4p, A.19.2.6p |
| | 3 | - | A.8.4.2p, A.14.1.1, A.14.1.4p, A.19.2.6p |
| | 4 | - | A.8.4.2p, A.14.1.1, A.14.1.4p, A.19.2.6p |
| ***Secção 4 - Direito de oposição e decisões individuais automatizadas*** | | | |
| 21 - Direito de oposição | 1 | - | A.19.2.4p, A.19.2.5p, A.19.3.2p, B.1.5.1 |
| | 2 | - | A.19.2.4p, A.19.2.5p, B.1.6.3 |
| | 3 | - | A.19.2.4p, A.19.2.5p, B.1.6.3 |
| | 4 | - | 7.4, A.19.1.1p, A.19.1.2p |
| | 5 | - | A.19.2.4p, A.19.2.5p |
| | 6 | - | A.19.2.4p, A.19.2.5p |
| 22 - Decisões individuais automatizadas, incluindo definição de perfis | 1 | - | A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.19.1.3p |
| | 2 | a | A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.19.1.3p, B.1.2.1, B.1.2.2 |
| | | b | A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.19.1.3p |
| | | c | A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.19.1.3p, B.1.1.1, B.1.1.2, B.1.1.3 |
| | 3 | - | A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.19.1.3p, B.1.1.1, B.1.1.2, B.1.1.3, B.1.2.1, B.1.2.2 |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| | 4 | - | A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.19.1.3p, B.1.1.1, B.1.1.2, B.1.1.3, B.1.2.1, B.1.2.2, B.2.3.1 |
| ***Secção 5 - Limitações*** | | | |
| 23 - Limitações | 1 | - | A.18.1.1, B.1.5.2, B.2.3.3 |
| | 2 | - | A.9.1.1, A.18.1.1 |
| **Capítulo IV - Responsável pelo tratamento e subcontratante** | | | |
| ***Secção 1 - Obrigações gerais*** | | | |
| 24 - Responsabilidade do responsável pelo tratamento | 1 | - | 5.1, 5.2, 6.1.2, 6.1.3, 6.2, 7.5.1, 8.3, 9.1, 9.2, 9.3, 10.1, A.5.1.2, A.18.1.1, A.18.1.4, A.18.3.1p, A.18.3.2p, A.19.3.1p |
| | 2 | - | 5.1, 5.2, A.5.1.1, A.5.1.2 |
| | 3 | - | 7.5.3, 8.1, 8.2, A.18.3.1p, A.18.3.2p |
| 25 - Proteção de dados desde a conceção e por defeito | 1 | - | 5.2, 6.1.2, 6.1.3, 6.2, 9.1, 9.2, 9.3, A.5.1.1, A.6.1.5, A.8.1.1, A.8.1.5p, A.8.4.1p, A.8.4.2p, A.10.2.1p, A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.14.3.1, A.18.3.2p, A.19.3.1p, A.19.3.2p, A.19.3.3p |
| | 2 | - | 5.2, 6.1.2, 6.1.3, A.5.1.1, A.6.1.5, A.8.4.1p, A.8.4.2p, A.9.1.1, A.14.1.1, A.14.1.4p, A.14.2.1, A.14.2.5, A.18.3.2p |
| | 3 | - | 7.5.3, 8.1, 8.2, A.8.4.1p, A.8.4.2p, A.18.3.2p |
| 26 - Responsáveis conjuntos pelo tratamento | 1 | - | A.15.1.2, A.19.1.1p, A.19.1.2p |
| | 2 | - | A.15.1.2, A.19.1.1p, A.19.1.2p |
| | 3 | - | A.15.1.2 |
| 28 - Subcontratante | 1 | - | 6.2, 9.1, 9.2, 9.3, 10.1, A.15.1.1, A.15.1.2, A.15.1.3, A.15.1.4p |
| | 2 | - | A.12.1.2, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.2 |
| | 3 | - | A.15.1.1, A.15.1.2, A.15.1.3 |
| | | a | 7.5.3, 8.1, 8.2, A.7.1.2, A.7.2.1, A.13.2.1, A.13.2.2, A.15.1.1, A.15.1.2 |
| | | b | A.7.1.2, A.7.2.1, A.9.1.1, A.13.2.4, A.15.1.1, A.15.1.2, A.15.1.3 |
| | | c | A.15.1.1, A.15.1.2 |
| | | d | A.15.1.1, A.15.1.2, A.15.1.3 |
| | | e | A.15.1.1, A.15.1.2 |
| | | f | A.15.1.1, A.15.1.2 |
| | | g | A.15.1.1, A.15.1.2 |
| | | h | 7.5.3, 8.1, 8.2, 10.1, A.15.1.1, A.15.1.2, A.15.1.4p, A.15.2.1, A.18.2.4p |
| | 4 | - | A.15.1.1, A.15.1.2, A.15.1.3 |
| | 5 | - | 7.5.3, 8.1, 8.2, A.15.1.2, A.15.1.4p, A.15.2.1, A.18.3.1p, A.18.3.2p |
| | 6 | - | A.15.1.2 |
| | 9 | - | A.15.1.2 |
| | 10 | - | A.15.1.2 |
| 29 - Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante | - | - | A.7.1.2, A.7.2.1, A.9.1.1, A.15.1.2, A.15.1.3 |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| 30 - Registos das atividades de tratamento | 1 | - | 7.5.3, 8.1, 8.2, A.19.3.1p |
| | | a | A.19.3.1p |
| | | b | A.19.3.1p |
| | | c | A.19.3.1p |
| | | d | A.19.3.1p |
| | | e | A.19.3.1p |
| | | f | A.19.3.1p |
| | | g | A.19.3.1p |
| | 2 | - | 7.5.3, 8.1, 8.2 |
| | | a | A.19.3.1p |
| | | b | A.19.3.1p |
| | | c | A.19.3.1p |
| | | d | A.19.3.1p |
| | 3 | - | 7.5.3, 8.1, 8.2, A.19.3.1p |
| | 4 | - | 7.5.3, 8.1, 8.2, A.15.3.1p |
| | 5 | - | 7.5.3, 8.1, 8.2, A.19.3.1p, B.2.3.1 |
| 31 - Cooperação com a autoridade de controlo | - | - | A.15.3.1p |
| ***Secção 2 - Segurança dos dados pessoais*** | | | |
| 32 - Segurança do tratamento | 1 | - | 4.1, 4.3, 5.1, 6.1.2, 6.1.3, 6.2, 8.2, 8.3, 9.1, 9.2, 9.3, A.10.1.1, A.10.1.2, A.10.2.1p, A.12.6.1 |
| | | a | 6.1.3, 6.2, 8.3, A.10.1.1, A.10.1.2, A.10.2.1p, A.14.3.1 |
| | | b | 6.1.3, 6.2, 8.3, A.17.1.1, A.17.1.2, A.17.1.3, A.17.3.1p, A.17.3.2p |
| | | c | 6.1.3, 6.2, 8.3, A.9.1.1, A.17.1.1, A.17.1.2, A.17.1.3, A.17.3.1p, A.17.3.2p |
| | | d | 5.1, 6.1.3, 6.2, 7.3, 9.1, 9.2, 9.3, A.12.6.1, A.18.2.2, A.18.2.3 |
| | 2 | - | 5.1, 6.1.2, 8.2, A.9.1.1, A.12.1.2 |
| | 3 | - | 7.5.3, 8.1, 8.2, A.18.3.1p, A.18.3.2p |
| | 4 | - | 5.1, A.7.1.2, A.7.2.1, A.9.1.1, A.15.1.2, A.15.1.3 |
| 33 - Notificação de uma violação de dados pessoais à autoridade de controlo | 1 | - | 6.2, 7.4, A.16.1.1, A.16.1.4, A.16.2.1p |
| | 2 | - | 7.4, A.16.1.1, A.16.1.2, A.16.1.4, A.16.2.1p, A.16.2.2p |
| | 3 | a | 7.4, A.16.1.1, A.16.1.4, A.16.1.7, A.16.2.1p |
| | | b | 7.4, A.16.1.1, A.16.2.1p |
| | | c | 7.4, A.16.1.1, A.16.2.1p |
| | | d | 7.4, A.16.1.1, A.16.1.5, A.16.2.1p |
| | 4 | - | 7.4, A.16.2.1p |
| | 5 | - | 7.5.3, 8.1, 8.2, A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.7 |
| 34 - Comunicação de uma violação de dados pessoais ao titular dos dados | 1 | - | 7.4, A.6.1.6p, A.16.2.3p |
| | 2 | - | 7.4, A.8.1.6p, A.16.2.3p |
| | 3 | - | 7.4, A.6.1.6p, A.8.1.6p, A.10.1.1, A.10.1.2, A.10.2.1p, A.16.2.3p |
| | 4 | - | 7.4, A.8.1.6p, A.16.2.3p |
| ***Secção 3 - Avaliação de impacto sobre a proteção de dados e consulta prévia*** | | | |
| 35 - Avaliação de impacto sobre a | 1 | - | 4.1, 6.1.2, 6.2, 8.2, A.8.4.1p, A.8.4.2p |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| proteção de dados | 2 | - | 5.3, 6.1.2, 8.2, A.6.1.1, A.6.1.2 |
| | 3 | - | 6.1.2, 8.2, A.19.1.3p, B.2.2.1, B.2.3.1 |
| | 7 | - | 6.1.2, 6.2, 7.5.3, 8.1, 8.2 |
| | 8 | - | 6.1.2 |
| | 9 | - | 6.1.2, 7.4, A.6.1.6p |
| | 10 | - | 6.1.2 |
| | 11 | - | 6.1.2, 6.2, 9.1, 9.2, 9.3 |
| 36 - Consulta prévia | 1 | - | 5.3, 7.4, A.6.1.1, A.15.3.4p |
| | 3 | - | A.15.3.4p |
| | 5 | - | A.15.3.4p, B.1.5.2, B.2.3.3 |
| ***Secção 4 - Encarregado da proteção de dados*** | | | |
| 37 - Designação do encarregado da proteção de dados | 1 | - | 5.3, A.6.1.1, B.2.2.1, B.2.3.1 |
| | 2 | - | 5.3, A.6.1.1 |
| | 3 | - | 5.3, A.6.1.1 |
| | 4 | - | 5.3, A.6.1.1 |
| | 5 | - | 5.3, 7.2, A.6.1.1, A.7.1.2, A.7.2.2 |
| | 6 | - | 5.3, A.6.1.1, A.7.1.2 |
| | 7 | - | 7.4, A.6.1.3, A.6.1.6p, A.8.1.6p |
| 38 - Posição do encarregado da proteção de dados | 1 | - | 5.1, 5.3, 7.4, A.6.1.1, A.7.2.1, A.9.1.1, A.9.2.2 |
| | 2 | - | 5.1, 7.1, 7.2, 7.4, A.7.2.1, A.7.2.2, A.9.1.1, A.9.2.2 |
| | 3 | - | 5.3, 7.4, A.6.1.1, A.6.1.2 |
| | 4 | - | 7.4, A.6.1.6p, A.8.1.6p, A.19.2.1p |
| | 5 | - | 7.4, A.7.1.2, A.9.1.1, A.13.2.4 |
| | 6 | - | A.6.1.2 |
| 39 - Funções do encarregado da proteção de dados | 1 | a | 5.1, 5.3, 7.2, 7.4, A.6.1.1 |
| | | b | 5.1, 5.3, 7.4, 9.1, 9.2, 9.3, A.6.1.1, A.7.2.2, A.18.1.4, A.18.2.2, A.18.2.3 |
| | | c | 5.1, 5.3, 6.1.2, 7.4, A.6.1.1 |
| | | d | 5.1, 5.3, 6.1.2, 7.4, A.6.1.1, A.8.1.6p |
| | | e | 5.1, 5.3, 6.1.3, 7.4, A.6.1.1, A.8.1.6p, A.15.3.4p |
| | 2 | - | 5.3, A.6.1.1 |
| ***Secção 5 - Códigos de conduta e certificação*** | | | |
| 40 - Códigos de conduta | 2 | - | 7.4, A.10.2.1p, A.14.3.1, A.18.3.1p, B.2.1.1 |
| | 3 | - | A.18.3.1p |
| | 4 | - | A.15.3.1p, A.18.3.1p |
| 42 - Certificação | 2 | - | A.13.2.2, A.18.3.2p |
| | 4 | - | A.18.3.2p |
| | 7 | - | A.18.3.2p |
| **Capítulo V - Transferências de dados pessoais para países terceiros ou organizações internacionais** | | | |
| 44 - Princípio geral das transferências | - | - | A.13.2.1, A.13.2.2 |
| 45 - Transferências com base numa decisão de adequação | 1 | - | A.13.2.1, A.13.2.2 |
| 46 - Transferências sujeitas a garantias adequadas | 1 | - | A.13.2.1, A.13.2.2 |
| | 2 | a | A.13.2.1, A.13.2.2 |
| | | b | A.13.2.1, A.13.2.2, A.13.2.5p |
| | | c | A.13.2.1, A.13.2.2 |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| | | d | A.13.2.1, A.13.2.2 |
| | | e | A.13.2.1, A.13.2.2, A.18.3.1p |
| | | f | A.13.2.1, A.13.2.2, A.18.3.2p |
| | 3 | a | A.13.2.1, A.13.2.2, A.15.3.5p, A.15.3.6p |
| | | b | A.13.2.1, A.13.2.2, A.15.3.5p, A.15.3.6p |
| 47 - Regras vinculativas aplicáveis às empresas | 1 | a | A.13.2.5p |
| | | b | A.13.2.5p |
| | | c | A.13.2.5p |
| | 2 | a | 4.1, A.13.2.5p |
| | | b | 4.1, A.13.2.5p |
| | | c | 4.1, A.13.2.5p |
| | | d | 4.1, A.6.1.5, A.6.1.6p, A.8.1.1, A.8.1.5p, A.13.2.5p, A.19.3.1p, A.19.3.2p, A.19.3.3p, B.2.3.1 |
| | | e | 4.1, A.6.1.6p, A.13.2.5p |
| | | f | 5.3, A.6.1.1, A.6.1.6p, A.13.2.5p |
| | | g | A.6.1.6p, A.8.1.6p, A.13.2.5p, A.19.1.1p, A.19.1.2p |
| | | h | 5.3, A.6.1.1, A.7.2.2, A.13.2.5p, A.18.2.2, A.18.2.3, A.18.4.1p |
| | | i | A.13.2.5p |
| | | j | 10.1, A.6.1.3, A.13.2.5p, A.15.3.1p, A.18.2.2, A.18.2.3, A.18.4.1p |
| | | k | 7.4, A.6.1.3, A.12.1.2, A.13.2.5p, A.15.2.2 |
| | | l | A.6.1.3, A.13.2.5p, A.15.3.1p |
| | | m | 7.4, A.6.1.3, A.13.2.5p, A.18.1.1 |
| | | n | A.7.2.2, A.9.1.1, A.13.2.5p |
| | 3 | - | A.13.2.5p, A.15.3.6p |
| 48 - Transferências ou divulgações não autorizadas pelo direito da União | - | - | A.13.2.1 |
| 49 - Derrogações para situações específicas | 1 | - | A.6.1.3, A.6.1.6p, A.13.2.1, A.15.3.5p, A.19.3.1p, B.1.6.8 |
| | | a | A.13.2.1, A.19.3.1p, B.1.1.1, B.1.1.3 |
| | | b | A.13.2.1, A.19.3.1p, B.1.2.1, B.1.2.2 |
| | | c | A.13.2.1, A.19.3.1p, B.1.2.1, B.1.2.2 |
| | | d | A.13.2.1, A.19.3.1p, B.1.5.1 |
| | | e | A.13.2.1, A.19.3.1p, B.1.3.2 |
| | | f | A.13.2.1, A.19.3.1p, B.1.4.1 |
| | | g | 7.4, A.13.2.1, A.19.3.1p, B.1.7.2 |
| | 2 | - | A.13.2.1, B.1.7.2 |
| | 6 | - | 7.5.3, 8.1, 8.2, A.19.3.1p |
| **Capítulo VI - Autoridades de controlo independentes** | | | |
| ***Secção 2 - Competência, atribuições e poderes*** | | | |
| 57 - Atribuições | 1 | d | A.6.1.3, A.7.2.2 |
| | | e | A.18.4.1p |
| | | f | A.18.4.1p |
| | | h | A.15.3.1p |
| | | i | A.14.1.5p |
| | | j | A.7.1.2, A.13.2.1, A.13.2.2, A.15.1.1, A.15.1.2 |
| | | k | 6.1.2 |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| | | l | A.15.3.4p |
| | | m | A.18.3.1p |
| | | n | A.18.3.2p |
| | | o | A.15.3.1p, A.18.3.2p |
| | | p | A.18.3.1p, A.18.3.2p |
| | | q | A.18.3.1p, A.18.3.2p |
| | | r | A.13.2.1, A.13.2.2, A.15.3.5p |
| | | s | A.13.2.5p, A.18.2.2, A.18.2.3 |
| | 2 | - | A.18.4.1p |
| 58 - Poderes | 1 | a | A.15.1.1, A.15.3.1p, A.18.4.2p |
| | | b | 10.1, A.15.1.1, A.15.3.1p, A.18.4.2p |
| | | c | A.15.3.1p, A.18.3.2p, A.18.4.2p |
| | | d | 10.1, A.15.3.1p, A.18.4.2p |
| | | e | A.9.1.1, A.15.1.1, A.15.3.1p, A.18.4.2p |
| | | f | A.9.1.1, A.11.1.2, A.15.3.1p, A.18.4.2p |
| | 2 | a | 10.1, A.15.3.1p, A.18.4.2p |
| | | b | 10.1, A.15.3.1p, A.18.4.2p |
| | | c | A.15.3.1p, A.18.4.2p, A.19.2.1p |
| | | d | 10.1, A.15.3.1p, A.18.4.2p |
| | | e | A.15.3.1p, A.16.2.3p, A.18.4.2p |
| | | f | A.15.3.1p, A.15.3.2p, A.18.4.2p |
| | | g | A.15.3.1p, A.15.3.2p, A.18.4.2p, A.19.2.4p, A.19.2.5p, A.19.3.3p |
| | | h | A.15.3.1p, A.18.3.2p, A.18.4.2p |
| | | i | A.15.3.1p, A.18.4.2p |
| | | j | A.15.3.1p, A.15.3.3p, A.18.4.2p |
| | 3 | a | A.15.3.4p, A.18.4.2p |
| | | b | A.18.1.1, A.18.4.2p |
| | | c | A.15.3.4p, A.18.4.2p |
| | | d | A.18.3.1p, A.18.4.2p |
| | | e | A.18.3.2p, A.18.4.2p |
| | | f | A.18.3.2p, A.18.4.2p |
| | | g | A.13.2.1, A.13.2.2, A.15.1.2, A.18.4.2p, A.19.2.3p |
| | | h | A.13.2.1, A.13.2.2, A.15.3.5p, A.15.3.6p, A.18.4.2p |
| | | i | A.13.2.1, A.13.2.2, A.15.3.5p, A.15.3.6p, A.18.4.2p |
| | | j | A.13.2.5p, A.15.3.6p, A.18.4.2p |
| | 4 | - | A.18.4.4p |
| | 5 | - | A.18.4.5p |
| | 6 | - | A.18.1.1 |
| **Capítulo VIII - Vias de recurso, responsabilidade e sanções** | | | |
| 77 - Direito de apresentar reclamação a uma autoridade de controlo | 1 | - | A.18.4.1p |
| 79 - Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante | 1 | - | A.18.4.5p |
| | 2 | - | A.18.4.5p |
| 80 - Representação dos titulares dos | 1 | - | A.18.4.1p, A.18.4.5p |

| ARTIGO DO GDPR | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| dados | 2 | - | A.18.4.1p, A.18.4.5p |
| 82 - Direito de indemnização e responsabilidade | 1 | - | A.18.4.5p |
| | 2 | - | A.15.1.2, A.15.1.3, A.18.4.5p, A.18.4.6p, A.18.4.7p |
| | 3 | - | A.15.1.2, A.15.1.3, A.18.4.5p, A.18.4.6p, A.18.4.7p |
| | 4 | - | A.15.1.2, A.15.1.3, A.18.4.5p, A.18.4.6p, A.18.4.7p |
| | 5 | - | A.15.1.2, A.15.1.3, A.18.4.5p, A.18.4.6p, A.18.4.7p |
| 83 - Condições gerais para a aplicação de coimas | 8 | - | A.18.4.4p |
| **Capítulo IX - Disposições relativas a situações específicas de tratamento** | | | |
| 85 - Tratamento e liberdade de expressão e de informação | 1 | - | A.18.1.1, B.1.7.1 |
| | 2 | - | A.18.1.1 |
| 86 - Tratamento e acesso do público aos documentos oficiais | - | - | 7.5.3, 8.1, 8.2, A.9.1.1, A.18.1.1, B.1.7.2 |
| 87 - Tratamento do número de identificação nacional | - | - | A.18.1.1 |
| 88 - Tratamento no contexto laboral | 1 | - | A.18.1.1, B.1.7.3, B.2.3.3 |
| | 2 | - | A.18.1.1, B.1.7.3 |
| 89 - Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos | 1 | - | A.8.1.5p, A.10.2.1p, A.14.3.1, A.18.1.1, B.1.7.4, B.1.7.5, B.1.7.6 |
| | 2 | - | A.18.1.1, B.1.7.5, B.1.7.6 |
| | 3 | - | A.18.1.1, B.1.7.4 |
| 90 - Obrigações de sigilo | 1 | - | A.7.1.2, A.9.1.1, A.13.2.4, A.15.3.1p, A.18.1.1 |

**Tabela 2-4** – Requisitos da Diretiva SRI aplicáveis ao setor da saúde em Portugal

| ARTIGO DA DIRETIVA SRI | PARÁG-RAFO | ALÍNEA | SGISIP |
|---|---|---|---|
| **Capítulo I – Disposições gerais** | | | |
| 1 - Objeto e âmbito de aplicação | 7 | - | 7.4, A.18.1.1 |
| 2 - Tratamento de dados pessoais | 1 | - | A.18.1.1 |
| 3 - Harmonização mínima | - | - | A.18.1.1 |
| 5 - Identificação dos operadores de serviços essenciais | 1 | - | A.18.1.1, B.3.1.x |
| | 2 | - | A.18.1.1, B.3.1.x |
| | 3 | - | A.18.1.1, B.3.1.x |
| | 5 | - | A.18.1.1, B.3.1.x |
| 6 - Efeito perturbador importante | 1 | - | A.18.1.1 |
| | 2 | - | A.18.1.1 |
| **Capítulo II – Quadros nacionais para a segurança das redes e dos sistemas de informação** | | | |
| 9 - Equipas de resposta a incidentes de segurança informática (CSIRT) | 1 | - | 4.2, A.18.1.1 |
| | 4 | - | A.18.1.1 |
| **Capítulo IV – Segurança das redes e dos sistemas de informação dos operadores de serviços essenciais** | | | |
| 14 - Requisitos de segurança e notificação de incidentes | 1 | - | 4.1, 4.3, 6.1.2, 6.1.3, 6.2, 7.3, 8.3, A.14.1.5p |
| | 2 | - | 4.1, 7.3, A.16.1.3, A.16.1.5, A.16.1.6, A.17.1.1, A.17.1.2, A.17.1.3, A.17.3.1p, A.17.3.2p |
| | 3 | - | 4.1, 7.3, 7.4, A.16.1.7, A.16.2.4p, A.17.1.1, A.17.1.2, A.17.1.3, A.17.3.1p, A.17.3.2p |
| | 4 | - | A.16.2.4p |
| | 7 | - | 7.4, A.16.2.4p, A.18.1.1 |
| 15 - Aplicação e execução | 1 | - | 4.1, A.15.3.1p |
| | 2 | a | 4.1, 7.5.1, 7.5.3, 8.1, 8.2, A.5.1.1, A.15.1.1, A.15.3.1p |
| | | b | 4.1, 7.5.1, A.15.1.1, A.15.3.1p, A.18.2.1, A.18.2.2, A.18.2.3 |
| | 3 | - | 7.5.1, 10.1, A.15.3.1p, A.18.2.1, A.18.2.2, A.18.2.3, A.18.4.2p |
| **Capítulo V - Segurança das redes e dos sistemas de informação dos prestadores de serviços digitais** | | | |
| 16 - Requisitos de segurança e notificação de incidentes | 5 | - | 4.3, 7.4, A.8.4.1p, A.15.1.2, A.15.1.3, A.16.2.4p, A.17.1.1, A.17.1.2, A.17.1.3, A.17.3.1p, A.17.3.2p, B.2.2.2 |
| **Capítulo VI – Normalização e notificação voluntárias** | | | |
| 19 - Normalização | 1 | - | A.18.1.1 |
| 20 - Notificação voluntária | 1 | - | 7.4, A.16.2.4p |
| | 2 | - | 7.4, A.16.2.4p |
| **Capítulo VII – Disposições finais** | | | |
| 25 - Transposição | 1 | - | A.18.1.1 |

## 2.4. MAPEAMENTO DOS REQUISITOS E CONTROLOS DO SGISIP COM OS REQUISITOS E RECOMENDAÇÕES DO GUIA DA SPMS.

NOTA: A atividade corresponde ao objetívo específico OBJ.03.

Finalmente, as recomendações e requisitos do Guia da SPMS (**Tabela 2-5** e **Tabela 2-6** respetivamente) foram mapeados com os requisitos e controlos do SGISIP definidos no âmbito da atividade anterior (parágrafo 2.3.2).

**Tabela 2-5** – Resumo das recomendações do Guia da SPMS dirigidas aos diferentes perfis dos profissionais do MS/SNS

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| **RECOMENDAÇÕES DIRIGIDAS AOS GESTORES HOSPITALARES** | | |
| **Equipa afeta à implementação do GDPR** | | |
| **RCM.GES.01a** | Alinhar a estratégia da Entidade com a estratégia global do sistema de informação da saúde bem como com o ENESIS 2020. | 4.1, 4.2, 5.1, A5.1.1 |
| **RCM.GES.01b** | Constituir uma equipa de projeto temporária responsável pelo acompanhamento e garantia da implementação dos requisitos do GDPR. A equipa deverá ser multidisciplinar, de forma a cobrir todas as variantes – desde logo, com elementos do departamento jurídico, do departamento de recursos humanos, da direção de compras, da área médica, e do TIC. Será essencial que o DPO (*Data Protection Officer*) integre, naturalmente, esta equipa e coordene os trabalhos de implementação do GDPR na Entidade. | 5.3, 7.1, 7.2, A6.1.1, A6.1.2 |
| **RCM.GES.01c** | Esta equipa deverá efetuar um levantamento do tratamento de dados existentes, identificando aspetos como, até à data, os dados estão a ser tratados, para que, posteriormente, se possam identificar as áreas que carecem de alteração de forma a assegurar o cumprimento do GDPR. | A6.1.1, A8.1.1, A19.3.1p |
| **RCM.GES.01d** | No final do projeto as responsabilidades pela monitorização das práticas e controlos relacionados deverão ser integradas nas estruturas transversais do eSIS e estruturas organizacionais da Instituição. | 5.3, 7.1, 7.2, 9.1, A6.1.1, A6.1.2, A15.2.1, A18.2.1, A18.2.2, A18.2.3 |
| **Governança** | | |
| **RCM.GES.02a** | Definir, em alinhamento com os modelos de governança e gestão do sistema de informação da saúde e do eSIS, a estrutura de governança da proteção de dados pessoais da Entidade e identificar um DPO (*Data Protection Officer*) que será responsável pelo acompanhamento dos temas de proteção de dados dentro de cada Entidade. | 5.3, 7.1, 7.2, A6.1.1, A6.1.2 |

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| **Consciencialização e sensibilização** | | |
| **RCM.GES.03a** | Garantir, através das ações da formação interna e sensibilização de todos os trabalhadores e colaboradores para os temas de proteção de dados pessoais, um conhecimento das regras e princípios que deverão ser seguidos na recolha e tratamento de dados pessoais e, consequentemente, assegurar o cumprimento dos requisitos decorrentes do GDPR. | 5.1, 7.3, 7.4, A6.1.1, A7.1.2, A7.2.1, A7.2.2 |
| **Políticas e condutas de códigos internos** | | |
| **RCM.GES.04a** | Definir as regras internas, veiculadas em políticas e códigos de conduta para assegurar a consciencialização de todos os colaboradores para os temas da privacidade e proteção de dados, bem como responsabilizá-los em caso de incumprimento. | 5.1, 7.3, 7.4, A6.1.1, A7.1.2, A7.2.1, A7.2.2, A7.2.3 |
| **Processos e procedimentos** | | |
| **RCM.GES.05a** | Adaptar e/ou criar processos e procedimentos internos que evidenciem o cumprimento das novas disposições legais. Desde logo, os processos e procedimentos internos devem especificar a necessidade de realização de avaliações de risco (PIA) pelo DPO, assim como a inclusão dos temas de proteção de dados em toda a cadeia de atividade da Entidade. O cumprimento destes requisitos deverá ser assegurado pelo DPO. | 5.1, 5.2, 5.3, 6.1.1, 6.1.2, 8.2, A5.1.1, A6.1.1 |
| **RCM.GES.05b** | Os processos deverão ainda incluir regras sobre a criação de ficheiros e bases próprias pelos colaboradores e prestadores de serviços, estipulando, nomeadamente, que não deverão ser criados ficheiros que repliquem a informação constante das bases de dados e aplicações em utilização na Entidade integrante do SNS. | A8.1.3 |
| **Relações com terceiros** | | |
| **RCM.GES.06a** | Assegurar que qualquer contratação de terceiros que, no âmbito da prestação de serviços, tenham acesso a dados pessoais da responsabilidade da Entidade, deverá ser precedida de uma análise das garantias de cumprimento da legislação de proteção de dados pessoais e da implementação de medidas de segurança por parte de tais terceiros. Os contratos a celebrar com estas entidades deverão, assim, incluir cláusulas específicas de proteção de dados que, desde logo, limitem o tratamento dos dados à execução do contrato e às instruções da Entidade. | A15.1.1, A15.1.2, A15.1.3, A15.1.4p |

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| **Estratégia de comunicação** | | |
| **RCM.GES.07a** | Definir, de antemão, uma estratégia de comunicação com as autoridades e os utentes em caso de um incidente de segurança e uma violação de dados pessoais. A comunicação deverá ser adaptada aos interlocutores e, naturalmente, às situações em causa – i.e. dependerá do tipo de incidente/violação, do número de registos afetados e da natureza dos dados em causa. Toda a comunicação externa, nomeadamente de incidentes de segurança e privacidade, deverá ser realizada de acordo com os procedimentos em vigor no sistema de informação da saúde. | A6.1.3, A6.1.4, A6.1.6p, A16.1.1, A16.1.5, A16.2.1p, A16.2.2p, A16.2.3p, A16.2.4p, A16.2.5p, A16.2.6p, A16.2.7p |
| **RECOMENDAÇÕES DIRIGIDAS AOS PROFISSIONAIS DE SAÙDE** | | |
| **Recolha de consentimento e prestação de informação** | | |
| **RCM.PSD.01a** | Observar, no momento da recolha de dados pessoais, o princípio da minimização – i.e. assegurar-se que apenas são recolhidos os dados pessoais que são estritamente necessários para o ato em questão, bem como garantir a prestação de informação acerca dos termos em que os dados pessoais irão ser utilizados, incluindo os elementos constantes nos artigos 13 e 14 do GDPR. | A19.1.1p, A19.1.2p |
| **RCM.PSD.01b** | Obter o consentimento para o tratamento dos dados, exceto nas situações previstas no GDPR (nomeadamente, para proteção de interesses vitais do titular). No caso de menores, o consentimento deverá ser prestado pelos titulares das responsabilidades parentais do menor. Idealmente, deve ser obtido um consentimento escrito e armazenada evidência de tal documento. Caso não seja possível, o profissional deverá registar no registo clínico do utente que recolheu o seu consentimento e prestou informação, incluindo a data em que o fez. | B1.1.1, B1.1.2, B1.1.3, B1.4.1, B2.1.1 |
| **Acesso aos sistemas de informação / plataformas** | | |
| **RCM.PSD.02a** | Garantir o acesso reservado aos sistemas de informação e plataformas nos quais são registados dados de saúde dos utentes, bem como abster-se de duplicar as bases de dados da responsabilidade da Entidade integrante do SNS, criando, por exemplo, ficheiros próprios com a informação da base de dados/aplicação a que acede. | A8.1.3, A9.1.1, A9.1.2, A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6, A9.3.1, A9.4.1, A9.4.2, A9.4.3, A9.4.4, A9.4.5, A14.1.1, A14.2.5 |

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| **Registo de acesso à informação clínica** | | |
| **RCM.PSD.03a** | O registo da informação clínica dos utentes deve ser efetuado, diretamente, pelo profissional da área de saúde. Apenas devem ser recolhidos e, consequentemente, registados os dados estritamente necessários para assegurar a prestação de cuidados médicos. O registo deve ser efetuado nas aplicações e sistemas aprovados no contexto do eSIS, não devendo, assim, ser registados quaisquer dados em dispositivos ou equipamentos da propriedade do profissional e/ou não aprovados. | A8.4.1p, A8.4.2p, A14.1.1, A14.2.5, A18.1.3, A19.1.1p, A19.1.2p, A19.3.1p, B1.2.1, B1.2.2, B1.3.1, B1.3.2, B1.4.1, B1.5.1, B1.5.2, B1.6.1, B1.6.2, B1.6.3, B1.6.4, B1.6.5, B1.6.6, B1.6.7, B1.6.8, B1.7.1, B1.7.2, B1.7.3, B1.7.4, B1.7.5, B1.7.6, B2.1.1, B2.2.1, B2.2.2, B2.3.1, B2.3.2, B2.3.3, B2.3.4, B2.3.5 |
| **RCM.PSD.03b** | O profissional de saúde deverá apenas aceder à informação clínica do utente, constante do Resumo Clinico Único ou outro, na medida em que tal seja necessário para a prossecução das suas funções. | A7.1.2, A8.1.3, A8.4.1p, A8.4.2p, A9.1.1, A9.1.2, A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6, A9.3.1, A9.4.1, A9.4.2, A9.4.3, A9.4.4, A9.4.5, A14.1.1, A14.2.5, B2.2.2 |
| **Partilha da informação clínica** | | |
| **RCM.PSD.04a** | A informação clínica não deve ser partilhada com terceiros, exceto para assegurar a continuidade da prestação de cuidados de saúde. Nessa situação, o profissional deve garantir que a partilha é efetuada, de forma segura e confidencial, a outro profissional sujeito à obrigação de confidencialidade e sigilo e que se tem todos os cuidados com esta partilha de informação. | A7.1.2, A8.1.3, A8.2.3, A8.4.1p, A8.4.2p, A13.2.1, A13.2.2, A13.2.3, A13.2.4, A15.1.1, A15.1.2, A15.1.3, A15.3.1p |
| **Transporte da informação clínica** | | |
| **RCM.PSD.05a** | Abster-se de, de alguma forma, transportar informação clínica constante do Resumo Clínico Único ou outro, para fora do serviço e do hospital ou centro de saúde, exceto nos casos autorizados pelos responsáveis da Instituição e para efeitos de garantia da continuidade da prestação de cuidados médios. Sempre que tal suceda, deverão ser adotadas medidas de segurança especiais, de forma a assegurar que a informação não é acedida por terceiros de forma indevida (em particular, a informação deverá ser anonimizada e/ou encriptada). | A6.1.1, A6.1.2, A6.2.1, A6.2.2, A7.1.2, A8.1.3, A8.2.3, A8.3.1, A8.3.3, A10.2.1p |

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| **Utilização de dispositivos pessoais** | | |
| **RCM.PSD.06a** | Não utilizar ou, de alguma forma, ligar dispositivos pessoais aos sistemas e plataformas da Instituição do SNS, exceto nos casos em que exista aprovação prévia dos responsáveis da Instituição. Caso tal suceda, e atenta à natureza da informação, o profissional deve ter em consideração que o acesso à rede através de dispositivos móveis pessoais acarreta riscos de segurança e confidencialidade, pelo que deve adotar as medidas de segurança necessárias para proteger os dados a que aceda, através do seu dispositivo, contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer outra forma de tratamento ilícito dos mesmos. | A6.1.1, A6.1.2, A6.2.1, A7.1.2, A8.1.3, A8.2.3, A8.3.1, A9.1.1, A9.1.2, A9.4.1 |
| **RCM.PSD.06b** | Deve ainda, em qualquer situação, manter a informação confidencial em regime de sigilo e estrita confidencialidade, não permitindo o acesso a terceiros. | A7.1.2, A8.1.3, A8.2.1, A8.2.3 |
| **Utilização dos dados para finalidades próprias** | | |
| **RCM.PSD.07a** | O profissional da área da saúde não pode tratar os dados recolhidos no âmbito da prestação de cuidados de saúde para finalidades próprias. Caso pretenda utilizar os dados para fins académicos ou de investigação, deverá obter a aprovação dos responsáveis da Instituição do SNS, devendo recolher o consentimento do utente para o efeito, prestando-lhe a informação necessária acerca dos termos em que os dados irão ser utilizados. Nesta situação, o profissional será considerado responsável pelo tratamento dos dados. | A6.1.1, A6.1.2, A6.1.6p, A7.1.2, A8.1.2, A8.1.3, B1.1.1, B1.1.2, B1.1.3, B1.7.1, B1.7.5, B2.3.3, B2.3.4 |
| **Comunicação de violações de dados pessoais** | | |
| **RCM.PSD.08a** | Comunicar de imediato ao DPO (*Data Protection Officer*) qualquer falha ou incidente que envolva dados pessoais de acordo com os procedimentos estabelecidos para o efeito. Na medida em que tenham informação acerca do incidente, deverão disponibilizá-la aquando da comunicação. Em particular, deverão comunicar a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa. | A6.1.1, A16.1.2, A16.1.3 |

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| | | |
| **RECOMENDAÇÕES DIRIGIDAS AOS PROFISSIONAIS TIC** | | |
| **Mapeamento dos sistemas e aplicações em utilização** | | |
| **RCM.TIC.01a** | Efetuado um levantamento de todos os sistemas e aplicações nas quais sejam registados dados pessoais, com identificação das respetivas funcionalidades, níveis de acesso e medidas de segurança implementadas. | A7.1.2, A8.1.3, A8.2.1, A8.2.3 |
| **Verificação das ferramentas de rastreabilidade** | | |
| **RCM.TIC.02a** | Verificar se existem ferramentas que permitam a rastreabilidade de acesso, inserção, alteração e eliminação de dados (*logs*) e, em caso afirmativo, se tal ferramenta se encontra implementada para todos os sistemas e/ou aplicações. | A6.1.1, A6.1.2, A6.1.6p, A7.1.2, A8.1.2, A8.1.3, B1.1.1, B1.1.2, B1.1.3, B1.7.1, B1.7.5, B2.3.3, B2.3.4 |
| **Avaliação de risco e vulnerabilidade** | | |
| **RCM.TIC.03a** | Realizar as avaliações de risco (PIA), testes de penetração e simulação de ataques por forma a avaliar se os sistemas e/ou aplicações são robustos e, consequentemente, são adequados a assegurar o cumprimento das novas obrigações decorrentes do GDPR e Diretiva SRI. | 6.1.1, 6.1.2, 8.2, A12.7.1, A14.2.3, A18.2.1, A18.2.2, A18.2.3, B3.1.1 |
| **Adaptação dos sistemas ao GDPR** | | |
| **RCM.TIC.04a** | Assegurar que os sistemas e aplicações permitem, desde logo, a Portabilidade dos dados. | A8.4.1p, A8.4.2p, A14.1.1, A14.1.4p, A19.2.6p |
| **RCM.TIC.04b** | Assegurar que os sistemas e aplicações permitem, desde logo, a Interoperabilidade. | A8.4.1p, A8.4.2p, A14.1.1, A14.1.4p, A19.2.6p |
| **RCM.TIC.04c** | Assegurar que os sistemas e aplicações permitem, desde logo, a Anonimização, pseudonimização e encriptação. | A8.4.1p, A8.4.2p, A10.1.1, A10.1.2, A10.2.1p, A14.1.1, A14.1.4p |
| **RCM.TIC.04d** | Assegurar que os sistemas e aplicações permitem, desde logo, a Segurança dos dados. | A8.4.1p, A8.4.2p, A14.1.1, A14.1.4p |
| **RCM.TIC.04e** | Assegurar que os sistemas e aplicações permitem, desde logo, o Acesso, retificação e apagamento dos dados. | A8.4.1p, A8.4.2p, A9.1.1, A9.1.2, A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6, A9.3.1, A9.4.1, A9.4.2, A9.4.3, A9.4.4, A9.4.5, A14.1.1, A14.1.4p, A19.2.1p, A19.2.2p, A19.2.3p, A19.2.4p A19.2.5p |
| **RCM.TIC.04f** | Assegurar que os sistemas e aplicações permitem, desde logo, os Sistemas de alerta em caso de incidente de segurança. | A8.4.1p, A8.4.2p, A14.1.1, A14.1.4p, A16.1.2, A16.1.4 |
| **RCM.TIC.04g** | Assegurar que os sistemas e aplicações permitem, desde logo, o Registo de operações de tratamento. | A8.4.1p, A8.4.2p, A14.1.1, A14.1.4p, A18.1.3, A19.3.1p |

| ID RECOMEN-DAÇÃO | RECOMENDAÇÃO | Requisitos e Controlos do SGISIP |
|---|---|---|
| **RCM.TIC.04h** | Assegurar que os sistemas e aplicações permitem, desde logo, as Auditorias. | 9.1, 9.2, 9.3, A8.4.1p, A8.4.2p, A14.1.1, A14.1.4p, A18.2.1, A18.2.2, A18.2.3, A18.2.4p |
| **RCM.TIC.04i** | Assegurar que os sistemas e aplicações permitem, desde logo, a Rastreabilidade dos dados comunicados a terceiros. | A8.4.1p, A8.4.2p, A13.2.1, A13.2.2, A13.2.3, A14.1.1, A14.1.4p, A15.1.1, A15.1.2, A15.1.3, A18.1.3, A19.3.1p |
| **RCM.TIC.04j** | Assegurar que os sistemas e aplicações permitem, desde logo, o Controlo de acessos. | A8.4.1p, A8.4.2p, A9.1.1, A9.1.2, A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6, A9.3.1, A9.4.1, A9.4.2, A9.4.3, A9.4.4, A9.4.5, A14.1.1, A14.1.4p, A19.2.2p |
| **Controlo de qualidade e melhoria contínua** | | |
| **RCM.TIC.05a** | Dar especial enfoque à segurança da informação no âmbito dos processos internos de garantia de qualidade e melhoria contínua. | 10.1, 10.2, A18.1.1, A18.1.2, A18.1.3, A18.1.4, A18.1.5, A18.2.1, A18.2.2, A18.2.3, A18.2.4p, A18.3.1p, A18.3.2p, A18.4.1p, A18.4.3p, A18.4.5p |
| **Partilha de informação de segurança** | | |
| **RCM.TIC.06a** | Partilhar, para criar maior *awareness*, a informação e dicas de segurança da informação por todos os intervenientes no ciclo de vida do tratamento de dados pessoais, ou de uma forma mais alargada por todas as Entidades integrantes do eSIS. | 5.1, 7.3, 7.4, A6.1.3, A6.1.4 |
| **Mecanismos de alerta** | | |
| **RCM.TIC.07a** | Implementar os sistemas e aplicações, de forma a serem gerados alertas em caso de vulnerabilidade e/ou ocorrência de violações de segurança. Estes mecanismos permitirão, aos responsáveis pelos sistemas de informação, identificar o incidente e por em prática as medidas necessárias de forma a minimizar os riscos para a privacidade. | A8.4.1p, A8.4.2p, A12.6.1, A14.1.1, A14.1.4p, A14.1.5p, A16.1.2, A16.1.4 |

**Tabela 2-6** – Requisitos do Guia da SPMS para auto-avaliação preliminar do nível de adequação e cumprimento das regras do GDPR

| ID REQUISITO | PERGUNTA | Requisitos e Controlos do SGISIP |
|---|---|---|
| **ESTRATÉGIA** | | |
| REQ.EST.01 | A comunicação sobre os requisitos de responsabilidade para a conformidade com o GDPR foi divulgada a todo a Instituição? | 5.1, 6.2, 7.3, 7.4, A7.2.2, A18.1.1 |
| REQ.EST.02 | As melhores práticas de proteção de dados foram documentadas e divulgadas a toda a Instituição? | 7.4, 7.5.1, 7.5.2, 7.5.3 A18.3.1p, A18.3.2p |
| REQ.EST.03 | A Instituição já documentou todos os riscos associados ao processamento de dados pessoais que formam a base para as auditorias? | 6.1.1, 6.1.2, 8.2 |
| REQ.EST.04 | A Gestão da Instituição está a par dos níveis detalhados de multas e infrações do GDPR? | 5.1, 6.2, 7.3, 7.4 A18.1.1 |
| REQ.EST.05 | A Gestão da Instituição conhece e entende as hipóteses de ações judiciais coletivas e potencial suspensão de atividades de processamento de dados por incumprimento continuado? | 5.1, 6.2, 7.3, 7.4 A18.1.1, A18.4.1p, A18.4.5p |
| **DADOS** | | |
| REQ.DAD.01 | Há um processo padrão para mapear e classificar os dados pessoais de forma consistente em todo a Instituição? | A8.1.1, A8.1.5p, A8.2.1 |
| REQ.DAD.02 | Foi realizada uma análise para documentar a utilização e o fluxo de dados pessoais na Instituição. Esta documentação serve de base para a monitorização das atividades de processamento? | 9.1, A19.3.1p |
| REQ.DAD.03 | É comunicado de forma clara e transparente aos titulares dos dados que é feita a recolha dos seus dados pessoais? | A19.1.1p, A19.1.2p |
| REQ.DAD.04 | Há na Instituição um controlo que relaciona os dados recolhidos à finalidade de processamento, e que permite a correta utilização e eliminação de dados? | A19.3.1p, A19.3.2p, A19.3.3p |
| REQ.DAD.05 | Existe um processo definido para a revisão de dados, em cada registo, quando esses dados são processados? | A19.3.1p |
| REQ.DAD.06 | Há na Instituição um processo, mesmo que manual, para rever a utilidade | A19.3.1p, A19.3.2p, A19.3.3p |
| REQ.DAD.07 | Há na Instituição um plano de continuidade hospitalar (incluindo pessoas, processos e tecnologias), implementado e testado? | A17.3.1p, A17.3.2p |
| REQ.DAD.08 | Há na Instituição um processo que identifica os dados que podem ser removidos e que posteriormente envolve equipas individuais para remoção? | A19.3.3p |
| REQ.DAD.09 | Em caso de armazenamento de dados na cloud, há a definição clara dos termos do contrato que permitem escolher a localização dos dados e a realização de auditorias? | A8.4.1p, A15.1.2 |

| ID REQUISITO | PERGUNTA | Requisitos e Controlos do SGISIP |
|---|---|---|
| **PESSOAS** | | |
| REQ.PES.01 | A Instituição comunica a gestão de dados pessoais à autoridade supervisora nacional (CNPD), mesmo que não esteja estabelecida formalmente uma organização de governança ou de procedimentos para este efeito? | 6.1.3, A6.1.3, A15.3.4p, A15.3.5p, A15.3.6p |
| REQ.PES.02 | A Instituição já nomeou, mesmo que a tempo parcial, um Responsável de Proteção de Dados? | 5.3, A6.1.1, A6.1.2 |
| **PROCESSOS** | | |
| REQ.PRO.01 | A Instituição tem implementada um processo de resposta em caso de incidente de violação de dados pessoais, mesmo que não esteja testado? | A16.1.1, A16.1.5 |
| REQ.PRO.02 | A Instituição tem implementado um processo de comunicação aos titulares dos dados e parceiros externos em caso de incidente de violação de dados pessoais, mesmo que não esteja testado? | A16.2.1p, A16.2.2p, A16.2.3p |
| REQ.PRO.03 | A Instituição opera de acordo com os princípios e práticas gerais de boas práticas de segurança da informação (ex. ISO 27001), mesmo que não tenha uma certificação? | 4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.3, 6.1.1, 6.1.2, 6.1.3, 6.2, 7.1, 7.2, 7.3, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 8.2, 8.3, 9.1, 9.2, 9.3, 10.1, 10.2 |
| REQ.PRO.04 | A Instituição já iniciou a revisão dos contratos com os fornecedores externos que processam dados pessoais? | A7.1.2, A15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2 |
| REQ.PRO.05 | Há na Instituição processos de consentimento que integram especificação, tais como: autorização de uso; duração de consentimento; e consentimento dado de livre vontade? | B1.1.1, B1.1.2, B1.1.3, A19.3.2p, A19.3.3p |
| REQ.PRO.06 | Existe na Instituição um processo de verificação de idade e obtenção de consentimento parental? | B1.1.3, B2.1.1 |
| REQ.PRO.07 | Existem requisitos de segurança definidos e documentados que se aplicam a departamentos/processos específicos, como os RH, TI e marketing, mesmo que não seja testado regularmente? | A14.1.4p, B1.1.1, B1.1.2, B1.1.3, B1.2.1, B1.2.2, B1.3.1, B1.3.2, B1.4.1, B1.5.1, B1.5.2, B1.6.1, B1.6.2, B1.6.3, B1.6.4, B1.6.5, B1.6.6, B1.6.7, B1.6.8, B1.7.1, B1.7.2, B1.7.3, B1.7.4, B1.7.5, B1.7.6 |
| **TECNOLOGIAS** | | |
| REQ.TEQ.01 | A Instituição tem capacidade de controlo dos sistemas para detetar todas as violações de dados pessoais num prazo de 72 horas e para implementar imediatamente medidas para reportar a violação? | A14.1.1, A16.1.2, A16.1.3, A16.1.4, A16.2.1p, A16.2.2p, A16.2.3p |
| REQ.TEQ.02 | A Instituição tem um processo automatizado para identificação dos dados a retificar ou as objeções ao processamento solicitadas pelos detentores dos dados? | A14.1.1, A19.2.1p, A19.2.3p, A19.2.4p, A19.2.5p |
| REQ.TEQ.03 | A Instituição tem no sistema de informação, mesmo que não seja uma solução específica, funcionalidades que permitam a implementação do direito à eliminação? | A14.1.1, A15.3.2p, A19.2.4p, A19.3.3p |

| ID REQUISITO | PERGUNTA | Requisitos e Controlos do SGISIP |
|---|---|---|
| REQ.TEQ.04 | Há na Instituição um processo implementado, mesmo que manual, para efetuar a portabilidade de dados pessoais? | A14.1.1, A14.1.4p, A19.2.6p |
| REQ.TEQ.05 | Os sistemas de informação da Instituição permitem a pseudonimização dos dados pessoais através da sua anonimização e/ou tokenização? | A10.2.1p, A14.1.1 |
| REQ.TEQ.06 | O sistema de informação da Instituição permite garantir um processo padronizado para codificação dos dados pessoais? | A10.1.1, A10.1.2, A14.1.1 |
| REQ.TEQ.07 | A Instituição tem um sistema de single sign-on que permite a otimização do controlo de acesso em todo a Instituição e a monitorização contínua da conformidade? | A9.1.1, A9.2.5, A9.2.6, A14.1.1 |
| REQ.TEQ.08 | A Instituição tem sistemas que registam o consentimento, mas não de forma centralizada? | A14.1.1, B1.1.1, B1.1.2, B1.1.3 |

## 2.5. ENTREGÁVEIS DO PROJETO

A tabela **Tabela 2-7** resume a estrutura do projeto, representando a ligação entre os conteúdos desenvolvidos (entregáveis) necessários para cumprir os objetivos específicos estabelecidos no parágrafo 2.2.

**Tabela 2-7** – Entregáveis do projeto.

| ENTREGÁVEL | | OBJETIVO ESPECÍFICO | REFERÊNCIA DO PROJETO |
|---|---|---|---|
| **Figura 2-1** | – *Mindmap* do Sistema de Gestão Integrada de Segurança da Informação e Privacidade | **OBJ.02** | **Parágrafo 2.3.2** |
| **Tabela 2-3** | – Requisitos do GDPR aplicáveis ao setor da saúde em Portugal | **OBJ.01** | **Parágrafo 2.3.2.4** |
| **Tabela 2-4** | – Requisitos da Diretiva SRI aplicáveis ao setor da saúde em Portugal | **OBJ.01** | **Parágrafo 2.3.2.4** |
| **Tabela 2-5** | – Resumo das recomendações do Guia da SPMS dirigidas aos diferentes perfis dos profissionais do MS/SNS | **OBJ.02** | **Parágrafo 2.4** |
| **Tabela 2-6** | – Requisitos do Guia da SPMS para auto-avaliação preliminar do nível de adequação e cumprimento das regras do GDPR | **OBJ.02** | **Parágrafo 2.4** |
| **ANEXO A** | SISTEMA DE GESTÃO INTEGRADA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE | **OBJ.02 OBJ.03** | **Parágrafo 2.3.2.1** |
| **ANEXO B** | CONTROLOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE | **OBJ.02 OBJ.03** | **Parágrafo 2.3.2.2** |
| **ANEXO C** | ÂMBITO DO SISTEMA DE GESTÃO INTEGRADA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE | **OBJ.02 OBJ.03** | **Parágrafo 2.3.2.3** |

# 3. CONCLUSÕES

O presente projeto foi desenvolvido com o intuito de contribuir para o processo geral de preparação à aplicação do GDPR (General Data Protection Regulation) do ponto de vista operacional junto das entidades do setor da Saúde em Portugal.

Partindo do alinhamento entre os requisitos do GDPR e controlos do Anexo A da norma ISO/IEC 27001:2013, proposto pela ENISA (ENISA, 2016) e CID (Mortensen, 2016), no âmbito do projeto foi desenvolvida uma *framework* geral para o **Sistema de Gestão Integrada de Segurança da Informação e Privacidade (SGISIP)** nas entidades do MS/SNS, alinhada com os requisitos e controlos da norma ISO/IEC 27001:2013 e com os requisitos do GDPR e da Diretiva SRI (Segurança das Redes e Informações). Adicionalmente, os requisitos e controlos do SGISIP foram mapeados com os requisitos e recomendações do Guia da SPMS a fim de indicar às instituições abrangidas no âmbito da estratégia ENESIS as medidas técnicas e organizativas cuja implementação contribuirá para a adoção do Guia exigida pelo Despacho n.º 3156/2017.

A *framework* desenvolvida é aplicável a todas as organizações do setor da saúde, independentemente da sua natureza, dimensão ou tipologia. As três dimensões da *framework* são detalhadas nos respetivos anexos ao presente documento, nomeadamente:

- **Requisitos do SGISIP** (ANEXO A do presente documento) - Os necessários para estabelecer, implementar, manter e melhorar de forma contínua um Sistema de Gestão Integrada de Segurança da Informação e Privacidade. Estes requisitos correspondem aos requisitos do corpo principal da norma ISO/IEC 27001:2013 e devem ser devidamente atualizados tendo em consideração os respetivos requisitos do GDPR e da Diretiva SRI. Para efeitos de comprovação da conformidade com o GDPR é crucial a implementação do **SGISIP** com especial enfoque nos requisitos relativos ao 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.

- **A – Controlos de Segurança da Informação e Privacidade** (ANEXO B do presente documento) - Lista abrangente de objetivos de controlo e controlos que devem ser usados no contexto do Tratamento do Risco de Segurança da Informação e Privacidade (sub-cláusula 6.1.3 dos Requisitos do SGISIP). Os controlos de segurança da informação (Anexo A da norma ISO/IEC 27001:2013) foram 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;

- **B – Âmbito do SGISIP** que pode ser definido utilizando a lista dos controlos apresentados no ANEXO C do presente documento. Todos os controlos deste anexo são novos e foram introduzidos para conduzir as unidades clínicas e operacionais das entidades do MS/SNS no processo da implementação do SGISIP, garantindo a licitude de tratamento de acordo com os requisitos do GDPR, bem como o cumprimento dos requisitos da Diretiva SRI para os prestadores dos serviços essenciais.

Assim, ao contrário do alinhamento simples entre os requisitos do GDPR e controlos do Anexo A da norma ISO/IEC 27001:2013, a abordagem proposta não é limitada apenas pelo campo de implementação de controlos mas, adicionalmente, prevê mecanismos que permitem definir o âmbito da implementação dos controlos, bem como sustentar e melhorar os controlos implementados e ajudar as organizações a cumprir **ininterruptamente** com as 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 GDPR.

## 3.1. APLICAÇÃO IMEDIATA

A aplicabilidade dos resultados deste projeto com o atual grau de aprofundamento permite:

1) Verificação simultânea do cumprimento dos requisitos do GDPR, da Diretiva SRI e do Guia da SPMS recorrendo aos ANEXOS A, B e C do presente documento como *check-list*;

2) Identificação das principais áreas de tratamento dos dados pessoais na organização utilizando o ANEXO C do presente documento (Âmbito do SGISIP), e não só como *check-list* mas também no delinear do âmbito do SGISIP a implementar na organização ou, sendo o caso, no alargamento do âmbito do Sistema de Gestão de Segurança da Informação (SGSI) implementado na organização em conformidade com a norma ISO/IEC 27001:2013;

3) Implementação do SGISIP ou atualização do SGSI de acordo com os requisitos do sistema de gestão consolidados no ANEXO A do presente documento, bem como com os requisitos relevantes do GDPR, da Diretiva SRI e do Guia da SPMS identificados para cada requisito do SGISIP;

4) Implementação ou atualização dos controlos de segurança da informação e privacidade, necessários para cumprir com os requisitos do GDPR, da Diretiva SRI e do Guia da SPMS, utilizando como referência o mapeamento apresentado no ANEXO B do presente documento (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 GDPR da Confederação da Indústria Dinamarquesa (Mortensen, 2016).

5) Implementação ou atualização dos processos de negócio e práticas de tratamento dos dados pessoais de acordo com os requisitos do GDPR, da Diretiva SRI e do Guia da SPMS, utilizando como referência o mapeamento apresentado no ANEXO C do presente documento (Âmbito do SGISIP).

## 3.2. PRÓXIMOS PASSOS

No entanto, considerando que para a maioria das empresas afetadas pela aplicação do GDPR o desafio não é apenas saber o que há a fazer, mas também como devem fazê-lo de forma adequada ao seu contexto empresarial (ENISA, 2015, p. 19), é crucial complementar o SGISIP com ***guidelines* de implementação** detalhados, por forma a garantir:

- Adoção atempada pelas Entidades do MS/SNS das novas regras no âmbito de proteção de dados estabelecidas pelo GDPR;
- Sustentabilidade e melhoria contínua dos controlos estabelecidos e do SGISIP em geral.

Este desafio ganha ainda maior relevância tendo em consideração o grau de complexidade do sistema a implementar face à escassez de recursos e competências ao nível de segurança da informação e proteção de dados para a sua implementação adequada nas Entidades do MS/SNS.

Neste sentido, para dar continuidade ao projeto, os seus resultados podem servir como *input* para projetos posteriores no âmbito da gestão de segurança da informação e privacidade. Para garantir o sucesso da implementação do SGISIP consideramos importante que estes projetos alcancem na próxima fase os seguintes objetivos específicos:

**OBJ.04** – Definir os métodos de avaliação necessários para medir o desempenho e o sucesso:

a) Método de avaliação da maturidade do SGISIP;

b) Método de avaliação da eficácia e eficiência do Programa da implementação do SGISIP.

**OBJ.05** – Definir o *Roadmap* para o Programa da implementação do SGISIP, tendo em conta a especificidade do setor da saúde em Portugal:

a) identificando um conjunto de passos, com especial ênfase nas fases iniciais do processo;

b) determinando os critérios de seleção das medidas de melhoria contínua a implementar;

c) incluindo as recomendações para definição do plano da gestão de mudança.

**OBJ.06** – 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 na organização, bem como para garantir a máxima integração possível dos processos e procedimentos, bem como a minimização dos recursos necessários para operacionalização conjunta das diferentes *frameworks*.

**OBJ.07** – Fazer levantamento da legislação nacional e recomendações internacionais no âmbito de segurança da informação, privacidade e proteção de dados aplicável ao setor da saúde em Portugal, por forma a garantir a adaptação dos controlos do SGISIP à realidade nacional.

# 4. BIBLIOGRAFIA


APDSI – Associação para a promoção e desenvolvimento da Sociedade da Informação. (2016, 27 de outubro). *APDSI co-organiza a conferência "Novo Regulamento de Proteçao de Dados – Preocupações, desafios e oportunidades para as empresas*. Retirado de http://www.apdsi.pt/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=1029&cntnt01returnid=122

Business Analytics Portugal. (2017). *GDPR: o actual quadro jurídico nacional não está a ser cumprido!* Retirado de http://businessanalytics.pt/gdpr-actual-quadro-juridico-nacional-nao-esta-cumprido/

BSI Group. (Sem data). ISO/IEC 27001 Mapping guide. Retirado de https://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf

Despacho n.º 913-A/2017 do Gabinete do Secretário de Estado da Saúde. Retirado de https://dre.pt/home/-/dre/105780413/details/maximized?serie=II&dreId=105780411

Despacho n.º 3156/2017 do Gabinete do Ministro. Retirado de https://dre.pt/application/file/a/106881682

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

ENISA – European Union Agency for Network and Information Security (2012). Shortlisting network and information security standards and good practices. Retirado de https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

Estratégia para o mercado único digital na europa (2015). A comunicação da comissão ao parlamento europeu, ao comité, ao conselho económico e social europeu e ao comité das regiões. Retirado de http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=PT

Hintzbergen, J., Hintzbergen, K., Smulders, A., Baars, H. (2015). Foundations of information security based on ISO 27001 e ISO 27002.

IBM X-Force® Research (2016). 2016 Cyber Security Intelligence Index. Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Retirado de https://www.autoindustrylawblog.com/wp-content/uploads/sites/8/2016/05/IBM_2016-cyber-security-intelligence-index.pdf.

IBM X-Force® Research (2015). 2015 Managed Security Services Report. Security trends in the healthcare industry. Retirado de http://www.as.techdata.eu/be/_media/uploaded_files/0622175333-ibm_security_healthcare_x-force.pdf

ISACA Germany Chapter (2017). Implementation Guideline ISO/IEC 27001:2013. Retirado de https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf

ISCSP – Instituto Superior de Ciências Sociais e Políticas (2015). Relatório final Think tank "eHealth em Portugal: Visão 2020". Retirado de http://spms.min-saude.pt/2015/11/disponivel-aqui-relatorio-do-think-tank-ehealth-em-portugal-visao-2020/

ISO/IEC 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retirado de http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Marques Lopes, S. D. (2016). Privacidade dos dados em ambientes de interoperabilidade – a área da saúde. Tese apresentada à Universidade de Évora para obtenção do Grau de Doutor em Gestão. Retirado de https://dspace.uevora.pt/rdpc/bitstream/10174/18165/11/Privacidade%20dos%20dados%20em%20ambientes%20de%20interoperabilidade%20Documento%20Final%20-%20vFinal.pdf

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

Programa do XXI Governo Constitucional 2015-2019 (2015). Retirado de http://www.portugal.gov.pt/media/18268168/programa-do-xxi-governo.pdf

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

Resolução do Conselho de Ministros n.º 62/2016. Retirado de https://dre.pt/web/guest/pesquisa/-/search/75542124/details/maximized

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. (2016). *SPMS promove reunião sobre Estratégia TIC 2020 do Ministério da Saúde*. Retirado de http://spms.min-saude.pt/2016/07/spms-promove-reuniao-estrategia-tic-2020-do-ministerio-da-saude/

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. (Sem data). *Segurança e privacidade no Setor da Saúde. Objetivos.* Retirado 16-07-2017 de http://spms.min-saude.pt/objectivos/

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. (2017). Guia de Privacidade da Informação do Setor da Saúde em Portugal. Retirado 16-07-2017 de http://spms.min-saude.pt/guia-rgpd/

Symantec™ (2016). Industry Focus: Medical Device Security. Retirado de https://www.symantec.com/content/dam/symantec/docs/data-sheets/symc-med-device-security-en.pdf

Toreon. (Sem data). *Security frameworks & standards.* Retirado 20-07-2017 de https://www.toreon.com/security-frameworks-standards/

U.S. Department of health and human services. (Sem data). Agency for Healthcare Research and Quality. Privacy and Security Solutions for Interoperable Health Information Exchange. Privacy and Security Assessment of Variation Toolkit - Appendix D: IT Privacy and Security Primer. Retirado de https://healthit.ahrq.gov/sites/default/files/docs/page/D_ITPrivacyandSecurityPrimer_0.pdf

Zaletel, M., Kralj, M. (2015). Methodological guidelines and recommendations for efficient and rational governance of patient registries. National Institute of Public Health, Slovenia (2015). Retirado de https://ec.europa.eu/health/sites/health/files/ehealth/docs/patient_registries_guidelines_en.pdf

# ANEXO A. SISTEMA DE GESTÃO INTEGRADA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Na tabela abaixo são utilizados os seguintes termos:

***Requisito atualizado (RA)*** - O texto do requisito da norma ISO/IEC 27001:2013 merece-nos uma atualização a fim de abranger, para alem da vertente de Segurança da informação, a dimensão de Privacidade e Proteção de Dados dentro da organização, sendo aplicável ao nível empresarial também;

***Requisito sem alterações (RSA)*** – O requisito da norma ISO/IEC 27001:2013 mantem o texto original.

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **4 – CONTEXTO DA ORGANIZAÇÃO** | | | | | |
| **4.1** | **COMPREENDER A ORGANIZAÇÃO E O SEU CONTEXTO** | ***Requisito atualizado (RA)*** | 32.1, 35.1, 47.2a, 47.2b, 47.2c, 47.2d, 47.2e | 14.1, 14.2, 14.3, 15.1, 15.2a, 15.2b | RCM.GES.01a, REQ.PRO.03 |
| **4.2** | **COMPREENDER AS NECESSIDADES E EXPECTATIVAS DAS PARTES INTERESSADAS** | ***Requisito atualizado (RA)*** | 4.1, 4.7, 4.8, 4.9, 4.10, 4.16, 4.17, 4.18, 4.19, 4.21, 4.22, 4.26 | 4.4, 4.6, 4.10, 4.15, 8.1, 8.3, 9.1 | RCM.GES.01a, REQ.PRO.03 |
| **4.3** | **DETERMINAR O ÂMBITO DO SISTEMA DE GESTÃO *INTEGRADA* DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE (SGISIP)**** | ***Requisito atualizado (RA)***<br>NOTA: Para além das questões referidas no respetivo requisito da norma ISO/IEC 27001:2013, a organização deve determinar os limites e aplicabilidade do Sistema de Gestão Integrada de Segurança da Informação e Privacidade para estabelecer o seu âmbito, considerando:<br>a) 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;<br>b) os serviços, prestados pela organização, que são essenciais para a manutenção de atividades societais e económicas cruciais, de acordo com a Diretiva SRI. | 1.1, 1.2, 1.3, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 3.3, 4.1, 4.2, 4.13, 4.14, 4.15, 32.1 | 1.1, 1.2, 1.3, 1.4, 14.1, 16.1, 16.5, 16.11 | REQ.PRO.03 |

*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **4.4** | **SISTEMA DE GESTÃO *INTEGRADA* DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE (SGISIP)**** | ***Requisito atualizado (RA)*** | | | REQ.PRO.03 |
| **5 - LIDERANÇA** | | | | | |
| **5.1** | **LIDERANÇA E COMPROMETIMENTO** | ***Requisito atualizado (RA)*** | 5.1a, 5.1b, 5.1c, 5.1d, 5.1e, 5.1f, 24.1, 24.2, 32.1, 32.1d, 32.2, 32.4, 38.1, 38.2, 39.1a, 39.1b, 39.1c, 39.1d, 39.1e | | RCM.GES.01a, RCM.GES.03a, RCM.GES.04a, RCM.GES.05a, RCM.TIC.06a, REQ.EST.01, REQ.EST.04, REQ.EST.05, REQ.PRO.03 |
| **5.2** | **POLÍTICA** | ***Requisito atualizado (RA)*** | 5.1a, 5.1b, 5.1c, 5.1d, 5.1e, 5.1f, 6.1a, 6.1b, 6.1c, 6.1d, 6.1e, 6.1f, 6.4, 7.1, 7.2, 7.3, 7.4, 8.1, 8.2, 9.1, 9.2a, 9.2b, 9.2c, 9.2e, 9.2f, 9.2g, 9.2h, 9.2i, 9.2j, 9.3, 10, 11.1, 11.2, 24.1, 24.2, 25.1, 25.2 | | RCM.GES.05a, REQ.EST.01, REQ.PRO.03 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **5.3** | **FUNÇÕES, RESPONSABILIDADES E AUTORIDADES NA ORGANIZAÇÃO** | ***Requisito atualizado (RA)*** | 35.2, 36.1, 37.1, 37.2, 37.3, 37.4, 37.5, 37.6, 38.1, 38.3, 39.1a, 39.1b, 39.1c, 39.1d, 39.1e, 39.2, 47.2f, 47.2h | | RCM.GES.01b, RCM.GES.01d, RCM.GES.02a, RCM.GES.05a, REQ.PES.02, REQ.PRO.03 |
| **6 - PLANEAMENTO** | | | | | |
| **6.1 - AÇÕES PARA ENDEREÇAR RISCOS E OPORTUNIDADES** | | | | | |
| **6.1.1** | **Generalidades** | ***Requisito atualizado (RA)*** | | | RCM.GES.05a, RCM.TIC.03a, REQ.EST.03, REQ.PRO.03 |
| **6.1.2** | **Avaliação do risco de segurança da informação *e privacidade**** | ***Requisito atualizado (RA)***<br>NOTA: Para além das atividades abrangidas pelo processo de avaliação do risco de segurança da informação, de acordo com o respetivo requisito 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. | 24.1, 25.1, 25.2, 32.1, 32.2, 35.1, 35.2, 35.3, 35.4, 35.7, 35.8, 35.9, 35.10, 35.11, 39.1c, 39.1d, 57.1k | 4.9, 14.1 | RCM.GES.05a, RCM.TIC.03a, REQ.EST.03, REQ.DAD.02, REQ.PRO.03 |

*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **6.1.3** | **Tratamento do risco de segurança da informação *e privacidade**** | ***Requisito atualizado (RA)***<br>NOTA: Para além das atividades abrangidas pelo processo de tratamento do risco de segurança da informação, de acordo com o respetivo requisito da norma ISO/IEC 27001:2013, o mesmo deve incluir 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. | 5.1f, 24.1, 25.1, 25.2, 32.1, 32.1a, 32.1b, 32.1c, 32.1d, 39.1e | 4.9, 14.1 | REQ.PES.01, REQ.PRO.03 |
| **6.2** | **OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** **E PLANEAMENTO PARA OS ALCANÇAR** | ***Requisito atualizado (RA)*** | 24.1, 25.1, 28.1, 32.1, 32.1a, 32.1b, 32.1c, 32.1d, 33.1, 35.1, 35.7, 35.11, | 14.1, 16.1 | REQ.EST.01, REQ.EST.04, REQ.EST.05, REQ.PRO.03 |
| **7 - SUPORTE** | | | | | |
| **7.1** | **RECURSOS** | ***Requisito atualizado (RA)*** | 38.2 | | RCM.GES.01b, RCM.GES.01d, RCM.GES.02a, REQ.PRO.03 |
| **7.2** | **COMPETÊNCIA** | ***Requisito atualizado (RA)*** | 37.5, 38.2, 39.1a | | RCM.GES.01b, RCM.GES.01d, RCM.GES.02a, REQ.PRO.03 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **7.3** | **CONSCIENCIALIZAÇÃO** | ***Requisito atualizado (RA)*** | 32.1d, 83.1, 83.2, 83.3, 83.4, 83.5, 83.6 | 14.1, 14.2, 14.3, 16.1, 16.2, 16.3 | RCM.GES.03a, RCM.GES.04a, RCM.TIC.06a, REQ.EST.01, REQ.EST.04, REQ.EST.05, REQ.PRO.03 |
| **7.4** | **COMUNICAÇÃO** | ***Requisito atualizado (RA)*** | 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 13.1, 13.2, 13.3, 13.4, 14.1, 14.2, 14.3, 14.4, 14.5, 17.2, 19, 21.4, 33.1, 33.2, 33.3a, 33.3b, 33.3c, 33.3d, 33.4, 34.1, 34.2, 34.3, 34.4, 35.9, 36.1, 36.2, 37.7, 38.1, 38.2, 38.3, 38.4, 38.5, 39.1a, 39.1b, 39.1c, 39.1d, 39.1e, 40.2, 47.2k, 47.2m, 49.1g | 1.2d, 1.3, 1.7, 10.2, 14.3, 14.5, 14.6, 14.7, 16.3, 16.4, 16.5, 16.7, 16.9, 16.10, 20.1, 20.2 | RCM.GES.03a, RCM.GES.04a, RCM.TIC.06a, REQ.EST.01, REQ.EST.02, REQ.EST.04, REQ.EST.05, REQ.PRO.03 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **7.5 - INFORMAÇÃO DOCUMENTADA** | | | | | |
| **7.5.1** | **Generalidades** | ***Requisito atualizado (RA)***<br>NOTA: Para além da informação documentada exigida no âmbito do respetivo requisito da norma ISO/IEC 27001:2013, o Sistema de Gestão Integrada de Segurança da Informação e Privacidade da organização deve incluir a informação documentada determinada pela organização como sendo necessária para poder comprovar a operacionalização efetiva das medidas exigidas na legislação aplicável | 7.1, 24.1 | 15.2a, 15.2b, 15.3 | REQ.EST.02, REQ.PRO.03 |
| **7.5.2** | **Criação e atualização** | ***Requisito sem alterações (RSA)*** | | | REQ.EST.02, REQ.PRO.03 |
| **7.5.3** | **Controlo da informação documentada** | ***Requisito atualizado (RA)*** | 4.24, 7.1, 11.2, 12.2, 12.5, 24.3, 25.3, 28.3a, 28.3h, 28.5, 30.1, 30.2, 30.3, 30.4, 30.5, 32.3, 33.5, 35.7, 49.6, 86 | 15.2a, 17.2a | REQ.EST.02, REQ.PRO.03 |
| **8 - OPERAÇÃO** | | | | | |
| **8.1** | **PLANEAMENTO E CONTROLO OPERACIONAL** | ***Requisito atualizado (RA)*** | 4.24, 7.1, 11.2, 12.2, 12.5, 24.3, 25.3, 28.3a, 28.3h, 28.5, 30.1, 30.2, 30.3, 30.4, 30.5, 32.3, 33.5, 35.7, 49.6, 86 | 15.2a, 17.2a | REQ.PRO.03 |

*O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa da norma NP ISO/IEC 27001:2013

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **8.2** | **AVALIAÇÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | ***Requisito atualizado (RA)*** | 4.24, 7.1, 11.2, 12.2, 12.5, 24.3, 25.3, 28.3a, 28.3h, 28.5, 30.1, 30.2, 30.3, 30.4, 30.5, 32.1, 32.2, 32.3, 33.5, 35.1, 35.2, 35.3, 35.7, 49.6, 86 | 15.2a, 17.2a | RCM.GES.05a, RCM.TIC.03a, REQ.EST.03, REQ.PRO.03 |
| **8.3** | **TRATAMENTO DO RISCO DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | ***Requisito atualizado (RA)*** | 5.1f, 24.1, 32.1, 32.1a, 32.1b, 32.1c | 14.1 | REQ.PRO.03 |
| **9 - AVALIAÇÃO DE DESEMPENHO** | | | | | |
| **9.1** | **MONITORIZAÇÃO, MEDIÇÃO, ANÁLISE E AVALIAÇÃO** | ***Requisito atualizado (RA)*** | 24.1, 25.1, 28.1, 32.1, 32.1d, 35.11, 39.1b | | RCM.GES.01d, RCM.TIC.04h, REQ.DAD.02, REQ.PRO.03 |
| **9.2** | **AUDITORIA INTERNA** | ***Requisito atualizado (RA)*** | 24.1, 25.1, 28.1, 32.1, 32.1d, 35.11, 39.1b | | RCM.TIC.04h, REQ.PRO.03 |
| **9.3** | **REVISÃO PELA GESTÃO** | ***Requisito atualizado (RA)*** | 24.1, 25.1, 28.1, 32.1, 32.1d, 35.11, 39.1b | | RCM.TIC.04h, REQ.PRO.03 |
| **10 - MELHORIA** | | | | | |
| **10.1** | **NÃO CONFORMIDADE E AÇÃO CORRETIVA** | ***Requisito atualizado (RA)*** | 24.1, 28.1, 28.3h, 47.2j, 58.1b, 58.1d, 58.2a, 58.2b, 58.2d | 15.3 | RCM.TIC.05a, REQ.PRO.03 |
| **10.2** | **MELHORIA CONTÍNUA** | ***Requisito atualizado (RA)*** | | | RCM.TIC.05a, REQ.PRO.03 |

# ANEXO B. CONTROLOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Na tabela abaixo são utilizados os seguintes termos:

***Controlo atualizado (CA)*** - O controlo do anexo A da norma ISO/IEC 27001:2013 merece-nos uma atualização a fim de abranger, para alem da vertente de Segurança da informação, a dimensão de Privacidade e Proteção de Dados dentro da organização, sendo aplicável ao nível empresarial também;

***Controlo sem alterações (CSA)*** – O controlo do anexo A da norma ISO/IEC 27001:2013 mantem o texto original.

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **4 – CONTEXTO DA ORGANIZAÇÃO** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.5.1 - LINHAS DE ORIENTAÇÃO DA GESTÃO PARA A SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | | | | |
| **A.5.1.1** | **Políticas para a Segurança da informação *e Privacidade**** | ***Controlo atualizado (CA)*** | 5.1a, 5.1b, 5.1c, 5.1d, 5.1e, 5.1f, , 6.1a, 6.1b, 6.1c, 6.1d, 6.1e, 6.1f, 6.4, 7.1, 7.2, 7.3, 7.4, 8.1, 8.2, 9.1, 9.2a, 9.2b, 9.2c, 9.2e, 9.2f, 9.2g, 9.2h, 9.2i, 9.2j, 9.3, 10, 11.1, 11.2, 24.2, 25.1, 25.2 | 15.2a, 17.2a | RCM.GES.01a, RCM.GES.05a, REQ.EST.01 |
| **A.5.1.2** | **Revisão das políticas para a segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | 24.1, 24.2 | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.6 - ORGANIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | | | | | |
| **SUB-CATEGORIA ALARGADA** | **A.6.1 - ORGANIZAÇÃO INTERNA** | | | | |
| **A.6.1.1** | **Papeis e responsabilidades de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | 35.2, 36.1, 37.1, 37.2, 37.3, 37.4, 37.5, 37.6, 38.1, 38.3, 39.1a, 39.1b, 39.1c, 39.1d, 39.1e, 39.2, 47.2f, 47.2h | | RCM.GES.01b, RCM.GES.01c, RCM.GES.01d, RCM.GES.02a, RCM.GES.03a, RCM.GES.04a, RCM.GES.05a, RCM.PSD.05a, RCM.PSD.06a, RCM.PSD.07a, RCM.PSD.08a, RCM.TIC.02a, REQ.PES.02 |
| **A.6.1.2** | **Segregação de funções** | ***Controlo atualizado (CA)*** | 35.2, 38.3, 38.6 | | RCM.GES.01b, RCM.GES.01d, RCM.GES.02a, RCM.PSD.05a, RCM.PSD.06a, RCM.PSD.07a, RCM.TIC.02a, REQ.PES.02 |
| **A.6.1.3** | **Contacto com autoridades competentes** | ***Controlo atualizado (CA)*** | 37.7, 47.2j, 47.2k, 47.2l, 47.2m, 49.1, 57.1d | | RCM.GES.07a, RCM.TIC.06a, REQ.PES.01 |
| **A.6.1.4** | **Contacto com grupos de interesse especial** | ***Controlo atualizado (CA)*** | | | RCM.GES.07a, RCM.TIC.06a |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.6.1.5** | **Segurança da informação *e privacidade** na gestão de projeto** | ***Controlo atualizado (CA)*** | 25.1, 25.2, 47.2d | | |
| **A.6.1.6p** | **Contacto com titulares dos dados pessoais** | ***Controlo novo (CN)***<br>Devem ser estabelecidos e mantidos os canais de comunicação apropriados com os titulares dos dados pessoais | 34.1, 34.3, 35.9, 37.7, 38.4, 47.2d, 47.2e, 47.2f, 47.2g, 49.1 | | RCM.GES.07a, RCM.PSD.07a, RCM.TIC.02a |
| **SUB-CATEGORIA ATUALIZADA** | **A.6.2- DISPOSITIVOS MÓVEIS E TELETRABALHO** | | | | |
| **A.6.2.1** | **Política de dispositivos móveis** | ***Controlo atualizado (CA)*** | | | RCM.PSD.05a, RCM.PSD.06a |
| **A.6.2.2** | **Teletrabalho** | ***Controlo atualizado (CA)*** | | | RCM.PSD.05a |
| **A.7 - SEGURANÇA *DA INFORMAÇÃO E PRIVACIDADE** NA GESTÃO DE RECURSOS HUMANOS** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.7.1 - ANTES DA RELAÇÃO CONTRATUAL** | | | | |
| **A.7.1.1** | **Verificação de credenciais e referências** | ***Controlo sem alterações (CSA)*** | | | |
| **A.7.1.2** | **Termos e condições da relação contratual** | ***Controlo atualizado (CA)*** | 9.2i, 9.3, 14.5, 28.3a, 28.3b, 29, 32.4, 37.5, 37.6, 38.5, 54.2, 57.1j, 90.1 | | RCM.GES.03a, RCM.GES.04a, RCM.PSD.03b, RCM.PSD.04a, RCM.PSD.05a, RCM.PSD.06a, RCM.PSD.06b, RCM.PSD.07a, RCM.TIC.01a, RCM.TIC.02a, REQ.PRO.04 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| SUB-CATEGORIA ATUALIZADA | **A.7.2 - DURANTE A RELAÇÃO CONTRATUAL** | | | | |
| **A.7.2.1** | **Responsabilidades da gestão** | ***Controlo atualizado (CA)*** | 28.3a, 28.3b, 29, 32.4, 38.1, 38.2 | | RCM.GES.03a, RCM.GES.04a |
| **A.7.2.2** | **Consciencialização, educação e formação em segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | 37.5, 38.2, 39.1b, 47.2h, 47.2n, 57.1d | | RCM.GES.03a, RCM.GES.04a, REQ.EST.01 |
| **A.7.2.3** | **Procedimento disciplinar** | ***Controlo atualizado (CA)*** | | | RCM.GES.04a |
| SUB-CATEGORIA ATUALIZADA | **A.7.3 - CESSAÇÃO E ALTERAÇÃO DA RELAÇÃO CONTRATUAL** | | | | |
| **A.7.3.1** | **Responsabilidades na cessação ou alteração da relação contratual** | ***Controlo atualizado (CA)*** | | | |
| **A.8 - GESTÃO DE ATIVOS** | | | | | |
| SUB-CATEGORIA ALARGADA | **A.8.1 - RESPONSABILIDADE PELOS ATIVOS** | | | | |
| **A.8.1.1** | **Inventário de ativos** | ***Controlo sem alterações (CSA)*** | 5.1c, 25.1, 47.2d | | RCM.GES.01c, REQ.DAD.01, REQ.DAD.06 |
| **A.8.1.2** | **Responsabilidade pelos ativos** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.07a, RCM.TIC.02a |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.8.1.3** | **Utilização aceitável dos ativos** | ***Controlo sem alterações (CSA)*** | | | RCM.GES.05b, RCM.PSD.02a, RCM.PSD.03b, RCM.PSD.04a, RCM.PSD.05a, RCM.PSD.06a, RCM.PSD.06b, RCM.PSD.07a, RCM.TIC.01a, RCM.TIC.02a |
| **A.8.1.4** | **Devolução de ativos** | ***Controlo sem alterações (CSA)*** | | | |
| **A.8.1.5p** | **Ciclo de vida dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para gestão do ciclo de vida dos dados pessoais, assegurando o cumprimento dos princípios relativos ao tratamento de dados pessoais | 5.1a, 5.1b, 5.1c, 5.1d, 5.1e, 5.1f, 25.1, 47.2d, 89.1 | | REQ.DAD.01 |
| **A.8.1.6p** | **Ciclo de vida da informação destinada ao público** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para gestão dos conteúdos da informação destinados ao público | 12.1, 12.5, 13.1, 13.2, 13.3, 13.4, 14.1, 14.2, 14.3, 14.4, 14.5, 34.2, 34.3, 34.4, 37.7, 38.4, 39.1d, 39.1e, 47.2g, 70.1d | 14.6, 16.7 | |
| **SUB-CATEGORIA ATUALIZADA** | **A.8.2 - CLASSIFICAÇÃO DE INFORMAÇÃO** | | | | |
| **A.8.2.1** | **Classificação da informação** | ***Controlo atualizado (CA)***<br>NOTA: O esquema da classificação da informação deve ser definido tendo em consideração a possibilidade de identificação de pessoas singulares. | | | RCM.PSD.06b, RCM.TIC.01a, REQ.DAD.01 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.8.2.2** | **Etiquetagem da informação** | ***Controlo sem alterações (CSA)*** | | | |
| **A.8.2.3** | **Manuseamento de ativos** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.04a, RCM.PSD.05a, RCM.PSD.06a, RCM.PSD.06b, RCM.TIC.01a |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.8.3 - MANUSEAMENTO DE SUPORTE DE DADOS** | | | | |
| **A.8.3.1** | **Gestão de suportes de dados amovíveis** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.05a, RCM.PSD.06a |
| **A.8.3.2** | **Eliminação de suportes de dados** | ***Controlo sem alterações (CSA)*** | | | |
| **A.8.3.3** | **Transporte de suportes de dados** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.05a |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **NOVA SUB-CATEGORIA** | **A.8.4 - REQUISITOS MÍNIMOS**<br><u>Objetivo</u>: Garantir a segurança da informação e privacidade consoante o tipo da tecnologia utilizada para o seu tratamento. | | | | |
| **A.8.4.1p** | **Definir os requisitos mínimos para as várias categorias dos ativos** | ***Controlo novo (CN)***<br>Deve ser definido e aprovado um conjunto de requisitos mínimos (técnicos e organizativos) para garantir a mitigação dos riscos associados à utilização das novas soluções tecnológicas para o tratamento dos dados pessoais, respeitando, em especial, os princípios da segurança da informação e proteção de dados desde a conceção e por defeito. | 25.1, 25.2, 25.3, 35.1, | 4.19, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11 | RCM.PSD.03a, RCM.PSD.03b, RCM.PSD.04a, RCM.TIC.04a, RCM.TIC.04b, RCM.TIC.04c, RCM.TIC.04d, RCM.TIC.04e, RCM.TIC.04f, RCM.TIC.04g, RCM.TIC.04h, RCM.TIC.04i, RCM.TIC.04j, RCM.TIC.07a, REQ.DAD.09 |
| **A.8.4.2p** | **Definir os requisitos mínimos para integração dos sistemas** | ***Controlo novo (CN)***<br>Deve ser definido e aprovado um conjunto de requisitos mínimos (técnicos e organizativos) para garantir a mitigação dos riscos associados à integração das diversas soluções tecnológicas entre si e/ou com sistemas obsoletos em explotação na organização | 13.2, 14.2, 20.1, 20.2, 20.3, 20.4, 25.1, 25.2, 25.3, 35.1 | | RCM.PSD.03a, RCM.PSD.03b, RCM.PSD.04a, RCM.TIC.04a, RCM.TIC.04b, RCM.TIC.04c, RCM.TIC.04d, RCM.TIC.04e, RCM.TIC.04f, RCM.TIC.04g, RCM.TIC.04h, RCM.TIC.04i, RCM.TIC.04j, RCM.TIC.07a |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.9 - CONTROLO DE ACESSO** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.9.1 - REQUISITOS DE NEGÓCIO PARA CONTROLO DE ACESSO** | | | | |
| **A.9.1.1** | **Política de controlo de acesso** | ***Controlo atualizado (CA)*** | 4.12, 5.1f, 9.2i, 9.3, 13.2, 14.2c, 14.2, 15.1, 15.3, 23.2, 25.2, 28.3b, 29, 32.1c, 32.2, 32.4, 38.1, 38.2, 38.5, 42.6, 45.2a, 47.2n, 54.2, 58.1e, 58.1f, 83.5e, 86, 90.1 | | RCM.PSD.02a, RCM.PSD.03b, RCM.PSD.06a, RCM.TIC.04e, RCM.TIC.04j, REQ.TEQ.07 |
| **A.9.1.2** | **Acesso a redes e a serviços de rede** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.PSD.06a, RCM.TIC.04e, RCM.TIC.04j |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.9.2 - GESTÃO DE ACESSO DE UTILIZADORES** | | | | |
| A.9.2.1 | Registo e cancelamento de utilizador | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| A.9.2.2 | Disponibilização de acesso aos utilizadores | ***Controlo sem alterações (CSA)*** | 38.1, 38.2 | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.9.2.3** | **Gestão de direitos de acesso privilegiado** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| **A.9.2.4** | **Gestão da informação secreta para autenticação de utilizadores** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| **A.9.2.5** | **Revisão de direitos de acesso de utilizadores** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j, REQ.TEQ.07 |
| **A.9.2.6** | **Remoção ou ajuste de direitos de acesso** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j, REQ.TEQ.07 |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.9.3 - RESPONSABILIDADES DOS UTILIZADORES** | | | | |
| **A.9.3.1** | **Utilização da informação secreta para autenticação** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02ª, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.9.4 - CONTROLO DE ACESSO A SISTEMAS E APLICAÇÕES** | | | | |
| **A.9.4.1** | **Restrição de acesso à informação** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.PSD.06a, RCM.TIC.04e, RCM.TIC.04j |
| **A.9.4.2** | **Procedimentos seguros de início de sessão** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| **A.9.4.3** | **Sistema de gestão de senhas** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| **A.9.4.4** | **Utilização de programas utilitários privilegiados** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| **A.9.4.5** | **Controlo de acesso ao código fonte de programas** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.02a, RCM.PSD.03b, RCM.TIC.04e, RCM.TIC.04j |
| **A.10 - CRIPTOGRAFIA *E PSEUDONIMIZAÇÃO**** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.10.1 - CONTROLOS CRIPTOGRÁFICOS** | | | | |
| **A.10.1.1** | **Política sobre a utilização de controlos criptográficos** | ***Controlo atualizado (CA)*** | 5.1f, 32.1, 32.1a, 34.3 | | RCM.TIC.04c, REQ.TEQ.06 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.10.1.2** | **Gestão de chaves** | ***Controlo sem alterações (CSA)*** | 5.1f, 32.1, 32.1a, 34.3 | | RCM.TIC.04c, REQ.TEQ.06 |
| **NOVA SUB-CATEGORIA** | **A.10.2 - PSEUDONIMIZAÇÃO E ANONIMIZAÇÃO**<br>Objetivo: Assegurar a utilização adequada e eficaz de pseudonimização e anonimização para reduzir os riscos para os titulares de dados. | | | | |
| **A.10.2.1p** | **Política sobre a Pseudonimização e Anonimização** | ***Controlo novo (CN)***<br>Deve ser desenvolvida e implementada uma política sobre a pseudonimização e anonimização para reduzir os riscos para os titulares de dados em questão garantindo que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. | 4.5, 5.1f, 6.4, 11.2, 25.1, 32.1, 32.1a, 34.3, 40.2, 89.1 | | RCM.PSD.05a, RCM.TIC.04c, REQ.TEQ.05 |
| **A.11 - SEGURANÇA FÍSICA E AMBIENTAL** | | | | | |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.11.1 - ÁREAS SEGURAS** | | | | |
| **A.11.1.1** | **Perímetro de segurança física** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.1.2** | **Controlos de entrada física** | ***Controlo sem alterações (CSA)*** | 58.1f | | |
| **A.11.1.3** | **Segurança em escritórios, salas e instalações** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.1.4** | **Proteção contra ameaças externas e ambientais** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.1.5** | **Trabalhar em áreas seguras** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.1.6** | **Áreas de carga e descarga** | ***Controlo sem alterações (CSA)*** | | | |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.11.2 – EQUIPAMENTO** | | | | |
| **A.11.2.1** | **Colocação e proteção de equipamentos** | ***Controlo sem alterações (CSA)*** | | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.11.2.2** | **Serviços básicos de suporte** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.3** | **Segurança da cablagem** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.4** | **Manutenção dos equipamentos** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.5** | **Remoção de ativos** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.6** | **Segurança de equipamentos e ativos fora das instalações** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.7** | **Eliminação e reutilização seguras de equipamentos** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.8** | **Equipamento de utilizador não vigiado** | ***Controlo sem alterações (CSA)*** | | | |
| **A.11.2.9** | **Política de mesa limpa e ecrã limpo** | ***Controlo sem alterações (CSA)*** | | | |
| **A.12 - SEGURANÇA DE OPERAÇÕES** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.12.1 - PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS** | | | | |
| **A.12.1.1** | **Procedimentos de operação documentados** | ***Controlo sem alterações (CSA)*** | | | |
| **A.12.1.2** | **Gestão de alterações** | ***Controlo atualizado (CA)*** | 4.2, 4.12, 28.2, 32.2, 47.2k | | |
| **A.12.1.3** | **Gestão da capacidade** | ***Controlo sem alterações (CSA)*** | | | |
| **A.12.1.4** | **Separação entre ambientes de desenvolvimento, teste e de produção** | ***Controlo sem alterações (CSA)*** | | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.12.2 - PROTEÇÃO CONTRA CÓDIGO MALICIOSO** | | | | |
| **A.12.2.1** | **Controlos contra código malicioso** | ***Controlo sem alterações (CSA)*** | | | |
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.12.3 - CÓPIAS DE SEGURANÇA** | | | | |
| **A.12.3.1** | **Cópias de segurança** | ***Controlo sem alterações (CSA)*** | | | |
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.12.4 - REGISTOS DE EVENTOS E MONITORIZAÇÃO** | | | | |
| **A.12.4.1** | **Registos de eventos** | ***Controlo sem alterações (CSA)*** | | | |
| **A.12.4.2** | **Proteção da informação registada** | ***Controlo sem alterações (CSA)*** | | | |
| **A.12.4.3** | **Registos de administrador e operador** | ***Controlo sem alterações (CSA)*** | | | |
| **A.12.4.4** | **Sincronização de relógio** | ***Controlo sem alterações (CSA)*** | | | |
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.12.5 - CONTROLO DE SOFTWARE EM SISTEMAS DE PRODUÇÃO** | | | | |
| **A.12.5.1** | **Instalação de software nos sistemas de produção** | ***Controlo sem alterações (CSA)*** | | | |
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.12.6 - GESTÃO DE VULNERABILIDADES TÉCNICAS** | | | | |
| **A.12.6.1** | **Gestão de vulnerabilidades técnicas** | ***Controlo sem alterações (CSA)*** | 32.1, 32.1d | | RCM.TIC.07a |
| **A.12.6.2** | **Restrições sobre a instalação de software** | ***Controlo sem alterações (CSA)*** | | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.12.7 - CONSIDERAÇÕES PARA AUDITORIAS A SISTEMAS DE INFORMAÇÃO** | | | | |
| **A.12.7.1** | **Controlos de auditoria nos Sistemas de Informação** | ***Controlo sem alterações (CSA)*** | | | RCM.TIC.03a |
| **A.13 - SEGURANÇA DE COMUNICAÇÕES** | | | | | |
| SUB-CATEGORIA SEM ALTERAÇÕES | **A.13.1 - GESTÃO DE SEGURANÇA NA REDE** | | | | |
| **A.13.1.1** | **Controlos da rede** | ***Controlo sem alterações (CSA)*** | | | |
| **A.13.1.2** | **Segurança de serviços de rede** | ***Controlo sem alterações (CSA)*** | | | |
| **A.13.1.3** | **Segregação das redes** | ***Controlo sem alterações (CSA)*** | | | |
| SUB-CATEGORIA ALARGADA | **A.13.2 - Transferência de informação** | | | | |
| **A.13.2.1** | **Políticas e procedimentos de transferência de informação** | ***Controlo sem alterações (CSA)*** | 28.3a, 44, 45.1, 46.1, 46.2a, 46.2b, 46.2c, 46.2d, 46.2e, 46.2f, 46.3a, 46.3b, 48, 49.1, 49.1a, 49.1b, 49.1c, 49.1d, 49.1e, 49.1f, 49.1g, 49.2, 49.4, 57.1j, 57.1r, 58.3g, 58.3h, 58.3i | | RCM.PSD.04a, RCM.TIC.04i |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.13.2.2** | **Acordos sobre transferência de informação** | ***Controlo sem alterações (CSA)*** | 28.3a, 42.2, 44, 45.1, 46.1, 46.2a, 46.2b, 46.2c, 46.2d, 46.2e, 46.2f, 46.3a, 46.3b, 57.1j, 57.1r, 58.3g, 58.3h, 58.3i | | RCM.PSD.04a, RCM.TIC.04i |
| **A.13.2.3** | **Mensagens eletrónicas** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.04a, RCM.TIC.04i |
| **A.13.2.4** | **Acordos de confidencialidade ou de não divulgação** | ***Controlo sem alterações (CSA)*** | 9.2i, 9.3, 14.5, 28.3b, 38.5, 54.2, 90.1 | | RCM.PSD.04a |
| **A.13.2.5p** | **Regras vinculativas aplicáveis às empresas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido, autorizado pela autoridade de controlo competente e implementado um conjunto das regras internas de proteção de dados juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento | 4.19, 4.20, 46.2b, 47.1a, 47.1b, 47.1c, 47.2a, 47.2b, 47.2c, 47.2d, 47.2e, 47.2f, 47.2g, 47.2h, 47.2i, 47.2j, 47.2k, 47.2l, 47.2m, 47.2n, 47.3, 57.1s, 58.3j | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.14 - AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS** | | | | | |
| **SUB-CATEGORIA ALARGADA** | **A.14.1 - REQUISITOS DE SEGURANÇA *DA INFORMAÇÃO E PRIVACIDADE** DE SISTEMAS DE INFORMAÇÃO** | | | | |
| **A.14.1.1** | **Especificação e análise de requisitos de segurança da informação *e privacidade para os sistemas de informação**** | ***Controlo atualizado (CA)***<br>NOTA: Os requisitos para os sistemas da informação devem incluir, para alem dos referidos no respetivo controlo do anexo A da norma ISO/IEC 27001:2013, os requisitos para a interoperabilidade, privacidade e proteção dos dados pessoais, bem como os requisitos para a tomada das decisões automatizadas. | 13.2, 14.2, 15.3, 20.1, 20.2, 20.3, 20.4, 22.1, 22.2a, 22.2b, 22.2c, 22.3, 22.4, 25.1, 25.2 | | RCM.PSD.02a, RCM.PSD.03a, RCM.PSD.03b, RCM.TIC.04a, RCM.TIC.04b, RCM.TIC.04c, RCM.TIC.04d, RCM.TIC.04e, RCM.TIC.04f, RCM.TIC.04g, RCM.TIC.04h, RCM.TIC.04i, RCM.TIC.04j, RCM.TIC.07a, REQ.TEQ.01, REQ.TEQ.02, REQ.TEQ.03, REQ.TEQ.04, REQ.TEQ.05, REQ.TEQ.06, REQ.TEQ.07, REQ.TEQ.08 |
| **A.14.1.2** | **Proteger serviços aplicacionais nas redes públicas** | ***Controlo sem alterações (CSA)*** | | | |
| **A.14.1.3** | **Proteger transações de serviços aplicacionais** | ***Controlo sem alterações (CSA)*** | | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.14.1.4p** | **Especificação e análise de requisitos para os processos de negócio** | ***Controlo novo (CN)***<br>Os requisitos relacionados com a segurança da informação, interoperabilidade, privacidade e proteção dos dados pessoais, bem como os requisitos para a tomada das decisões automatizadas devem ser incluídos nos requisitos para novos processos de negócio ou para melhorias nos processos de negócio existentes | 13.2, 14.2, 15.3, 20.1, 20.2, 20.3, 20.4, 22.1, 22.2a, 22.2b, 22.2c, 22.3, 22.4, 25.1, 25.2 | | RCM.TIC.04a, RCM.TIC.04b, RCM.TIC.04c, RCM.TIC.04d, RCM.TIC.04e, RCM.TIC.04f, RCM.TIC.04g, RCM.TIC.04h, RCM.TIC.04i, RCM.TIC.04j, RCM.TIC.07a, REQ.PRO.07, REQ.TEQ.04 |
| **A.14.1.5p** | **Levantamento dos progressos técnicos mais recentes** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para acompanhar fatos novos relevantes e a evolução a nível 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, com especial enfoque nas novas ameaças cibernéticas, as vulnerabilidades que podem ser exploradas por elas e as possíveis medidas tecnológicas para o tratamento do risco associado | 57.1i | 14.1 | RCM.TIC.07a |
| **SUB-CATEGORIA ATUALIZADA** | **A.14.2 – SEGURANÇA *DA INFORMAÇÃO E PRIVACIDADE** NO DESENVOLVIMENTO E NOS PROCESSOS DE SUPORTE** | | | | |
| **A.14.2.1** | **Política de desenvolvimento seguro** | ***Controlo atualizado (CA)*** | 22.1, 22.2a, 22.2b, 22.2c, 22.3, 22.4, 25.1, 25.2 | | |
| **A.14.2.2** | **Procedimentos de controlo de alterações aos sistemas** | ***Controlo sem alterações (CSA)*** | | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.14.2.3** | **Revisão técnica das aplicações após alterações na plataforma de produção** | ***Controlo sem alterações (CSA)*** | | | RCM.TIC.03a |
| **A.14.2.4** | **Restrições sobre alterações em pacotes de software** | ***Controlo sem alterações (CSA)*** | | | |
| **A.14.2.5** | **Princípios de engenharia de sistemas seguros** | ***Controlo atualizado (CA)***<br>NOTA: Os princípios de engenharia de sistemas seguros devem prever a segurança da informação e proteção de dados desde a conceção e por defeito | 22.1, 22.2a, 22.2b, 22.2c, 22.3, 22.4, 25.1, 25.2 | | RCM.PSD.02a, RCM.PSD.03a, RCM.PSD.03b |
| **A.14.2.6** | **Ambiente de desenvolvimento seguro** | ***Controlo sem alterações (CSA)*** | | | |
| **A.14.2.7** | **Desenvolvimento subcontratado** | ***Controlo sem alterações (CSA)*** | | | |
| **A.14.2.8** | **Testes de segurança de sistemas** | ***Controlo sem alterações (CSA)*** | | | |
| **A.14.2.9** | **Testes de aceitação de sistemas** | ***Controlo sem alterações (CSA)*** | | | |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.14.3 - DADOS PARA TESTE** | | | | |
| **A.14.3.1** | **Proteção de dados de teste** | ***Controlo sem alterações (CSA)*** | 4.5, 6.4, 25.1, 32.1a, 40.2, 89.1 | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.15 - RELAÇÕES *COM TERCEIROS**** | | | | | |
| **SUB-CATEGORIA ALARGADA** | **A.15.1 - SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE NAS RELAÇÕES COM OS TERCEIROS**** | | | | |
| **A.15.1.1** | **Política de segurança da informação *e privacidade para as relações com terceiros**** | ***Controlo atualizado (CA)***<br>NOTA: O âmbito do respetivo controlo 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 a 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. | 28.1, 28.2, 28.3, 28.3a, 28.3b, 28.3c, 28.3d, 28.3e, 28.3f, 28.3g, 28.3h, 28.4, 57.1j, 58.1a, 58.1b, 58.1e | 4.13, 15.2a, 15.2b | RCM.GES.06a, RCM.PSD.04a, RCM.TIC.04i, REQ.PRO.04 |
| **A.15.1.2** | **Endereçar *as questões de* segurança *da informação e privacidade nos acordos com terceiros**** | ***Controlo atualizado (CA)***<br>NOTA: O âmbito do respetivo controlo 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 e os responsáveis pelo tratamento que delegam a organização o tratamento dos dados pessoais por sua conta, bem como com cada subcontratante que efetua o tratamento dos dados pessoais por conta da organização. | 4.7, 26.1, 26.2, 26.3, 28.1, 28.2, 28.3, 28.3a, 28.3b, 28.3c, 28.3d, 28.3e, 28.3f, 28.3g, 28.3h, 28.4, 28.5, 28.6, 28.7, 28.8, 28.9, 28.10, 29, 32.4, 57.1j, 58.3g, 82.2, 82.3, 82.4, 82.5 | 16.5 | RCM.GES.06a, RCM.PSD.04a, RCM.TIC.04i, REQ.DAD.09, REQ.PRO.04 |
| **A.15.1.3** | **Cadeia de fornecimento de tecnologias de informação e comunicação** | ***Controlo atualizado (CA)*** | 28.1, 28.2, 28.3, 28.3b, 28.3d, 28.4, 29, 32.4, 82.2, 82.3, 82.4, 82.5 | 16.5 | RCM.GES.06a, RCM.PSD.04a, RCM.TIC.04i, REQ.PRO.04 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.15.1.4p** | **Verificação de credenciais e referências dos subcontratantes** | ***Controlo novo (CN)***<br>Devem ser realizadas verificações 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 de negócio, à classificação da informação que será acedida e aos riscos percecionados. | 28.1, 28.3h, 28.5 | | RCM.GES.06a |
| **SUB-CATEGORIA ATUALIZADA** | **A.15.2 - GESTÃO DA ENTREGA DO SERVIÇO PELOS FORNECEDORES *E SUBCONTRATANTES**** | | | | |
| **A.15.2.1** | **Monitorizar e rever serviços de fornecedores *e subcontratantes**** | ***Controlo atualizado (CA)***<br>NOTA: A monitorização dos serviços de subcontratantes deve também abranger a verificação do cumprimento das obrigações contratuais e instruções documentadas pelos seus subcontratantes, garantindo que os subcontratantes que efetuam o tratamento dos dados pessoais por conta da organização cumpram os requisitos do GDPR | 28.3h, 28.5 | | RCM.GES.01d, REQ.PRO.04 |
| **A.15.2.2** | **Gerir alterações aos serviços de fornecedores *e subcontratantes**** | ***Controlo atualizado (CA)*** | 4.2, 4.12, 28.2, 47.2k | | REQ.PRO.04 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **NOVA SUB-CATEGORIA** | **A.15.3 - RELAÇÕES COM AS AUTORIDADES COMPETENTES**<br>Objetivo: Garantir o cumprimento dos procedimentos estabelecidos por lei no que respeita a exercício pelas autoridades competentes dos seus poderes de investigação e de correção, bem como dos poderes consultivos e de autorização. | | | | |
| **A.15.3.1p** | **Cooperação com as autoridades competentes (autoridades de controlo)** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para facilitar a realização das auditorias e garantir o seguimento atempado dos pedidos das autoridades competentes efetuados na prossecução das suas atribuições e poderes de investigação | 30.4, 31, 40.4, 47.2j, 47.2l, 57.1h, 57.1o, 58.1a, 58.1b, 58.1c, 58.1d, 58.1e, 58.1f, 58.2a, 58.2b, 58.2c, 58.2d, 58.2e, 58.2f, 58.2g, 58.2h, 58.2i, 58.2j, 90.1 | 15.1, 15.2a, 15.2b, 15.3 | RCM.PSD.04a |
| **A.15.3.2p** | **Retificação, apagamento e limitação do tratamento dos dados pessoais imposta pela autoridade de controlo** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a retificação, apagamento e/ou limitação temporária ou definitiva do tratamento de dados pessoais, ou mesmo a sua proibição, exigida pela autoridade de controlo competente | 58.2f, 58.2g | | REQ.TEQ.03 |
| **A.15.3.3p** | **Suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais por pedido da autoridade de controlo competente** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais na sequência de um pedido da autoridade de controlo competente | 58.2j, 83.5e | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.15.3.4p** | **Consulta prévia** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para realização da consulta a autoridade de controlo antes de proceder ao tratamento dos dados pessoais | 36.1, 36.2, 36.3, 36.5, 39.1e, 57.1l, 58.3a, 58.3c | | REQ.PES.01 |
| **A.15.3.5p** | **Autorização da autoridade de controlo para transferência de informação** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para obtenção da autorização da entidade de controlo para transferência de dados pessoais para um país terceiro ou organização internacional | 46.3a, 46.3b, 49.1, 57.1r, 58.3h, 58.3i | | REQ.PES.01 |
| **A.15.3.6p** | **Autorização da autoridade de controlo para estabelecimento de acordos administrativos, regras vinculativas e cláusulas contratuais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para obtenção da autorização por parte da entidade de controlo para estabelecimento de acordos administrativos, regras vinculativas aplicáveis às empresas e as cláusulas contratuais | 46.3a, 46.3b, 47.3, 58.3h, 58.3i, 58.3j | | REQ.PES.01 |
| **A.16 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.16.1 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE** E MELHORIAS** | | | | |
| **A.16.1.1** | **Responsabilidades e procedimentos** | ***Controlo atualizado (CA)*** | 33.1, 33.2, 33.3a, 33.3b, 33.3c, 33.3d, 33.5 | | RCM.GES.07a, REQ.PRO.01 |
| **A.16.1.2** | **Reportar eventos de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)***<br>NOTA: Deve ser garantido que os eventos de segurança da informação e privacidade são reportados ao longo da toda a cadeia de fornecimento através dos canais de gestão apropriados e o mais rapidamente possível | 33.2 | | RCM.PSD.08a, RCM.TIC.04f, RCM.TIC.07a, REQ.TEQ.01 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.16.1.3** | **Reportar pontos fracos de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | | 14.2 | RCM.PSD.08a, REQ.TEQ.01 |
| **A.16.1.4** | **Avaliação e decisão sobre eventos de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | 33.1, 33.2, 33.3a, 33.5 | | RCM.TIC.04f, RCM.TIC.07a, REQ.TEQ.01 |
| **A.16.1.5** | **Resposta a incidentes de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | 33.3d, 33.5 | 14.2 | RCM.GES.07a, REQ.PRO.01 |
| **A.16.1.6** | **Aprender com os incidentes de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | | 14.2 | |
| **A.16.1.7** | **Recolha de evidências** | ***Controlo sem alterações (CSA)*** | 33.3a, 33.5 | 1.6, 14.3 | |
| **NOVA SUB-CATEGORIA** | **A.16.2 - COMUNICAÇÃO DE INCIDENTES**<br>Objetivo: Garantir a notificação atempada às partes interessadas dos incidentes de segurança da informação e de violações de dados pessoais relevantes. | | | | |
| **A.16.2.1p** | **Notificação de violação de dados pessoais à autoridade de controlo** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação dos incidentes de privacidade (violações de dados pessoais) à autoridade de controlo competente sem demora injustificada | 33.1, 33.2, 33.3a, 33.3b, 33.3c, 33.3d, 33.4 | | RCM.GES.07a, REQ.PRO.02, REQ.TEQ.01 |
| **A.16.2.2p** | **Comunicação de violação de dados pessoais ao responsável pelo tratamento** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação dos incidentes de privacidade (violações de dados pessoais) aos respetivos responsáveis pelo tratamento | 33.2 | | RCM.GES.07a, REQ.PRO.02, REQ.TEQ.01 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.16.2.3p** | **Comunicação de violação de dados pessoais aos titulares dos dados** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação dos incidentes de privacidade (violações de dados pessoais) aos respetivos titulares dos dados | 34.1, 34.2, 34.3, 34.4, 58.2e | | RCM.GES.07a, REQ.PRO.02, REQ.TEQ.01 |
| **A.16.2.4p** | **Notificação dos incidentes com um impacto importante na continuidade dos serviços essenciais às autoridades competentes ou as CSIRT** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação obrigatória ou voluntária dos incidentes com um impacto importante na continuidade dos serviços essenciais às autoridades competentes ou às CSIRT sem demora injustificada | | 14.3, 14.4, 14.7, 16.5, 20.1, 20.2 | RCM.GES.07a |
| **A.16.2.5p** | **Comunicação por subcontratantes de incidentes com impacto importante na continuidade dos serviços ao prestador de serviço essencial** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir que os subcontratantes informam sem demora injustificada os prestadores de serviços essenciais sobre os incidentes com um impacto importante na continuidade dos serviços prestados | | | RCM.GES.07a |
| **A.16.2.6p** | **Notificação obrigatória centralizada dos incidentes de cibersegurança às autoridades competentes ou às CSIRT** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a notificação sem demora injustificada dos incidentes de cibersegurança às autoridades competentes ou às CSIRT | | | RCM.GES.07a |
| **A.16.2.7p** | **Comunicação de atividades ilícitas e crimes públicos** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para efetuar a comunicação às autoridades criminais/judiciais de atividades ilícitas e crimes públicos identificadas no âmbito da resposta a incidentes de segurança da informação e privacidade, bem como para entrega de evidências recolhidas | | 1.6 | RCM.GES.07a |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.17 - *RESILIÊNCIA DOS SISTEMAS E DOS SERVIÇOS DE TRATAMENTO**** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A.17.1 - CONTINUIDADE DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | | | | |
| **A.17.1.1** | **Planeamento da continuidade de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | 32.1b, 32.1c | 14.2, 14.3, 16.1c, 16.2, 16.5 | |
| **A.17.1.2** | **Implementação da continuidade de segurança da informação e privacidade** | ***Controlo atualizado (CA)*** | 32.1b, 32.1c | 14.2, 14.3, 16.1c, 16.2, 16.5 | |
| **A.17.1.3** | **Verificar, rever e avaliar a continuidade de segurança da informação e privacidade** | ***Controlo atualizado (CA)*** | 32.1b, 32.1c | 14.2, 14.3, 16.1c, 16.2, 16.5 | |
| **SUB-CATEGORIA SEM ALTERAÇÕES** | **A.17.2 – REDUNDÂNCIAS** | | | | |
| **A.17.2.1** | **Disponibilidade dos recursos de processamento da informação** | ***Controlo sem alterações (CSA)*** | | | |
| **NOVA SUB-CATEGORIA** | **A17.3 - CONTINUIDADE DO NEGÓCIO**<br>Objetivo: Garantir a recuperação célere de incidentes disruptivos quando surgem, garantindo a disponibilidade e o acesso aos sistemas, informação e dados pessoais de forma atempada. | | | | |
| **A.17.3.1p** | **Gestão da continuidade operacional** | ***Controlo novo (CN)***<br>A organização deve desenvolver e implementar a estratégia de continuidade do serviço e os planos de contingência, bem como as capacidades de recuperação de desastres | 32.1b, 32.1c | 14.2, 14.3, 16.1c, 16.2, 16.5 | REQ.DAD.07 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.17.3.2p** | **Exercícios relativos a planos de contingência** | ***Controlo novo (CN)***<br>A organização deve definir e testar os seus planos de contingência para garantir que eles sejam eficientes, eficazes e consistentes com os objetivos de continuidade de negócio da organização | 32.1b, 32.1c | 14.2, 14.3, 16.1c, 16.2, 16.5 | REQ.DAD.07 |
| **A18 - CONFORMIDADE** | | | | | |
| **SUB-CATEGORIA ATUALIZADA** | **A18.1 - CONFORMIDADE COM REQUISITOS LEGAIS E CONTRATUAIS** | | | | |
| **A.18.1.1** | **Identificação da legislação aplicável e de requisitos contratuais** | ***Controlo atualizado (CA)*** | 5.2, 6.2, 6.3, 9.4, 23.1, 23.2, 24.1, 47.2m, 49.5, 58.3b, 58.6, 84.1, 85.1, 85.2, 86, 87, 88.1, 88.2, 89.1, 89.2, 89.3, 89.4, 90.1, 91.1 | 1.7, 2.1, 3, 5.1, 5.2, 5.3, 5.5, 6.1, 6.2, 9.1, 9.4, 14.7, 19.1, 25.1 | RCM.TIC.05a, REQ.EST.01, REQ.EST.04, REQ.EST.05 |
| **A.18.1.2** | **Direitos de propriedade intelectual** | ***Controlo atualizado (CA)*** | | | RCM.TIC.05a |
| **A.18.1.3** | **Proteção de registo** | ***Controlo sem alterações (CSA)*** | | | RCM.PSD.03a, RCM.TIC.04g, RCM.TIC.04i, RCM.TIC.05a |
| **A.18.1.4** | **Privacidade e proteção de dados pessoais** | ***Controlo sem alterações (CSA)*** | 4.24, 24.1, 39.1b | | RCM.TIC.05a |
| **A.18.1.5** | **Regulamentação de controlos criptográficos** | ***Controlo sem alterações (CSA)*** | | | RCM.TIC.05a |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **SUB-CATEGORIA ALARGADA** | **A.18.2 - REVISÕES DE SEGURANÇA DA INFORMAÇÃO *E PRIVACIDADE**** | | | | |
| **A.18.2.1** | **Revisão independente de segurança da informação *e privacidade**** | ***Controlo atualizado (CA)*** | | 15.2b, 15.3 | RCM.GES.01d, RCM.TIC.03a, RCM.TIC.04h, RCM.TIC.05a |
| **A.18.2.2** | **Conformidade com as políticas e normas de segurança *da informação e privacidade**** | ***Controlo atualizado (CA)*** | 32.1d, 39.1b, 47.2h, 47.2j, 57.1s | 15.2b, 15.3 | RCM.GES.01d, RCM.TIC.03a, RCM.TIC.04h, RCM.TIC.05a |
| **A.18.2.3** | **Revisão da conformidade técnica** | ***Controlo atualizado (CA)*** | 32.1d, 39.1b, 47.2h, 47.2j, 57.1s | 15.2b, 15.3 | RCM.GES.01d, RCM.TIC.03a, RCM.TIC.04h, RCM.TIC.05a |
| **A.18.2.4p** | **Auditorias e inspeções conduzidas pelos clientes** | ***Controlo novo (CN)***<br>A organização deve desenvolver e implementar um conjunto de normas e procedimentos apropriados para facilitar a realização de auditorias de segurança da informação e privacidade e garantir o seguimento atempado dos pedidos dos seus clientes | 28.3h | | RCM.TIC.04h, RCM.TIC.05a |
| **NOVA SUB-CATEGORIA** | **A.18.3 - COMPROVAÇÃO DE CONFORMIDADE COM OS REQUISITOS LEGAIS E REGULAMENTARES**<br>Objetivo: Demonstrar o cumprimento das obrigações do responsável pelo tratamento de acordo com a legislação aplicável. | | | | |
| **A.18.3.1p** | **Adesão a um código de conduta** | ***Controlo novo (CN)***<br>A organização deve recorrer a um código de conduta em matéria de proteção de dados, aprovado nos termos do artigo 40º do GDPR, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos | 24.1, 24.3, 28.5, 32.3, 40.2, 40.3, 40.4, 40.5, 46.2e, 57.1m, 57.1p, 57.1q, 58.3d | | RCM.TIC.05a, REQ.EST.02 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.18.3.2p** | **Certificação em matéria de proteção de dados, selos e marcas de proteção de dados** | ***Controlo novo (CN)***<br>A organização deve recorrer a um procedimento de certificação em matéria de proteção de dados, aprovado nos termos do artigo n. 42.o do GDPR, para demonstrar o cumprimento do GDPR, em especial no que respeita à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos. | 24.1, 24.3, 25.1, 25.2, 25.3, 28.5, 32.3, 42.2, 42.4, 42.7, 46.2f, 57.1n, 57.1o, 57.1p, 57.1q, 58.1c, 58.2h, 58.3e, 58.3f | | RCM.TIC.05a, REQ.EST.02 |
| **NOVA SUB-CATEGORIA** | **A.18.4 - VIAS DE RECURSO E RESPONSABILIDADE**<br>Objetivo: Garantir o tratamento adequado das reclamações e uma representação adequada nos eventuais processos judiciais a fim de minimizar os prejuízos associados. | | | | |
| **A.18.4.1p** | **Reclamações dos titulares dos dados pessoais contra a organização** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para recolha e tratamento de reclamações de titulares dos dados pessoais | 47.2h, 47.2j, 57.1e, 57.1f, 57.2, 77.1, 80.1, 80.2 | | RCM.TIC.05a, REQ.EST.05 |
| **A.18.4.2p** | **Reclamação contra a autoridade competente** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para avaliar a fiabilidade e eventualmente apresentar uma reclamação à autoridade competente a fim de minimizar os danos associados à aplicação inadequada das disposições do GDPR e da Diretiva SRI ou quebra do sigilo comercial | 58.1a, 58.1b, 58.1c, 58.1d, 58.1e, 58.1f, 58.2a, 58.2b, 58.2c, 58.2d, 58.2e, 58.2f, 58.2g, 58.2h, 58.2i, 58.2j, 58.3a, 58.3b, 58.3c, 58.3d, 58.3e, 58.3f, 58.3g, 58.3h, 58.3i, 58.3j | 15.3 | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.18.4.3p** | **Queixa contra prestador de serviços digitais junto da entidade competente** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para avaliar a fiabilidade e eventualmente apresentar uma queixa à autoridade competente contra um prestador de serviços digitais que não cumpra os requisitos estabelecidos na Diretiva SRI, especialmente na sequência de um incidente | | 17.1 | RCM.TIC.05a |
| **A.18.4.4p** | **Ação judicial efetiva contra autoridade de controlo** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para avaliar a fiabilidade e eventualmente intentar um processo judicial contra a autoridade de controlo competente a fim de minimizar os danos associados à aplicação inadequada das disposições do GDPR e da Diretiva SRI ou quebra do sigilo comercial | 58.4, 83.8 | | |
| **A.18.4.5p** | **Ação judicial contra a organização** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para responder às ações judiciais intentadas contra a organização, alegando a violação das disposições do GDPR | 58.5, 79.1, 79.2, 80.1, 80.2, 81.1, 81.2, 81.3, 82.1, 82.2, 82.3, 82.4, 82.5, 82.6 | | RCM.TIC.05a, REQ.EST.05 |
| **A.18.4.6p** | **Reclamação de parte da indemnização paga, atendendo à corresponsabilidade pelo dano** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para reclamar perante outros responsáveis conjuntos pelo tratamento e/ou subcontratantes de parte da indemnização paga na sequência de uma ação judicial | 82.2, 82.3, 82.4, 82.5 | | |
| **A.18.4.7p** | **Resposta à reclamação de parte da indemnização paga, atendendo à corresponsabilidade pelo dano** | ***Controlo novo (CN)*** Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para responder às reclamações de outros responsáveis conjuntos pelo tratamento e/ou subcontratantes de parte da indemnização paga na sequência de uma ação judicial | 82.2, 82.3, 82.4, 82.5 | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.19 - PRIVACIDADE DE OPERAÇÕES** | | | | **NOVA CATEGORIA** | |
| **NOVA SUB-CATEGORIA** | **A.19.1 - TRANSPARÊNCIA NAS RELAÇÕES COM OS TITULARES DOS DADOS**<br>Objetivo: Garantir a transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. | | | | |
| **A.19.1.1p** | **Recolha dos dados pessoais junto do titular** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para facultar ao titular dos dados toda a informação exigida pelo GDPR aquando a recolha dos dados pessoais - incluindo as categorias especiais de dados pessoais - junto do titular dos mesmos | 12.1, 12.5, 12.7, 13.1, 13.2, 13.3, 13.4, 21.4, 26.1, 26.2, 47.2g | | RCM.PSD.01a, RCM.PSD.03a, REQ.DAD.03 |
| **A.19.1.2p** | **Recolha dos dados pessoais a partir de outra fonte** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para facultar ao titular dos dados toda a informação exigida pelo GDPR quando os dados pessoais - incluindo as categorias especiais de dados pessoais - não forem recolhidos junto do titular | 9.2e, 12.1, 12.5, 12.7, 14.1, 14.2, 14.3, 14.4, 14.5, 21.4, 26.1, 26.2, 47.2g | | RCM.PSD.01a, RCM.PSD.03a, REQ.DAD.03 |
| **A.19.1.3p** | **Decisões automatizadas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados que vise permitir o exercício dos direitos dos titulares dos dados 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 | 22.1, 22.2a, 22.2b, 22.2c, 22.3, 22.4, 35.3 | | |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **NOVA SUB-CATEGORIA** | **A.19.2 - PEDIDOS DOS TITULARES DOS DADOS PESSOAIS**<br>Objetivo: Garantir que os titulares dos dados pessoais usufruam de controlo efetivo sobre os mesmos, assegurando a resposta atempada aos seus pedidos. | | | | |
| **A.19.2.1p** | **Resposta aos pedidos dos titulares dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para – no sentido de dar resposta a pedido de titulares dos dados - garantir o cumprimento dos direitos e liberdades de terceiros, observando também o segredo comercial ou a propriedade intelectual e, em particular, os direitos de autor que protejam o software | 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 38.4, 58.2c | | RCM.TIC.04e, REQ.TEQ.02 |
| **A.19.2.2p** | **Disponibilização de acesso do titular aos seus dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para - na sequência de um pedido do titular dos dados - facultar a este o acesso aos mesmos, bem como às informações adicionais, de acordo com os requisitos do GDPR | 15.1, 15.2, 15.3, 15.4 | | RCM.TIC.04e, RCM.TIC.04j |
| **A.19.2.3p** | **Retificação dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados que permitam a retificação dos dados pessoais inexatos, na sequencia de um pedido do seu titular e sem demora injustificada | 16, 18.1a, 19, 58.2g | | RCM.TIC.04e, REQ.TEQ.02 |
| **A.19.2.4p** | **Apagamento dos dados pessoais por pedido do titular dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o apagamento, sem demora injustificada, dos dados pessoais na sequência de um pedido do seu titular e que manifeste oposição ao tratamento | 7.3, 17.1, 17.2, 17.3, 18.1d, 19, 21.1, 21.2, 21.3, 21.5, 21.6, 58.2g | | RCM.TIC.04e, REQ.TEQ.02, REQ.TEQ.03 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.19.2.5p** | **Limitação do tratamento dos dados pessoais a pedido do titular dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a limitação do tratamento dos dados pessoais na sequência de um pedido do seu titular e que manifeste oposição ao tratamento, embora parcial | 18.1a. 18.1b, 18.1c, 18.1d, 18.2, 18.3, 19, 21.1, 21.2, 21.3, 21.5, 21.6, 58.2g | | RCM.TIC.04e, REQ.TEQ.02 |
| **A.19.2.6p** | **Portabilidade dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para - a pedido do titular dos dados - garantir a transferência dos dados pessoais para si ou a outro responsável pelo tratamento | 20.1, 20.2, 20.3, 20.4 | | RCM.TIC.04a, RCM.TIC.04b, REQ.TEQ.04 |
| **NOVA SUB-CATEGORIA** | **A.19.3 - LICITUDE CONTÍNUA**<br>Objetivo: Manter a licitude de tratamento ao longo do ciclo da vida dos dados pessoais. | | | | |
| **A.19.3.1p** | **Registo das atividades de tratamento** | ***Controlo novo (CN)***<br>Deve ser criado e devidamente mantido (revisto e atualizado) um registo de todas as atividades de tratamento efetuadas pela organização na qualidade de responsável pelo tratamento e/ou na qualidade de subcontratante sob a responsabilidade de um ou vários responsáveis pelo tratamento ou ainda, se aplicável, os seus representantes | 5.1c, 6.1a, 6.1b, 6.1c, 6.1d, 6.1e, 6.1f, 7.1, 9.2a, 9.2b, 9.2c, 9.2e, 9.2f, 9.2g, 9.2h, 9.2i, 9.2j, 24.1, 25.1, 30.1, 30.1a, 30.1b, 30.1c, 30.1d, 30.1e, 30.1f, 30.1g, 30.2, 30.2a, 30.2b, 30.2c, 30.2d, 30.3, 30.5, 47.2d, 49.1, 49.1a, 49.1b, 49.1c, 49.1d, 49.1e, 49.1f, 49.1g, 49.6 | | RCM.GES.01c, RCM.PSD.03a, RCM.TIC.04g, RCM.TIC.04i, REQ.DAD.02, REQ.DAD.04, REQ.DAD.05, REQ.DAD.06 |

| *O estilo itálico sublinhado realça a atualização efetuada em comparação com a versão portuguesa do Anexo A da norma NP ISO/IEC 27001:2013 | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **A.19.3.2p** | **Tratamento posterior dos dados pessoais para outros fins** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos | 5.1c, 6.4, 21.1, 25.1, 47.2d | | REQ.DAD.04, REQ.PRO.05, REQ.DAD.06 |
| **A.19.3.3p** | **Apagamento dos dados pessoais para garantir a licitude de tratamento** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o apagamento, sem demora injustificada, dos dados pessoais para garantir a licitude de tratamento, bem como o cumprimento das obrigações jurídicas | 5.1c, 17.1, 17.2, 17.3, 18.1b, 18.1c, 19, 25.1, 47.2d, 58.2g | | REQ.DAD.04, REQ.DAD.08, REQ.PRO.05, REQ.TEQ.03, REQ.DAD.06 |

## ANEXO C. ÂMBITO DO SISTEMA DE GESTÃO INTEGRADA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.1 - LICITUDE DE TRATAMENTO** | | | | **NOVA CATEGORIA** | |
| **NOVA SUB-CATEGORIA** | **B.1.1 – CONSENTIMENTO**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para a obtenção do consentimento informado. | | | | |
| **B.1.1.1** | **Consentimento para tratamento dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a obtenção, registo e cancelamento do consentimento do titular de dados pessoais (incluindo as categorias especiais de dados pessoais) para uma ou mais finalidades específicas de tratamento | 6.1a, 7.2, 7.4, 9.1, 9.2a, 22.2c, 22.3, 22.4, 49.1a | | RCM.PSD.01b, RCM.PSD.07a, RCM.TIC.02a, REQ.PRO.05, REQ.PRO.07, REQ.TEQ.08 |
| **B.1.1.2** | **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 novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a obtenção, registo e cancelamento do consentimento do titular de dados pessoais (incluindo as categorias especiais de dados pessoais) para os efeitos de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos | 6.1a, 7.2, 7.4, 9.1, 9.2a, 22.2c, 22.3, 22.4 | | RCM.PSD.01b, RCM.PSD.07a, RCM.TIC.02a, REQ.PRO.05, REQ.PRO.07, REQ.TEQ.08 |
| **B.1.1.3** | **Consentimento para tratamento dos dados pessoais de crianças em relação aos serviços da sociedade da informação** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a obtenção, registo e cancelamento do consentimento ou autorização dos titulares das responsabilidades parentais da criança para tratamento dos dados pessoais da mesma (incluindo as categorias especiais de dados pessoais) | 6.1a, 7.2, 7.4, 8.1, 8.2, 9.1, 9.2a, 22.2c, 22.3, 22.4, 49.1a | | RCM.PSD.01b, RCM.PSD.07a, RCM.TIC.02a, REQ.PRO.05, REQ.PRO.06, REQ.PRO.07, REQ.TEQ.08 |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **NOVA SUB-CATEGORIA** | **B.1.2 - EXECUÇÃO DE CONTRATO**<br>Objetivo: Garantir a licitude de tratamento através da execução de contratos | | | | |
| **B.1.2.1** | **Tratamento dos dados pessoais necessário para a formalização de um contrato** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a recolha dos dados pessoais a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar e consequente formalização das relações contratuais em que o titular dos dados seja parte. | 6.1b, 7.4, 9.1, 9.2h, 9.3, 22.2a, 22.3, 22.4, 49.1b, 49.1c | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.2.2** | **Tratamento dos dados pessoais no âmbito de contrato formalizado** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir o tratamento dos dados pessoais no âmbito da execução de um contrato em cujo titular dos dados pessoais seja parte contratante, observando os requisitos contratuais e legislação aplicável | 6.1b, 7.4, 9.1, 9.2h, 9.3, 22.2a, 22.3, 22.4, 49.1b, 49.1c | | RCM.PSD.03a, REQ.PRO.07 |
| **NOVA SUB-CATEGORIA** | **B.1.3 - OBRIGAÇÃO JURÍDICA**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessários para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito | | | | |
| **B.1.3.1** | **Tratamento dos dados pessoais de acordo com uma obrigação jurídica** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito | 6.1c, 6.2, 6.3 | | RCM.PSD.03a, REQ.PRO.07 |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.1.3.2** | **Tratamento dos dados pessoais necessário à declaração, ao exercício ou à defesa de um direito num processo judicial** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário à declaração, ao exercício ou à defesa de um direito num processo judicial | 49.1e | | RCM.PSD.03a, REQ.PRO.07 |
| **NOVA SUB-CATEGORIA** | **B.1.4 - INTERESSES VITAIS DO TITULAR**<br>Objetivo: Garantir a proteção dos dados pessoais cujo tratamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular | | | | |
| **B.1.4.1** | **Tratamento dos dados pessoais para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento de dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento | 6.1a, 6.1d, 9.1, 9.2c, 49.1f | | RCM.PSD.01b, RCM.PSD.03a, REQ.PRO.07 |
| **NOVA SUB-CATEGORIA** | **B.1.5 - INTERESSE PÚBLICO OU AUTORIDADE PÚBLICA**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito decorrente do direito da União ou de um Estado-Membro | | | | |
| **B.1.5.1** | **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 novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o exercício das funções de interesse público ou prerrogativas de autoridade pública | 6.1e, 6.2, 6.3, 9.1, 9.2g, 9.2h, 9.2i, 9.2j, 21.1, 49.1d, 49.3, 49.4 | | RCM.PSD.03a, REQ.PRO.07 |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.1.5.2** | **Tratamento dos dados pessoais por motivo de interesse público no domínio da saúde pública** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para o exercício das funções de interesse público no domínio da saúde pública com base no direito da União ou dos Estados Membros | 9.1, 9.2i, 17.3, 23.1, 36.5 | | RCM.PSD.03a, REQ.PRO.07 |
| **NOVA SUB-CATEGORIA** | **B.1.6 - INTERESSE LEGÍTIMO**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para proteger os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros | | | | |
| **B.1.6.1** | **Tratamento dos dados pessoais dos clientes** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais dos clientes da organização em casos quando as relações contratuais não são devidamente formalizadas | 6.1f, 9.2h | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.6.2** | **Tratamento dos dados pessoais dos titulares dos dados que estão ao serviço do responsável pelo tratamento** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais dos titulares dos dados que prestam serviços ao responsável pelo tratamento independentemente da existência da remuneração | 6.1f | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.6.3** | **Tratamento dos dados pessoais para efeitos de comercialização direta** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para efeitos de comercialização direta | 6.1f, 21.2, 21.3 | | RCM.PSD.03a, REQ.PRO.07 |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.1.6.4** | **Tratamento dos dados pessoais para assegurar a segurança da rede e das informações** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir o tratamento dos dados pessoais na medida estritamente necessária e proporcionada para garantir a segurança das redes e das informações | | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.6.5** | **Tratamento dos dados pessoais no âmbito do grupo de empresas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais no âmbito do grupo de empresas | | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.6.6** | **Indicação de eventuais atos criminosos ou ameaças à segurança pública a autoridades competentes** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para a indicação pelo responsável pelo tratamento a uma autoridade competente de eventuais atos criminosos ou ameaças à segurança pública e à transmissão dos dados pessoais pertinentes | | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.6.7** | **Tratamento de dados pessoais necessário à prevenção e controlo da fraude** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para efeitos de controlo e prevenção de fraudes e da evasão fiscal de acordo com a legislação aplicável | | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.6.8** | **Transferências não repetitivas** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para transferências que possam ser classificadas como não repetitivas e que apenas digam respeito a um número limitado de titulares de dados | 49.1 | | RCM.PSD.03a, REQ.PRO.07 |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **NOVA SUB-CATEGORIA** | **B.1.7 - SITUAÇÕES ESPECÍFICAS**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para garantir a legalidade e lealdade do tratamento relativo as situações específicas de tratamento | | | | |
| **B.1.7.1** | **Tratamento dos dados pessoais para fins jornalísticos e para fins de expressão académica, artística ou literária** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) para fins jornalísticos e para fins de expressão académica, artística ou literária | 6.2, 6.3, 9.1, 9.2e, 85.1 | | RCM.PSD.03a, RCM.PSD.07a, RCM.TIC.02a, REQ.PRO.07 |
| **B.1.7.2** | **Disponibilização do acesso do público aos documentos oficiais a divulgar** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para garantir a divulgação segura dos documentos oficiais na posse de uma autoridade pública ou de um organismo público | 6.2, 6.3, 49.1g, 49.2, 86 | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.7.3** | **Tratamento dos dados pessoais no contexto laboral** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais dos trabalhadores no contexto laboral | 6.2, 6.3, 9.2b, 9.2h, 88.1, 88.2 | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.7.4** | **Arquivo de interesse público** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para fins de arquivo de interesse público | 5.1e, 9.2j, 11.1, 11.2, 62, 89.1, 89.3, 89.4 | | RCM.PSD.03a, REQ.PRO.07 |
| **B.1.7.5** | **Investigação científica ou histórica** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para fins de investigação científica ou histórica | 5.1e, 9.2j, 11.1, 11.2, 89.1, 89.2, 89.4 | | RCM.PSD.03a, RCM.PSD.07a, RCM.TIC.02a, REQ.PRO.07 |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.1.7.6** | **Fins estatísticos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados pessoais para fins estatísticos | 5.1e, 9.2j, 11.1, 11.2, 89.1, 89.2, 89.4 | | RCM.PSD.03a, REQ.PRO.07 |
| **B.2 - PROTEÇÃO ESPECÍFICA** | | | | | **NOVA CATEGORIA** |
| **NOVA SUB-CATEGORIA** | **B.2.1 - GRUPOS DE TITULARES**<br>Objetivo: Garantir a proteção específica dos direitos e liberdades das pessoas singulares vulneráveis | | | | |
| **B.2.1.1** | **Proteção especial das crianças quanto aos seus dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção especial das crianças, nomeadamente em casos da utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como da recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças | 6.1f, 8.1, 8.2, 8.3, 12.1, 40.2 | | RCM.PSD.01b, RCM.PSD.03a, REQ.PRO.06 |
| **NOVA SUB-CATEGORIA** | **B.2.2 - CONTEXTO DE TRATAMENTO**<br>Objetivo: Garantir a proteção específica dos dados pessoais quando o contexto do seu tratamento poderá implicar riscos significativos para os direitos e liberdades fundamentais | | | | |
| **B.2.2.1** | **Tratamento dos dados pessoais em grande escala** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados sensíveis cujo tratamento seja realizado em grande escala, bem como quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala | 27.2a, 35.3, 37.1 | | RCM.PSD.03a |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.2.2.2** | **Intercâmbio de dados pessoais com os registos nacionais e internacionais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados pessoais partilhados com outras organizações através de plataformas de interoperabilidade | | 4.19, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11 | RCM.PSD.03a, RCM.PSD.03b |
| **NOVA SUB-CATEGORIA** | **B.2.3 - DADOS SENSÍVEIS**<br>Objetivo: Garantir a proteção específica das categorias especiais dos dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais | | | | |
| **B.2.3.1** | **Tratamento de categorias especiais dos dados pessoais** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para o tratamento dos dados sensíveis | 9.1, 9.2a, 9.2b, 9.2c, 9.2e, 9.2f, 9.2g, 9.2h, 9.2i, 9.2j, 9.3, 9.4, 22.4, 27.2a, 30.5, 35.3, 37.1, 47.2d, 49.5, 83.2g | | RCM.PSD.03a |
| **B.2.3.2** | **Tratamento dos dados biométricos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados biométricos quando forem processados por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular | 4.14, 9.1, 9.4 | | RCM.PSD.03a |
| **B.2.3.3** | **Tratamento dos dados pessoais relativos à saúde** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados pessoais relativos ao estado de saúde dos titulares dos dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro | 4.4, 4.13, 4.15, 9.1, 9.2h, 9.2i, 9.4, 17.3, 23.1, 36.5, 88.1 | | RCM.PSD.03a, RCM.PSD.07a, RCM.TIC.02a |

| | | | GDPR | Diretiva SRI | Guia SPMS |
|---|---|---|---|---|---|
| **B.2.3.4** | **Tratamento dos dados genéticos** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados genéticos de acordo com a legislação aplicável | 4.1, 4.13, 9.1, 9.4 | | RCM.PSD.03a, RCM.PSD.07a, RCM.TIC.02a |
| **B.2.3.5** | **Tratamento dos dados da localização ou deslocações do titular dos dados** | ***Controlo novo (CN)***<br>Deve ser desenvolvido e implementado um conjunto de normas e procedimentos apropriados para assegurar a licitude de tratamento e garantir a proteção adequada dos dados da localização ou deslocações do titular dos dados de acordo com a legislação aplicável | 4.1, 4.4 | | RCM.PSD.03a |
| **B.3 - SERVIÇOS ESSENCIAIS** | | | | **NOVA CATEGORIA** | |
| **NOVA SUB-CATEGORIA** | **B.3.1 - Instalações de prestação de cuidados de saúde**<br>Objetivo: Assegurar a implementação correta e segura dos procedimentos específicos para o tratamento dos dados pessoais (incluindo as categorias especiais de dados pessoais) necessário para prestação dos serviços essenciais no setor da saúde | | | | |
| **B.3.1.x** | A lista dos controlos deve ser definida de acordo com a lista dos serviços essenciais definida por cada Estado-Membro. | | | 4.4, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 | RCM.TIC.03a |