Universidade do Estado do Rio de Janeiro

Centro Biomédico

Faculdade de Ciências Médicas

Guilherme Gondim Querido

Manual de boas práticas de segurança da informação para os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls

Rio de Janeiro

2023

Guilherme Gondim Querido

Manual de boas práticas de segurança da informação para os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Telemedicina e Telessaúde, da Universidade do Estado do Rio de Janeiro.

Orientadora: Prof.ª Dra. Vera Maria Benjamim Werneck

Coorientadora: Prof.ª Dra. Lucila Maria de Souza Bento

Rio de Janeiro

2023

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/CBA

Q4 Querido, Guilherme Gondim.
Manual de boas práticas de segurança da informação para os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls / Guilherme Gondim Querido. - 2023.
128 f.

Orientadora: Prof.ª Dra.Vera Maria Benjamim Werneck.
Coorientadora: Prof.ª Dra. Lucila Maria de Souza Bento.

Dissertação (Mestrado) – Universidade do Estado do Rio de Janeiro, Faculdade de Ciências Médicas.

1. Gestão da segurança – Teses. 2. Segurança da informação – Teses. 3. Segurança da informação – Normas - Teses. 4. Segurança da informação – Riscos – Teses. 5. ISO 27002. 6. Telemedicina – Teses. I. Werneck, Vera Maria Benjamim. II. Bento, Lucila Maria de Souza. III. Universidade do Estado do Rio de Janeiro. Faculdade de Ciências Médicas. IV. Título.

CDU 65.012.8

Bibliotecária: Diana Amado B. dos Santos CRB7/6171

_____ _____

Assinatura Data

Guilherme Gondim Querido

Manual de boas práticas de segurança da informação para os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Telemedicina e Telessaúde, da Universidade do Estado do Rio de Janeiro.

Aprovado em 6 de junho de 2023.

Coorientadora: Prof.ª Dra. Lucila Maria de Souza Bento
Universidade do Estado do Rio de Janeiro

Banca Examinadora:

_____

Prof.ª Dra. Vera Maria Benjamim Werneck (Orientadora)
Universidade do Estado do Rio de Janeiro

_____

Prof.ª Dra. Rosa Maria Esteves Moreira da Costa
Universidade do Estado do Rio de Janeiro

_____

Prof.ª Dra. Fernanda Claudia Alves Campos
Universidade Federal de Juiz de Fora

Rio de Janeiro
2023

DEDICATÓRIA

Primeiramente a Deus, por conceder saúde e sabedoria para seguir continuamente em frente. Agradecido por ser minha fonte inspiradora em todos os momentos da minha vida.

Aos meus pais, Jaime (em memória) e Vanda (em memória) pelo carinho, apoio e incentivo em todos os momentos de minha vida. Por não medirem esforços para que meus sonhos fossem realizados. Pelos sacrifícios e renúncias em benefício da minha formação e educação. Sem vocês eu jamais conseguiria. Meu amor por vocês é imensurável!

Ao meu irmão Leandro, pelo apoio prestado em todos os momentos de minha vida.

Dedico este trabalho a quem colaborou diretamente comigo: minha orientadora Profa. Dra. Vera Maria Benjamim Werneck e minha coorientadora: Profa. Dra. Lucila Maria de Souza Bento, sem aos quais eu não teria concluído este projeto. A conclusão deste trabalho resume-se em dedicação, empenho que vi ao longo desses anos em cada um dos professores deste curso, a quem dedico este trabalho.

Por último, agradeço a todos aqueles que de alguma forma contribuíram, de maneira direta e indireta, para a realização deste trabalho, o meu sincero agradecimento.

AGRADECIMENTOS

Às professoras Vera Maria Benjamim Werneck e Lucila Maria de Souza Bento por suas inestimáveis orientações que foram fundamentais para este trabalho. Suas opiniões, além de fazer com que o trabalho final ficasse melhor, revigoraram meu brio e faziam o trabalho fluir com naturalidade.

Aos meus amigos do curso de mestrado pela troca de conhecimento e por toda ajuda que me foi oferecida durante os dois anos do curso. Sem vocês ficaria difícil terminar este curso!

A todos que de alguma forma contribuíram para a realização deste trabalho, o meu muito obrigado!

A todos aqui mencionados, meu muito obrigado!

Feliz aquele que transfere o que sabe e aprende o que ensina!

Cora Coralina

RESUMO

QUERIDO, G.G. **Manual de boas práticas de segurança da informação para os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls**. 2023. 128 f. Dissertação (Mestrado Profissional em Telemedicina e Telessaúde) – Faculdade de Ciências Médicas, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

Organizações que utilizam a ISO/IEC 27002 e o framework CIS Controls para gestão de segurança de suas informações se preocupam com a confiabilidade, integridade e disponibilidade da informação, significando que elas conseguem gerenciar de forma segura suas informações. Atualmente, existem legislações com o propósito de tratar a proteção de dados, sendo esses padrões um importante aliado à adequação de tais normas. A adequação à ISO/IEC 27002 e ao framework CIS Controls são compulsórias para qualquer organização que deseja se manter competitiva assegurando as melhores práticas de mercado. A grande questão a ser relatada é que a proteção da informação dentro de uma organização depende de uma série de fatores, tanto internos como externos, que necessitam ser gerenciados. A norma ISO/IEC 27002 e o framework CIS Controls são genéricos para serem aplicados em qualquer setor, não sendo, portanto, instanciados na forma de um manual de boas práticas para o setor da Telemedicina. Nesse sentido, a principal contribuição deste estudo é a apresentação de uma proposta para processos e subprocessos orientados e sistematizados, na forma de um manual de boas práticas, que direcionam e guiam a implementação e manutenção de um sistema de gestão de segurança da informação para a Telemedicina, objetivando garantir a confiabilidade, integridade e disponibilidade das informações através da norma ISO/IEC 27002 e do framework CIS Controls. Em outras palavras, as boas práticas apresentadas para atender a todos os sistemas de Telemedicina têm a finalidade de garantir um grau aceitável de Segurança da Informação, evitando que os dados sejam compartilhados de forma indevida. Com esse intuito, o manual de boas práticas foi apresentado para orientar os profissionais que atuam no ramo da saúde quanto aos procedimentos que devem ser adotados nos sistemas de telemedicina no que se refere a segurança das informações.

Palavras-chave: Gestão de Segurança da Informação. ISO/IEC 27002. CIS Controls. Telemedicina. Riscos em segurança da informação.

ABSTRACT

QUERIDO, G.G. **Information Security Best Practices Manual for Telemedicine Systems in accordance with ABNT NBR ISO/IEC 27002 and CIS Controls standards**. 2023. 128 f. Dissertação (Mestrado Profissional em Telemedicina e Telessaúde) – Faculdade de Ciências Médicas, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

Organizations that use ISO/IEC 27002 and the CIS Controls framework for managing the security of their information are concerned with the reliability, integrity and availability of information meaning that they can securely manage their information. Currently, there are laws with the purpose of dealing with data protection, and these standards are relevant support in compliance with such rules. Compliance with ISO/IEC 27002 and the CIS Controls framework are mandatory for any organization that wants to remain competitive by ensuring the best market practices. The big issue to be reported is that the information protection within an organization depends on several internal and external factors that need previously to be managed. The ISO/IEC 27002 standard and the CIS Controls framework are generic to be applied in any sector, therefore not being instantiated in a good practice manual for the Telemedicine sector. In this sense, the main contribution of this study is the presentation of a proposal for oriented and systematized processes and sub-processes in the form of a manual of good practices, which direct and guide the implementation and maintenance of an information security management system for the Telemedicine, aiming to guarantee the reliability, integrity, and availability of information through the ISO/IEC 27002 standard and the CIS Controls framework. In other words, the good practices presented to serve all Telemedicine systems are intended to guarantee an acceptable degree of Information Security, preventing data from being improperly shared. For this purpose, the best practices manual was presented to guide professionals in the health sector regarding the procedures that must be adopted in telemedicine systems concerning information security.

Keywords: Information Security Management. ISO/IEC 27002. CIS Controls. Telemedicine. Information security risks.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CFM	Conselho Federal de Medicina
CIO	Chief Information Officer
CIS	Center for Internet Security
DICOM	Digital Imaging and Communications in Medicine
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira
NIST CF	NIST Cybersecurity Framework
PDCA	Plan Do Check Act
PIMS	Privacy Information Management System
PoS	Point of Sale
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação
STRING	Letra
TI	Tecnologia da Informação

SUMÁRIO

INTRODUÇÃO

A Telemedicina é uma modalidade de atendimento médico da área da Telessaúde determinada como um conjunto de tecnologias que fazem com que as ações médicas possam ser realizadas à distância, em qualquer hora e em qualquer lugar. Atualmente, vem sendo empregada em teleconsultas, exames de rotina, exames laboratoriais, urgências médicas, assistências a pacientes com dificuldade de locomoção e outras situações médicas que dependem dessa tecnologia para facilitar o acesso à saúde. Além disso, a Telemedicina realiza não somente atendimento à distância, mas também permite que a tecnologia seja benéfica com o propósito de fazer a troca de informações de profissionais médicos para o acompanhamento dos pacientes.

Uma das vantagens que a Telemedicina oferece é a ampliação da cobertura de médicos especialistas para todo o país, já que todos os indivíduos da região, tanto nacionais como países vizinhos, têm acesso a profissionais que são eminências em diferentes patologias, podendo escolher, para ter a melhor opinião médica (BLARDONE, 2013a).

As organizações que fornecem serviços de saúde devem ter controles[1] implementados a fim de dar proteção às informações geradas por elas. O Conselho Federal de Medicina (CFM), no Brasil, publicou no ano de 2007 a resolução 1.643/2002 que estabelece as diretrizes desse novo tipo de atendimento médico.

As regras que normalmente estão válidas nesse seguimento da medicina remota somente regulam a prática de forma geral. As normas atualmente válidas não conseguem englobar todas as particularidades e as várias oportunidades que essa nova modalidade pode oferecer ao atendimento médico. Sendo assim, a atualização da normatização pode garantir a execução mais concreta da tecnologia.

A lei n° 13.989/20, que padroniza a utilização da Telemedicina no decurso da crise oriunda do coronavírus, somente define esta ferramenta como a prática da medicina regulada por tecnologias para fins de pesquisa, assistência, precaução de doenças e lesões e divulgação de saúde. Essa normatização estabelece que nem sempre é possível a realização de exames durante uma teleconsulta, mas pode acontecer em alguns casos. A resolução n° 1.643/02

[1] De acordo com o NIST (NIST, 2006), um controle de segurança é uma salvaguarda ou contramedida de natureza gerencial, operacional ou técnica, prescrita para um sistema de informações, de modo a proteger a confidencialidade, integridade e disponibilidade do sistema de sua informação.

determina que os serviços oriundos da Telemedicina devem possuir infraestrutura tecnológica adequadas sem entrar em detalhes específicos.

Nesse contexto, a resolução 1.643/02 define que a telemedicina pode ser compreendida como a utilização de recursos que possam permitir a influência mútua de imagens, áudio e informações com o propósito de auxiliar no campo da saúde, fortalecendo a pesquisa e proporcionando a educação. Diante dessa perspectiva é fato que as informações que são geradas e trafegadas nessa modalidade de atendimento médico são valiosas e não podem ser perdidas nem ser alvo de ataques fazendo com que toda dinâmica da Telemedicina seja confiável, íntegra e disponível. Com isso, a proteção dos dados tem um papel importante nas organizações, demandando a implementação de um Sistema de Gestão de Segurança da Informação para garantir a melhoria contínua dos processos das organizações no que se refere à segurança da informação demonstrando seu comprometimento com o tema.

Segundo (SÁNCHEZ *et al.*, 2006, p. 2), um Sistema de Gestão de Segurança da Informação (SGSI) pode ser determinado como um sistema de gestão utilizado para estabelecer e manter um ambiente seguro para as informações.

Problemática e Motivação

À medida que a Tecnologia da Informação se faz cada vez mais presente nas organizações de saúde com o propósito de dar celeridade a todo o processo de atendimento, diagnóstico, tratamento e alta dos pacientes, a TI estão da mesma forma diretamente envolvida com os riscos relacionados à confiabilidade, integridade e disponibilidade das informações que foram geradas, pois a TI é suscetível a erros, fazendo com que todo o processo de tratamento envolvendo o paciente se torne duvidoso trazendo riscos específicos aos pacientes.

Um artigo publicado no sítio da Internet CISO Advisor, em setembro de 2020, (REDAÇÃO, 2020), informou que um ataque de ransomware na Clínica da Universidade de Dusseldorf, na Alemanha, impediu o registro da internação urgente de uma paciente. Um enfermo, em risco de vida que deveria ter sido internado, precisou ser transferido para um hospital em Wuppertal, a cerca de 32 quilômetros de distância. Os médicos perderam uma hora antes de iniciar o tratamento e ele veio a óbito.

Nos dois últimos anos, mais de 80% dos responsáveis pela Tecnologia da Informação (TI) das empresas na área da saúde confidenciaram ter sido atingidos pelo menos uma vez por botnet, malware ou outros tipos de ataques. Foram entrevistados mais de 150 executivos de TI

das organizações de planos de saúde com mais de 400 milhões de dólares anuais de receita (REALPROTECT, 2015). Por envolver dados confidenciais, o dano causado por invasões cibernéticas no setor de TI é imensurável. No entanto, apenas 60% dos planos de saúde e 50% dos estabelecimentos hospitalares, que, contribuíram para esta análise, estão adequadamente preparados para estes tipos de ataque. Porém o dado que causa maior preocupação é que, aproximadamente, 15% das organizações hospitalares relataram não conseguir identificar ataques em tempo real. Isso é um grande percalço pois os hackers mais experientes gostam de ficar anônimos com o propósito de pegar a maior quantidade de dados possível na plataforma invadida.

Algumas explicações para que os ataques às plataformas de TI das organizações do ramo da saúde crescessem recentemente são: (a) mudança para os registros digitais e a adoção de processos automáticos nos sistemas hospitalares; (b) utilização de forma incorreta dos registros eletrônicos; (c) informações eletrônicas de saúde disseminadas de forma rápida e fácil, pelos dispositivos móveis, e externamente, em serviços de nuvem e empresas terceirizadas e (d) utilização de sistemas heterogêneos em aplicações hospitalares e o crescimento do valor no mercado negro dos dados dos pacientes. Em se tratando das instituições de saúde, os ataques cibernéticos se sobrepõem aos ataques financeiros se consolidando como os principais causadores de prejuízos (SECURING CONNECTED HOSPITALS: A RESEARCH ON EXPOSED MEDICAL SYSTEMS AND SUPPLY CHAIN RISKS, [*s. d.*]) .

Segundo presidente da Sociedade Brasileira de Informática em Saúde (ALVO DE HACKERS, DADOS SOBRE SUA SAÚDE VALEM MAIS QUE SEU CARTÃO DE CRÉDITO, [*s. d.*]), os dados confidenciais médicos podem valer muito mais se comparados com dados de cartão de crédito. O valor é mais elevado por não ser possível alterar ou cancelar com facilidade os dados médicos, se comparado com o simples cancelamento de um determinado cartão de crédito, exemplificando. Segundo noticiado pelo site da Forbes, o prejuízo foi tão grande que um determinado ataque ficou entre os maiores ataques virtuais que causaram pesados prejuízos em meados de julho de 2014, no Departamento de Estado dos Estados Unidos da América. Este ataque foi realizado em meados de 2013, entretanto a invasão somente foi descoberta no segundo trimestre de 2014. Esta violação de dados deve ter envolvido por volta de 1 milhão de americanos (LYNGAAS, [*s. d.*]).

Para que os serviços de TI sejam normalizados, as organizações são obrigadas a pagar uma certa quantia financeira. Mesmo assim, diante desse pagamento não é garantido que a normalidade volte, que outros ataques não ocorrem ou ainda que novas cobranças financeiras

possam ser realizadas mais à frente. Como exemplo, no ambiente de TI hospitalar, é a invasão da rede de computadores de uma organização de saúde. Assim, os hackers invadem a rede dessa organização e danificam o acesso aos prontuários eletrônicos pedindo mais tarde uma quantia financeira para restabelecer o acesso dessa plataforma.

Criminosos virtuais podem realizar ataques alterando a dose de medicamentos de modo a torná-los fatais para os pacientes. Sendo assim, como exemplo, isso pode acontecer com marcapassos e bombas de insulina. Um pesquisador de segurança descobriu brechas em alguns tipos de bomba de infusão (BRECHAS DE SEGURANÇA PODEM AFETAR ATÉ EQUIPAMENTOS MÉDICOS, 2014).

Existe um movimento para que a segurança desses dispositivos seja eficaz. Mesmo assim, estes tipos de ataques são preocupantes. Segundo uma pesquisa realizada por uma renomada empresa de auditoria de TI cerca de 85% dos hospitais e 90% das companhias de saúde garantiram que, em se tratando de segurança cibernética, os investimentos nesta área aumentaram (REALPROTECT, 2015).

Estudo detalhado acerca da cibersegurança no ambiente hospitalar, realizada por duas grandes empresas de auditoria de TI, abrange o funcionamento dos sistemas e dispositivos da área médica que dependem da Internet para funcionar, como por exemplo bases de dados de sistemas hospitalares e gerenciadores administrativos, como também as características dos cibercriminosos que invadem os sistemas desses ambientes médicos (SOLUÇÕES DE SEGURANÇA CORPORATIVA, 2023).

É notório que os ambientes de tecnologia da informação da área da saúde se encontram ultrapassados em se tratando de padrões de cibersegurança. Como exemplo, é citado o renomado serviço de saúde britânico que foi invadido por um vírus do tipo ransomware apelidado WannaCry em meado de 2017. Esse ataque conseguiu comprometer mais de 35 hospitais sendo que indiretamente atingiu mais de 40 e infectou mais de 600 clínicas e outras organizações ligadas ao sistema de saúde britânico deixando estes estabelecimentos em desordem por vários dias (REPORT, 2018).

Ativos específicos do ambiente hospitalar também podem representar problemas para a Segurança. Um exemplo é a ferramenta DICOM, Digital Imaging and Communications in Medicine, que realiza a digitalização dos exames de imagens. Imagens desta ferramenta, como as imagens de ultrassom, endoscopia, mamografia, ressonância magnética e raio-X podem ser expostas.

A pesquisa foi realizada em 20 países que detém o maior número de servidores e dispositivos DICOM com vulnerabilidades na segurança de informação sendo que o Brasil ficou localizado no terceiro lugar, atrás apenas dos Estados Unidos e da China (REPORT, 2018).

Vale ressaltar que um dispositivo nem sempre está vulnerável por constatar que este dispositivo ou sistema esteja exposto. Porém, o que não é tolerável, em hipótese alguma, é que em se tratando de imagens de sistemas DICOM sejam acessadas por pessoas para visualização pública e possam ser acessadas por cibercriminosos.

Prontuários médicos e informações pessoais de pacientes podem ser expostos caso os sistemas se encontrem a mostra na Internet. Outro dado relevante constatado no estudo foi a falta de obstáculos em descobrir novas interfaces de software dos sistemas de gestão farmacêutica (REPORT, 2018). Neste tipo de software utilizado em farmácias para funções adaptadas como, por exemplo, a coordenação dos medicamentos sem receita médica, varredura de narcóticos, vida pregressa de prescrições dos pacientes, pagamentos em pontos de venda (PoS).

Outro ponto a se destacar nos ambientes de TI nos hospitais foram as ameaças de fornecedores de serviços e bens hospitalares. Estes tipos de ameaças oferecem riscos importantes: um cibercriminoso pode manipular os dados hospitalares, pode atrapalhar as operações diárias, introduzir dispositivos maléficos, instalar softwares adulterados e influenciar de forma negativa a continuidade do negócio. No ano de 2016, foi constatado que a origem de violações de fornecedores oriundas de aproximadamente 30% das infrações em ambientes de healthcare. Fornecedores terceirizados possuem credenciais como logins e senhas que eventualmente podem fornecer acesso aos registros, aos equipamentos de escritório e aos dispositivos médicos (REPORT, 2018).

Em se tratando do serviço de inteligência de ameaça no ambiente de saúde, historicamente e em todo mundo, é moroso e manual sendo que o objetivo principal de um hospital é o cuidado com os pacientes sendo também que é neste setor que é investido a maioria dos recursos. Sendo assim, os investimentos ligados a cibersegurança em hospitais são realizados de maneira prescindível.

Seguem abaixo as principais razões para o atraso da cibersegurança nos sistemas de healthcare:

a) Embora os sistemas requisitem autenticação de acesso, a grande maioria dos dispositivos médicos pode sofrer ataque e ser explorado tendo o atacante sucesso em sua investida (REPORT, 2018).

b) Foram descobertos usuários e senhas definidos pelo fabricante do equipamento (REPORT, 2018). Neste tipo de situação o administrador não consegue alterar as senhas definidas na fábrica, que não foram trocadas, sistemas com senhas fracas e sistemas que se encontram desatualizados, permitindo assim a exploração das vulnerabilidades.

Os profissionais que acessam equipamentos médicos de diagnóstico e computadores hospitalares (técnicos, médicos e enfermeiros) circulam livremente pelo hospital em que atuam.

Com isso, a política de cibersegurança e os procedimentos para autenticação acabam ficando afetados dificultando a introdução das políticas de cibersegurança e dos procedimentos para realizar autenticação, principalmente se estas políticas prejudicam as operações diárias do estabelecimento hospitalar;

Os equipamentos hospitalares de diagnósticos são muito custosos sendo que é grande o prejuízo para os hospitais que estes dispositivos permaneçam offline em longos períodos de manutenção. A Atualização do sistema operacional destes equipamentos ou modificação de suas configurações pode acarretar, por invalidar a certificação, a cobertura e a garantia do dispositivo e, nesse sentido, estes equipamentos médicos permanecem inalterados por longo período.

Não são todos os hospitais que possuem uma equipe de cibersegurança exclusiva para esta finalidade. Em grande parte dos hospitais, a área de TI fica responsável pelas funções de investigar e eliminar todos os incidentes que poderão ocorrer além de fornecer suporte às outras áreas que o hospital necessite. Este padrão possui desvantagem devido à má distribuição dos recursos para as duas funções (REPORT, 2018).

Atualmente, dada e relevância e a criticidade da cibersegurança em ambientes hospitalares, o objeto deste estudo é apresentar processos para a implementação e a manutenção da segurança da informação nos sistemas dos ambientes informatizados da área da Telemedicina.

Inúmeras organizações possuem um Sistema de Gestão de Segurança da Informação, porém na área da saúde poucas instituições se importam com um SGSI em seu favor. Sendo assim, se faz necessário que as organizações de saúde que atuam com a Telemedicina possuam um SGSI com a finalidade de proteger a informação corporativa com seus critérios de confidencialidade, integridade e disponibilidade, além de proteger as informações das partes interessadas. A implantação de um SGSI baseado nas normas ISO/IEC 27002 e no CIS

Controls garante o tratamento dos problemas de SI segundo as melhores práticas atualmente aceitas no mercado.

Objetivos

O objetivo geral deste trabalho é a proposta conceitual de processos estruturados para implementação e manutenção da Segurança da Informação nos sistemas de Telemedicina no setor da saúde com base nas normas ABNT NBR ISO/IEC 27001, ISO/IEC 27002 e o CIS Controls.

Para que possamos alcançar o Objetivo Geral deste trabalho são delineados os seguintes Objetivos Específicos:

a) Partindo de um levantamento bibliográfico, realizar a análise dos macroprocessos de implementação da Segurança da Informação no ambiente da Telemedicina conforme definidos nas normas ISO/IEC 27001, ISO/IEC 27002 e no CIS Controls.
b) A partir dos processos selecionados, realizar a identificação dos subprocessos para a implementação e manutenção da Segurança da Informação no ambiente da Telemedicina, verificando as entradas destes subprocessos, ferramentas, técnicas e suas saídas.

Metodologia

Esta dissertação está embasada nos métodos científicos descritos a seguir.

Com relação à aplicação prática da ciência, a Pesquisa Aplicada da Ciência ou também denominada Pesquisa Prática utiliza teorias, conhecimentos, métodos e técnicas acumuladas das comunidades de pesquisa para um propósito específico. Esta pesquisa é utilizada para encontrar soluções para problemas cotidianos, normalmente direcionados para um determinado problema (QUE É PESQUISA APLICADA?, 2022).

Na Pesquisa Aplicada, o pesquisador busca orientação prática à solução imediata de problemas concretos do cotidiano (BARROS; LEHFELD, 2014).

Em se tratando da abordagem do problema, classifica-se como pesquisa qualitativa, ao passo que é descritiva e os dados são fornecidos para a própria conclusão.

O método exploratório é aquele que, realizada a pesquisa de um tema pouco explorado, justificado pelo fato do assunto abordado ser novo em termos de Brasil e a nível mundial, torna-se necessário abordar os processos de implementação e manutenção da Segurança da Informação da ISO/IEC 27001, ISO/IEC 27002 e do CIS Controls e sua forma de implementação.

A pesquisa exploratória realiza descrições precisas da situação e busca descobrir as relações existentes entre seus elementos componentes. Esse tipo de pesquisa requer um planejamento bastante flexível para possibilitar a consideração dos mais diversos aspectos de um problema ou de uma situação. Recomenda-se a pesquisa exploratória quando há pouco conhecimento sobre o problema a ser estudado (CERVO; BERVIAN; DA SILVA, 2007).

No que diz respeito aos procedimentos técnicos adotados, esta dissertação se classifica como uma pesquisa bibliográfica, pois se baseia no conteúdo de normas técnicas de Segurança da Informação aplicadas ao tema.

Entende-se que a pesquisa bibliográfica, em termos genéricos, é um conjunto de conhecimentos reunidos de obras de toda natureza. Tem como finalidade conduzir o leitor à pesquisa de determinados assuntos, proporcionando o saber. Ela é fundamentada em vários procedimentos metodológicos, desde a leitura até como fichar, organizar, arquivar, resumir o texto e a base para as demais pesquisas. Todo tipo de estudo deve, primeiramente, ter o apoio e o respaldo da pesquisa bibliográfica, mesmo que esse se baseie em outro tipo de pesquisa, seja de campo, de laboratório, documental ou pura, pois, pesquisa bibliográfica tanto pode conduzir um estudo em si mesmo, quanto constituir-se em uma pesquisa preparatória para outro tipo de pesquisa (FACHIN; BARROS, 2017).

Organização do trabalho

Esta dissertação apresenta uma análise dos processos e subprocesso do framework CIS Controls da norma ISO/IEC 27002 e do NIST CF para implementação de um manual de boas práticas para o setor da Telemedicina.

Na conceituação foram definidas as vantagens de utilizarmos normas técnicas de segurança da informação com o propósito de utilizarmos melhores práticas para a segurança da informação nas organizações. Na conveniência das políticas e regulamentos para a segurança da informação mostra a importância das organizações identifiquem seus requisitos e estabeleçam uma política de segurança da informação que corroboram para o processo de segurança da informação da organização. Foram citadas as funcionalidades do CIS Controls,

sendo um dos frameworks mais aceitos no mercado, ressaltando os grupos de controles, grupos de implementação, o Nist Cybersecurity Framework e o mapeamento para a ISO/IEC 27002 e para o NIST CF. Foi mencionadas a história da ISO/IEC 27001 e da ISO/IEC 27002, foi detalhado o Sistema de Gestão de Segurança da Informação que irá aparecer na implantação da ISO/IEC 27001. Foi criado um paralelo da Gestão de Riscos com a Política de Segurança da Informação devido a Gestão de riscos fazer parte da política de segurança da informação. O ciclo PDCA foi mencionado pois realiza o controle e melhoria contínua dos processos sendo indispensável para toda organização.

Para isso foi realizado um mapeamento sistemático da literatura com a finalidade de buscar o que existe sobre este tema ajudando na construção do manual de boas práticas para os sistemas de telemedicina. No mapeamento sistemático da literatura foi criada uma string de busca com as strings Telemedicina ou Telemedicine, Segurança da Informação ou Information Security, ISO/IEC 27001 ou ISO/IEC 27002. Em seguida foi realizada uma avaliação crítica dos artigos encontrados no período de janeiro de 2021 a junho de 2022 com critérios de aceitação. Foi realizada a montagem de uma tabela dos autores com título, assunto, controles e requisitos dando subsídios para encontrarmos características particulares dos sistemas de telemedicina. A partir dessas peculiaridades foi montado um manual de boas práticas utilizando o CIS Controls como referência para os sistemas de telemedicina.

1 **CONCEITUAÇÃO**

1.1 **Normas técnicas de Segurança da Informação**

As normas técnicas de Segurança da Informação são documentos desenvolvidos por organizações interessadas no tema ou grupo de pesquisadores para fornecer os princípios gerais, melhores práticas e diretrizes relacionadas à implementação da gestão da Segurança da Informação pelas organizações. As normas apoiam a produção de documentos ou procedimentos para gestão da Segurança e garantem sua uniformização, facilidade de compreensão, tendo em vista que toda a documentação foi concebida por um mesmo padrão.

A série 27000 de normas da International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) concentra-se nos requisitos, controles de segurança e orientação para implementação de um SGSI na organização.

1.2 **A Conveniência das políticas e regulamentos para a Segurança da Informação**

Toda organização que se importa com a Segurança da Informação necessita de uma política de segurança da informação fazendo com que toda a metodologia para realizar a segurança da informação deva ser preparada, estabelecida e preservada. Estas políticas, processos e procedimentos estabelecem como serão efetivadas as diretrizes, as metas e serem alcançadas e o rumo que a organização irá tomar com os controles a serem implementados no cuidado com a informação.

Segundo a norma ISO/IEC 27002, o processo de Segurança da Informação está relacionado diretamente com a construção de políticas que atenderão de maneira eficaz cada organização com suas particularidades.

É primordial que a organização identifique seus requisitos para a Segurança da Informação sendo as principais fontes a avaliação de riscos, os estatutos, a legislação vigente e as cláusulas contratuais que a organização possui com seus parceiros e o grupo de princípios particulares e os requisitos do negócio.

Várias organizações na área da saúde possuem dificuldades para a criação e desenvolvimento de políticas de segurança da informação. Gestores dessas unidades de saúde relatam que a segurança da informação é importante, mas nenhuma delas possui uma política eficaz para essa segurança. Possuem no ambiente computacional algumas regras gerais de controles.

Os gestores, na sua maioria, consideram que falta conhecimento de como mapear as necessidades para se desenvolver uma política de segurança da informação formal (ALBERTIN; PINOCHET, 2010).

A Segurança da informação cobre uma área maior que a área da Tecnologia da Informação, contudo, esta área progressivamente mais, armazena e processa as informações da organização. Dessa forma, o atendimento dos objetivos estratégicos e as atividades operacionais da organização são cada vez mais dependentes da tecnologia da informação e da informação.

Por conseguinte, é mandatório que a informação seja protegida e que diretrizes sejam definidas com o propósito de que esta proteção disponha de regras que possam direcionar estrategicamente e operacionalmente a sua essência.

1.3 **As normas da família ABNT NBR ISO/IEC 27000**

A ABNT NBR ISO/IEC 27000 é um conjunto de normas e padrões que objetiva o tratamento do Sistema de Gestão de Segurança da Informação (SGSI).

1.4 **História da ISO/IEC 27001**

Começou com o padrão BS7799 divulgado pelo BSI Group em 1995. O Departamento de Comércio e Indústria (DTI) do Governo do Reino Unido escreveu e foi feito em várias seções.

Na primeira seção foram publicadas as melhores práticas para a Gestão de Segurança da Informação, revisada em 1988; os órgãos de padronização em todo o mundo decidiram adotar em 2000 pela ISO o ISO/IEC 17799, Tecnologia da Informação - Código de Prática de

Segurança da Informação. Em 2005 a ISO/IEC 17799 sofreu revisão sendo incorporada na série de padrões ISO 27000 e chamada de ISO/IEC 27002 no ano de 2007.

A segunda seção do BS7799 foi publicada inicialmente pela BSI no ano de 1999, sendo chamada BS 7799 Parte 2, Sistema de Gerenciamento de Segurança da Informação - Especificação com orientação para uso. Já a BS 7799-2 foi desenvolvida como implementar um Sistema de Gerenciamento de Segurança da Informação (SGSI), que se referia à parte da estrutura de gerenciamento de segurança da informação e os controles sendo identificados na BS7799-2. Mais tarde, passou a ser chamada de ISO/IEC 27001:2005 e a BS 7799 Parte 2 foi incorporada pela ISO como ISO/IEC 27001 em 2005.

A parte 3 da BS 7799, publicada em 2005, cobriu a análise de gerenciamento de risco e está em conformidade com a ISO/IEC 27001:2005. Pouca utilização e referência foram realizadas nos padrões BS em consonância com a ISO/IEC 27001.

1.5 **ISO/IEC 27002**

A norma NBR ISO/IEC 27002 faz a estruturação da administração da segurança da informação. Nela são delineados os elementos que devem ser levados em conta para a devida proteção da informação de acordo com um código de boas práticas que norteiam a informação. Esta norma conceitua que controles complementares e conselhos adicionais podem ser indispensáveis. Apesar de mostrar não ser dependente dos controles adicionais, esta norma aconselha a agregação dos controles.

O objetivo da ISO/IEC 27002 é determinar princípios e diretrizes para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Nesta norma, os objetivos fornecem diretrizes globais no que se refere às metas normalmente adotadas na gestão da segurança da informação.

Instituições de tamanhos e tipos diferenciados, podendo ser o setor público e privado, instituições comerciais e sem fins lucrativos, recolhem, processam, guardam e propagam informações em formatos diversos, podendo ser físico, eletrônico e verbal.

1.6 **O Sistema de Gestão de Segurança da Informação (SGSI)**

Com o início da implementação da ABNT NBR ISO/IEC 27001 o Sistema de Gestão de Segurança da Informação (SGSI) aparece como uma abordagem sistemática para a gestão da proteção de dados de uma organização. O SGSI representa um conjunto de políticas, procedimentos e outros controles que irão definir as regras de Segurança da Informação de uma organização.

Os tipos de regras (controles) para a Segurança da Informação, que serão implementados em uma organização, estão relacionados com os resultados da avaliação de riscos e nos requisitos das partes interessadas. Sendo assim, os controles utilizados na Segurança da Informação serão empregados adequando-os às necessidades específicas. Vários controles são necessários para cada risco.

1.7 **A Gestão de Riscos e a Política de Segurança da Informação**

A Criação da Política de Segurança da Informação deverá ser criada primeiro para que depois a Gestão de Risco seja definida e implantada tendo o efeito desejado de acordo com a Política de Segurança da Informação concebida.

A NBR ISO/IEC 27005 que, trata da gestão de riscos de segurança da informação, recomenda que a gestão de risco faça parte da gestão de segurança da informação sendo definida onde será empregada: em toda a organização, em uma parte da organização, em um sistema dessa organização ou em controles especificados.

Ao tratar da análise, da avaliação e do tratamento de riscos, a ISO/IEC 27002 aconselha que a gestão de riscos esteja contida nas atividades de gestão de segurança da informação sendo aplicada nas operações rotineiras como também na implementação.

Para que a gestão de riscos seja eficaz é recomendado que a análise/avaliação de riscos no ambiente da segurança da informação possua um escopo bem definido. Este escopo e limites da gestão de riscos da segurança da informação estão vinculados ao escopo e limites do Sistema de Gestão de Segurança da Informação.

Com isso, a gestão de riscos será uma parte do Sistema de Gestão de Segurança da Informação fazendo com que este sistema se mantenha ininterrupto.

É recomendável que regularmente sejam realizadas análises e avaliações para que sejam considerada as modificações nas exigências da segurança da informação e no próprio risco, ou seja, vulnerabilidades, ativos, impactos, ameaças, avaliação de riscos e quando acontecer uma mudança relevante.

Sendo assim, a ISO/IEC 27002 aconselha a utilização de controles e o emprego da gestão de riscos para que a existência desses controles sejam identificáveis e relevantes.

1.8 **O Ciclo PDCA**

Conceito que se encontra incorporado à ISO/IEC 27001 e ISO/IEC 27002 desenvolvido há quase 60 anos por um famoso consultor em gestão da qualidade chamado William Edwards Deming. É um método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos. Também conhecido como círculo/ciclo/roda de Deming ou PDCA.

Este ciclo é composto por quatro estágios conforme mostrado a seguir:

Planejar (Plan) – Antes de começar a executar o processo é preciso planejar as atividades, definir a meta e o método.

Executar (Do) – Implementar o plano, executar o processo e fazer o produto. Nesta etapa começa-se a implementar a segurança da informação, continuidade do negócio, procedimentos de qualidade ou qualquer que seja o foco na ISO que esteja sendo abordado.

Checar (check) – Realiza o monitoramento do sistema e faz a medição para verificar se atingiu o que foi planejado, se os objetivos foram alcançados.

Agir (ackt) – Ações corretivas são realizadas sobre os resultados alcançados e os resultados esperados. Faz a análise das diferenças para determinar suas causas.

1.9 **CIS Controls**

Concebido pelo Center for Internet Security (CIS), consiste em um conjunto de práticas que são recomendadas para a área de segurança da informação que podem ajudar a mitigar ataques mais generalizados. Este framework foi desenvolvido pelo Centro para a Segurança da Internet, no setor da Segurança da Informação, onde faz recomendações atuais para auxiliar as organizações na postura de Segurança da Informação diante de determinados controles de segurança da informação.

O Center for Internet Security procura manter o CIS Controls atualizado, com tecnologias em evolução, base de comentários e cenários de ameaças em permanente mudança. Devido às organizações atualmente utilizarem seus serviços de Tecnologia da Informação em nuvem, e devido ao aumento dos trabalhos remotos foi verificado que deveriam revisar os controles para garantir que as advertências ofereçam orientações para uma segurança da informação eficaz.

O CIS Controls é um dos padrões mais aceitos no mercado em relação à padronização de procedimentos de Segurança da Informação sendo um framework genérico e universalmente aplicável. Ele separa os controles em três categorias: básico, fundamental e organizacional, independente da organização e setor em que será utilizado. Possui uma orientação herdada da versão anterior que faz a priorização da utilização dos controles conhecida como Grupo de Implementação ajudando as organizações a catalogar e destacar seus recursos de segurança da informação, se beneficiando do valor dos controles do CIS. Apresenta 18 controles sendo os 6 primeiros obrigatórios em todas as organizações para que possa ser realizada a preparação para a defesa cibernética. Os 6 primeiros controles do CIS são: 1) Inventário e Controle de Ativos. 2) Inventário e Controle de Ativos de Software. 3) Proteção de dados. 4) Configuração segura de ativos e softwares corporativos. 5) Gerenciamento de contas e 6) Gerenciamento de controle de acesso. Seguindo as referências do CIS, diante desses 6 primeiros controles, grandes benefícios são observados mesmo sendo estes os únicos controles que as organizações implementem em suas políticas. É importante salientar que o CIS não abrange apenas software, hardware e dados, mas também processos e pessoas.

Os grupos de implementação são definidos como referências indicadas para favorecer a implementação dos controles CIS. As organizações que utilizam o CIS são orientadas a utilizar primeiramente o grupo de implementação 1, seguido pelo grupo de implementação 2 e

por fim utilizar o grupo de implementação 3. As organizações que possuem recursos limitados e que se enquadram na sensibilidade de dados baixa devem implementar os subcontroles que se apresentam na categoria grupo de implementação 1, IG1, em que toda organização se defende de ataques mais comuns. Já às organizações que possuem recursos moderados e apresentam maior exposição ao risco para tratar dados e ativos mais confidenciais é recomendado implementar os controles do grupo de implementação 2, IG2, juntamente com os controles do grupo 1, IG1, onde as organizações que empregam este nível intermediário de proteção processam e armazenam informações confidenciais podendo resistir a um curto período de interrupção de serviço. Nas organizações com recursos significativos e com exposição alta de risco existe a necessidade de utilizar os subcontroles do grupo de implementação 3, IG3, juntamente com o G1 e o IG2 capazes de mitigar ataques sofisticados. Este nível de proteção realiza o tratamento da disponibilidade de serviços, e a integridade e confidencialidade dos dados sensíveis.

1.10 **NIST Cybersecurity Framework**

O NIST CF (Cybersecurity Framework) consiste em uma lista de diretrizes, padrões e práticas construídas para auxiliar as organizações a administrar e mitigar o risco cibernético de todos os tipos, podendo abranger roubo de senha, malware, ataques DDoS, ataques de phishing, engenharia social, interceptação de tráfego e outros tipos de ataques. É um instrumento importante para apoiar a prática de gerenciamento de riscos de toda organização, ajudando o processo permanente de gerenciamento de riscos cibernéticos. Os níveis de riscos cibernéticos podem ser mensurados pelas equipes de segurança utilizando esta estrutura, indicar prioridades de segurança, alinhar os objetivos de segurança ao risco e estabelecer orçamento de segurança para mitigar as ameaças.

O NIST CF possui cinco funções que são distribuídas em um total de 23 categorias. As funções, são as seguintes:

a) Identificar. Produzir uma compreensão organizacional com o propósito de controlar os riscos de segurança cibernética para ativos, dados, recursos e sistemas;
b) Proteger. Implementar e desenvolver as salvaguardas pertinentes com a finalidade de garantir a entrega de serviços de infraestrutura crítica;

c) Detectar. Implementar e desenvolver as atividades adequadas para apontar o acontecimento de um evento de segurança cibernética;
d) Responder. Implementar e desenvolver as atividades compatíveis para agir em relação a um evento de segurança cibernética identificada.
e) Recuperar. Implementar e desenvolver as atividades adequadas para manter estratégia de resiliência e restabelecer quaisquer serviços ou recursos que foram danificados devido a uma ocorrência de segurança cibernética.

1.11 **CIS Controls mapeado para ISO/IEC 27002:2022 e para o NIST CF**

O CIS Controls possui compatibilidade com outros padrões de conformidade e segurança, sendo que as organizações utilizam este framework como um auxílio para atingir a conformidade. Diante disso, o Center for Internet Security apresenta um mapeamento do CIS Controls para a ISO/IEC 27002 e para o NIST CF, além de outros importantes frameworks de Segurança utilizados no mercado. O mapeamento é disponibilizado em https://www.cisecurity.org/cybersecurity-tools/mapping-compliance.

2 **MAPEAMENTO SISTEMÁTICO DA LITERATURA**

O Mapeamento Sistemático da Literatura ou revisão de escopo (scoping review) é utilizado quando não é necessário responder com profundidade questões específicas, mas sim uma visão geral mais ampla de determinada área (MOHER; SHEKELLE, 2015). Este tipo de estudo tem, em geral, um foco na categorização do tópico de pesquisa de interesse. Considera-se também a condução de mapeamentos sistemáticos em tópicos de pesquisa nos quais poucas evidências são disponíveis na literatura (KITCHENHAM; CHARTERS, 2007).

Um Mapeamento Sistemático (MS) tem a função de ser uma revisão ampla dos estudos primários existentes em um tópico de pesquisa específico que visa identificar a evidência disponível nesse tópico. Assim, um MS é um estudo secundário que tem como objetivo identificar e classificar a pesquisa relacionada a um tópico amplo de pesquisa (KITCHENHAM; CHARTERS, 2007).

O Mapeamento Sistemático da literatura tem a função de detectar, classificar e analisar todas as pesquisas que estão disponíveis e são pertinentes para um questionamento de uma pesquisa, área ou fenômeno específico (KITCHENHAM, 2007). Dessa forma, as abordagens qualitativas e revisões sistemáticas admitem, através da análise da literatura, demarcar, encontrar, examinar e sumarizar as questões da análise (DE-LA-TORRE-UGARTE-GUANILO; TAKAHASHI; BERTOLOZZI, 2011).

De acordo com (PETERSEN et al., 2008) as etapas a serem seguidas para se realizar um Mapeamento Sistemático são: Definição do objetivo da busca, condução da busca, exibição dos documentos, classificação utilizando palavras chaves e extração dos dados e processos de mapeamento.

2.1 **Objetivo do Mapeamento Sistemático da Literatura**

Pesquisar e agrupar de forma sistemática a compreensão sobre as práticas de Segurança da Informação para os Sistemas de Telemedicina tendo como base as ISO/IEC 27001, ISO/IEC 27002 e o CIS Controls.

Desenvolver e apresentar um mapeamento que reúna e classifique os vestígios produzidos neste campo no intervalo definido do ano de janeiro de 2017 até junho de 2022 podendo ser utilizados em pelo menos duas formas complementares:

Na prática da Segurança da Informação na área da saúde;

Na investigação da Segurança da Informação nos Sistemas de Telemedicina.

2.2 **Objetivo Específico do Mapeamento Sistemático da Literatura**

Realizar uma pesquisa do mapeamento sistemático sobre a Segurança da Informação nos Sistemas de Telemedicina;

Identificar indicadores que corroborem os tópicos de pesquisa analisados, o cenário metodológico, como é realizada a segurança da informação, os principais resultados obtidos e as melhores evidências.

Pesquisar e classificar de forma sistemática, os objetos de pesquisa, o ambiente da metodologia, os principais resultados e o tipo de segurança da informação que é mais realizado.

Com o agrupamento dos resultados obtidos, sugerir um mapeamento que faça a junção do conhecimento da área, demonstre boas práticas e novas áreas de pesquisa.

2.3 **Elaboração da pergunta de pesquisa**

A etapa de fundamental importância para verificar o que está sendo criado em relação ao problema proposto é a elaboração da pergunta tendo que ser bem delineada (PEREIRA; BACHION, 2006). Para ajudar na tomada de decisão sobre o que deve ou não ser incluído na revisão é necessário criar uma pergunta bem formulada. Para facilitar na elaboração da pergunta de pesquisa foi empregada o critério PICOC (Population, Intervention, Comparison, Outcome, Context) (KITCHENHAM, 2007), resumido na Tabela 1.

a) População (Population): Para qual população particularizada ou grupo de populações a revisão se enquadra? Neste cenário, seria para a segurança da

informação voltada para a telemedicina utilizando como base a ISO/IEC 27001, ISO/IEC 27002 e o CIS Controls.

b) Intervenção (Intervention): A intervenção é procedimento, metodologia, tecnologia ou a ferramenta que analisa um problema específico, e estabelece diretrizes para resolvê-los. Sendo assim, a intervenção tem o papel de ser um facilitador quanto a segurança da informação da telemedicina.

c) Comparação (Comparison): Este é o procedimento, técnica, metodologia ou ferramenta com que a intervenção está sendo confrontada. Neste estudo, a comparação é relevante pois o objetivo desse estudo é realizar comparações realizando um mapeamento do que existe e do que não existe do assunto por meio de uma pesquisa exploratória.

d) Resultados (Outcomes): Os resultados devem se relacionar com a segurança da informação nos sistemas de telemedicina. Neste caso, como é realizada a segurança da informação para a telemedicina.

e) Contexto (Context): Contexto em que é realizado este estudo. Neste caso, o contexto compreende a área da telemedicina.

Quadro 1 - Componentes da pergunta de pesquisa, seguindo o critério PICOC

Descrição	**Abreviação**	**Componentes**
População (Population)	**P**	Telemedicina
Intervenção (Intervention)	**I**	Segurança da Informação nos Sistemas de Telemedicina
Comparação (Comparison)	**C**	Tomando como base a ABNT NBR ISO 27001/2 e o CIS Controls
Resultados (Outcomes)	**O**	Características da Segurança da Informação na Telemedicina
Contexto (Context)	**C**	Área na qual a Telemedicina será contemplada pela Segurança da Informação

Fonte: O autor, 2021.

2.4 **Localização e seleção das publicações**

Com o objetivo de eleger as publicações que irão fazer parte do Mapeamento Sistemático da Literatura foram selecionadas as seguintes bases de dados eletrônicas: ACM digital library, IEEE explore, PubMed, Portal Regional BVS e Scopus.

Quadro 2 - Bases de dados eletrônicas.

Fonte de Pesquisa	Endereço Eletrônico
ACM digital library	https://dl.acm.org/
IEEE explore	https://ieeexplore.ieee.org/Xplore/home.jsp
PubMed	https://pubmed.ncbi.nlm.nih.gov/
Portal Regional BVS	https://bvsalud.org/
Scopus	https://www.scopus.com/standard/marketing.uri

Fonte: O autor, 2021.

2.5 **Estratégia de busca**

O período de busca de periódicos nacionais e internacionais foi de janeiro de 2017 a junho de 2022, para selecionar os artigos mais atuais, utilizando as seguintes palavras-chave, de acordo com as questões de pesquisa: “Segurança da Informação”, “Telemedicina”, “ISO/IEC 27001” e “ISO/IEC 27002”. Em relação ao idioma, a busca bibliográfica não se restringiu aos trabalhos publicados em alguns países específicos sendo todos os continentes contemplados.

2.6 **String de busca**

A partir das palavras-chave desenvolveu-se uma string de busca ou expressões de busca, usando os operadores booleanos OR e AND.

("Telemedicina" OR "Telemedicine") OR ("Segurança da Informação" OR "Information Security") AND ("ISO/IEC 27001" OR "ISO/IEC 27002") OR “Pesquisa” OR “Research”.

2.7 **Avaliação Crítica dos Artigos**

Esta avaliação se destina a estabelecer quais os artigos serão válidos para a revisão, sendo utilizados os critérios de aceitação de seleção dos artigos. Os artigos que não cumpriram os critérios de busca foram descartados da revisão.

2.8 Critérios de Aceitação

Os critérios utilizados para a seleção foram artigos, periódicos nacionais e internacionais, resoluções, leis, portarias, manuais do governo, teses e dissertações sobre o tema abordado. A busca incluiu os artigos públicos em português, espanhol e inglês e de outros países no período compreendido entre janeiro de 2017 a junho de 2022.

Os parâmetros de exclusão foram artigos que não disponibilizaram o texto completo e que não se enquadravam no tema Telemedicina ou Telemedicine, Segurança da Informação ou Information Security, ISO/IEC 27001, ISO/IEC 27002 e Sistema de Gestão de Segurança da Informação ou Information Security Management System.

2.9 **Quadro dos autores com título, assuntos, controles e requisitos**

Os artigos selecionados foram separados por ano de publicação, citação, assuntos, controles e requisitos na quadro 3. Importante destacar que todo artigo obrigatoriamente possui um ou mais assunto(s), podendo haver artigos com controle(s) e com requisito(s) como também podendo aparecer artigos com controle(s) e sem requisito(s) como também podendo

existir artigos sem controle(s) e com requisito(s) e finalizando com artigos sem controle(s) e sem requisito(s).

Assuntos abordados: Questões de segurança da informação para telemedicina (A1), O papel da tecnologia da informação na área da saúde (A2), A política de tecnologia da informação na área da saúde (A3), A tecnologia da segurança da informação para telemedicina (A4), A metodologia de segurança da informação para telemedicina (A5), A conformidade regulatória de segurança da informação para telemedicina (A6) e A ética da segurança da informação para telemedicina (A7).

Controles de Segurança da Informação: Criptografia de ponta a ponta (C1), Privacidade das informações (C2), Confidencialidade das informações (C3), Acesso individualizado (C4), Controle de autenticação (C5), Sistema de validação de transferência de arquivos (C6), Sistema de armazenamento seguro (C7), Assinatura digital (C8) e Rastreabilidade das informações (C9).

Requisitos de Segurança da Informação: Senha de alta complexidade (R1), Cadastro dos usuários (R2), Acesso criptografado (R3), Gerenciamento de vulnerabilidades (R4), Aplicativos de mensagens (R5) e o Armazenamento seguro dos dados (R6).

Quadro 3 – Artigos Selecionados (continua)

#	Ano	Título e Autores	Assuntos	Controles	Requisitos
1	2017	The uncap experience in developing ICT for health: "HTA by design" (ANZIVINO; et al., 2017).	A2 e A3		
2	2017	Application of I-COMO device towards geographic disease enrichment pattern revealed from electronic medical record at a large Urban academic medical center (DANIELETTO; LI; DUDLEY, 2017).	A1, A2 e A4	C1, C2, C3 e C7	R1, R2, R3 e R6
3	2017	Research for Building High Performance Communication Service Based on Netty Protocol in Smart Health (DUAN, 2017).	A1 e A4	C1, C3 e C5	R3
4	2017	Addressing challenges in promoting healthy lifestyles: the al-chatbot approach (FADHIL; GABRIELLI; KESSLER, 2017).	A4	C1, C2, C3 e C4	R2 e R3
5	2017	Protecting Future Maritime Communication (FRØYSTAD; BERNSMED; MELAND, 2017).	A1 e A2	C1, C2, C3, C4, C5, C6, C7 e C8	R1, R2, R3, R4, R5 e R6
6	2017	An efficient secure ECG compression based on 2D-SPIHT and SIT algorithm (JATI; et al., 2018).	A4	C1 e C3	R3
7	2017	2017 - CareNet: Building a Secure Software-defined Infrastructure for Home-based Healthcare (LI et al., 2017).	A1, A2, A4 e A6	C1, C3, C4, C5 e C7	R1, R2, R3 e R6
8	2017	A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine (MURILLO-ESCOBAR; et al., 2017).	A1 e A4	C1, C2, C3, C4 e C5	R3
9	2017	Validating the Tele-diagnostic Potential of Affordable Thermography in a Big-data Data-enabled ICU (SETHI et al., 2017).	A4 e A5		
10	2018	SD-WAN Source Route Based on Protocol-oblivious Forwarding (CHEN; et al., 2018).	A4		

Quadro 3 – Artigos Selecionados (continuação)

#	Ano	Título e Autores	Assuntos	Controles	Requisitos
8	2017	A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine (MURILLO-ESCOBAR; et al., 2017).	A1 e A4	C1, C2, C3, C4 e C5	R3
9	2017	Validating the Tele-diagnostic Potential of Affordable Thermography in a Big-data Data-enabled ICU (SETHI et al., 2017).	A4 e A5		
10	2018	SD-WAN Source Route Based on Protocol-oblivious Forwarding (CHEN; et al., 2018).	A4		
11	2018	Industry-Academia Panel: Transforming Healthcare with IT (KISHORE; et al., 2018).	A2	C2	R3
12	2018	A Gamification Engine Architecture for Enhancing Behavioral Change Support Systems (LITHOXOIDOU et al., 2018).	A5		
13	2018	Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine (MACARTY; et al., 2018).	A4	C1 e C3	R3
14	2018	Social Networking App Use Among Primary Health Care Professionals:Web-Based Cross-Sectional Survey (MARIN-GOMEZ; et al., 2018).	A1 e A5		
15	2018	Health Recommender System design in the context of CAREGIVERSPRO-MMD Project (OLIVA-FELIPE; et al., 2018).	A4		
16	2018	Solving Data Integration Problems in Medical Imaging System: A Case Study in Almazov National Medical Research Centre (RADCHENKO; et al., 2018).	A1 e A5	C3 e C9	R3
17	2018	Practical and secure telemedicine systems for user mobility (REZAEIBAGHA; MU, 2018).	A4	C3	R3
18	2018	Visualizing Collaboration Characteristics and Topic Burst on International Mobile Health Research: Bibliometric Analysis (SHEN; et al., 2018).	A1 e A5		
19	2018	IEEE Access Special Section Editorial: Information Security Solutions for Telemedicine Applications (SINGH; et al., 2018).	A1 e A4	C1, C3, C7 e C9	R1, R2, R3 e R6
20	2018	An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing (KUMAR, 2018).	A1 e A5	C1, C3 e C5	R3
21	2019	IoT-based healthcare systems: a survey (HMEIDI; MRAYAN; KHAMAYSEH, 2019).	A4	C2 e C7	R3 e R6
22	2019	Multi-source heterogeneous data fusion based on perceptual semantics in narrow-band Internet of Things (LIU, 2019).	A4		
23	2019	Citizen Attitude: Potential Impact of Social Media Based Government (MADYATMADJA; NINDITO; PRISTINELLA, 2019).	A1, A2 e A5	C2, C3 e C5	R3
24	2019	Mobile Health System Framework in India (PAI; ALATHUR, 2019).	A1, A2 e A3		
25	2019	Privacy and protection of medical images ROI using SPLSB and bit-plane based watermarking (RUPA; DEVI, 2019).	A1 e A5	C1 e C3	R3
26	2019	Exile Within Borders: Understanding the Limits of the Internally Displaced People (IDPs) in Iraq (SABIE; et al., 2019).	A2		
27	2019	Lightweight Cryptography Techniques for MHealth Cybersecurity (SHAHBODIN et al., 2019).	A1 e A4	C1, C2 e C3	
28	2019	eHealth and telemedicine: Practices and beliefs among healthcare professionals and medical students at a medical university (WERNHART; GAHBAUER; HALUZA, 2019).	A1 e A2	C2	R1
29	2019	Assessment of the impact of teledermatology using discrete event simulation (ZEHROUNI et al., 2019).	A1 e A5		
30	2020	A Robust Quasi-Quantum Walks-Based Steganography Protocol for Secure Transmission of Images on Cloud-Based E-healthcare Platforms (ABD-EL-ATTY; et al., 2020).	A4	C1 e C7	R6
31	2020	Region-based Selective Compression and Selective Encryption of Medical Images (AHMAD; SHIN, 2020).	A4	C1	R3
32	2020	Measuring the awareness of health care providers at Benghazi Medical Center for Health Informatics (ALBAYOOD,et al.2020).	A1 e A2		

Quadro 3 – Artigos Selecionados (continuação)

#	Ano	Título e Autores	Assuntos	Controles	Requisitos
33	2020	Public and private healthcare organizations: a socio-technical model for identifying cybersecurity aspects (ANASTASOPOULOU et al., 2020)	A1 e A5		
34	2020	To Infinity and Beyond: The Past, Present, and Future of Tele-Anesthesia (BRIDGES; MCSWAIN; WILSON, 2020).	A1 e A6	C1 e C7	R3 e R6
35	2020	Implementation and Application of Telemedicine in China: Cross-Sectional Study (CUI; et al., 2020).	A2		
36	2020	Risk management-based security evaluation model for telemedicine systems (DONG-WON, 2020).	A1, A2, A3 e A5		
37	2020	A Review of Data Privacy Techniques for Wireless Body Area Networks in Telemedicine (GORBACH et al., 2020).	A1 e A4	C1, C2 e C3	R1 e R3
38	2020	Complex Methodological Approach to Introduction of Modern Telemedicine Technologies into the Healthcare System on Federal, Regional and Municipal Levels (GORELOV; et al., 2020).	A2 e A5		
39	2020	A Telemedicine Platform to Care for Patients in a Biocontainment Unit (GOSSEN; et al., 2020).	A1 e A4		
40	2020	Telemedicine and Medical Education in the Age of COVID-19 (JUMREORNVONG; et al., 2020).	A2 e A7	C2	R3
41	2020	Revisiting Health Information Technology Ethical, Legal, and Social Issues and Evaluation: Telehealth/Telemedicine and COVID-19 (KAPLAN, 2020).	A2 e A7		
42	2020	Implementation of Synchronous Telemedicine into Clinical Practice (KHOSLA,2020).	A2 e A4		
43	2020	A Lightweight Internet Sharing Scheme for Sectional Medical Images according to Existing Hospital Network Facilities and Basic Information Security Rules (LIANG, 2020).	A4		
44	2020	Telemedicine adoption issues in the United States and Brazil: Perception of healthcare professionals (LUCIANO et al., 2020).	A2		
45	2020	Use of the HoloLens2 Mixed Reality Headset for Protecting Health Care Workers During the COVID-19 Pandemic: Prospective, Observational Evaluation (MARTIN; et al., 2020).	A4	C3	R1
46	2020	Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine (MA et al.,20).	A4	C1 e C2	R1 e R3
47	2020	A critical review of emerging technologies for tackling COVID-19 pandemic (MBUNGE; et al., 2020).	A4	C2	
48	2020	A technological and innovative approach to COVID-19 in Uruguay (MILANO; VALLESPIR; VIOLA, 2020).	A4	C2	
49	2020	Use of mobile health technologies for postoperative care in pediatric surgery: A systematic review (NGUYEN; et al., 2020).	A2	C3	R3
50	2020	A Lightweight Internet Sharing Scheme for Sectional Medical Images according to Existing Hospital Network Facilities and Basic Information Security Rules (QIAO; et al., 2020).	A1 e A4		
51	2020	An Extensive Analysis of the Ad Hoc Network (RASHID; ISAWI; MAHMOOD, 2020)	A1 e A4		
52	2020	A framework for patient-centered telemedicine: Application and lessons learned from vulnerable populations (TALAL, 2020)	A4		
53	2020	CryptoLesion:A Privacy-preserving Model for Lesion Segmentation Using Whale Optimization over Cloud (TANWARet al.2020)	A2	C1, C2, C3 e C7	R1, R3 e R6
54	2020	Integration of Health and Public Transport Data to Enable Decision Support for Seniors to Reduce Risk of Infection with Communicable Diseases (URBAUER; FORJAN, 2020).	A4		
55	2020	Preliminary Analysis of The Application and Development of Big Data, Cloud Computing, IoT, Mobile Internet, AI, and Blockchain In The Power Scene (ZHANG; ZHAO; LI, 2020).	A4	C1, C2, C3 e C7	R3 e R6

Quadro 3 – Artigos Selecionados (continuação)

#	Ano	Título e Autores	Assuntos	Controles	Requisitos
56	2021	Prototype of multi-layer personal cardiac monitoring system for data interoperability problem (PRAMUKANTORO; GOFUKU, 2021).	A4		
57	2021	Construction of a Chaotic Map-Based Authentication Protocol for TMIS (DHARMINDER, 2021)	A2 e A4		
58	2021	FABEMD based Innovative Watermarking Method (ESWARAIAH, 2021)	A4	C1, C2 e C3	R3
59	2021	A holistic nonlinear framework for developing a national eHealth vision based on Moroccan experience (FAKHKHARI; et al., 2021)	A4	C2 e C7	R6
60	2021	A mixed-methods survey to explore issues with virtual consultations for musculoskeletal care during the COVID-19 pandemic (GILBERT, 2021)	A2		
61	2021	Medical and Legal Aspects of the Practice of Teledermatology in Spain. / Aspectos medicolegales de la práctica de la teledermatología en España (GÓMEZ ARIAS, 2021)	A2 e A7	C2, C3, C6 e C7	R6
62	2021	Secure Transmission of Medical Images using Improved Hybrid Cryptosystem: Authentication, Confidentiality and Integrity (HAFSA, 2021)	A4	C2, C3, C5 e C8	R3
63	2021	Access Control Design Based on User Role Type in Telemedicine System Using Ethereum Blockchain (HAMZAH; et al., 2021)	A4	C2 e C5	
64	2021	Blockchain-Enabled Telehealth Services Using Smart Contracts (HASAN, 2021)	A4	C1, C3, C5 e C7	R3, R4 e R6
65	2021	Attitude and potential benefits of modern information and communication technology use and telemedicine in cross-sectoral solid organ transplant care (HOLDERRIED, 2021)	A1, A2 e A4		
66	2021	A Review of Malicious Altering Healthcare Imagery using Artificial Intelligence (HUSSAIN, 2021)	A2 e A4		
67	2021	A Testbed for Implementing Lightweight Physical Layer Security in an IoT-based Health Monitoring System (HUSSAIN; et al., 2021)	A1 e A4		
68	2021	Telemedicine, privacy, and information security in the age of COVID-19 (JALALI, 2021)	A1, A2 e A3	C1, C2 e C3	R3 e R5
69	2021	Taipei Veterans General Hospital secure open-source telemedicine system-TeleCARE (KUAN, 2021)	A1 e A4	C1, C3, C5 e C7	R3, R5 e R6
70	2021	Using DWT-DCT-SVD Watermarking For Securing Medical Images (KUMAR; et al.,2021)	A1 e A4	C2 e C3	
71	2021	Towards a software system for spatio-temporal authorization (LAIL, 2021)	A2 e A3		
72	2021	Medical cooperative authenticated key agreement schemes with involvement of personal care assistant in telemedicine (LEE, 2021)	A1 e A4		
73	2021	A Smartcard-Based User-Controlled Single Sign-On for Privacy Preservation in 5G-IoT Telemedicine Systems (LIN, 2021)	A1 e A4	C1, C2, C3, C4 e C5	R1, R2, R3 e R6
74	2021	Secured telemedicine of medical imaging based on dual robust watermarking (MENDOZA; et al., 2022)	A1 e A4		
75	2021	Leveled Design of Cryptography Algorithms Using Cybernetic Methods for Using in Telemedicine Applications (NOROUZZADEH GIL MOLK, 2021)	A4	C1 e C2	R3
76	2021	A Risk Assessment Framework Proposal Based on Bow-Tie Analysis for Medical Image Diagnosis Sharing within Telemedicine (POLETO, 2021)	A1 e A5	C1, C2 e C8	R3
77	2021	Challenges and Solutions for Resilient Telemedicine Services (ROMANOVS; et al., 2021)	A2 e A5		
78	2021	A Review on Wireless Telemedicine Technology Challenges and Possible Solution (ROY, 2021)	A2		
79	2021	Towards the Use of Blockchain in Mobile Health Services and Applications (SANTOS, 2021)	A1 e A4		
80	2021	Network Architecture of Telemedicine System for Monitoring the Person's Condition (SOKOLOVA, 2021)	A1 e A4		
81	2021	Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic (SOLIMINI, 2021)	A1 e A7	C2 e C3	
82	2021	A comprehensive review on medical image steganography based on LSB technique and potential challenges (SHTAYT, 2021) R3	A4	C1 e C3	

Quadro 3 – Artigos Selecionados (conclusão)

#	Ano	Título e Autores	Assuntos	Controles	Requisitos
83	2021	Research on high-reliability intelligent-sensing health service support platform and key technologies based on Biometrics and blockchain security technology (TANG; et al., 2021)	A4		
84	2021	Impact of data protection regulation on Slovenian eHealth (TEPEJ JOCIC, 2021)	A6		
85	2021	Medical image encryption based on biometric keys and lower-upper decomposition with partial pivoting (WANG; et al., 2021)	A4	C1	R3
86	2021	A privacy protection scheme for telemedicine diagnosis based on double blockchain (WANG; et al., 2021)	A4		
87	2022	Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis (ALFAWSAN; et al., 2022)	A3		
88	2022	Best Practices for the Provision of Virtual Care: A Systematic Review of Current Guidelines (ANVARI; et al., 2022)	A5		
89	2022	Secure and resource-efficient communications for telemedicine systems (CHEN; et al., 2022)	A4	C1 e C5	R3
90	2022	Hospital based specialists' perspectives of teleconsultation use during the COVID-19 pandemic (CHOU, 2022)	A1 e A2		
91	2022	A State-Of-Art Model of Encrypting Medical Image Using DNA Cryptography and Hybrid Chaos Map - 2d Zaslavaski Map: Review (DEEPA, 2022)	A4	C1 e C3	R3
92	2022	Challenges in Telemedicine: Even When the Road is Hard, Never Give up (FILHO, 2022)	A4		
93	2022	A Novel Homomorphic Approach for Preserving Privacy of Patient Data in Telemedicine (IQBAL; et al., 2022)	A4	C1 e C2	R3
94	2022	Medical cooperative authenticated key agreement schemes with involvement of personal care assistant in telemedicine (LEE; et al., 2022)	A4		
95	2022	The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities (LIU; et al., 2022)	A1 e A4	C2, C5 e C7	R6
96	2022	Security of medical images for telemedicine: a systematic review (MAGDY; et al., 2022)	A1 e A4	C1	R3
97	2022	Tecnologias móveis em saúde: reflexões sobre desenvolvimento, aplicações, legislação e ética (MARENGO; et al., 2022)	A1 e A7	C2 e C4	
98	2022	Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda (POOL; et al., 2022)	A2		
99	2022	Analysis of Different Encryption Techniques used in Watermarking Algorithm for the Security of Medical Image (PULGAM, 2022)	A4	C1, C3, C6 e C7	R3 e R6
100	2022	Securing Multimedia using a Deep Learning based Chaotic Logistic Map (RUPA, 2022)	A4	C1 e C3	R3
101	2022	Secure Telemedicine System Design for COVID-19 Patients Treatment Using Service Oriented Architecture (SHAIKH, 2022)	A4	C6	R5
102	2022	7 Security and Privacy challenge in Smart Healthcare and Telemedicine systems (SHARMA; et al., 2022)	A4	C2, C5 e C7	
103	2022	Secure transmission and integrity verification for color medical images in telemedicine applications (SAYAH; 2022)	A4		
104	2022	The Road-ahead for E-healthcare 4.0: A Review of Security Challenges (TALATI, 2022)	A4	C2 e C3	
105	2022	Enhancing the Security of Medical Images in Telemedicine Using Region-based Crypto-Watermarking Approach (VERMA, 2022)	A1 e A4	C1, C2 e C3	R3
106	2022	Blockchain-based Secure Medical Data Management and Disease Prediction (WANG; et al., 2022).	A4	C2 e C5	R4 e R6
107	2022	A high-capacity and reversible patient data hiding scheme for telemedicine (ZHANG, 2022)	A4		

Fonte: O autor, 2023.

2.10 **Interpretação dos dados**

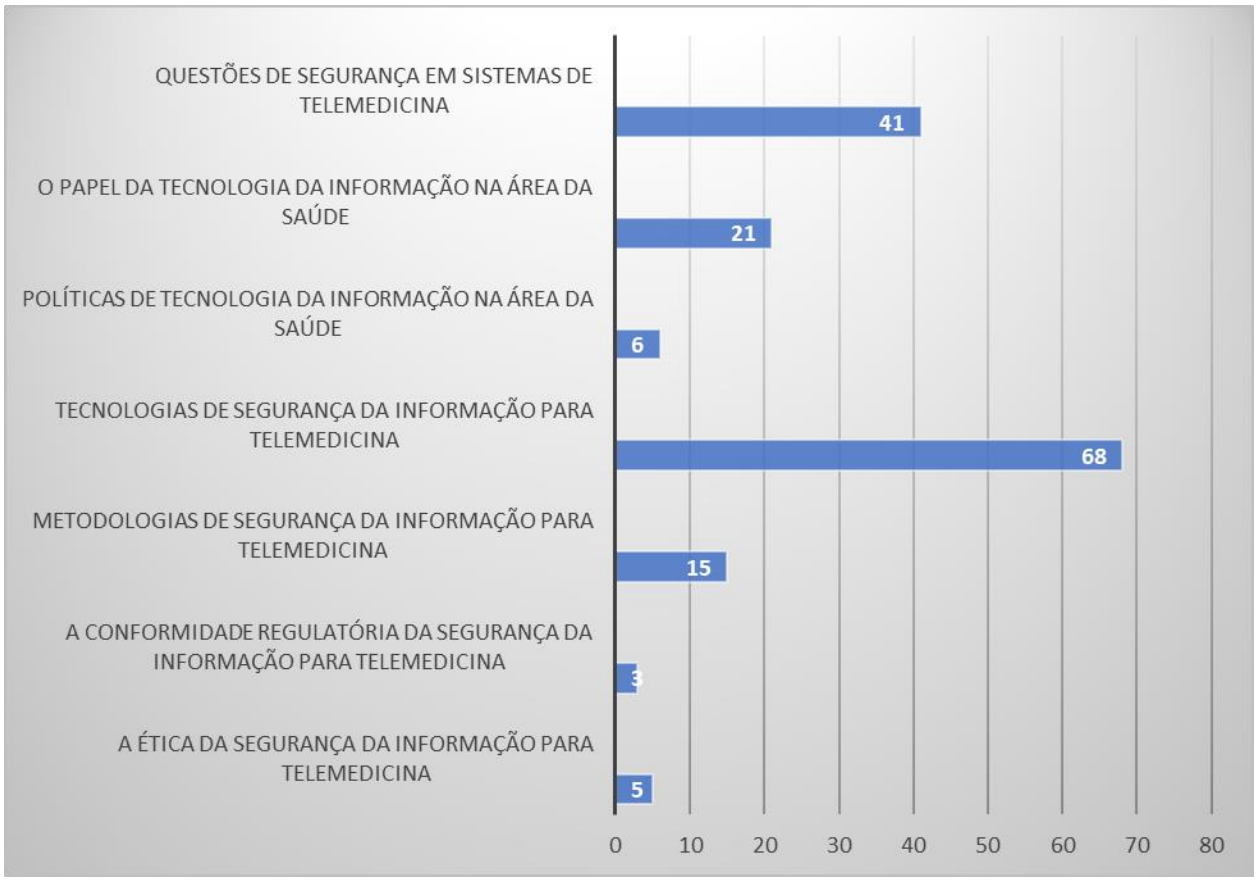
A revisão da literatura encontrou 107 artigos no período de busca entre janeiro de 2017 e junho de 2022.

Os artigos foram separados conforme os assuntos abordados, tais como: Questões de segurança da informação em sistemas de Telemedicina, o papel da tecnologia da informação na área da saúde, políticas de tecnologia da informação na área da saúde, tecnologias de segurança da informação para Telemedicina, metodologias de segurança da informação para Telemedicina, a conformidade regulatória da segurança da informação para a Telemedicina e a ética da segurança da informação para a Telemedicina.

2.11 **Resultados**

Como resultado da revisão foram encontrados 107 artigos na totalidade. Os assuntos abordados dos artigos encontrados, como mostrado na figura 1, foram: 41 artigos citaram sobre questões de segurança em sistemas de Telemedicina, 21 artigos citaram sobre o papel da tecnologia da informação na área da saúde, 6 artigos mencionaram sobre políticas de tecnologia da informação na área da saúde, 68 artigos relataram sobre tecnologias de segurança da informação para Telemedicina, 15 apontaram sobre metodologias de segurança da informação para Telemedicina, 3 artigos comentaram sobre a conformidade regulatória da segurança da informação para Telemedicina e 5 artigos citaram sobre a ética da segurança da informação para Telemedicina.

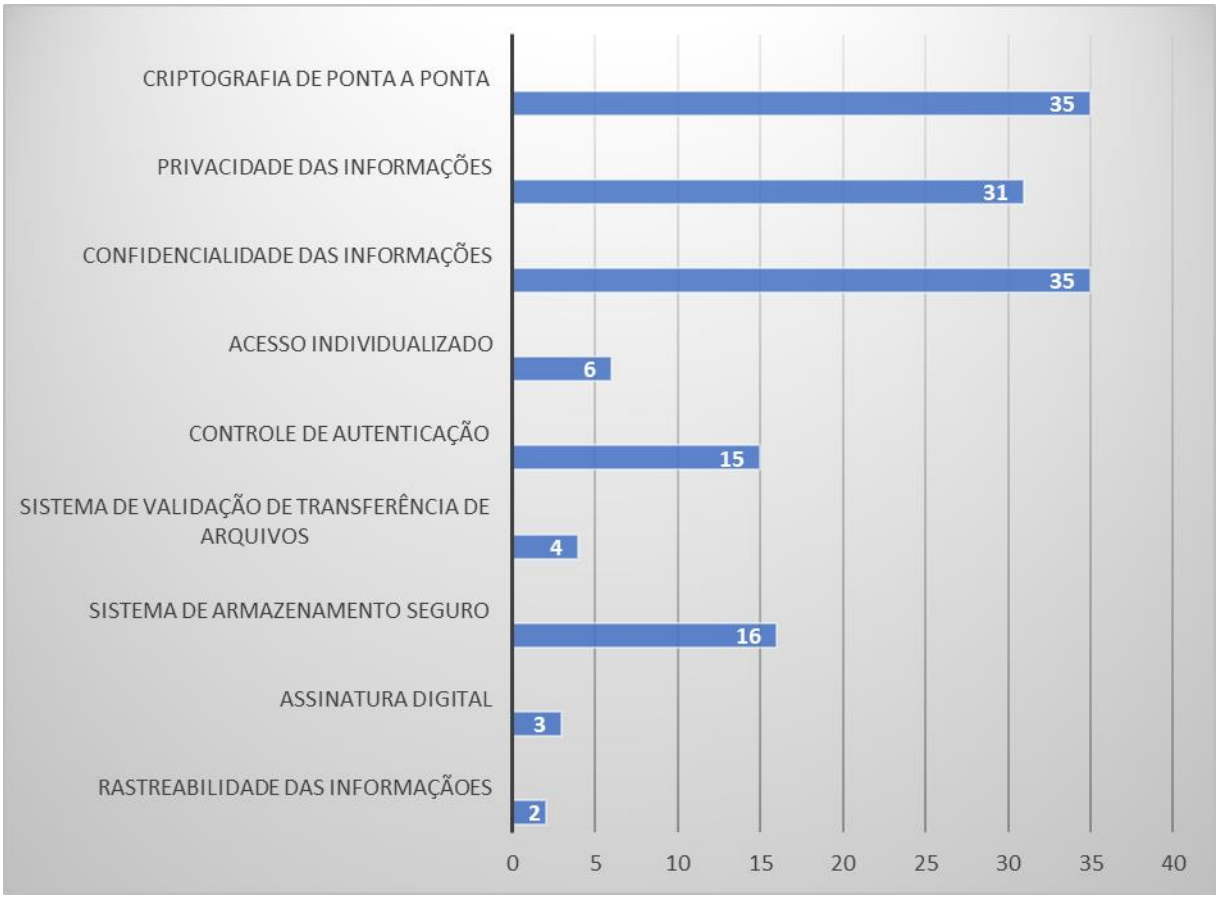
Figura 1 – Artigos por assuntos abordados



Fonte: O autor, 2021.

Em se tratando de controles de segurança da informação, conforme mostrado na Figura 2, os artigos encontrados foram: 35 artigos citaram sobre a Criptografia de ponta a ponta, 31 artigos citaram sobre a Privacidade das informações, 35 artigos citaram sobre a Confidencialidade das informações, 6 artigos citaram sobre o Acesso individualizado, 15 artigos citaram sobre o Controle de autenticação, 4 artigos citaram sobre o Sistema de validação de transferência de arquivos, 16 artigos citaram sobre o Sistema de armazenamento seguro, 3 artigos citaram sobre a Assinatura digital e 2 artigos citaram sobre a Rastreabilidade das informações.

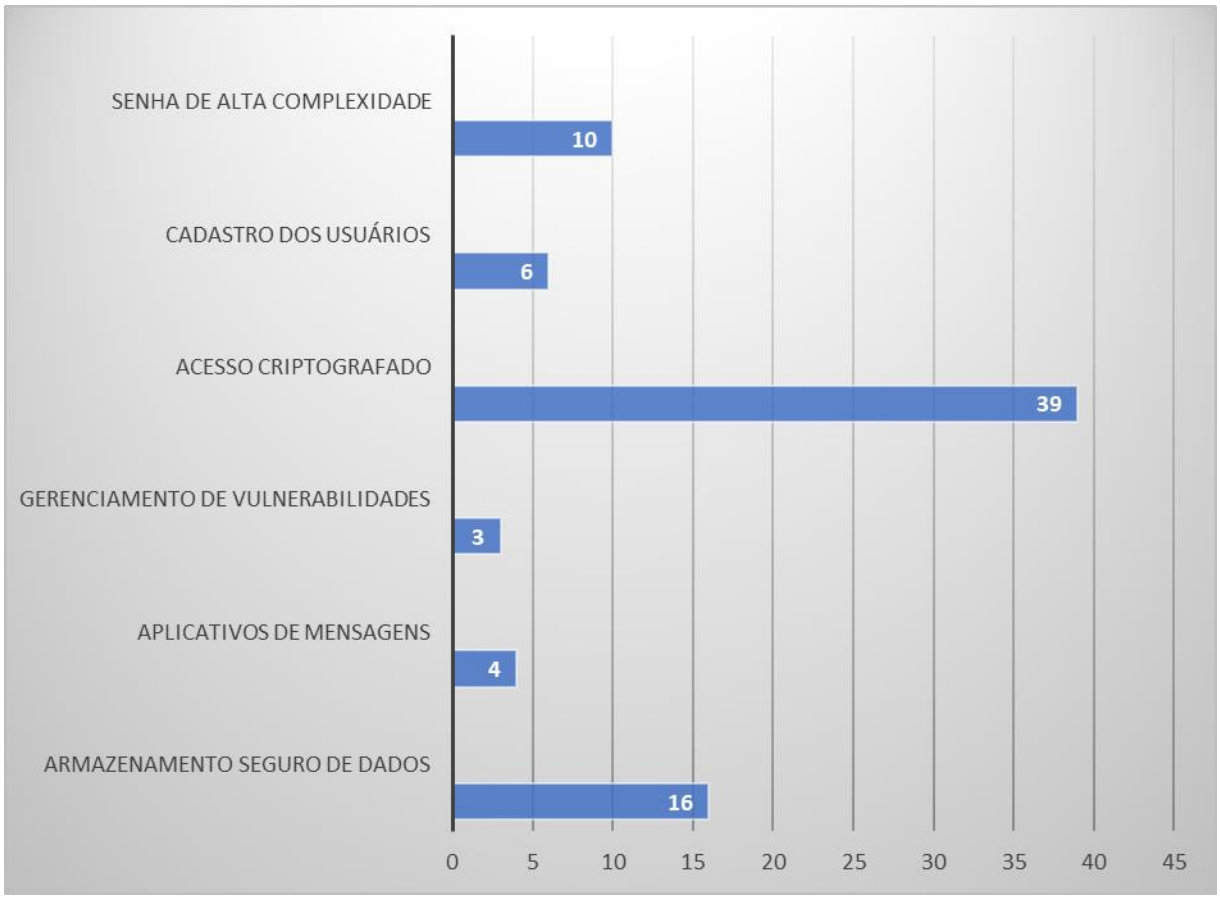
Figura 2 – Artigos por controles de segurança da informação



Fonte: O autor, 2021.

Acerca dos Requisitos de Segurança da Informação, como mostrado na Figura 3, foram encontrados: 10 artigos citaram sobre Senha de alta complexidade, 6 artigos citaram o Cadastro dos usuários, 39 artigos citaram o Acesso criptografado, 3 artigos citaram o Gerenciamento de vulnerabilidades, 4 artigos citaram os Aplicativos de mensagens e 16 artigos citaram o Armazenamento seguro dos dados.

Figura 3 – Artigos por requisitos de segurança da informação



Fonte: O autor, 2021.

Diante dos assuntos abordados, dos controles de segurança da informação e dos requisitos de segurança da informação foram utilizados como base para iniciarmos o manual de boas práticas os controles e requisitos sendo fundamentais para atingirmos o objetivo final.

3 **SOLUÇÃO PROPOSTA**

Atendendo aos desafios descritos no item Problemática e Motivação do presente documento, os requisitos e controles de Segurança identificados no levantamento da literatura serviram como ponto de partida para a definição do manual de boas práticas de Segurança da Informação para sistemas de Telemedicina. De maneira geral, o manual de boas práticas é um documento que apresenta um conjunto de padrões que podem ser adotados com o objetivo de nivelar os recursos tecnológicos com foco no negócio e na segurança podendo, assim, antecipar prováveis problemas, realizar o monitoramento do ambiente e criar uma gestão estratégica de Tecnologia da Informação para os sistemas de telemedicina. Sendo assim, o manual de boas práticas pode mitigar ataques de cibercriminosos, que podem ser um obstáculo para os sistemas de telemedicina. Desse modo, aplicar as melhores práticas de segurança da informação nas organizações de saúde, onde a telemedicina se faz presente, pode contribuir para uma rotina mais segura, estruturada e acertada. Em outras palavras, os requisitos mostrados na Figura 3, e reproduzidos a seguir, nortearam a definição dos controles de segurança recomendados no presente trabalho para serem implementados nos ambientes de Telemedicina. Tais requisitos são:

Uso de senha pelos usuários com alta complexidade.

Necessidade de cadastro individualizado para os usuários.

Realização de acesso criptografado para acesso remoto.

Gerenciamento de vulnerabilidades.

Uso de aplicações de mensagens homologadas para comunicação.

Armazenamento seguro das informações.

Dentre as normas e frameworks de Segurança da Informação existentes no mercado e na literatura, o CIS Controls foi considerado como a principal referência para definição dos controles para garantir o atendimento às exigências identificadas. A escolha do CIS Controls se deu por este ser um conjunto prioritário e prescritivo de práticas recomendadas de segurança cibernética desenvolvido por uma organização extremamente respeitada e conceituada na área de Segurança da Informação e este ser muito utilizado no mercado. Além disso, as ações defensivas recomendadas são atuais, concretas e podem ajudar a prevenir os mais diversos tipos de ataque, dando suporte à conformidade de outras normas e frameworks de segurança. O CIS Controls também apresenta grupos de implementação dos controles de acordo com a quantidade de recursos financeiros e exposição ao risco das organizações, de

modo a ser possível identificar facilmente quais controles são mais críticos de serem implementados para obter um nível inicial de gerenciamento da segurança.

Os controles de segurança, identificados no levantamento, e mostrados na Figura 2, também foram fundamentais para a criação do manual de boas práticas, uma vez que guiaram a análise do framework CIS Controls na perspectiva de sua aplicabilidade para os sistemas de telemedicina. É válido relatar que o setor da saúde é um dos setores mais afetados por invasões e ataques devido à natureza sensível dos dados que são trafegados. Em virtude disso, e face à diversidade dos controles disponíveis no CIS Controls e dos controles encontrados no mapeamento sistemático, os controles foram analisados de acordo com as seguintes perspectivas:

a) Controles voltados a criptografia de dados na organização.
b) Controles que proveem acesso individualizado aos dados na organização.
c) Controles relacionados a rastreabilidade das informações.
d) Controles focados no armazenamento seguro das informações.

Para tornar o manual mais abrangente e aderente ao preconizado por agências internacionais para a gestão da segurança das informações em organizações de saúde, a análise do CIS Controls para seleção dos controles que compõem o manual também considerou as dez dicas de segurança cibernética apontadas pelo Departamento de saúde e serviços humanos dos EUA como fundamentais para a área da saúde. Essas dicas são:

a) Estabelecer uma cultura de segurança na organização.
b) Proteger dispositivos móveis.
c) Manter bons hábitos no computador.
d) Utilizar firewall.
e) Instalar / manter software antivírus.
f) Planejar o inesperado.
g) Controlar o acesso as informações de saúde.
h) Utilizar senhas fortes e modificá-las regularmente.
i) Limitar o acesso à rede da organização e
j) Controlar o acesso físico da organização.

Sendo assim, numa totalidade de 18 controles do CIS Controls, foram considerados - para efeito do presente trabalho - aplicáveis aos ambientes de telemedicina o total de 12

grupos de controles, com 61 salvaguardas[2] a serem implementadas nas entidades de saúde para os sistemas de telemedicina.

O conjunto de controles que compõem o manual é apresentado no capítulo a seguir em quadros, onde cada quadro apresenta um grupo de controle com suas salvaguardas. Cada salvaguarda especificada possui o número do controle de referência no CIS Controls e o mapeamento para o controle da ISO/IEC 27002 correspondente, assim como a função do NIST CF. Tal mapeamento tem como objetivo auxiliar aos usuários do manual a compreender o quanto dos controles desses outros frameworks estão sendo atendidos ao implementar os controles presentes no manual.

Os quadros do manual apresentam os campos:

a) Control # – identificação do grupo do controle no CIS.
b) CIS Salvaguarda – se refere às medidas de segurança.
c) Tipo de ativo – se refere aos tipos de ativos que o controle contempla. Podem ser classificados como: dispositivos, aplicações, dados, usuários ou rede.
d) Grupo de Implementação 1 (Gl1) – organizações com recursos limitados e com baixa exposição ao risco (definido pelo CIS Controls).
e) Grupo de Implementação 2 (Gl2) – organizações com recursos moderados e com média exposição ao risco (definido pelo CIS Controls).
f) Grupo de Implementação 3 (Gl3) – organizações com recursos significativos e com exposição alta ao risco (definido pelo CIS Controls).
g) Relação – tipo de relação entre os conceitos (mapeamento do CIS v8 com a ISO/IEC 27002:2022). Pode ser classificado como: Equivalente (mesmo conceito), Superconjunto (conceito mais amplo e está totalmente relacionado), Subconjunto (conceito que está parcialmente relacionado ou em parte relacionado), Interseção (conceitos com muitas semelhanças) e Sem relacionamento (controles sem nenhuma relação).
h) # Controle ISO – se refere ao número do controle da norma ISO/IEC 27002.
i) Título do Controle ISO – se refere ao título do controle da norma ISO/IEC 27002.
j) Texto do Controle ISO – se refere ao texto do controle da norma ISO/IEC 27002.

[2] De acordo com o NIST (NIST, 2006), salvaguardas são medidas de proteção prescritas para alcançar requisitos de segurança que foram especificadas para um sistema de informação. Salvaguardas são sinônimos de controles e contramedidas de segurança.

k) Função de segurança – se refere ao tipo de segurança que o controle oferece ao considerar o NIST CF.

4 MANUAL PARA DEFINIÇÃO DE SGSI EM AMBIENTES DE TELEMEDICINA

Os Sistemas de Gestão de Segurança da Informação (SGSI) são importantes para os sistemas de telemedicina pois contribuem para salvaguardar as informações das organizações de saúde e seus critérios de confidencialidade, integridade e disponibilidade. As vantagens de um SGSI são inúmeras e incluem, mas não se limitam: (1) auxiliar a organização interna da empresa; (2) reduzir custos; (3) cumprir a legislação em vigor; (4) aumentar a credibilidade e confiança do negócio; (5) demonstrar compromisso com a segurança da informação; (6) identificar oportunidade para melhorias contínuas; (7) identificar e eliminar riscos, ameaças e vulnerabilidades; (8) aumentar a credibilidade no negócio; (9) prevenir, gerir e resolver falhas a nível de segurança da informação (CONHEÇA OS 8 BENEFÍCIOS DA AQUISIÇÃO DE UMA SGSI BASEADO NA ISO 27001, 2021).

Um SGSI voltado para os sistemas de telemedicina deve possuir apenas controles que possam auxiliar na mitigação de vulnerabilidades dos sistemas das organizações desse segmento. Dessa forma, este manual foi elaborado selecionando os melhores controles de segurança da informação que atendem aos sistemas de telemedicina das organizações de saúde onde se torna possível que um SGSI seja implementado por meio da utilização destes controles e contribuindo para a segurança da informação nos sistemas de telemedicina. A utilização de todos os controles que contemplam este manual é facultativa dependendo em que sistema de telemedicina ele será implementado e o grau de segurança necessário para este sistema.

Como citado anteriormente, o manual foi estruturado com a criação de grupos de controles, sendo elaborado um total de 12 grupos, onde cada controle que pertence a um determinado grupo possui uma relação de afinidade entre si. É importante destacar que cada controle desse manual foi baseado no CIS Controls possuindo um mapeamento direto para a ISO/IEC 27002 e para o NIST CF; assim podemos verificar o que é preconizado pelo CIS Controls como também o que é relatado na ISO/IEC 27002:2022 e o que é mencionado no NIST CF. Com esse mapeamento do CIS Controls, da ISO/IEC 27002 e do NIST CF um profissional de Tecnologia da Informação que porventura queira utilizar o manual poderá fazê-lo tendo três referências de conformidade e fazendo a utilização de controles que contribuirão de forma eficaz para o gerenciamento da segurança da informação nos sistemas de telemedicina. A definição de um SGSI utilizando este manual favorece um melhor entendimento do ambiente em que a organização de saúde atua e compreende quais requisitos

de segurança da informação devem ser atendidos, possibilitando ao profissional responsável pela Segurança focar nas informações mais sensíveis da organização.

De maneira geral, o manual de boas práticas é um documento que apresenta um conjunto de padrões que podem ser adotados com o objetivo de nivelar os recursos tecnológicos com foco no negócio e na segurança podendo, assim, antecipar prováveis problemas, realizar o monitoramento do ambiente e criar uma gestão estratégica de Tecnologia da Informação para os sistemas de telemedicina. Sendo assim, o manual de boas práticas pode mitigar ataques de cibercriminosos, que podem ser um obstáculo para os sistemas de telemedicina. Desse modo, aplicar as melhores práticas de segurança da informação nas organizações de saúde onde a telemedicina se faz presente pode contribuir para uma rotina mais segura, estruturada e acertada.

4.1 **Políticas internas de Segurança da Informação**

É indispensável a definição de políticas internas de segurança da informação que devem ser determinadas a partir do planejamento estratégico das organizações de saúde. A alta gestão das organizações deve estabelecer as bases da governança corporativa, os objetivos estratégicos e o apetite ao risco que irá nortear a criação das políticas internas.

4.2 **Objetivos dos controles de Segurança da Informação**

Os controles de segurança da informação possuem como objetivos impedir, evitar, detectar, neutralizar ou minimizar os riscos de segurança para as informações, propriedades físicas, sistemas de computador, redes de computadores e outros tipos de ativos.

4.3 **Grupos de controles elegidos para a segurança da informação dos sistemas de telemedicina**

O quadro 4, apresenta os grupos de controles selecionados com os controles em cada grupo, que fazem parte do manual de boas práticas para os sistemas de telemedicina. Note-se que as colunas "# Grupo de Controle" e "Nome do Grupo de controle" apresentam o mesmo código e descrição do controle no CIS Controls, respectivamente.

Quadro 4 - Grupos de Controles Selecionados

# Grupo de Controle	Nome do Grupo de controle	# Controles
1	Inventário e controle de ativos	3
2	Inventário e controle de ativos de software	3
3	Proteção de dados	14
7	Gerenciamento contínuo de vulnerabilidades	5
8	Gerenciamento de log de auditoria	3
9	Proteções de e-mail e navegador da Web	3
11	Recuperação de dados	4
12	Gerenciamento de infraestrutura de rede	6
13	Monitoramento e defesa de rede	5
14	Conscientização sobre segurança e treinamento de habilidades	7
17	Gerenciamento de resposta a incidentes	4
18	Teste de penetração	4
Total	12 grupos de controle	61 controles

Fonte: O autor, 2021.

4.4 **Melhores práticas para sistemas de Telemedicina**

O objetivo do manual de boas práticas é fornecer diretrizes ou regras que norteiam a segurança da informação nos sistemas de telemedicina podendo ser utilizado de forma sistemática. O principal objetivo deste manual é mitigar as vulnerabilidades trazendo confiabilidade para os sistemas de telemedicina.

O cenário de utilização deste manual é compreendido na área da saúde aonde os sistemas de telemedicina estão presentes e necessitam ser gerenciados para que se possa atingir um grau de segurança da informação adequado para cada sistema de telemedicina.

Tendo em vista que os sistemas de telemedicina são heterogêneos podemos realizar a segurança da informação aproveitando os controles que irão proteger o ambiente da

telemedicina na área da saúde. Este manual procura fornecer um linguajar básico para que pessoas que não são da área da Tecnologia da Informação possam utilizá-lo sem a necessidade de recorrer a profissionais da área de Segurança da Informação. Ele é objetivo e procura ser transparente e didático de modo que profissionais da área da saúde se sintam à vontade com relação à escolha dos controles que podem ser adotados nos sistemas de telemedicina. O manual de boas práticas de Segurança da Informação para sistemas de Telemedicina proposto neste trabalho é apresentado nas próximas subseções, onde cada subseção representa um grupo de controle.

4.4.1 Inventário e Controle de Ativos

Gerencia ativamente (inventário, rastreie e corrija) todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/Internet das Coisas (IoT) e servidores) conectados à infraestrutura fisicamente, virtualmente, remotamente, e aqueles, em ambientes de nuvem, para conhecer com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também dará suporte à identificação de ativos não autorizados e não gerenciados para remover ou corrigir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

4.4.1.1 Salvaguarda 1: Estabelecimento e Manutenção do Inventário Detalhado de Ativos

Estabelecimento e manutenção de um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, não computacionais/IoT dispositivos e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo corporativo, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuários finais, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Esse inventário inclui ativos conectados à

infraestrutura fisicamente, virtualmente, remotamente e em ambientes de nuvem. Além disso, inclui ativos conectados regularmente à infraestrutura de rede da empresa, mesmo que não estejam sob controle da empresa. Revisa e atualiza o inventário de todos os ativos corporativos semestralmente ou com mais frequência (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

Um inventário atualizado e detalhado de ativos ajuda na administração dos recursos das organizações da saúde objetivando alcançar uma maior acurácia, auxiliando nos ajustes contábeis e averiguando as não conformidades. Em se tratando de dispositivos particulares é boa prática uma medida de contenção.

4.4.1.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle Inventário e Controle de Ativos pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na quadro a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
1	1.1	Dispositivos	X	X	X	Subconjunto	5.9	Inventário de informações e outros ativos associados.	Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.1.2 Salvaguarda 2: Nome de ativos não autorizados

Entende-se por ativo não autorizado os elementos que não são aprovados a agregar valor ao negócio. Certifique-se de que existe um processo para tratar de ativos não autorizados semanalmente. A empresa pode optar por remover o ativo da rede, impedir que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

Administrar os ativos portáteis na rede é relevante para ter um maior controle do seu parque de ativos minimizando repetição de incidentes e fazendo com que todos os ativos sejam monitorados e protegidos dentro das organizações de saúde.

4.4.1.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A tabela a seguir mostra o mapeamento da Salvaguarda 2 do grupo de controle Inventário e Controle de Ativos para o CIS Controls, ISO 27002 e NIST CF. Note-se que não há um controle da ISO 27002 para o qual a referida salvaguarda é mapeada (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]), indicando que as organizações que implementarem a Salvaguarda 2 não implementarão um controle da ISO 27002.

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
1	1.2	Dispositivos	X	X	X	-	-	-	-	Responder

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.1.3 Salvaguarda 3: Utilização de uma ferramenta de descoberta de ativo

Utilização de uma ferramenta de descoberta ativa para identificar ativos conectados à rede da empresa. Configure a ferramenta de descoberta ativa para executar diariamente ou com maior frequência (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).
É importante que todos os ativos não autorizados como também os ativos internos e não gerenciados sejam conhecidos e tenham medidas para garantir a segurança da rede nas organizações da saúde.

4.4.1.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

Assim como ocorreu na Salvaguarda 2, a Salvaguarda 3 não possui mapeamento para um controle da ISO 27002, como pode ser observado no quadro de mapeamento apresentada a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
1	1.3	Dispositivos		X	X	-	-	-	-	Detectar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.2 Inventário e Controle de Ativos de Software

Gerencie-se ativamente (inventário, rastreie-se e corrija-se) todos os softwares (sistemas operacionais e aplicativos) na rede para que apenas softwares autorizados sejam instalados e possam ser executados, e que softwares não autorizados e não gerenciados sejam encontrados e impedidos de instalação ou execução (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

4.4.2.1 Salvaguarda 1: Estabelecimento e manutenção de um inventário de software.

Estabelecimento e manutenção de um inventário detalhado de todos os softwares licenciados instalados nos ativos da empresa. O inventário de software deve documentar o título, editor, data inicial de instalação/uso e finalidade comercial de cada entrada; quando apropriado, inclua o Uniform Resource Locator (URL), loja(s) de aplicativos, versão(ões), mecanismo de implantação e data de desativação. Revisa-se e atualiza-se o inventário de software semestralmente ou com mais frequência. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Um inventário de software detalhado e atualizado semestralmente ajuda na antecipação de problemas técnicos e ajuda na realização da proteção dos dados além de possibilitar o gerenciamento de vulnerabilidades (seja manual ou automatizado).

4.4.2.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle Inventário e Controle de Ativos de Software pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na quadro a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
2	2.1	Aplicações	**X**	**X**	**X**	Subconjunto	5.9	Inventário de informações e outros ativos associados.	Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.2.2 Salvaguarda 2 e 3: Software autorizado da lista de permissões

Utilização de controles técnicos, como lista de permissões de aplicativos, para garantir que apenas softwares autorizados possam ser executados ou acessados. Reavalie-se semestralmente ou com mais frequência. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Os controles técnicos devem ser utilizados para avaliar quais softwares podem ser acessados ou executados pelos usuários do sistema garantindo assim a proteção dos ativos da organização, a exatidão de seus registros e adesão aos padrões da gestão corporativa. As listas de permissões de softwares devem ser reavaliadas periodicamente para garantir que somente softwares autorizados possam ser utilizados com um nível de segurança acordado.

4.4.2.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle Inventário e Controle de Ativos de software pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
2	2.5	Aplicações		**X**	**X**	Subconjunto	8.7	Proteção contra malware.	A proteção contra malware deve ser implementada e suportada pela conscientização apropriada do usuário.	Proteger
2	2.5	Aplicações		**X**	**X**	-	8.19	Instalação de software em sistemas operacionais.	Procedimentos e medidas devem ser implementados para gerenciar com segurança a instalação de software em sistemas operacionais.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3 Proteção de dados

Desenvolvam-se processos e controles técnicos para identificar, classificar, manipular, reter e descartar dados com segurança. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

4.4.3.1 Salvaguarda 1, 2 e 3: Estabelecimento e manutenção de um processo de gerenciamento de dados

Estabelecimento e manutenção de um processo de gerenciamento de dados. No processo, aborda-se a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base nos padrões de

sensibilidade e retenção da organização. Revise-se e atualize-se a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

O gerenciamento de dados promove a análise de dados com eficácia, transparência das operações e minimização de erros, oferecendo segurança e qualidade aos dados das organizações. O gerenciamento de dados possibilita o aumento da qualidade dos dados, promovendo precisão na tomada de decisões. Um inventário de dados, abrangendo proprietários nas organizações de saúde, deve ser extenso e garantir a conformidade com a (LGPD), particularizando os dados pessoais coletados e seu fluxo dentro e fora da organização. O gerenciamento de dados também viabiliza a transparência das operações mantendo uma organização sólida em todo o processo que envolve este ativo ocasionando simplificação do trabalho. Toda a informação dos dispositivos dos usuários que podem estar armazenadas, sendo processadas ou estar acessíveis devem ter um grau de proteção adequado.

4.4.3.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

As Salvaguardas 1, 2 e 3 do grupo de controle Proteção de dados pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
3	3.1	Dados	X	X	X	Subconjunto	5.10	Uso aceitável de informações e outros ativos associados.	Regras para o uso aceitável e procedimentos para lidar com informações e outros ativos associados devem ser identificados, documentados e implementados.	Identificar
3	3.1	Dados	X	X	X	Subconjunto	5.9	Inventário de informações e outros ativos associados.	Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.	Identificar
3	3.1	Dados	X	X	X	Subconjunto	8.1	Dispositivos terminais do usuário.	As informações armazenadas, processadas ou acessíveis por meio de dispositivos terminais do usuário devem ser protegidas.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.2 Salvaguarda 4: Configuração de listas de controle de acesso a dados

Configuração de listas de controle de acesso a dados com base na necessidade de um usuário saber. Apliquem-se listas de controle de acesso a dados, também conhecidas como permissões de acesso, devam ser aplicadas a sistemas de arquivos, bancos de dados e aplicativos locais e remotos (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

As listas de controle de acesso a dados definem permissões pertinentes para os usuários, promovendo um controle individualizado ou por função sobre os usuários do sistema.

4.4.3.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle Proteção de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
3	3.3	Dados	**X**	**X**	**X**	Subconjunto	8.4	Acesso ao código fonte.	O acesso de leitura e gravação ao código-fonte, ferramentas de desenvolvimento e bibliotecas de software deve ser gerenciado adequadamente.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.3 Salvaguarda 5: Aplicação de retenção de dados

Retenção de dados de acordo com o processo de gerenciamento de dados da empresa. A retenção de dados deve incluir prazos mínimos e máximos. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

O ciclo de vida dos dados dos clientes deve ser realizado conforme preconiza a Lei Geral de Proteção de Dados (LGPD).

4.4.3.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle Proteção de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
3	3.4	Dados	X	X	X	Subconjunto	5.33	Proteção de registros.	Os registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.4 Salvaguarda 6 e 7: Descarte de Dados com Segurança

Descarte-os dados com segurança conforme descrito no processo de gerenciamento de dados da empresa devem ser descartados. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Os dados armazenados nos sistemas de telemedicina devem ser mantidos pelo tempo estipulado conforme sua classificação e tendo o titular a liberdade de pedir o descarte, caso seja necessário. Os dados devem ser descartados e não podem ser recuperados pela organização ou por cibercriminosos, conforme orienta a LGPD.

4.4.3.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle Proteção de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
3	3.5	Dados	**X**	**X**	**X**	Subconjunto	5.10	Uso aceitável de informações e outros ativos associados.	Regras para o uso aceitável e procedimentos para lidar com informações e outros ativos associados devem ser identificados, documentados e implementados.	Proteger
3	3.5	Dados	**X**	**X**	**X**	Subconjunto	7.10	Mídia de armazenamento.	A mídia de armazenamento deve ser gerenciada ao longo de seu ciclo de vida de aquisição, uso, transporte e descarte de acordo com o esquema de classificação da organização e os requisitos de manuseio.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.5 Salvaguarda 8: Criptografia de dados em dispositivos de usuário final

Criptografia de dados em dispositivos de usuários finais que contenham dados confidenciais. As implementações de exemplo podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A criptografia dos dados deve ser utilizada como um mecanismo de segurança que possibilite realizar a proteção de dados confidenciais.

4.4.3.5.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Proteção de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
3	3.6	Dispositivos	**X**	**X**	**X**	Subconjunto	6.7	Trabalho remoto.	As medidas de segurança devem ser implementadas quando o pessoal estiver trabalhando remotamente para proteger as informações acessadas, processadas ou armazenadas fora das instalações da organização.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.6 Salvaguarda 9, 10 e 11: Estabelecimento e manutenção de um esquema de classificação de dados

Estabelecimento e manutenção de um esquema geral de classificação de dados para a organização. As organizações podem usar rótulos, como "Sensível", "Confidencial" e "Público", e classificar seus dados de acordo com esses rótulos. Revise-se e atualize-se o esquema de classificação anualmente, ou quando ocorrerem mudanças significativas na organização que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A classificação dos dados nos sistemas de telemedicina visa a segurança do dado em todo o percurso, desde seu armazenamento, processamento até o seu manuseio proporcionando a possibilidade de parâmetro de proteção adequado à sua importância nas organizações de saúde.

4.4.3.6.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Proteção de dados pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
3	3.7	Dados		X	X	Subconjunto	5.9	Inventário de informações e outros ativos associados.	Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.	Identificar
3	3.7	Dados		X	X	Subconjunto	5.12	Classificação das informações.	As informações devem ser classificadas de acordo com as necessidades de segurança da informação da organização com base na confidencialidade, integridade, disponibilidade e requisitos relevantes das partes interessadas.	Identificar
3	3.7	Dados		X	X	Subconjunto	8.12	Prevenção de vazamento de dados.	As medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações confidenciais.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.7 Salvaguarda 12: Criptografia de dados confidenciais em trânsito

Criptografia de dados confidenciais em trânsito. Exemplos de implementações podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH). (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Devem ser utilizados protocolos criptográficos para transferência de informações entre organizações e redes particulares.

4.4.3.7.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Proteção de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Control e ISO	Título do Controle ISO	Texto do Controle ISO	Função
3	3.10	Dados		X	X	Subconjunto	5.14	Transferência de informação.	Regras, procedimentos ou acordos de transferência de informações devem estar em vigor para todos os tipos de instalações de transferência dentro da organização e entre a organização e outras partes.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.8 Salvaguarda 13: Criptografia de dados confidenciais em repouso

Criptografia de dados confidenciais em repouso em servidores, aplicativos e bancos de dados que contenham dados confidenciais. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende ao requisito mínimo desta Salvaguarda. Métodos de criptografia adicionais podem incluir criptografia de camada de aplicativo, também conhecida como criptografia do lado do cliente, onde o acesso ao(s) dispositivo(s) de armazenamento de dados não permite acesso aos dados de texto simples. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Em caso de dados confidenciais armazenados nos servidores e no lado dos aplicativos é boa prática realizar a criptografia para garantir a confidencialidade de tais dados.

4.4.3.8.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Proteção de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
3	3.11	Dados		**X**	**X**	Subconjunto	5.33	Proteção de registros.	Os registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.3.9 Salvaguarda 14: Registro de acesso a dados confidenciais

Registro de acesso a dados confidenciais, incluindo modificação e descarte. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O armazenamento de logs é aconselhável pois ajuda a identificar e/ou rastrear violações de segurança.

4.4.3.9.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Proteção de dados pode ser mapeada para a função "Detectar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISSO**	**Texto do Controle ISO**	**Função**
3	3.14	Dados			**X**	Subconjunto	8.15	Logging.	Logs que registram atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.	Detectar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.4 Gerenciamento Contínuo de Vulnerabilidades

Desenvolvimento de um plano para avaliar e rastrear continuamente as vulnerabilidades em todos os ativos corporativos na infraestrutura da empresa, a fim de corrigir e minimizar a janela de oportunidade para os invasores. Monitorar fontes públicas e privadas do setor em busca de novas informações sobre ameaças e vulnerabilidades devem ser monitoradas. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

4.4.4.1 Salvaguarda 1: Estabelecimento e manutenção de um processo de gerenciamento de vulnerabilidades

Estabelecimento e manutenção de um processo de gerenciamento de vulnerabilidades documentado para ativos corporativos. Revise-se e atualize-se a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O gerenciamento contínuo de vulnerabilidades propicia maior gerência de segurança, controlando e mitigando riscos na organização.

4.4.4.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Gerenciamento Contínuo de Vulnerabilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
7	7.1	Aplicações	X	X	X	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.4.2 Salvaguarda 2: Estabelecimento e manutençãoo de um processo de correção

Estabelecimento e manutenção de uma estratégia de remediação baseada em riscos documentada em um processo de remediação, com revisões mensais ou mais frequentes. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O gerenciamento de vulnerabilidades permite detectar e corrigir falhas, podendo as fragilidades serem controladas e monitoradas nas organizações de saúde.

4.4.4.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Gerenciamento Contínuo de Vulnerabilidades pode ser mapeada para a função "Responder" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
7	7.2	Aplicações	**X**	**X**	**X**	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Responder

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.4.3 Salvaguarda 3: Execução do gerenciamento automatizado de patches de aplicativos

Realização de atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com mais frequência (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

O gerenciamento de vulnerabilidades técnicas ajuda a controlar a atualização dinâmica dos sistemas corporativos onde patches de aplicativos são instalados/atualizados em períodos determinados na organização de saúde contendo histórico das versões que estão instaladas em cada ativo e das vulnerabilidades presentes em cada equipamento, podendo controlar o tempo que uma vulnerabilidade permanece ativa no ambiente.

4.4.4.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Gerenciamento Contínuo de Vulnerabilidades pode ser mapeada para a função "Responder" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
7	7.4	Aplicações	X	X	X	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Responder

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.4.4 Salvaguarda 4: Execução de verificações automatizadas de vulnerabilidades de ativos corporativos expostos externamente

Execução de verificações automatizadas de vulnerabilidades de ativos corporativos expostos externamente usando uma ferramenta de verificação de vulnerabilidades compatível com SCAP. Execute-se verificações mensalmente ou com mais frequência (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

No gerenciamento contínuo de vulnerabilidades é boa prática utilizar ferramentas específicas, como o Wireshark, Nessus e a Aircrack-ng para o auxílio na verificação de

fragilidades de ativos corporativos expostos externamente e internamente pois podem realizar a classificação de falhas de segurança cibernética e a mitigação destas. Assim, todo o ciclo de vida de uma vulnerabilidade é acompanhado, desde a sua descoberta até sua retificação.

4.4.4.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Gerenciamento Contínuo de Vulnerabilidades pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
7	7.6	Aplicações	**X**	**X**	**X**	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.4.5 Salvaguarda 5: Correção de vulnerabilidades detectadas

Correção de vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente ou com mais frequência, com base no processo de correção (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

É boa prática realizar a correção das vulnerabilidades.

4.4.4.5.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Gerenciamento Contínuo de Vulnerabilidades pode ser mapeada para a função "Responder" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
7	7.7	Aplicações	X	X	X	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Responder

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.5 Gerenciamento de Log de Auditoria

Descrição: Colete, alerte, revise e retenha logs de auditoria de eventos que podem ajudar a detectar, entender ou se recuperar de um ataque. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

4.4.5.1 Salvaguarda 1: Estabelecimento e manutenção de um processo de gerenciamento de log de auditoria

Estabelecimento e manutenção de um processo de gerenciamento de log de auditoria que defina os requisitos de log da empresa. No mínimo, trate da coleta, revisão e retenção de logs de auditoria para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O processo de gerenciamento de logs é benéfico pois identifica violações de políticas, identifica incidentes, problemas operacionais e atividades fraudulentas.

4.4.5.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de Gerenciamento de Log de Auditoria pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
8	8.1	Rede	**X**	**X**	**X**	Equivalente	8.15	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.5.2 Salvaguarda 2: Garanta o armazenamento adequado de logs de auditoria

Certifique-se de que os destinos de registro mantenham armazenamento adequado para cumprir o processo de gerenciamento de registro de auditoria da empresa. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Nos sistemas de telemedicina os logs devem ter local adequado para armazenamento para garantir que agentes maliciosos não sejam capazes de acessar e modificá-los.

4.4.5.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle de Gerenciamento de Log de Auditoria pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
8	8.3	Rede	X	X	X	Subconjunto	8.6	Gerenciamento de capacidade.	O uso de recursos deve ser monitorado e ajustado de acordo com os requisitos de capacidade atuais e esperados.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.5.3 Salvaguarda 3: Retenção de registros de auditoria

Retenção dos logs de auditoria nos ativos corporativos por no mínimo 90 dias. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

O gerenciamento de log de auditoria deve determinar período específico convencionado conforme política adotada para a guarda dos logs da organização.

4.4.5.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle de Gerenciamento de Log de Auditoria pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
8	8.10	Rede		X	X	Subconjunto	5.28	Coleta de provas.	A organização deve estabelecer e implementar procedimentos para a identificação, coleta, aquisição e preservação de evidências relacionadas a eventos de segurança da informação.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.6 Proteções de e-mail e navegador da Web

Melhorar as proteções e detecções de ameaças de vetores de e-mail e web, pois essas são oportunidades para os invasores manipularem o comportamento humano por meio de envolvimento direto. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

4.4.6.1 Salvaguarda 1: Garanta o uso de apenas navegadores e clientes de e-mail totalmente compatíveis

Certificação de que apenas navegadores e clientes de e-mail totalmente suportados tenham permissão para serem executados na empresa, usando apenas a versão mais recente de navegadores e clientes de e-mail fornecidos pelo fornecedor. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A atualização de navegadores e clientes de e-mail são importantes para que sejam realizadas recomendações e correções e sejam implantadas medidas para garantir a segurança da informação enquanto estas ferramentas estão sendo utilizadas. Somente navegadores homologados pela equipe de segurança da informação devem ser utilizados pelos usuários da organização.

4.4.6.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle de Proteções de e-mail e navegador da Web pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
9	9.1	Aplicações	**X**	**X**	**X**	Subconjunto	8.1	Dispositivos terminais de usuários.	As informações armazenadas, processadas ou acessíveis por meio de dispositivos terminais do usuário devem ser protegidas.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.6.2 Salvaguarda 2: Estabelecimento e aplicação de filtros de URL baseados em rede

Aplicação e atualização de filtros de URL baseados em rede para limitar a conexão de um ativo corporativo a sites potencialmente maliciosos ou não aprovados. As implementações de exemplo incluem filtragem baseada em categoria, filtragem baseada em reputação ou por meio do uso de listas de bloqueio. Aplique filtros para todos os ativos corporativos. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A filtragem de URL permite que as organizações possam realizar o bloqueio de páginas web e o bloqueio de arquivos individuais com a finalidade de delimitar o conteúdo que os usuários podem acessar e, consequentemente, aumentar a proteção do ambiente interno

4.4.6.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle de Proteções de e-mail e navegador da Web pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
9	9.3	Rede		**X**	**X**	Subconjunto	8.7	Proteção contra malware.	A proteção contra malware deve ser implementada e suportada pela conscientização apropriada do usuário.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.6.3 Salvaguarda 3: Implantação e manutenção de proteções antimalware do servidor de e-mail

Implante e mantenha proteções antimalware do servidor de e-mail, como verificação de anexos e/ou sandboxing. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

As ferramentas de antimalware devem ser mantidas em todos os dispositivos da organização (em particular, nos servidores de e-mail), a fim de garantir que todos os arquivos que chegam e saem destes sejam inspecionados e bloqueados, quando identificados como maliciosos

4.4.6.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle de Proteções de e-mail e navegador da Web pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
9	9.7	Rede		**X**	**X**	Subconjunto	8.7	Proteção contra malware.	A proteção contra malware deve ser implementada e suportada pela conscientização apropriada do usuário.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.7 Recuperação de dados

Estabeleça e mantenha práticas de recuperação de dados suficientes para restaurar os ativos corporativos no escopo para um estado pré-incidente e confiável. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

4.4.7.1 Salvaguarda 1: Estabelecimento e manutenção de um processo de recuperação de dados

Estabelecimento e manutenção de um processo de recuperação de dados. No processo, aborde o escopo das atividades de recuperação de dados, priorização de recuperação e a segurança dos dados de backup. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Além de ataques cibernéticos, panes e problemas tecnológicos podem ocorrer e inviabilizar a utilização de sistemas, tornando necessário um plano de recuperação de dados eficiente para voltar ao seu estado operacional.

4.4.7.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle de Recuperação de dados pode ser mapeada para a função "Recuperar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
11	11.1	Dados		**X**	**X**	Subconjunto	8.13	Backup de informações.	Cópias de backup de informações, software e sistemas devem ser mantidas e testadas regularmente de acordo com a política de backup específica do tópico acordada.	Recuperar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.7.2 Salvaguarda 2: Proteção dos dados de recuperação

Proteção dos dados de recuperação com controles equivalentes aos dados originais. Criptografia de referência ou separação de dados, com base nos requisitos. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A proteção dos dados de recuperação é relevante pois certifica que em caso de algum sinistro a organização continue funcionando de forma segura e sem prejuízos financeiros ou de imagem.

4.4.7.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle de Recuperação de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Control e ISO	Título do Controle ISO	Texto do Controle ISO	Função
11	11.3	Dados	X	X	X	Subconjunto	8.12	Prevenção de vazamento de dados.	As medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações confidenciais.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.7.3 Salvaguarda 3: Proteção dos dados de recuperação

Proteção dos dados de recuperação com controles equivalentes aos dados originais. Criptografia de referência ou separação de dados, com base nos requisitos. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A criptografia das cópias de segurança ajuda na confidencialidade da informação impedindo que pessoas não autorizadas tenham acesso à informação.

4.4.7.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle de Recuperação de dados pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
11	11.3	Dados	X	X	X	Subconjunto	8.13	Backup de informações.	Cópias de backup de informações, software e sistemas devem ser mantidas e testadas regularmente de acordo com a política de backup específica do tópico acordada.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.7.4 Salvaguarda 4: Estabelecimento e manutenção de uma instância isolada de dados de recuperação

Estabelecimento e manutenção de uma instância isolada de dados de recuperação. Exemplos de implementações incluem destinos de backup de controle de versão por meio de sistemas ou serviços offline, na nuvem ou fora do local. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Os dados de recuperação devem ser mantidos em locais isolados para que possam ser preservadas a sua confidencialidade e integridade além de garantir que somente pessoas autorizadas tenham acesso.

4.4.7.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle de Recuperação de dados pode ser mapeada para a função "Recuperar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
11	11.4	Dados	X	X	X	Subconjunto	8.13	Backup de informações.	Cópias de backup de informações, software e sistemas devem ser mantidas e testadas regularmente de acordo com a política de backup específica do tópico acordada.	Recuperar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.8 Gerenciamento de infraestrutura de rede

Estabeleça, implemente e gerencie ativamente (rastreie, relate, corrija) dispositivos de rede, a fim de evitar que invasores explorem serviços de rede e pontos de acesso vulneráveis. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.].

4.4.8.1 Salvaguarda 1: Garantia de que a infraestrutura de rede esteja atualizada

Garantia de que a infraestrutura de rede seja mantida atualizada. As implementações de exemplo incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de rede como serviço (NaaS) atualmente suportadas. Revise as versões do software mensalmente ou com mais frequência para verificar o suporte ao software. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A atualização da infraestrutura de rede é importante pois oferece maior performance e confiabilidade, além de manter a compatibilidade com as aplicações e reduzir os incidentes.

4.4.8.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle de Gerenciamento de infraestrutura de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

A tabela a seguir mostra o mapeamento da Salvaguarda 1 do grupo de controle Gerenciamento de infraestrutura de rede para o CIS Controls, ISO 27002 e NIST CF. Note que não há um controle da ISO 27002 para o qual a referida salvaguarda é mapeada (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]), indicando que as organizações que implementarem a Salvaguarda 1 não implementarão um controle da ISO 27002.

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Control e ISO	Título do Controle ISO	Texto do Controle ISO	Função
12	12.1	Rede	X	X	X	-	-	-	-	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.8.2 Salvaguarda 2: Estabelecimento e manutenção de diagrama(s) de arquitetura

Estabelecimento e manutenção de diagrama(s) de arquitetura e/ou outra documentação do sistema de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A revisão e atualização da documentação dos sistemas de rede corroboram para a correta prevenção de acessos não autorizados a equipamentos, instalações, materiais ou documentos contribuindo para a criação de um ambiente de TI mais estruturado e seguro.

4.4.8.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle de Gerenciamento de infraestrutura de rede pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

A tabela a seguir mostra o mapeamento da Salvaguarda 2 do grupo de controle Gerenciamento de infraestrutura de rede para o CIS Controls, ISO 27002 e NIST CF. Note que não há um controle da ISO 27002 para o qual a referida salvaguarda é mapeada (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]), indicando que as organizações que implementarem a Salvaguarda 2 não implementarão um controle da ISO 27002.

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Control e ISO	Título do Controle ISO	Texto do Controle ISO	Função
12	12.4	Rede		X	X	-	-	-	-	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.8.3 Salvaguarda 3: Garantia de que os dispositivos remotos utilizem uma VPN e estejam se conectando à infraestrutura AAA de uma empresa

Exija que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

As medidas de segurança no trabalho remoto, como as VPNs, devem ser utilizadas para garantir a privacidade dos participantes estabelecendo uma conexão segura nas organizações de saúde.

4.4.8.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle de Gerenciamento de infraestrutura de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

A tabela a seguir mostra o mapeamento da Salvaguarda 3 do grupo de controle Gerenciamento de infraestrutura de rede para o CIS Controls, ISO 27002 e NIST CF. Note que não há um controle da ISO 27002 para o qual a referida salvaguarda é mapeada (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]), indicando que as organizações que implementarem a Salvaguarda 3 não implementarão um controle da ISO 27002.

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
12	12.7	Dispositivos		X	X	Subconjunto	6.7	-	-	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.8.4 Salvaguarda 4: Garanta que os dispositivos remotos utilizem uma VPN e estejam se conectando à infraestrutura AAA de uma empresa

Exija que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Serviços de autenticação e de rede virtual privada são soluções fundamentais para realizar o compartilhamento de dados de forma segura reduzindo a exposição das organizações.

4.4.8.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle de Gerenciamento de infraestrutura de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

A tabela a seguir mostra o mapeamento da Salvaguarda 4 do grupo de controle Gerenciamento de infraestrutura de rede para o CIS Controls, ISO 27002 e NIST CF. Note que não há um controle da ISO 27002 para o qual a referida salvaguarda é mapeada (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]), indicando que as organizações que implementarem a Salvaguarda 4 não implementarão um controle da ISO 27002.

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Control e ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
12	12.7	Dispositivos		X	X	Subconjunto	8.1	Dispositivos terminais do usuário.	As informações armazenadas, processadas ou acessíveis por meio de dispositivos terminais do usuário devem ser protegidas.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.8.5 Salvaguarda 5: Estabelecimento e manutenção de recursos de computação dedicados para todo o trabalho administrativo

Estabelecimento e manutenção de recursos de computação dedicados, separados física ou logicamente, para todas as tarefas administrativas ou que exijam acesso administrativo. Os recursos de computação devem ser segmentados a partir da rede primária da empresa e não devem ter acesso à Internet. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A segmentação de recursos de computação simplifica o gerenciamento da rede e as respostas aos incidentes.

4.4.8.5.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle de Gerenciamento de infraestrutura de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Control e ISO	Título do Controle ISO	Texto do Controle ISO	Função
12	12.8	Dispositivos			X	Subconjunto	8.2	Direitos de acesso privilegiado.	A alocação e uso de direitos de acesso privilegiado devem ser restritos e gerenciados.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.8.6 Salvaguarda 6: Estabelecimento e manutenção de recursos de computação dedicados para todo o trabalho administrativo

Estabelecimento e manutenção de recursos de computação dedicados, separados física ou logicamente, para todas as tarefas administrativas ou que exijam acesso administrativo. Os recursos de computação devem ser segmentados a partir da rede primária da empresa e não devem ter acesso à Internet. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A segregação de recursos de computação garante que privilégios são divididos entre usuários de forma que apenas usuários autorizados sejam capazes de controlar e executar tais artifícios.

4.4.8.6.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 6 do grupo de controle de Gerenciamento de infraestrutura de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO

27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
12	12.8	Dispositivos			X	Subconjunto	8.22	Segregação de redes.	Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.9 Monitoramento e defesa de rede

Opere processos e ferramentas para estabelecer e manter monitoramento de rede abrangente e defesa contra ameaças de segurança em toda a infraestrutura de rede e base de usuários da empresa. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

4.4.9.1 Salvaguarda 1: Centralização de alertas de eventos de segurança

Centralização de alertas de eventos de segurança nos ativos corporativos para correlação e análise de logs. A implementação de melhores práticas requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de logs configurada com alertas de correlação relevantes para a segurança também atende a essa proteção. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

A centralização de logs do sistema ajuda na realização da busca, fazendo com que seja mais rápida e favorecendo a proteção de dados, colaborando para a identificação de potenciais incidentes tendo em vista que os problemas são resolvidos de forma mais célere.

4.4.9.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle Monitoramento e defesa de rede pode ser mapeada para a função "Detectar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
13	13.1	Rede		**X**	**X**	Subconjunto	8.15	Logging.	Logs que registram atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.	Detectar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.9.2 Salvaguarda 2: Implantação de uma solução de detecção de intrusão baseada em host

Implantação de uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou suportado. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Justificativa: Solução de detecção de intrusão baseada em host auxiliam o monitoramento do comportamento do sistema operacional e das informações armazenadas ajudando a identificar comportamento anormais.

4.4.9.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle Monitoramento e defesa de rede pode ser mapeada para a função "Detectar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
13	13.2	Rede		X	X	Subconjunto	8.16	Atividades de monitoramento.	Redes, sistemas e aplicativos devem ser monitorados quanto a comportamento anômalo e ações apropriadas devem ser tomadas para avaliar possíveis incidentes de segurança da informação.	Detectar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.9.3 Salvaguarda 3: Implantar uma solução de detecção de intrusão de rede

Implante uma solução de detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Sistema de Detecção de Intrusão de Rede (NIDS) ou serviço de provedor de serviços de nuvem (CSP) equivalente. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Justificativa: Solução de detecção de intrusão baseada em rede auxilia na identificação de comportamentos suspeitos ajudando a fornecer uma visão abrangente da rede e de potenciais incidentes de segurança.

4.4.9.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle Monitoramento e defesa de rede pode ser mapeada para a função "Detectar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
13	13.3	Rede		X	X	Subconjunto	8.21	Segurança dos serviços de rede.	Mecanismos de segurança, níveis de serviço e requisitos de serviço de serviços de rede devem ser identificados, implementados e monitorados.	Detectar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.9.4 Salvaguarda 4: Gerenciamento do controle de acesso para ativos remotos

Gerenciamento do controle de acesso para ativos que se conectam remotamente a recursos corporativos. Determine a quantidade de acesso aos recursos corporativos com base em: software antimalware atualizado instalado, conformidade de configuração com o processo de configuração segura da empresa e garantia de que o sistema operacional e os aplicativos estejam atualizados. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Justificativa: O gerenciamento do controle de acesso de ativos remotos apoia as práticas de monitoramento, gestão e manutenção da infraestrutura de rede da organização.

4.4.9.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle Monitoramento e defesa de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
13	13.5	Dispositivo		**X**	**X**	Subconjunto	8.3	Restrição de acesso a informações.	O acesso a informações e outros ativos associados deve ser restrito de acordo com a política específica de tópico estabelecida sobre controle de acesso.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.9.5 Salvaguarda 5: Ajustar limites de alerta de eventos de segurança

Ajuste os limites de alerta de eventos de segurança mensalmente ou com mais frequência. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

A periodicidade de atualização dos alertas de eventos ajuda os operadores do sistema a se manter informados, recebendo notificações automatizadas que beneficiam na rápida resolução de incidentes.

4.4.9.5.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Monitoramento e defesa de rede pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
13	13.11	Rede			X	Subconjunto	5.7	Inteligência de ameaças.	As informações relacionadas às ameaças à segurança da informação devem ser coletadas e analisadas para produzir inteligência sobre ameaças.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10 Conscientização sobre segurança e treinamento de habilidades

Estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento entre a força de trabalho a ser consciente da segurança e adequadamente qualificada para reduzir os riscos de segurança cibernética para a empresa. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

4.4.10.1 Salvaguarda 1: Estabelecimento e manutenção de um programa de conscientização de segurança

Estabelecimento e manutenção de um programa de conscientização de segurança. O objetivo de um programa de conscientização de segurança é educar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Realizar treinamento na contratação e, no mínimo, anualmente. Revise e atualize o conteúdo anualmente, ou quando ocorrerem mudanças corporativas significativas que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Programas de conscientização de segurança da informação devem ser realizados por todos os usuários que trabalham e auxiliam na proteção dos ativos da organização, garantindo assim a continuidade do negócio.

4.4.10.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
14	14.1	N/A	**X**	**X**	**X**	Equivalente	6.3	Conscientização, educação e treinamento em segurança da informação.	O pessoal da organização e as partes interessadas relevantes devem receber conscientização, educação e treinamento de segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicos de tópicos, conforme relevante para sua função de trabalho.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10.2 Salvaguarda 2: Treinamento de membros da força de trabalho para reconhecer ataques de engenharia social

Treinamento dos membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, pré-texto e tailgating. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Manter software antivírus atualizado auxilia os usuários no reconhecimento de ataques sendo importantes para ajudar a identificar atividades anormais que podem afetar de forma significativa os sistemas da organização. Reconhecer ataques de engenharia social, como o phishing, onde um cibercriminoso consegue forjar comunicação com a vítima, que acredita ser um e-mail legítimo. Fraudadores comumente se passam por bancos ou empresas de cartão de crédito para realizar este tipo de ataque.

4.4.10.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
14	14.2	N/A	X	X	X	Subconjunto	8.7	Proteção contra malware.	A proteção contra malware deve ser implementada e suportada pela conscientização apropriada do usuário.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10.3 Salvaguarda 3: Treinar a força de trabalho nas melhores práticas de manipulação de dados

Treine os membros da força de trabalho sobre como identificar e armazenar, transferir, arquivar e destruir adequadamente dados confidenciais. Isso também inclui o treinamento dos membros da força de trabalho em práticas recomendadas de tela e mesa limpas, como bloquear a tela quando se afastam de seus ativos corporativos, apagar quadros brancos físicos e virtuais no final das reuniões e armazenar dados e ativos com segurança. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O treinamento para manipulação de dados é relevante para a compreensão dos funcionários sobre a importância de seguir regras de segurança da informação na organização e o valor da criticidade das informações manipuladas.

4.4.10.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
14	14.4	N/A	X	X	X	Subconjunto	5.10	Uso aceitável de informações e outros ativos associados.	Regras para o uso aceitável e procedimentos para lidar com informações e outros ativos associados devem ser identificados, documentados e implementados.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10.4 Salvaguarda 4: Treinar os membros da força de trabalho sobre as causas da exposição não intencional de dados

Treine os membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Os tópicos de exemplo incluem entrega incorreta de dados confidenciais, perda de um dispositivo portátil de usuário final ou publicação de dados para públicos não intencionais. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O treinamento dos membros da força de trabalho ajuda a evitar a exposição intencional de dados auxiliando na segurança da informação da organização.

4.4.10.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
14	14.5	N/A	**X**	**X**	**X**	Subconjunto	6.3	Conscientização, educação e treinamento em segurança da informação.	O pessoal da organização e as partes interessadas relevantes devem receber conscientização, educação e treinamento de segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicos de tópicos, conforme relevante para sua função de trabalho.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10.5 Salvaguarda 5: Treinar os membros da força de trabalho para reconhecer e relatar incidentes de segurança

Treine os membros da força de trabalho para serem capazes de reconhecer um incidente em potencial e de relatar tal incidente. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O treinamento dos membros da força de trabalho auxilia na identificação de incidentes ajudando no correto funcionamento da organização.

4.4.10.5.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 5 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
14	14.6	N/A	X	X	X	Subconjunto	6.8	Relatórios de eventos de segurança da informação.	Convém que a organização forneça um mecanismo para o pessoal relatar eventos de segurança da informação observados ou suspeitos por meio de canais apropriados em tempo hábil.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10.6 Salvaguarda 6: Treinar a força de trabalho sobre os perigos da conexão e transmissão de dados corporativos em redes inseguras

Treine os membros da força de trabalho sobre os perigos de se conectar e transmitir dados por redes inseguras para atividades corporativas. Se a empresa tiver funcionários

remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O treinamento da força de trabalho auxilia os usuários nas boas práticas de como se deve realizar a transmissão de dados nas atividades corporativas da organização.

4.4.10.6.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 6 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
14	14.8	N/A	**X**	**X**	**X**	Subconjunto	6.3	Conscientização, educação e treinamento em segurança da informação.	O pessoal da organização e as partes interessadas relevantes devem receber conscientização, educação e treinamento de segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicos de tópicos, conforme relevante para sua função de trabalho.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.10.7 Salvaguarda 7: Realização de treinamento de habilidades e conscientização de segurança específica da função

Realização de conscientização de segurança e treinamento de habilidades específicas da função. As implementações de exemplo incluem cursos de administração de sistemas seguros para profissionais de TI (OWASP® Top 10 treinamento de prevenção e conscientização de vulnerabilidades para desenvolvedores de aplicativos da Web e

treinamento avançado de conscientização de engenharia social para funções de alto perfil. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O treinamento de habilidades e conscientização de segurança específica da função é importante pois os usuários devem conhecer as vulnerabilidades associadas a sua área de atuação na função que desempenha para que se reduza fragilidades nas organizações.

4.4.10.7.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 7 do grupo de controle Conscientização sobre segurança e treinamento de habilidades pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
14	14.9	N/A		X	X	Subconjunto	6.3	Conscientização, educação e treinamento em segurança da informação.	O pessoal da organização e as partes interessadas relevantes devem receber conscientização, educação e treinamento de segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicos de tópicos, conforme relevante para sua função de trabalho.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.11 Gerenciamento de Resposta a Incidentes

Estabelece um programa para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

4.4.11.1 Salvaguarda 1: Designar Pessoal para Gerenciar o Tratamento de Incidentes

Designe uma pessoa chave e pelo menos um backup para gerenciar o processo de tratamento de incidentes da empresa. A equipe de gerenciamento é responsável pela coordenação e documentação dos esforços de recuperação e resposta a incidentes e pode consistir em funcionários internos da empresa, fornecedores terceirizados ou uma abordagem híbrida. Se estiver usando um fornecedor terceirizado, designe pelo menos uma pessoa interna da empresa para supervisionar qualquer trabalho de terceiros. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

É boa prática definir qual é a pessoa ou grupo de pessoas que será responsável pela resposta ao incidente, para que cada pessoa ou grupo assuma sua responsabilidade imputada sabendo como proceder de maneira célere e eficaz.

4.4.11.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle Gerenciamento de Resposta a Incidentes pode ser mapeada para a função "Responder" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
17	17.1	N/A	X	X	X	Subconjunto	5.24	Planejamento e preparação de gerenciamento de incidentes de segurança da informação.	A organização deve planejar e se preparar para gerenciar incidentes de segurança da informação, definindo, estabelecendo e comunicando processos, funções e responsabilidades de gerenciamento de incidentes de segurança da informação.	Responder

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.11.2 Salvaguarda 2: Estabelecimento e manutenção de um processo de resposta a incidentes

Estabelecimento e manutenção de um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

O processo de resposta a incidentes é o processo que uma organização possui para responder a ameaças de TI, como violação de segurança e ataques cibernéticos. Possui o objetivo de identificar ameaças de segurança reais, limitar danos causados, traçar planos para colocar a situação sob controle e reduzir custos de recuperação. Dessa forma, as organizações podem evitar mais perdas e reduzir os danos.

4.4.11.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle Gerenciamento de Resposta a Incidentes pode ser mapeada para a função "Responder" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	CIS Salvaguarda	Tipo de Ativo	GI 1	GI 2	GI 3	Relação	# Controle ISO	Título do Controle ISO	Texto do Controle ISO	Função
17	17.4	N/A		X	X	Subconjunto	5.24	Planejamento e preparação de gerenciamento de incidentes de segurança da informação.	A organização deve planejar e se preparar para gerenciar incidentes de segurança da informação, definindo, estabelecendo e comunicando processos, funções e responsabilidades de gerenciamento de incidentes de segurança da informação.	Responder

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.11.3 Salvaguarda 3: Realizar exercícios de rotina de resposta a incidentes

Planejamento e condução de exercícios e cenários de resposta a incidentes de rotina para o pessoal-chave envolvido no processo de resposta a incidentes para se preparar para responder a incidentes do mundo real. Os exercícios precisam testar canais de comunicação, tomada de decisão e fluxos de trabalho. Realizar testes anualmente, no mínimo. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Os exercícios de respostas a incidentes contribuem para uma solução eficaz sendo necessário realizar esses exercícios para validar se os procedimentos mapeados para responder aos incidentes permanecem válidos e se todos os contatos necessários podem ser acionados e o tempo para condução da resposta é satisfatório.

4.4.11.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle Gerenciamento de Resposta a Incidentes pode ser mapeada para a função "Responder" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
17	17.7	N/A		**X**	**X**	Subconjunto	5.30	Prontidão de TIC para continuidade de negócios.	A prontidão de TIC deve ser planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade de TIC.	Recuperar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.11.4 Salvaguarda 4: Realizar revisões pós-incidente

Realização de revisões pós-incidente. As revisões pós-incidente ajudam a prevenir a recorrência de incidentes por meio da identificação de lições aprendidas e ações de acompanhamento. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A realização de revisões pós-incidentes colabora para absorver todas as lições aprendidas conduzindo assim uma análise retrospectiva do incidente e fazendo a escrita de novos procedimentos, melhoria dos existentes e propagação do conhecimento.

4.4.11.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle Gerenciamento de Resposta a Incidentes pode ser mapeada para a função "Recuperar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
17	17.8	N/A		**X**	**X**	Subconjunto	5.24	Aprendendo com incidentes de segurança da informação.	O conhecimento adquirido com os incidentes de segurança da informação deve ser usado para fortalecer e melhorar os controles de segurança da informação.	Recuperar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.12 Teste de Penetração

Teste a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de pontos fracos nos controles (pessoas, processos e tecnologia) e simulando os objetivos e as ações de um invasor. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

4.4.12.1 Salvaguarda 1: Estabelecimento e manutenção de um programa de testes de penetração

Estabelecimento e manutenção de um programa de teste de penetração adequado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de penetração incluem escopo, como rede, aplicativo da Web, Interface de programação de aplicativos (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações de ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; e requisitos retrospectivos. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Programa de testes de penetração contribuem para que se conheça a capacidade de segurança do sistema para minimizar a exposição a ciberataques à organização.

4.4.12.1.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 1 do grupo de controle Teste de Penetração pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
18	18.1	N/A		**X**	**X**	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.12.2 Salvaguarda 2: Realize testes periódicos de penetração externa

Realize testes de penetração externos periódicos com base nos requisitos do programa, pelo menos anualmente. O teste de penetração externo deve incluir reconhecimento empresarial e ambiental para detectar informações exploráveis. O teste de penetração requer habilidades e experiência especializadas e deve ser realizado por uma parte qualificada. O teste pode ser caixa transparente ou caixa opaca. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Os testes de penetração externos colaboram para uma maior confiabilidade da infraestrutura de tecnologia da informação, conhecendo as vulnerabilidades e minimizando os riscos na organização.

4.4.12.2.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 2 do grupo de controle Teste de Penetração pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Controle ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
18	18.2	Rede		**X**	**X**	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.12.3 Salvaguarda 3: Validar medidas de segurança

Validação das medidas de segurança após cada teste de penetração. Se necessário, modifique conjuntos de regras e recursos para detectar as técnicas usadas durante o teste. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

A validação das medidas de segurança depois de um teste de penetração ajuda na melhoria de práticas e rotinas contribuindo para o bom funcionamento da organização.

4.4.12.3.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 3 do grupo de controle Teste de Penetração pode ser mapeada para a função "Proteger" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Control e ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
18	18.4	Rede			**X**	Subconjunto	8.8	Gerenciamento de vulnerabilidades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Proteger

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

4.4.12.4 Salvaguarda 4: Realize testes periódicos de penetração interna

Realização de testes de penetração internos periódicos com base nos requisitos do programa, pelo menos anualmente. O teste pode ser caixa branca ou caixa preta. (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.])

Testes de penetração internos contribuem para que a organização esteja protegida contra ameaças internas, entendendo possíveis vulnerabilidades encontradas e fazendo com que se aprimore a segurança da informação.

4.4.12.4.1 Mapeamento do controle para a ISO 27002 e NIST CF

A Salvaguarda 4 do grupo de controle Teste de Penetração pode ser mapeada para a função "Identificar" do NIST CF e para os controles do CIS e ISO 27002 mostrados na tabela a seguir (CIS CONTROLS V8 MAPPING TO ISO/IEC 27002, [s. d.]).

CIS Controls						Mapeamento ISO 27002				NIST CF
Control #	**CIS Salvaguarda**	**Tipo de Ativo**	**GI 1**	**GI 2**	**GI 3**	**Relação**	**# Control e ISO**	**Título do Controle ISO**	**Texto do Controle ISO**	**Função**
18	18.5	N/A			**X**	Subconjunto	8.8	Gerencia mento de vulnerabili dades técnicas.	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas.	Identificar

Fonte: CIS Controls v8 Mapping to ISO/IEC 27002:2022, 2023.

CONCLUSÃO

Este projeto foi concebido no intuito de colaborar para a segurança da informação nos sistemas de telemedicina, do ponto de vista operacional, visando ajudar as organizações de saúde.

Partindo do alinhamento do CIS Controls, da ISO/IEC 27001 e da ISO/IEC 27002, no âmbito do projeto foi desenvolvido um manual de boas práticas para os sistemas de telemedicina alinhados com os requisitos dos controles do CIS Controls mapeado com os requisitos dos controles da ISO/IEC 27002:2022 e do NIST CF. A partir do Mapeamento Sistemático da Literatura foram encontrados controles que contribuem de forma eficaz para a segurança da informação nas organizações de saúde onde a telemedicina se faz presente e outros controles foram elegidos de forma que complementam a eficácia do manual. O CIS Controls foi utilizado pois estabelece um grupo de práticas prescritivas e priorizadas aconselhadas de segurança cibernética e ações defensivas que podem ajudar a mitigar ataques com o intuito de escolhermos os processos que podem ser utilizados nos sistemas de telemedicina tanto para pequenas organizações de saúde como também para organizações de saúde de porte médio e para organizações de saúde de grande porte.

O manual é aplicável a todas as organizações do setor da saúde, independente da sua dimensão, natureza ou tipologia desde que possua sistema de telemedicina.

Considerando que o ambiente de tecnologia da informação nos sistemas de telemedicina é dinâmico onde novas tecnologias são criadas e novas vulnerabilidades são descobertas sendo de fundamental importância que os atuais controles sejam atualizados e novos controles sejam utilizados para que se possa mitigar de forma efetiva a ocorrência de ameaças que possam ocorrer. Nesse sentido, a sustentabilidade e a melhoria contínua dos controles se faz necessária perante a complexidade dos sistemas de telemedicina face à carência de competências e recursos ao nível da segurança da informação e proteção de dados nas organizações de saúde que possuem sistemas de telemedicina. Com o surgimento e necessidade de adequação à Lei Geral de Proteção de Dados (LGPD) e a General Data Protection Regulation (GDPR), existe a necessidade futura de realizar a implementação da ISO/IEC 27701 por se tratar de fazer o processamento de dados pessoais e por realizar o controle e efetuar a utilização de dados pessoais. Isso significa que além dos controles previstos num SGSI, que realiza a garantia da integridade, confidencialidade e disponibilidade dos dados, este sistema de gestão deve ser desenvolvido para um Privacy Information

Management System (PIMS), que também é um sistema de gestão, porém preocupado também com a gestão da privacidade de dados pessoais.

REFERÊNCIAS

QUE É PESQUISA APLICADA? | DIFERENÇAS COM A PESQUISA BÁSICA |. [*S. l.*], 2022. Disponível em: https://www.metodologiacientifica.org/tipos-de-pesquisa/pesquisa-aplicada/. Acesso em: 16 abr. 2023.

A DOUBLE CHAOTIC LAYER ENCRYPTION ALGORITHM FOR CLINICAL SIGNALS IN TELEMEDICINE | SPRINGERLINK. [*S. l.*], [*s. d.*]. Disponível em: https://link.springer.com/article/10.1007/s10916-017-0698-3. Acesso em: 1 jul. 2022.

ABD-EL-ATTY, B. *et al.* A Robust Quasi-Quantum Walks-Based Steganography Protocol for Secure Transmission of Images on Cloud-Based E-healthcare Platforms. **Sensors (Basel, Switzerland)**, [*s. l.*], v. 20, n. 11, p. E3108, 2020.

ABDUNABI, R.; RAY, I.; FRANCE, R. Specification and analysis of access control policies for mobile applications. *Em*: THE 18TH ACM SYMPOSIUM, 2013, Amsterdam, The Netherlands. **Proceedings of the 18th ACM symposium on Access control models and technologies - SACMAT '13**. Amsterdam, The Netherlands: ACM Press, 2013. p. 173. Disponível em: http://dl.acm.org/citation.cfm?doid=2462410.2463206. Acesso em: 1 jul. 2022.

AHMAD, I.; SHIN, S. Region-based Selective Compression and Selective Encryption of Medical Images. *Em*: SMA 2020: THE 9TH INTERNATIONAL CONFERENCE ON SMART MEDIA AND APPLICATIONS, 2020, Jeju Republic of Korea. **The 9th International Conference on Smart Media and Applications**. Jeju Republic of Korea: ACM, 2020. p. 34–38. Disponível em: https://dl.acm.org/doi/10.1145/3426020.3426027. Acesso em: 1 jul. 2022.

ALBAYOOD, Z. S. A.; ELFALLAH, E. A. O.; ELGHRIANI, A. Measuring the awareness of health care providers at Benghazi Medical Center for Health Informatics. *Em*: ICEMIS'20: THE 6TH INTERNATIONAL CONFERENCE ON ENGINEERING & MIS 2020, 2020, Almaty Kazakhstan. **Proceedings of the 6th International Conference on Engineering & MIS 2020**. Almaty Kazakhstan: ACM, 2020. p. 1–6. Disponível em: https://dl.acm.org/doi/10.1145/3410352.3410733. Acesso em: 1 jul. 2022.

ALBERTIN, A. L.; PINOCHET, L. H. C. **Política de Segurança de Informações**. [*S. l.*]: Elsevier, 2010.

AL-HAJ, A.; AMER, A. Secured telemedicine using region-based watermarking with tamper localization. **Journal of Digital Imaging**, [*s. l.*], v. 27, n. 6, p. 737–750, 2014.

ALHARBE, N.; ATKINS, A. S.; AKBARI, A. S. Application of ZigBee and RFID Technologies in Healthcare in Conjunction with the Internet of Things. *Em*: INTERNATIONAL CONFERENCE, 2013, Vienna, Austria. **Proceedings of International Conference on Advances in Mobile Computing & Multimedia - MoMM '13**. Vienna, Austria: ACM Press, 2013. p. 191–195. Disponível em: http://dl.acm.org/citation.cfm?doid=2536853.2536904. Acesso em: 1 jul. 2022.

ALVO DE HACKERS, DADOS SOBRE SUA SAÚDE VALEM MAIS QUE SEU CARTÃO DE CRÉDITO. [*S. l.*], [*s. d.*]. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/11/04/dados-sobre-sua-saude-valem-mais-que-os-do-seu-cartao-de-credito.htm. Acesso em: 18 mar. 2023.

ANAIS_CBIS_2016_ARTIGOS_COMPLETOS-1041-1050.PDF. , [*s. d.*]. Disponível em: https://docs.bvsalud.org/biblioref/2018/07/906776/anais_cbis_2016_artigos_completos-1041-1050.pdf. Acesso em: 1 jul. 2022.

ANASTASOPOULOU, K. *et al.* Public and private healthcare organisations: a socio-technical model for identifying cybersecurity aspects. *Em*: ICEGOV 2020: 13TH INTERNATIONAL CONFERENCE ON THEORY AND PRACTICE OF ELECTRONIC GOVERNANCE, 2020, Athens Greece. **Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance**. Athens Greece: ACM, 2020. p. 168–175. Disponível em: https://dl.acm.org/doi/10.1145/3428502.3428525. Acesso em: 1 jul. 2022.

ANTONESCU, B.; BASAGNI, S. Wireless Body Area Networks: Challenges, Trends and Emerging Technologies. *Em*: 8TH INTERNATIONAL CONFERENCE ON BODY AREA NETWORKS, 2013, Boston, United States. **Proceedings of the 8th International Conference on Body Area Networks**. Boston, United States: ACM, 2013. Disponível em: http://eudl.eu/doi/10.4108/icst.bodynets.2013.253722. Acesso em: 1 jul. 2022.

ANZIVINO, S.; TESSAROLO, F. THE UNCAP EXPERIENCE IN DEVELOPING ICT FOR HEALTH: "HTA BY DESIGN. [*s. l.*], 2010. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3183624.3183625.

ARORA, S.; YTTRI, J.; NILSE, W. Privacy and Security in Mobile Health (mHealth) Research. **Alcohol Research: Current Reviews**, [*s. l.*], v. 36, n. 1, p. 143–151, 2014.

ASSLABER, M.; ZATLOUKAL, K. Biobanks: transnational, European and global networks. **Briefings in Functional Genomics**, [*s. l.*], v. 6, n. 3, p. 193–201, 2007. Disponível em: https://doi.org/10.1093/bfgp/elm023. Acesso em: 18 fev. 2022.

AVANCHA, S.; BAXI, A.; KOTZ, D. Privacy in mobile technology for personal healthcare. **ACM Computing Surveys**, [*s. l.*], v. 45, n. 1, p. 1–54, 2012. Disponível em: https://dl.acm.org/doi/10.1145/2379776.2379779. Acesso em: 1 jul. 2022.

ÁVILA, R. Como usar o Ciclo PDCA para melhorar a sua gestão financeira. *Em*: BLOG LUZ. 2015. Disponível em: https://blog.luz.vc/como-fazer/como-usar-o-ciclo-pdca-para-melhorar-a-sua-gestao-financeira/. Acesso em: 7 jun. 2021.

AWOTWI, J. E. ICT-enabled delivery of maternal health services. *Em*: THE 6TH INTERNATIONAL CONFERENCE, 2012, Albany, New York. **Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance - ICEGOV '12**. Albany, New York: ACM Press, 2012. p. 369. Disponível em: http://dl.acm.org/citation.cfm?doid=2463728.2463798. Acesso em: 1 jul. 2022.

AZEVEDO, J.; PEREIRA, R. L.; CHAINHO, P. An API proposal for integrating sensor data into web apps and WebRTC. *Em*: EUROSYS '15: TENTH EUROSYS CONFERENCE 2015, 2015, Bordeaux France. **Proceedings of the 1st Workshop on All-Web Real-Time Systems**. Bordeaux France: ACM, 2015. p. 1–5. Disponível em: https://dl.acm.org/doi/10.1145/2749215.2749221. Acesso em: 1 jul. 2022.

BARROS, A. J. da S.; LEHFELD, N. A. de S. **Fundamentos de Metodologia Científica**. [*S. l.: s. n.*], 2014. *E-book*. Disponível em: Acesso em: 6 jul. 2021.

BETH. Telemedicina: como garantir a segurança de dados do paciente. *Em*: PORTAL TELEMEDICINA. 13 nov. 2019. Disponível em: https://portaltelemedicina.com.br/blog/como-garantir-a-seguranca-de-dados-dos-pacientes. Acesso em: 20 ago. 2022.

BLARDONE, S. **Telemedicina: ¿qué es y para qué se utiliza?**. [*S. l.*], 2013a. Disponível em: /2013/11/17/1524294-telemedicina-que-es-y-que-se-utiliza/. Acesso em: 7 jun. 2021.

BLARDONE, S. **Telemedicina: ¿qué es y para qué se utiliza?**. [*S. l.*], 2013b. Disponível em: /2013/11/17/1524294-telemedicina-que-es-y-que-se-utiliza/. Acesso em: 7 jun. 2021.

BOLLE, S. R.; HASVOLD, P.; HENRIKSEN, E. Video calls from lay bystanders to dispatch centers - risk assessment of information security. **BMC health services research**, [*s. l.*], v. 11, p. 244, 2011.

BRECHAS DE SEGURANÇA PODEM AFETAR ATÉ EQUIPAMENTOS MÉDICOS. [*S. l.*], 2014. Disponível em: https://exame.com/tecnologia/brechas-de-seguranca-podem-afetar-ate-equipamentos-medicos/. Acesso em: 18 mar. 2023.

BRIDGES, K. H.; MCSWAIN, J. R.; WILSON, P. R. To Infinity and Beyond: The Past, Present, and Future of Tele-Anesthesia. **Anesthesia and Analgesia**, [*s. l.*], v. 130, n. 2, p. 276–284, 2020.

BRUST, C. S.; CLARK, R. System simulation as decision data in heathcare it. *Em*: 2014 WINTER SIMULATION CONFERENCE - (WSC 2014), 2014, Savanah, GA, USA. **Proceedings of the Winter Simulation Conference 2014**. Savanah, GA, USA: IEEE, 2014. p. 1317–1328. Disponível em: http://ieeexplore.ieee.org/document/7019987/. Acesso em: 1 jul. 2022.

BURKE, W. *et al*. Cybersecurity Indexes for eHealth. *Em*: , 2019, New York, NY, USA. **Proceedings of the Australasian Computer Science Week Multiconference**. New York, NY, USA: Association for Computing Machinery, 2019. p. 1–8. Disponível em: https://doi.org/10.1145/3290688.3290721. Acesso em: 9 mar. 2022.

CERVO, A. L.; BERVIAN, P. A.; DA SILVA, R. **Que é Pesquisa Exploratória? | Objetivos | Técnicas | Exemplos**. [*S. l.*], 2007. Disponível em: https://www.metodologiacientifica.org/tipos-de-pesquisa/pesquisa-exploratoria/. Acesso em: 7 jun. 2021.

CHEN, Y. *et al.* SD-WAN Source Route Based on Protocol-oblivious Forwarding. *Em*: THE 8TH INTERNATIONAL CONFERENCE, 2018, Qingdao, China. **Proceedings of the 8th International Conference on Communication and Network Security - ICCNS 2018**. Qingdao, China: ACM Press, 2018. p. 95–99. Disponível em: http://dl.acm.org/citation.cfm?doid=3290480.3290486. Acesso em: 1 jul. 2022.

CICLO PDCA. *Em*: WIKIPÉDIA, A ENCICLOPÉDIA LIVRE. [*S. l.*: *s. n.*], 2021. Disponível em: https://pt.wikipedia.org/w/index.php?title=Ciclo_PDCA&oldid=61236583. Acesso em: 7 jun. 2021.

CIS CONTROLS®. [*S. l.*], [*s. d.*]. Disponível em: https://documentacao.senior.com.br/seguranca-da-informacao/frameworks/cis-controls.htm. Acesso em: 13 out. 2022.

CIS CONTROLS V8 MAPPING TO ISO/IEC 27002:2002. [*S. l.*], [*s. d.*]. Disponível em: https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-iso-iec2-27002-2022. Acesso em: 5 dez. 2022.

COMO IMPLEMENTAR COM SUCESSO OS CONTROLES CIS CONTROLS V8. [*S. l.*], 2021. Disponível em: https://www.gat.digital/blog/implementacao-de-controles-cis/. Acesso em: 11 out. 2022.

CONHEÇA OS 8 BENEFÍCIOS DA AQUISIÇÃO DE UMA SGSI BASEADO NA ISO 27001. *Em*: DUALSYS INFORMÁTICA. 8 jul. 2021. Disponível em: https://dualsys.com.br/blog/conheca-os-8-beneficios-da-aquisicao-de-uma-sgsi-baseado-na-iso-27001/. Acesso em: 18 abr. 2023.

CONTROLES DE SEGURANÇA: MAPEANDO O CIS E A NOVA ISO/IEC 27002. [*S. l.*], [*s. d.*]. Disponível em: https://pt.linkedin.com/pulse/controles-de-seguran%C3%A7a-mapeando-o-cis-e-nova-isoiec-27002-bastos. Acesso em: 15 out. 2022.

CRUZ, C. H. **A telemedicina e os direitos dos pacientes**. [*S. l.*], 2020. Disponível em: https://chcadvocacia.adv.br/blog/telemedicina/. Acesso em: 7 jun. 2021.

CUI, F. *et al.* Implementation and Application of Telemedicine in China: Cross-Sectional Study. **JMIR mHealth and uHealth**, [*s. l.*], v. 8, n. 10, p. e18426, 2020. Disponível em: https://mhealth.jmir.org/2020/10/e18426. Acesso em: 1 jul. 2022.

CYBERSECURITY INDEXES FOR EHEALTH | PROCEEDINGS OF THE AUSTRALASIAN COMPUTER SCIENCE WEEK MULTICONFERENCE. [*S. l.*], [*s. d.*]. Disponível em: https://dl.acm.org/doi/abs/10.1145/3290688.3290721. Acesso em: 1 jul. 2022.

DE-LA-TORRE-UGARTE-GUANILO, M. C.; TAKAHASHI, R. F.; BERTOLOZZI, M. R. Revisão sistemática: noções gerais. **Revista da Escola de Enfermagem da USP**, [*s. l.*], v. 45, n. 5, p. 1260–1266, 2011. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0080-62342011000500033&lng=pt&tlng=pt. Acesso em: 18 fev. 2022.

DERMEVAL, D.; BITTENCOURT, I. I. Mapeamento Sistemático e Revisão Sistemática da Literatura em Informática na Educação. [*s. l.*], p. 26,

DESIGN AND DEVELOP A VIDEO CONFERENCING FRAMEWORK FOR REAL-TIME TELEMEDICINE APPLICATIONS USING SECURE GROUP-BASED COMMUNICATION ARCHITECTURE | SPRINGERLINK. [*S. l.*], [*s. d.*]. Disponível em: https://link.springer.com/article/10.1007/s10916-014-0133-y. Acesso em: 1 jul. 2022.

DEVOTEAM, I. **ISO 27001**. [*S. l.*], [*s. d.*]. Portal Informativo. Disponível em: https://www.27001.pt/. Acesso em: 18 fev. 2022.

DIRIN, M.; DIRIN, A.; LAINE, T. H. User-centered design of a context-aware nurse assistant (CANA) at Finnish elderly houses. *Em*: IMCOM '15: THE 9TH INTERNATIONAL CONFERENCE ON UBIQUITOUS INFORMATION MANAGEMENT AND COMMUNICATION, 2015, Bali Indonesia. **Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication**. Bali Indonesia: ACM, 2015. p. 1–8. Disponível em: https://dl.acm.org/doi/10.1145/2701126.2701225. Acesso em: 1 jul. 2022.

DUAN, D.; HUANG, M.; MU, Y. Research for Building High Performance Communication Service Based on Netty Protocol in Smart Health. *Em*: THE 9TH INTERNATIONAL CONFERENCE, 2017, Auckland, New Zealand. **Proceedings of the 9th International Conference on Signal Processing Systems - ICSPS 2017**. Auckland, New Zealand: ACM Press, 2017. p. 18–21. Disponível em: http://dl.acm.org/citation.cfm?doid=3163080.3163121. Acesso em: 1 jul. 2022.

ELDEIB, A. M. Interactive telemedicine solution based on a secure mHealth application. *Em*: 2014 36TH ANNUAL INTERNATIONAL CONFERENCE OF THE IEEE ENGINEERING IN MEDICINE AND BIOLOGY SOCIETY, 2014. **2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society**. [*S. l.: s. n.*], 2014. p. 3699–3702.

E-SAÚDE E DESAFIOS À PROTEÇÃO DA PRIVACIDADE NO BRASIL | POLITICS. [*S. l.*], [*s. d.*]. Disponível em: https://politics.org.br/edicoes/e-sa%C3%BAde-e-desafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil. Acesso em: 12 mar. 2022.

FABIANA. 10 Benefícios ISO 27001 para a sua organização. *Em*: TEMPLUM PORTUGAL. 10 set. 2021. Disponível em: https://templum.pt/10-beneficios-iso-27001-para-a-sua-organizacao/. Acesso em: 22 fev. 2023.

FACHIN, O.; BARROS, L. **Conceito de Pesquisa Bibliográfica | Como fazer?**. [*S. l.*], 2017. Disponível em: https://www.metodologiacientifica.org/tipos-de-pesquisa/pesquisa-bibliografica/. Acesso em: 7 jun. 2021.

FADHIL, A.; GABRIELLI, S.; KESSLER, F. Addressing Challenges in Promoting Healthy Lifestyles: The AI-Chatbot Approach. [*s. l.*], 2017. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3154862.3154914.

FAZIO, M. *et al.* A Hybrid Storage Service for the Management of Big e-Health Data: A Tele-Rehabilitation Case of Study. *Em*: MSWIM '16: 19TH ACM INTERNATIONAL CONFERENCE ON MODELING, ANALYSIS AND SIMULATION OF WIRELESS AND MOBILE SYSTEMS, 2016, Malta Malta. **Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks**. Malta Malta: ACM, 2016. p. 1–8. Disponível em: https://dl.acm.org/doi/10.1145/2988272.2988276. Acesso em: 1 jul. 2022.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. 1. ed. [*S. l.*]: Brasport, 2012.

FRØYSTAD, C.; BERNSMED, K.; MELAND, P. H. Protecting Future Maritime Communication. *Em*: ARES '17: INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, 2017, Reggio Calabria Italy. **Proceedings of the 12th International Conference on Availability, Reliability and Security**. Reggio Calabria Italy: ACM, 2017. p. 1–10. Disponível em: https://dl.acm.org/doi/10.1145/3098954.3103169. Acesso em: 1 jul. 2022.

GARCIA, T. M. MAPEAMENTO SISTEMÁTICO: Adoção de Padrões de Interoperabilidade no Governo. [*s. l.*], p. 15,

GARG, V.; BREWER, J. Telemedicine security: a systematic review. **Journal of Diabetes Science and Technology**, [*s. l.*], v. 5, n. 3, p. 768–777, 2011.

GARG, V.; CAMP, L. J. Gandhigiri in cyberspace: a novel approach to information ethics. **ACM SIGCAS Computers and Society**, [*s. l.*], v. 42, n. 1, p. 9–20, 2012. Disponível em: https://dl.acm.org/doi/10.1145/2422512.2422514. Acesso em: 1 jul. 2022.

GHOSE, A. *et al.* Mobile healthcare infrastructure for home and small clinic. *Em*: THE 2ND ACM INTERNATIONAL WORKSHOP, 2012a, Hilton Head, South Carolina, USA. **Proceedings of the 2nd ACM international workshop on Pervasive Wireless Healthcare - MobileHealth '12**. Hilton Head, South Carolina, USA: ACM Press, 2012. p. 15. Disponível em: http://dl.acm.org/citation.cfm?doid=2248341.2248347. Acesso em: 1 jul. 2022.

GHOSE, A. *et al.* Mobile healthcare infrastructure for home and small clinic. *Em*: , 2012b, New York, NY, USA. **Proceedings of the 2nd ACM international workshop on Pervasive Wireless Healthcare**. New York, NY, USA: Association for Computing Machinery, 2012. p. 15–20. Disponível em: https://doi.org/10.1145/2248341.2248347. Acesso em: 8 jun. 2022.

GHOSH, A.; HUI, Y.-K.; CHIANG, M. Model-based architecture analysis for wireless healthcare. *Em*: THE FIRST ACM MOBIHOC WORKSHOP, 2011, Paris, France. **Proceedings of the First ACM MobiHoc Workshop on Pervasive Wireless Healthcare - MobileHealth '11**. Paris, France: ACM Press, 2011. p. 1. Disponível em: http://portal.acm.org/citation.cfm?doid=2007036.2007051. Acesso em: 1 jul. 2022.

GORBACH, V.; ALI, M. L.; THAKUR, K. A Review of Data Privacy Techniques for Wireless Body Area Networks in Telemedicine. *Em*: 2020 IEEE INTERNATIONAL IOT, ELECTRONICS AND MECHATRONICS CONFERENCE (IEMTRONICS), 2020. **2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)**. [*S. l.: s. n.*], 2020. p. 1–6.

GORELOV, V. A. *et al.* Complex Methodological Approach to Introduction of Modern Telemedicine Technologies into the Healthcare System on Federal, Regional and Municipal Levels. *Em*: 2020 INTERNATIONAL CONFERENCE QUALITY MANAGEMENT, TRANSPORT AND INFORMATION SECURITY, INFORMATION TECHNOLOGIES (IT&QM&IS), 2020. **2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)**. [*S. l.: s. n.*], 2020. p. 468–473.

GOSSEN, A. *et al.* The Isolation Communication Management System. A Telemedicine Platform to Care for Patients in a Biocontainment Unit. **Annals of the American Thoracic Society**, [*s. l.*], v. 17, n. 6, p. 673–678, 2020. Disponível em: https://www.atsjournals.org/doi/10.1513/AnnalsATS.202003-261IP. Acesso em: 1 jul. 2022.

GRAVENHORST, F. *et al.* Mobile phones as medical devices in mental disorder treatment: an overview. **Personal and Ubiquitous Computing**, [*s. l.*], v. 19, n. 2, p. 335–353, 2015. Disponível em: https://doi.org/10.1007/s00779-014-0829-5. Acesso em: 1 jul. 2022.

GSTI, P. **O que é ISO 27001 e ISO 27002 - Portal GSTI**. [*S. l.*], [*s. d.*]. Portal Informativo. Disponível em: https://www.portalgsti.com.br/iso-27001-iso-27002/sobre/. Acesso em: 18 fev. 2022 a.

GSTI, P. **Sistema de Gestão de Segurança da Informação (SGSI) - Portal GSTI**. [*S. l.*], [*s. d.*]. Portal Informativo. Disponível em: https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html. Acesso em: 18 fev. 2022 b.

HABIB, A.; BHATTACHARJEE, M. K.; CHOWDHURY, D. IT-based Services through UISC: A Framework towards Digital Bangladesh. *Em*: THE 2014 CONFERENCE, 2014, St. Petersburg, Russian Federation. **Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia - EGOSE '14**. St. Petersburg, Russian Federation: ACM Press, 2014. p. 45–53. Disponível em: http://dl.acm.org/citation.cfm?doid=2729104.2729123. Acesso em: 1 jul. 2022.

HALUZA, D. *et al.* Prevailing Opinions on Connected Health in Austria: Results from an Online Survey. **International Journal of Environmental Research and Public Health**, [*s. l.*], v. 13, n. 8, p. E813, 2016.

HARJITO, B.; POTDAR, V.; SINGH, J. Watermarking technique for wireless multimedia sensor networks: a state of the art. [*s. l.*], p. 9,

HENRIKSEN, E. *et al.* Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. **BMC medical informatics and decision making**, [*s. l.*], v. 13, p. 85, 2013.

HOFER, T.; SCHUMACHER, M.; BROMURI, S. COMPASS: an Interoperable Personal Health System to Monitor and Compress Signals in Chronic Obstructive Pulmonary Disease. *Em*: 9TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING TECHNOLOGIES FOR HEALTHCARE, 2015, Istanbul, Turkey. **Proceedings of the 9th International Conference on Pervasive Computing Technologies for Healthcare**. Istanbul, Turkey: ICST, 2015. Disponível em: http://eudl.eu/doi/10.4108/icst.pervasivehealth.2015.259186. Acesso em: 1 jul. 2022.

HSU, W.-S.; PAN, J.-I. Secure mobile agent for telemedicine based on P2P networks. **Journal of Medical Systems**, [*s. l.*], v. 37, n. 3, p. 9947, 2013.

HUANG, L.-C.; LIU, W.-C.; CHOU, S.-C. T. Howcare: a personal health cloud archive and care-partners' community. [*s. l.*], p. 5, 2013.

ISO 27001. [*S. l.*], [*s. d.*]. Disponível em: https://www.pwiki.org/wiki/ISO_27001#Hist%C3%B3ria_da_ISO/IEC_27001. Acesso em: 14 jul. 2021.

ISO 27002: BOA PRÁTICAS PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO. *Em*: OSTEC | SEGURANÇA DIGITAL DE RESULTADOS. 30 dez. 2016. Disponível em: https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi/. Acesso em: 26 jul. 2021.

JATI, G. *et al.* An efficient secure ECG compression based on 2D-SPIHT and SIT algorithm. *Em*: 2017 INTERNATIONAL WORKSHOP ON BIG DATA AND INFORMATION SECURITY (IWBIS), 2017. **2017 International Workshop on Big Data and Information Security (IWBIS)**. [*S. l.: s. n.*], 2017. p. 155–160.

JUMREORNVONG, O. *et al.* Telemedicine and Medical Education in the Age of COVID-19. **Academic Medicine**, [*s. l.*], v. 95, n. 12, p. 1838–1843, 2020. Disponível em: https://journals.lww.com/10.1097/ACM.0000000000003711. Acesso em: 1 jul. 2022.

KACHURINA, P. *et al.* The Synergy of Gamification and Mathematical Modelling in eHealthcare. *Em*: EGOSE '15: CHALLENGES IN EURASIA, 2015, St. Petersburg Russian Federation. **Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia**. St. Petersburg Russian Federation: ACM, 2015. p. 116–122. Disponível em: https://dl.acm.org/doi/10.1145/2846012.2846046. Acesso em: 1 jul. 2022.

KAPLAN, B. REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. **International Journal of Medical Informatics**, [*s. l.*], v. 143, p. 104239, 2020a.

KAPLAN, B. REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. **International Journal of Medical Informatics**, [*s. l.*], v. 143, p. 104239, 2020b.

KAPLAN, B. REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. **International Journal of Medical Informatics**, [*s. l.*], v. 143, p. 104239, 2020c. Disponível em: https://www.sciencedirect.com/science/article/pii/S1386505620309382. Acesso em: 1 jul. 2022.

KHOSLA, S. Implementation of Synchronous Telemedicine into Clinical Practice. **Sleep Medicine Clinics**, [*s. l.*], v. 15, n. 3, Telehealth in Sleep Medicine, p. 347–358, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1556407X20300424. Acesso em: 1 jul. 2022.

KIM, E. *et al.* A Hypertension Management System with Emergency Monitoring. *Em*: 2008 INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND ASSURANCE (ISA 2008), 2008. **2008 International Conference on Information Security and Assurance (isa 2008)**. [*S. l.: s. n.*], 2008. p. 301–306.

KIM, S. S. *et al.* Encoder design for healthcare signals. **Personal and Ubiquitous Computing**, [*s. l.*], v. 17, n. 7, p. 1373–1381, 2013. Disponível em: https://doi.org/10.1007/s00779-012-0572-8. Acesso em: 1 jul. 2022.

KIM, D.-W.; CHOI, J.-Y.; HAN, K.-H. Risk management-based security evaluation model for telemedicine systems. **BMC Med Inform Decis Mak**, [*s. l.*], p. 106–106, 2020a. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7286211. Acesso em: 1 jul. 2022.

KIM, D.; CHOI, J.; HAN, K. Risk management-based security evaluation model for telemedicine systems. **BMC Medical Informatics and Decision Making**, [*s. l.*], v. 20, n. 1, p. 106, 2020. Disponível em: https://doi.org/10.1186/s12911-020-01145-7. Acesso em: 12 mar. 2022.

KIM, D.-W.; CHOI, J.-Y.; HAN, K.-H. Risk management-based security evaluation model for telemedicine systems. **BMC medical informatics and decision making**, [*s. l.*], v. 20, n. 1, p. 106, 2020b.

KISHORE, R. *et al.* Industry-Academia Panel: Transforming Healthcare with IT. *Em*: SIGMIS-CPR '18: 2018 COMPUTERS AND PEOPLE RESEARCH CONFERENCE, 2018, Buffalo-Niagara Falls NY USA. **Proceedings of the 2018 ACM SIGMIS Conference on Computers and People Research**. Buffalo-Niagara Falls NY USA: ACM, 2018. p. 6–8. Disponível em: https://dl.acm.org/doi/10.1145/3209626.3226589. Acesso em: 1 jul. 2022.

KOROSTELEV, M. *et al.* Body Sensor Networks in Fetal Monitoring with NFC Enabled Android Devices. *Em*: 7TH INTERNATIONAL CONFERENCE ON BODY AREA NETWORKS, 2012, Oslo, Norway. **Proceedings of the 7th International Conference on Body Area Networks**. Oslo, Norway: ACM, 2012. Disponível em: http://eudl.eu/doi/10.4108/icst.bodynets.2012.249947. Acesso em: 1 jul. 2022.

KOSUGI, N. *et al.* A Prototype System of Remote Music Therapy Using the Latest Communication Technology in Japan. *Em*: INTERNATIONAL CONFERENCE, 2013, Vienna, Austria. **Proceedings of International Conference on Information Integration and Web-based Applications & Services - IIWAS '13**. Vienna, Austria: ACM Press, 2013. p. 671–675. Disponível em: http://dl.acm.org/citation.cfm?doid=2539150.2539265. Acesso em: 1 jul. 2022.

KOSUTIC, D. **Como definir o escopo do SGSI**. [*S. l.*], [*s. d.*]. Disponível em: https://advisera.com/27001academy/pt-br/knowledgebase/como-definir-o-escopo-do-sgsi/. Acesso em: 23 fev. 2023.

KOSUTIC, D. **O que é um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ISO 27001? | 27001Academy**. [*S. l.*], 2016. Disponível em: https://advisera.com/27001academy/pt-br/blog/2016/05/30/o-que-e-um-sistema-de-gestao-de-seguranca-da-informacao-sgsi-de-acordo-com-a-iso-27001/. Acesso em: 7 jun. 2021.

KREISER, D. *et al.* The all IHP sensor node: highly integrated sensor nodes using IHP components. *Em*: THE 10TH ACM INTERNATIONAL SYMPOSIUM, 2012, Paphos, Cyprus. **Proceedings of the 10th ACM international symposium on Mobility management and wireless access - MobiWac '12**. Paphos, Cyprus: ACM Press, 2012. p. 147. Disponível em: http://dl.acm.org/citation.cfm?doid=2386995.2387022. Acesso em: 1 jul. 2022.

KUMAR, V.; JANGIRALA, S.; AHMAD, M. An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing. **J Med Syst**, [*s. l.*], p. 142–142, 2018. Disponível em: https://dx.doi.org/10.1007/s10916-018-0987-5. Acesso em: 1 jul. 2022.

LI, P. *et al.* CareNet: Building a Secure Software-defined Infrastructure for Home-based Healthcare. *Em*: CODASPY '17: SEVENTH ACM CONFERENCE ON DATA AND APPLICATION SECURITY AND PRIVACY, 2017a, Scottsdale Arizona USA. **Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization**. Scottsdale Arizona USA: ACM, 2017. p. 69–72. Disponível em: https://dl.acm.org/doi/10.1145/3040992.3041007. Acesso em: 12 mar. 2022.

LI, P. *et al.* CareNet: Building a Secure Software-defined Infrastructure for Home-based Healthcare. *Em*: CODASPY '17: SEVENTH ACM CONFERENCE ON DATA AND APPLICATION SECURITY AND PRIVACY, 2017b, Scottsdale Arizona USA. **Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization**. Scottsdale Arizona USA: ACM, 2017. p. 69–72. Disponível em: https://dl.acm.org/doi/10.1145/3040992.3041007. Acesso em: 1 jul. 2022.

LITHOXOIDOU, E. E. *et al.* A Gamification Engine Architecture for Enhancing Behavioral Change Support Systems. *Em*: PETRA '18: THE 11TH PERVASIVE TECHNOLOGIES RELATED TO ASSISTIVE ENVIRONMENTS CONFERENCE, 2018, Corfu Greece. **Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference**. Corfu Greece: ACM, 2018. p. 482–489. Disponível em: https://dl.acm.org/doi/10.1145/3197768.3201561. Acesso em: 1 jul. 2022.

LIU, Y. Multi-source heterogeneous data fusion based on perceptual semantics in narrow-band Internet of Things. **Personal and Ubiquitous Computing**, [*s. l.*], v. 23, n. 3–4, p. 413–420, 2019. Disponível em: https://doi.org/10.1007/s00779-019-01202-7. Acesso em: 1 jul. 2022.

LOBO, E. J. R. **Segurança da Informação. Ameaças e Controles**. 1. ed. [*S. l.*]: Ciência Moderna, 2019.

LUCIANO, E.; MAHMOOD, M. A.; MANSOURI RAD, P. Telemedicine adoption issues in the United States and Brazil: Perception of healthcare professionals. **Health Informatics Journal**, [*s. l.*], v. 26, n. 4, p. 2344–2361, 2020.

LYNGAAS, S. **Sistema de saúde da Flórida é invadido e dados de 1,3 milhão são expostos**. [*S. l.*], [*s. d.*]. Disponível em: https://www.cnnbrasil.com.br/tecnologia/sistema-de-saude-da-florida-e-invadido-e-dados-de-13-milhao-sao-expostos/. Acesso em: 18 mar. 2023.

MA, M.; FAN, S.; FENG, D. Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine. **Journal of Information Security and Applications**, [*s. l.*], v. 55, p. 102652, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214212620308103. Acesso em: 1 jul. 2022.

MACADAR, M. A.; LHEUREUX-DE-FREITAS, J. Porto Alegre: a Brazilian city searching to be smarter. *Em*: DG.O 2013: 14TH ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 2013, Quebec Canada. **Proceedings of the 14th Annual International Conference on Digital Government Research**. Quebec Canada:

ACM, 2013. p. 56–64. Disponível em: https://dl.acm.org/doi/10.1145/2479724.2479736. Acesso em: 1 jul. 2022.

MACHADO, F. N. R. **Segurança da informação: Princípios e controle de ameaças**. 1. ed. [*S. l.*]: Érica, 2014.

MADYATMADJA, E. D.; NINDITO, H.; PRISTINELLA, D. Citizen Attitude: Potential Impact of Social Media Based Government. *Em*: ICEEL 2019: 2019 3RD INTERNATIONAL CONFERENCE ON EDUCATION AND E-LEARNING, 2019, Barcelona Spain. **Proceedings of the 2019 3rd International Conference on Education and E-Learning**. Barcelona Spain: ACM, 2019. p. 128–134. Disponível em: http://dl.acm.org/doi/10.1145/3371647.3371653. Acesso em: 1 jul. 2022.

MANUAL_REVISAO_BIBLIOGRAFICA-SISTEMATICA-INTEGRATIVA.PDF. , [*s. d.*]. Disponível em: http://biblioteca.cofen.gov.br/wp-content/uploads/2019/06/manual_revisao_bibliografica-sistematica-integrativa.pdf. Acesso em: 18 fev. 2022.

MARIN-GOMEZ, F. X. *et al.* Social Networking App Use Among Primary Health Care Professionals: Web-Based Cross-Sectional Survey. **JMIR mHealth and uHealth**, [*s. l.*], v. 6, n. 12, p. e11147, 2018.

MÁRQUEZ, G.; ASTUDILLO, H.; TARAMASCO, C. Exploring security issues in telehealth systems. *Em*: , 2019a, Montreal, Quebec, Canada. **Proceedings of the 1st International Workshop on Software Engineering for Healthcare**. Montreal, Quebec, Canada: IEEE Press, 2019. p. 65–72. Disponível em: https://doi.org/10.1109/SEH.2019.00019. Acesso em: 9 mar. 2022.

MÁRQUEZ, G.; ASTUDILLO, H.; TARAMASCO, C. Exploring security issues in telehealth systems. *Em*: , 2019b, Montreal, Quebec, Canada. **Proceedings of the 1st International Workshop on Software Engineering for Healthcare**. Montreal, Quebec, Canada: IEEE Press, 2019. p. 65–72. Disponível em: https://doi.org/10.1109/SEH.2019.00019. Acesso em: 8 jun. 2022.

MÁRQUEZ, G.; ASTUDILLO, H.; TARAMASCO, C. Exploring security issues in telehealth systems. *Em*: , 2019c, Montreal, Quebec, Canada. **Proceedings of the 1st International Workshop on Software Engineering for Healthcare**. Montreal, Quebec, Canada: IEEE Press, 2019. p. 65–72. Disponível em: https://doi.org/10.1109/SEH.2019.00019. Acesso em: 1 jul. 2022.

MARTIN, G. *et al.* Use of the HoloLens2 Mixed Reality Headset for Protecting Health Care Workers During the COVID-19 Pandemic: Prospective, Observational Evaluation. **Journal of Medical Internet Research**, [*s. l.*], v. 22, n. 8, p. e21486, 2020.

MAZILU, S. *et al.* A Wearable Assistant for Gait Training for Parkinson's Disease with Freezing of Gait in Out-of-the-Lab Environments. **ACM Transactions on Interactive Intelligent Systems**, [*s. l.*], v. 5, n. 1, p. 1–31, 2015. Disponível em: https://dl.acm.org/doi/10.1145/2701431. Acesso em: 1 jul. 2022.

MBUNGE, E. *et al.* A critical review of emerging technologies for tackling COVID-19 pandemic. **Human Behavior and Emerging Technologies**, [*s. l.*], v. 3, n. 1, p. 25–39, 2021.

MEDICINA, C. F. CFM publicará nova regulamentação sobre telemedicina no Brasil. *Em*: SUMMIT SAÚDE. 24 set. 2020. Disponível em: https://summitsaude.estadao.com.br/novos-medicos/cfm-publicara-nova-regulamentacao-sobre-telemedicina-no-brasil/. Acesso em: 7 jun. 2021.

MICHEL-MACARTY, J. A. *et al.* Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine. **Comput Methods Programs Biomed**, [*s. l.*], p. 165–175, 2018a. Disponível em: https://dx.doi.org/10.1016/j.cmpb.2018.05.021. Acesso em: 1 jul. 2022.

MICHEL-MACARTY, J. A. *et al.* Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine. **Computer Methods and Programs in Biomedicine**, [*s. l.*], v. 162, p. 165–175, 2018b.

MILANO, G.; VALLESPIR, D.; VIOLA, A. A technological and innovative approach to COVID-19 in Uruguay. **Communications of the ACM**, [*s. l.*], v. 63, n. 11, p. 53–55, 2020. Disponível em: https://dl.acm.org/doi/10.1145/3422826. Acesso em: 1 jul. 2022.

MISURACA, G.; BROSTER, D.; CENTENO, C. Envisioning digital Europe 2030: scenario design on ICT for governance and policy modelling. [*s. l.*], p. 10,

MONTEIRO, S. *et al.* HygeiaTel: an intelligent telemedicine system with cognitive support. *Em*: THE FIRST ACM WORKSHOP, 2011, Seattle, Washington. **Proceedings of the First ACM Workshop on Mobile Systems, Applications, and Services for Healthcare - mHealthSys '11**. Seattle, Washington: ACM Press, 2011. p. 1. Disponível em: http://dl.acm.org/citation.cfm?doid=2064942.2064955. Acesso em: 1 jul. 2022.

NBR, A. **ISO/IEC 27001 Tecnologia da Informação. Técnicas de Segurança. Sistema de Gestão de Segurança da Informação. Requisitos.** Rio de Janeiro: [*s. n.*], 2006.

NBR, A. **ISO/IEC 27002 Tecnologia da Informação. Técnicas de Segurança. Código de Prática para a Gestão da Segurança da Informação.** Rio de Janeiro: [*s. n.*], 2005.

NGUYEN, N. *et al.* Use of mobile health technologies for postoperative care in paediatric surgery: A systematic review. **Journal of Telemedicine and Telecare**, [*s. l.*], v. 28, n. 5, p. 331–341, 2022. Disponível em: http://journals.sagepub.com/doi/10.1177/1357633X20934682. Acesso em: 1 jul. 2022.

OLIVA-FELIPE, L. *et al.* Health Recommender System design in the context of CAREGIVERSPRO-MMD Project. *Em*: PETRA '18: THE 11TH PERVASIVE TECHNOLOGIES RELATED TO ASSISTIVE ENVIRONMENTS CONFERENCE, 2018, Corfu Greece. **Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference**. Corfu Greece: ACM, 2018. p. 462–469. Disponível em: https://dl.acm.org/doi/10.1145/3197768.3201558. Acesso em: 1 jul. 2022.

ONYEJEKWE, E. R. Big Data in Health Informatics Architecture. *Em*: 2014 IEEE/ACM INTERNATIONAL CONFERENCE ON ADVANCES IN SOCIAL NETWORKS ANALYSIS AND MINING (ASONAM), 2014, China. **2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)**. China: IEEE, 2014. p. 728–736. Disponível em: http://ieeexplore.ieee.org/document/6921667/. Acesso em: 1 jul. 2022.

OTACILIO DOS SANTOS, V. **Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008**. 2012. Mestra em Engenharia Elétrica - Universidade Estadual de Campinas, Campinas, 2012. Disponível em: http://acervus.unicamp.br/index.asp?codigo_sophia=897647. Acesso em: 5 maio 2021.

PDCA (PLAN, DO, CHECK, ACTION). [*S. l.*], [*s. d.*]. Disponível em: https://www.infoescola.com/administracao_/pdca-plan-do-check-action/. Acesso em: 24 jun. 2021.

PEREIRA, M. G.; GALVÃO, T. F. Etapas de busca e seleção de artigos em revisões sistemáticas da literatura. **Epidemiologia e Serviços de Saúde**, [*s. l.*], v. 23, n. 2, p. 369–371, 2014. Disponível em: http://scielo.iec.pa.gov.br/scielo.php?script=sci_arttext&pid=S1679-49742014000200019&lng=en&nrm=iso&tlng=en. Acesso em: 18 fev. 2022.

PÉREZ, J. D. G. *et al.* Ubiquitous low-cost sports training system for athletes. *Em*: THE 6TH EURO AMERICAN CONFERENCE, 2012, Valencia, Spain. **Proceedings of the 6th Euro American Conference on Telematics and Information Systems - EATIS '12**. Valencia, Spain: ACM Press, 2012. p. 105. Disponível em: http://dl.acm.org/citation.cfm?doid=2261605.2261621. Acesso em: 1 jul. 2022.

PITON, R. Para que serve um Data Warehouse? *Em*: 2017a. Disponível em: https://rafaelpiton.com.br/blog/data-warehouse-para-que-serve/. Acesso em: 4 jun. 2021.

PITON, R. Tabela Dimensão: os 5 tipos que você deve conhecer. *Em*: RAFAEL PITON. 2017b. Disponível em: https://rafaelpiton.com.br/blog/data-warehouse-tipos-dimensoes/. Acesso em: 4 jun. 2021.

PRAMUKANTORO, E. S.; GOFUKU, A. Prototype of multi-layer personal cardiac monitoring system for data interoperability problem. *Em*: SIET '20: 5TH INTERNATIONAL CONFERENCE ON SUSTAINABLE INFORMATION ENGINEERING AND TECHNOLOGY, 2020, Malang Indonesia. **Proceedings of the 5th International Conference on Sustainable Information Engineering and Technology**. Malang Indonesia: ACM, 2020. p. 84–89. Disponível em: https://dl.acm.org/doi/10.1145/3427423.3427442. Acesso em: 1 jul. 2022.

PROPOSED FRAME WORK OF E-LEARNING SERVICES THROUGH CLOUD | PROCEEDINGS OF THE SECOND INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGY FOR COMPETITIVE STRATEGIES. [*S. l.*], [*s. d.*]. Disponível em: https://dl.acm.org/doi/abs/10.1145/2905055.2905080. Acesso em: 1 jul. 2022.

QIAO, L. *et al.* A Lightweight Internet Sharing Scheme for Sectional Medical Images according to Existing Hospital Network Facilities and Basic Information Security Rules. **J Healthc Eng**, [*s. l.*], p. 8838390–8838390, 2020b. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7737442. Acesso em: 1 jul. 2022.

QIAO, L. *et al.* A Lightweight Internet Sharing Scheme for Sectional Medical Images according to Existing Hospital Network Facilities and Basic Information Security Rules. **Journal of Healthcare Engineering**, [*s. l.*], v. 2020, p. 8838390, 2020a.

R. PAI, R.; ALATHUR, S. Mobile Health System Framework in India. *Em*: DG.O 2019: 20TH ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 2019, Dubai United Arab Emirates. **Proceedings of the 20th Annual International Conference on Digital Government Research**. Dubai United Arab Emirates: ACM, 2019. p. 186–195. Disponível em: https://dl.acm.org/doi/10.1145/3325112.3325235. Acesso em: 1 jul. 2022.

RADCHENKO, I. *et al.* Solving Data Integration Problems in Medical Imaging System: A Case Study in Almazov National Medical Research Centre. *Em*: THE 14TH CENTRAL AND EASTERN EUROPEAN SOFTWARE ENGINEERING CONFERENCE RUSSIA, 2018, Moscow, Russian Federation. **Proceedings of the 14th Central and Eastern European Software Engineering Conference Russia on ZZZ - CEE-SECR '18**. Moscow, Russian Federation: ACM Press, 2018. p. 1–5. Disponível em: http://dl.acm.org/citation.cfm?doid=3290621.3290625. Acesso em: 1 jul. 2022.

RASHID, M. M.; ISAWI, M.; MAHMOOD, B. A. An Extensive Analysis of the Ad Hoc Network. *Em*: ICEMIS'20: THE 6TH INTERNATIONAL CONFERENCE ON ENGINEERING & MIS 2020, 2020, Almaty Kazakhstan. **Proceedings of the 6th International Conference on Engineering & MIS 2020**. Almaty Kazakhstan: ACM, 2020. p. 1–9. Disponível em: https://dl.acm.org/doi/10.1145/3410352.3410816. Acesso em: 1 jul. 2022.

REALPROTECT. Prejuízos das ameaças cibernéticas para o setor da saúde. *Em*: 2015. Disponível em: https://realprotect.net/prejuizos-das-ameacas-ciberneticas-para-o-setor-da-saude/. Acesso em: 7 jun. 2021.

REDAÇÃO, D. Ransomware em sistema hospitalar leva paciente à morte. *Em*: HTTPS://WWW.CISOADVISOR.COM.BR/. 2020. Disponível em: https://www.cisoadvisor.com.br/ransomware-em-hospital-retardou-atendimento-paciente-morreu/. Acesso em: 7 jun. 2021.

REPORT, S. SI hospitalar: dados e exames sob a mira dos hackers. *Em*: SECURITY REPORT. 17 maio 2018. Disponível em: https://www.securityreport.com.br/destaques/si-hospitalar-dados-e-exames-sob-a-mira-dos-hackers/. Acesso em: 24 jun. 2021.

REZAEIBAGHA, F.; MU, Y. Practical and secure telemedicine systems for user mobility. **Journal of Biomedical Informatics**, [*s. l.*], v. 78, p. 24–32, 2018.

RIBAS, C. E. **Sistema de gestão de segurança da informação em organizações da área da saúde**. 2010. Mestrado em Fisiopatologia Experimental - Universidade de São Paulo, São Paulo, 2010. Disponível em: http://www.teses.usp.br/teses/disponiveis/5/5160/tde-27092010-145036/. Acesso em: 5 maio 2021.

RISK MANAGEMENT-BASED SECURITY EVALUATION MODEL FOR TELEMEDICINE SYSTEMS | SPRINGERLINK. [*S. l.*], [*s. d.*]. Disponível em: https://link.springer.com/article/10.1186/s12911-020-01145-7?utm_source=getftr&utm_medium=getftr&%20utm_campaign=getftr_pilot. Acesso em: 1 jul. 2022.

RODRIGUES, R. S. CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA. [*s. l.*], p. 99,

RODRIGUES, R. S. **Estudo de um processo estruturado de segurança da informação em sistema de informação do setor de saúde com base na norma ISO 27799:2008 - Unidade de Pós-Graduação, Extensão e Pesquisa - Programa de Pós-Graduação - CPS**. [*S. l.*], 2010. Disponível em: http://www.pos.cps.sp.gov.br/dissertacao/estudo-de-um-processo-estruturado-de-seguranca-da-informacao-em-sistema-de-informacao-do-setor-de-saude-com-base-na-norma-iso-27799-2008. Acesso em: 7 jun. 2021.

ROZENBLIT, J.; SAMETINGER, J. Models in Healthcare Simulation: Typology and Security Issues. [*s. l.*], p. 5,

RUPA, Ch.; DEVI, C. Privacy and protection of medical images ROI using SPLSB and bit-plane based watermarking. *Em*: THE 3RD INTERNATIONAL CONFERENCE, 2019a, Kuala Lumpur, Malaysia. **Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19**. Kuala Lumpur, Malaysia: ACM Press, 2019. p. 211–215. Disponível em: http://dl.acm.org/citation.cfm?doid=3309074.3309088. Acesso em: 13 mar. 2022.

RUPA, Ch.; DEVI, C. Privacy and protection of medical images ROI using SPLSB and bit-plane based watermarking. *Em*: THE 3RD INTERNATIONAL CONFERENCE, 2019b, Kuala Lumpur, Malaysia. **Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19**. Kuala Lumpur, Malaysia: ACM Press, 2019. p. 211–215. Disponível em: http://dl.acm.org/citation.cfm?doid=3309074.3309088. Acesso em: 1 jul. 2022.

SABIE, D. *et al.* Exile Within Borders: Understanding the Limits of the Internally Displaced People (IDPs) in Iraq. *Em*: LIMITS '19: FIFTH WORKSHOP ON COMPUTING WITHIN LIMITS, 2019, Lappeenranta Finland. **Proceedings of the Fifth Workshop on Computing within Limits**. Lappeenranta Finland: ACM, 2019. p. 1–16. Disponível em: https://dl.acm.org/doi/10.1145/3338103.3338104. Acesso em: 1 jul. 2022.

SACHDEVA, S.; BHALLA, S. Semantic interoperability in standardized electronic health record databases. **Journal of Data and Information Quality**, [*s. l.*], v. 3, n. 1, p. 1–37, 2012. Disponível em: https://dl.acm.org/doi/10.1145/2166788.2166789. Acesso em: 1 jul. 2022.

SAIGI-RUBIÓ, F.; JIMÉNEZ-ZARCO, A.; TORRENT-SELLENS, J. DETERMINANTS OF THE INTENTION TO USE TELEMEDICINE: EVIDENCE FROM PRIMARY CARE PHYSICIANS. **International Journal of Technology Assessment in Health Care**, [*s. l.*], v. 32, n. 1–2, p. 29–36, 2016a. Disponível em: https://www.cambridge.org/core/journals/international-journal-of-technology-assessment-in-health-care/article/determinants-of-the-intention-to-use-telemedicine-evidence-from-primary-care-physici%20ans/477390ECBD0E85A2CD51098A3034F7C3. Acesso em: 1 jul. 2022.

SAIGI-RUBIÓ, F.; JIMÉNEZ-ZARCO, A.; TORRENT-SELLENS, J. DETERMINANTS OF THE INTENTION TO USE TELEMEDICINE: EVIDENCE FROM PRIMARY CARE PHYSICIANS. **International Journal of Technology Assessment in Health Care**, [*s. l.*], v. 32, n. 1–2, p. 29–36, 2016b.

SÁNCHEZ, L. E. *et al.* Practical approach of a secure management system based on ISO/IEC 17799. *Em*: FIRST INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY (ARES'06), 2006. **First International Conference on Availability, Reliability and Security (ARES'06)**. [*S. l.: s. n.*], 2006. p. 8 pp. – 592.

SANTHI, B.; DHEEPTHA, B. A novel edge based embedding in medical images based on unique key generated using sudoku puzzle design. **SpringerPlus**, [*s. l.*], v. 5, n. 1, p. 1670, 2016.

SECURING CONNECTED HOSPITALS: A RESEARCH ON EXPOSED MEDICAL SYSTEMS AND SUPPLY CHAIN RISKS. [*s. l.*],

SETHI, T. *et al.* Validating the Tele-diagnostic Potential of Affordable Thermography in a Big-data Data-enabled ICU. *Em*: , 2017, New York, NY, USA. **Proceedings of the Special Collection on eGovernment Innovations in India**. New York, NY, USA: Association for Computing Machinery, 2017. p. 64–69. Disponível em: https://doi.org/10.1145/3055219.3055234. Acesso em: 1 jul. 2022.

SHAHBODIN, F. *et al.* Lightweight Cryptography Techniques for MHealth Cybersecurity. *Em*: THE 2019 ASIA PACIFIC INFORMATION TECHNOLOGY CONFERENCE, 2019, Jeju Island, Republic of Korea. **Proceedings of the 2019 Asia Pacific Information Technology Conference on - APIT 2019**. Jeju Island, Republic of Korea: ACM Press, 2019. p. 44–50. Disponível em: http://dl.acm.org/citation.cfm?doid=3314527.3314536. Acesso em: 1 jul. 2022.

SHEN, L. *et al.* Visualizing Collaboration Characteristics and Topic Burst on International Mobile Health Research: Bibliometric Analysis. **JMIR mHealth and uHealth**, [*s. l.*], v. 6, n. 6, p. e135, 2018.

SHIN, Sangwon; WON, K.; SHIN, Sung. Size efficient preprocessed symmetric rsa for wireless body area network. **ACM SIGAPP Applied Computing Review**, [*s. l.*], v. 20, n. 1, p. 15–23, 2020a. Disponível em: https://doi.org/10.1145/3392350.3392352. Acesso em: 8 jun. 2022.

SHIN, Sangwon; WON, K.; SHIN, Sung. Size efficient preprocessed symmetric rsa for wireless body area network. **ACM SIGAPP Applied Computing Review**, [*s. l.*], v. 20, n. 1, p. 15–23, 2020b. Disponível em: https://dl.acm.org/doi/10.1145/3392350.3392352. Acesso em: 1 jul. 2022.

SIDÉN, J. *et al.* Home care with NFC sensors and a smart phone. *Em*: THE 4TH INTERNATIONAL SYMPOSIUM, 2011, Barcelona, Spain. **Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies - ISABEL '11**. Barcelona, Spain: ACM Press, 2011. p. 1–5. Disponível em: http://dl.acm.org/citation.cfm?doid=2093698.2093848. Acesso em: 1 jul. 2022.

SINGH, A. K. *et al.* IEEE Access Special Section Editorial: Information Security Solutions for Telemedicine Applications. **IEEE Access**, [*s. l.*], v. 6, p. 79005–79009, 2018.

SINGH, B.; KAUR, M. IT applications in healthcare. *Em*: , 2010a, New York, NY, USA. **Proceedings of the International Conference and Workshop on Emerging Trends in Technology**. New York, NY, USA: Association for Computing Machinery, 2010. p. 170–172. Disponível em: https://doi.org/10.1145/1741906.1741940. Acesso em: 12 mar. 2022.

SINGH, B.; KAUR, M. IT applications in healthcare. *Em*: , 2010b, New York, NY, USA. **Proceedings of the International Conference and Workshop on Emerging Trends in Technology**. New York, NY, USA: Association for Computing Machinery, 2010. p. 170–172. Disponível em: https://doi.org/10.1145/1741906.1741940. Acesso em: 1 jul. 2022.

SINGHAL, R. A national public healthcare framework using grid. *Em*: THE 1ST AMRITA ACM-W CELEBRATION, 2010, Coimbatore, India. **Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India - A2CWiC '10**. Coimbatore, India: ACM Press, 2010. p. 1–5. Disponível em: http://portal.acm.org/citation.cfm?doid=1858378.1858398. Acesso em: 1 jul. 2022.

SOLUÇÕES DE SEGURANÇA CORPORATIVA. [*S. l.*], 2023. Disponível em: https://www.ibm.com/br-pt/security. Acesso em: 18 mar. 2023.

TALAL, A. H. *et al.* A framework for patient-centered telemedicine: Application and lessons learned from vulnerable populations. **Journal of Biomedical Informatics**, [*s. l.*], v. 112, p. 103622, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1532046420302501. Acesso em: 1 jul. 2022.

TANWAR, V. K. *et al. CryptoLesion*: A Privacy-preserving Model for Lesion Segmentation Using Whale Optimization over Cloud. **ACM Transactions on Multimedia Computing, Communications, and Applications**, [*s. l.*], v. 16, n. 2, p. 1–23, 2020. Disponível em: https://dl.acm.org/doi/10.1145/3380743. Acesso em: 1 jul. 2022.

TELEMEDICINA. *Em*: WIKIPÉDIA, A ENCICLOPÉDIA LIVRE. [*S. l.: s. n.*], 2022. Disponível em: https://pt.wikipedia.org/w/index.php?title=Telemedicina&oldid=63550509. Acesso em: 7 jun. 2022.

TELEMEDICINA: COMO FUNCIONA E QUAIS AS VANTAGENS? [*S. l.*], 2019. Disponível em: https://www.boaconsulta.com/blog/como-funciona-e-quais-as-vantagens-da-telemedicina/. Acesso em: 6 jun. 2022.

TELEMEDICINE AND CYBERSECURITY: SECURING HEALTH DATA! *Em*: STEALTHLABS. 18 ago. 2020. Disponível em: https://www.stealthlabs.com/blog/telemedicine-and-cybersecurity-securing-health-data/. Acesso em: 26 jul. 2021.

THAMRIN, N. M.; AHMAD, I.; HANI, M. K. A secure field programmable gate array based System-on-Chip for Telemedicine application. *Em*: INTERNATIONAL CONFERENCE ON INFORMATION SOCIETY (I-SOCIETY 2011), 2011. **International Conference on Information Society (i-Society 2011)**. [*S. l.: s. n.*], 2011. p. 105–109.

TOOR, R.; CHANA, I. Application of IT in Healthcare: A Systematic Review. [*s. l.*], p. 8, 2014.

TOP 10 TIPS FOR CYBERSECURITY IN HEALTH CARE. [*s. l.*],

UESUGI, J. H. E. *et al.* Aplicações da telemedicina no cenário da pandemia de COVID-19. **Research, Society and Development**, [*s. l.*], v. 11, n. 1, p. e29211124877, 2022. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/24877. Acesso em: 12 mar. 2022.

UPADHYAY, A.; DAVE, M. Fuzzy-BPN Based Improved Technique for Color Image Watermarking. *Em*: ICIA-16: INTERNATIONAL CONFERENCE ON INFORMATICS AND ANALYTICS, 2016, Pondicherry India. **Proceedings of the International Conference on Informatics and Analytics**. Pondicherry India: ACM, 2016. p. 1–10. Disponível em: https://dl.acm.org/doi/10.1145/2980258.2980438. Acesso em: 1 jul. 2022.

URBAUER, P.; FORJAN, M. Integration of Health and Public Transport Data to Enable Decision Support for Seniors to Reduce Risk of Infection with Communicable Diseases. *Em*: DSAI 2020: 9TH INTERNATIONAL CONFERENCE ON SOFTWARE DEVELOPMENT AND TECHNOLOGIES FOR ENHANCING ACCESSIBILITY AND FIGHTING INFO-EXCLUSION, 2020, Online Portugal. **9th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion**. Online Portugal: ACM, 2020. p. 168–173. Disponível em: https://dl.acm.org/doi/10.1145/3439231.3439236. Acesso em: 1 jul. 2022.

VADREVU, C. S. K. *et al.* Degraded Service Provisioning in Mixed-Line-Rate WDM Backbone Networks Using Multipath Routing. **IEEE/ACM Transactions on Networking**, [*s. l.*], v. 22, n. 3, p. 840–849, 2014. Disponível em: http://ieeexplore.ieee.org/document/6514935/. Acesso em: 1 jul. 2022.

VALLATHAN, G.; DEVI, G. G.; KANNAN, A. V. Enhanced data concealing technique to secure medical image in telemedicine applications. *Em*: 2016 INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS, SIGNAL PROCESSING AND NETWORKING (WISPNET), 2016. **2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)**. [*S. l.: s. n.*], 2016. p. 186–190.

WAGNER, S. *et al.* Common Ambient Assisted Living Home Platform for Seamless Care. *Em*: 8TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING TECHNOLOGIES FOR HEALTHCARE, 2014, Oldenburg, Germany. **Proceedings of the 8th International Conference on Pervasive Computing Technologies for Healthcare**. Oldenburg, Germany: ICST, 2014. Disponível em: http://eudl.eu/doi/10.4108/icst.pervasivehealth.2014.255803. Acesso em: 1 jul. 2022.

WERNHART, A.; GAHBAUER, S.; HALUZA, D. eHealth and telemedicine: Practices and beliefs among healthcare professionals and medical students at a medical university. **PloS One**, [*s. l.*], v. 14, n. 2, p. e0213067, 2019.

WIKIPÉDIA. **Ética na Big Data**. *Em*: WIKIPÉDIA, A ENCICLOPÉDIA LIVRE. [*S. l.: s. n.*], 2019. Disponível em: https://pt.wikipedia.org/w/index.php?title=%C3%89tica_na_Big_Data&oldid=56930297. Acesso em: 4 jun. 2021.

YANG, C. C.; LEROY, G.; ANANIADOU, S. Smart Health and Wellbeing. **ACM Transactions on Management Information Systems**, [*s. l.*], v. 4, n. 4, p. 1–8, 2013. Disponível em: https://dl.acm.org/doi/10.1145/2555810.2555811. Acesso em: 1 jul. 2022.

YASSEIN, M. B. *et al.* IoT-based healthcare systems: a survey. *Em*: THE SECOND INTERNATIONAL CONFERENCE, 2019, Dubai, United Arab Emirates. **Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems - DATA '19**. Dubai, United Arab Emirates: ACM Press, 2019. p. 1–9. Disponível em: http://dl.acm.org/citation.cfm?doid=3368691.3368721. Acesso em: 1 jul. 2022.

YIGZAW, K. Y. *et al.* Towards privacy-preserving computing on distributed electronic health record data. *Em*: THE 2013 MIDDLEWARE DOCTORAL SYMPOSIUM, 2013, Beijing, China. **Proceedings of the 2013 Middleware Doctoral Symposium on - MDS '13**. Beijing, China: ACM Press, 2013. p. 1–6. Disponível em: http://dl.acm.org/citation.cfm?doid=2541534.2541593. Acesso em: 1 jul. 2022.

YOU, J.; ZHANG, J. Relational contract, government support and stable collaboration: an empirical research on district medical collaboration platform in China. [*s. l.*], p. 10,

ZEHROUNI, A. *et al.* Assessment of the Impact of Teledermatology Using Discrete Event Simulation. *Em*: 2019 WINTER SIMULATION CONFERENCE (WSC), 2019, National Harbor, MD, USA. **2019 Winter Simulation Conference (WSC)**. National Harbor, MD, USA: IEEE, 2019. p. 1255–1266. Disponível em: https://ieeexplore.ieee.org/document/9004782/. Acesso em: 1 jul. 2022.

ZHANG, L.; HUANG, Y.; JIANG, T. High-speed Railway Environmental Monitoring Data Identity Authentication Scheme Based on Consortium Blockchain. *Em*: ICBTA 2019: 2019 2ND INTERNATIONAL CONFERENCE ON BLOCKCHAIN TECHNOLOGY AND APPLICATIONS, 2019, Xi'an China. **Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications**. Xi'an China: ACM, 2019. p. 7–13. Disponível em: https://dl.acm.org/doi/10.1145/3376044.3376045. Acesso em: 1 jul. 2022.

ZHANG, Z.; ZHAO, J.; LI, Z. Preliminary Analysis of The Application and Development of Big Data, Cloud Computing, IoT, Mobile Internet, AI, and Blockchain In The Power Scene. *Em*: ICITEE2020: THE 3RD INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGIES AND ELECTRICAL ENGINEERING, 2020, Changde City Hunan China. **Proceedings of the 3rd International Conference on Information Technologies and Electrical Engineering**. Changde City Hunan China: ACM, 2020. p. 526–530. Disponível em: https://dl.acm.org/doi/10.1145/3452940.3453043. Acesso em: 1 jul. 2022.