Capítulo 1

Saúde Sob Ataque: Da Avaliação de Riscos ao Desenvolvimento de Estratégias de Investimentos em Cibersegurança na Área da Saúde

Muriel Figueredo Franco[1], Laura Rodrigues Soares[2], Jéferson Campos Nobre[2]

[1]Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)
Departamento de Ciências Exatas e Sociais Aplicadas, Porto Alegre, Brasil
[2]Universidade Federal do Rio Grande do Sul (UFRGS)
Instituto de Informática (INF), Porto Alegre, Brasil

Abstract. *Cybersecurity is one of the essential pillars of the digital revolution. Cybercriminals are increasingly targeting governments and companies from different sectors. These attacks have different technical impacts on their infrastructures and services, which result in direct and indirect economic impacts on their business models. In addition, the social and reputational impacts have been increasingly frequent as society increasingly depends on digital services. The health sector has been most affected by cybercriminals' financial incentives to obtain sensitive data and make critical services unavailable. The World Health Organization (WHO) has emphasized the profound impact of cyberattacks on hospitals and health services, calling for urgent and collective global action to tackle this growing crisis. Therefore, in this work, we will analyze and understand the risks and particularities of the health sector, as well as define the main steps for efficient planning of cybersecurity strategies for the health sector. In addition, we will map the primary cybersecurity efforts of academia and industry aimed at the healthcare sector.*

Resumo. *A cibersegurança é um dos pilares essenciais durante a revolução digital. Governos e empresas de diferentes setores têm sido, cada vez mais, alvos de ataques de cibercriminosos. Tais ataques têm diferentes impactos técnicos em suas infraestruturas e serviços, que resultam em impactos econômicos diretos e indiretos em seus modelos de negócios. Além disso, os impactos sociais e de reputação têm sido cada vez mais frequentes, já que a sociedade depende cada vez mais de serviços digitais. O setor da saúde tem sido um dos mais afe-*

tados, principalmente devido aos incentivos financeiros que os cibercriminosos possuem para obter dados sensíveis e tornar serviços críticos indisponíveis. A Organização Mundial da Saúde (OMS) vem enfatizando o grave impacto dos ataques cibernéticos em hospitais e serviços de saúde, exigindo uma ação global urgente e coletiva para enfrentar essa crise crescente. Portanto, neste trabalho, iremos analisar e compreender os riscos e as particularidades do setor da saúde, bem como definir os principais passos para um planejamento eficiente de estratégias de cibersegurança para o setor da saúde. Além disso, serão mapeados os principais esforços em cibersegurança da academia e da indústria direcionados ao setor da saúde.

1.1. Introdução

A atenção e preocupação com a cibersegurança têm aumentado na última década devido à sua importância para manter sistemas digitais e serviços interdependentes disponíveis. Incidentes de cibersegurança têm sido noticiados pela mídia de forma cada vez mais constante, já que governos, empresas e a sociedade se tornaram dependentes de sistemas computacionais [Singer and Friedman 2013]. Com isso, a cibersegurança emerge como um pilar essencial para a sociedade. Investimentos em cibersegurança têm-se tornado cada vez mais comuns; porém, a cibersegurança ainda é vista como um custo [Gordon et al. 2018] e não como a prioridade necessária para manter a disponibilidade de serviços, a operação de negócios e garantir a proteção de dados de usuários.

A rápida evolução tecnológica tem criado um cenário fértil para inovações e permitido acesso a serviços cada vez mais complexos e automatizados. Tal evolução permite benefícios diretos para a sociedade, como serviços para comunicação, gestão financeira e monitoramento de saúde, e também oportunidades para empresas. Porém, com a dependência tecnológica, também existe um aumento crescente de ciberataques (por exemplo, ransomware, phishing e negação de serviço) a sistemas e usuários, com diversos impactos técnicos, econômicos, legais e sociais [Franco et al. 2023a]. Tais impactos reforçam a ideia de que a cibersegurança não deve ser pensada apenas sob uma perspectiva técnica.

Os ciberataques podem gerar prejuízos significativos, independentemente do setor de atuação ou do tamanho da organização. Em situações como a interrupção de serviços ou o vazamento de dados, os impactos econômicos são imediatos, envolvendo perda de clientes, danos à reputação e eventuais ações judiciais decorrentes da exposição de informações sensíveis. Além das consequências financeiras, esses ataques também podem provocar efeitos sociais diretos, especialmente quando atingem infraestruturas críticas, como os sistemas de transporte [Islam et al. 2023], energia [Beerman et al. 2023] e saúde [Javaid et al. 2023], afetando diretamente a vida e o bem-estar da população.

De acordo com relatórios de vazamento de dados, dados médicos ainda são os mais vazados e com maiores custos [IBM Security 2024], seguidos de dados bancários e dados pessoais. Em um estudo conduzido com 22.052 incidentes de vazamentos de dados [Verizon Business 2025], foi observado que o setor da saúde permanece como um dos principais alvos de ciberataques. Tal motivação se deve ao alto valor econômico e social dos dados e sistemas. O setor é um dos mais visados, por exemplo, por ataques de ransomware devido à urgência de acesso a dados e sistemas, onde uma disrupção nos serviços pode ocasionar impactos críticos em um curto período de tempo. Ciberataques

como negação de serviço e phishing permanecem, junto com ransomware, como as maiores ameaças em todos os setores.

O setor da saúde se caracteriza pelo uso da tecnologia em diferentes frentes para possibilitar serviços otimizados para gestores, profissionais da saúde e cuidados ao paciente. O uso de diferentes tecnologias pode ser observado, como, por exemplo, equipamentos de diagnóstico e monitoramento, aplicações para gerenciamento de consultas e exames e sensores. Tais sistemas e equipamentos possuem integrações e geram dados sensíveis que podem ser acessados por diferentes partes interessadas. Por exemplo, médicos precisam ter acesso às informações mais recentes sobre a saúde de um paciente durante um procedimento. Portanto, ciberataques que visam o setor podem explorar desde a necessidade de disponibilidade de serviços e equipamentos até mesmo a confidencialidade das informações médicas e sensíveis geradas e armazenadas sobre procedimentos e pacientes.

Devido à complexidade e importância do ecossistema do setor da saúde, existem diversas oportunidades também para atacantes. Por exemplo, ataques de ransomware podem tornar indisponível o acesso a sistemas de internação, bloquear o acesso a equipamentos de exames e afetar até mesmo cirurgias. Ataques dessa magnitude podem causar impactos em atendimentos em todo um país, como o caso reportado no Reino Unido, em 2017 (*cf.* Seção 1.4.2). Além disso, ciberataques de phishing com foco em pacientes ou profissionais da saúde podem possibilitar a obtenção de acesso a sistemas críticos. Além do componente humano, diversas aplicações existentes para o setor (por exemplo, mHealth, prontuários eletrônicos, telessaúde e sistemas de apoio à decisão clínica) são, muitas vezes, desenvolvidas ou utilizadas sem os cuidados necessários com a cibersegurança [Aljedaani and Babar 2021], permitindo assim que ciberataques possam comprometer sistemas críticos e informações sensíveis.

A cibersegurança consolidou-se como um dos principais desafios tecnológicos da atualidade para diversos setores. Entre os obstáculos mais relevantes destacam-se: *(i)* a carência de educação e treinamento adequados, o que torna o fator humano um dos principais vetores de ataque; *(ii)* a escassez de investimentos e a ausência de estratégias e planejamentos eficazes; *(iii)* a dificuldade de quantificar os riscos e impactos decorrentes de ciberataques; e *(iv)* a falta de conscientização sobre a importância da cibersegurança por parte de organizações, governos e sociedade. Diante desse cenário, este capítulo abordará os principais riscos e impactos de ciberataques, apresentando também práticas para o planejamento de estratégias de cibersegurança. O capítulo terá como foco o setor da saúde, que é historicamente vulnerável a incidentes de segurança cibernética, e cujas consequências vão além da perspectiva técnica, gerando impactos econômicos, jurídicos e sociais significativos.

A organização deste capítulo está apresentada na Figura 1.1, auxiliando na compreensão dos principais tópicos que serão abordados nas diferentes seções deste capítulo. Na Seção 1.2 são apresentados os conceitos básicos sobre cibersegurança relacionados à confidencialidade, integridade e disponibilidade. Também, é apresentada nesta seção uma breve descrição e modus operandi dos principais ciberataques (por exemplo, ransomware, negação de serviço e phishing). Na Seção 1.3 é conduzido um estudo do estado da arte, incluindo soluções disponíveis na indústria e academia, regulamentações e documentos

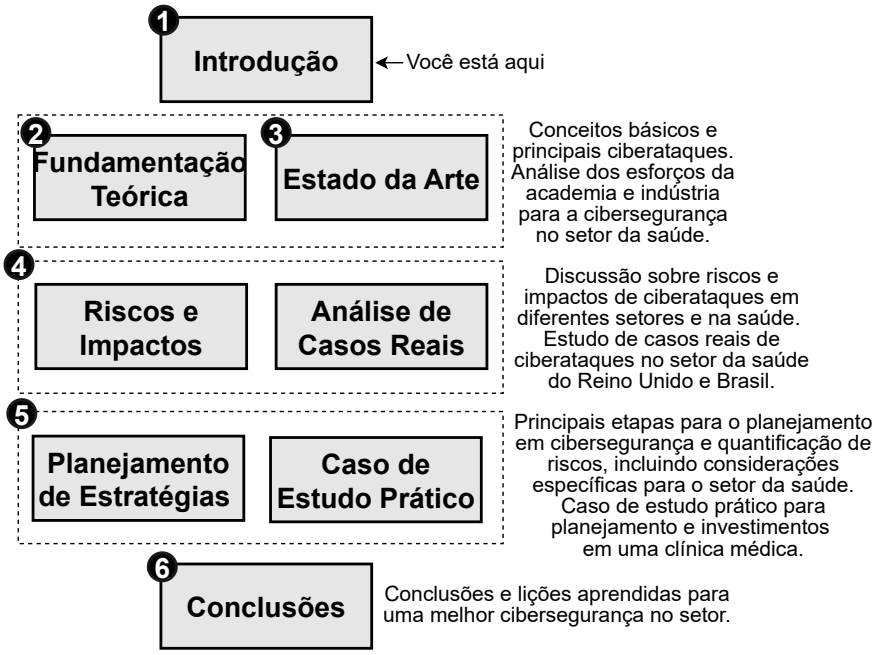


Figura 1.1. Organização do Capítulo

de boas práticas. A seção é concluída com uma discussão sobre tendências, desafios e oportunidades na área de cibersegurança na saúde.

Já na Seção 1.4 são apresentados e discutidos os riscos e impactos de ciberataques em diferentes setores, tendo como foco apresentar as nuances do setor da saúde. Também, nesta seção, são apresentados dois estudos de caso de ciberataques passados no mundo real: ataque de ransomware no Reino Unido e vazamento de dados no sistema de saúde do Brasil. A Seção 1.5 introduz as principais etapas para o planejamento em cibersegurança e também para a quantificação de riscos, discutindo as tarefas críticas para o setor da saúde. Nesta seção também é conduzido um caso de estudo utilizando uma plataforma educacional para planejamento e simulação de riscos em cibersegurança. Por fim, na Seção 1.6 são apresentadas as conclusões e lições aprendidas para uma cibersegurança mais robusta no setor da saúde em curto, médio e longo prazo.

1.2. Fundamentação Teórica

Para melhor compreender o impacto que ataques cibernéticos têm em organizações de saúde, é necessário primeiro abordar alguns conceitos básicos de cibersegurança. Essa seção explora as propriedades de segurança desejáveis em sistemas de informação, bem como a maneira com que atacantes (ou seja, adversários) podem tentar comprometer essas propriedades para obter acesso indevido a dados. Por fim, são apresentados exemplos de cada tipo de ataque dentro do setor da saúde e suas consequências técnicas e financeiras para indivíduos e organizações.

Um dos principais objetivos de ferramentas de segurança é fornecer as proprie-

dades de Confidencialidade, Integridade e Disponibilidade (Confidentiality, Integrity, and Availability, CIA), que são pilares da cibersegurança. Garantir a confidencialidade da informação é garantir que ela não está disponível e nem pode ser descoberta por indivíduos, entidades ou processos que não têm autorização para acessá-la [Beckers et al. 2015]. Manter a integridade dos dados significa ter a garantia de que os dados estão corretos e completos durante todo o seu ciclo de vida, assim assegurando que os dados não foram modificados de forma não autorizada [Boritz 2005]. Por fim, a disponibilidade é a propriedade que garante que a informação pode ser acessada no momento em que ela é necessária, ou seja, de que os sistemas usados para seu armazenamento e processamento estão funcionando corretamente, assim como as medidas de segurança usadas para protegê-la e os canais de comunicação necessários para acessá-la.

Em sua maioria, os mecanismos de segurança usados em sistemas computacionais buscam garantir as propriedades da tríade CIA em alguma medida. Para garantir a confidencialidade de uma informação, por exemplo, é necessário garantir que um usuário possua a autenticação necessária e esteja autorizado a acessá-la. Mecanismos de autenticação servem também para determinar se uma tentativa de acesso é legítima, ou seja, se o usuário ou dispositivo é quem diz ser. Já um mecanismo de autorização serve para garantir que o usuário tem as permissões necessárias para realizar o acesso em questão. Um exemplo de mecanismo de segurança que garante a integridade dos dados é o cálculo de somas de verificação (*checksum*) de arquivos. A disponibilidade, por sua vez, é o principal objetivo de diversos mecanismos de segurança que buscam impedir a interrupção de serviços, como mecanismos de redundância, *backups* e planos de recuperação.

Durante ataques cibernéticos, adversários tentam contornar a estrutura de cibersegurança que garante a confidencialidade, integridade e a disponibilidade de informações e serviços. Para isso, atacantes contam com oportunidades como, por exemplo, vulnerabilidades em sistemas de informação e erro humano, ou usam força bruta e grande quantidade de recursos (por exemplo, processamento e rede) para sobrecarregar os sistemas. No restante dessa seção, são introduzidos os principais ataques que afetam o setor da saúde e também discutido como tais ataques conseguem contornar estruturas de segurança de uma organização para obter acesso indevido ou impedir o funcionamento de sistemas.

1.2.1. Ransomware

Ransomware, palavra em inglês derivada de sequestro (*ransom*) e *software*, é um tipo específico de malware que, ao ter acesso a um sistema, criptografa os dados existentes (por exemplo, dados pessoais ou sistemas da vítima) e impede seu acesso até que um valor de resgate seja pago [Young and Yung 1996]. Se tratando de organizações, bancos de dados inteiros podem ficar inacessíveis. Na maioria das ocasiões, o atacante também ameaça divulgar publicamente os dados. Caso a organização não tenha as medidas de cibersegurança necessárias para se proteger desse tipo de ataque, as consequências são a disrupção de serviços, perda de reputação e perda financeira. Tais impactos ocorrem devido ao tempo de interrupção do serviço, à perda permanente dos dados caso o resgate não seja pago, e a potenciais multas relacionadas com infrações de *compliance* caso esses dados sejam vazados pelos criminosos. Os responsáveis pelo ataque geralmente pedem o pagamento do resgate através de moedas digitais, como Bitcoin e Monero, de modo que o valor pago se torna indetectável e, na maioria das vezes, não possa ser rastreado. Um

ataque de ransomware geralmente tem origem quando um usuário do sistema recebe e executa um arquivo malicioso que aparenta ser legítimo, por exemplo, no anexo de um e-mail de phishing. Depois de executado, esse tipo de malware se espalha rapidamente dentro do sistema, infectando outras máquinas conectadas à mesma rede e criptografando todos os dados os quais consegue acesso.

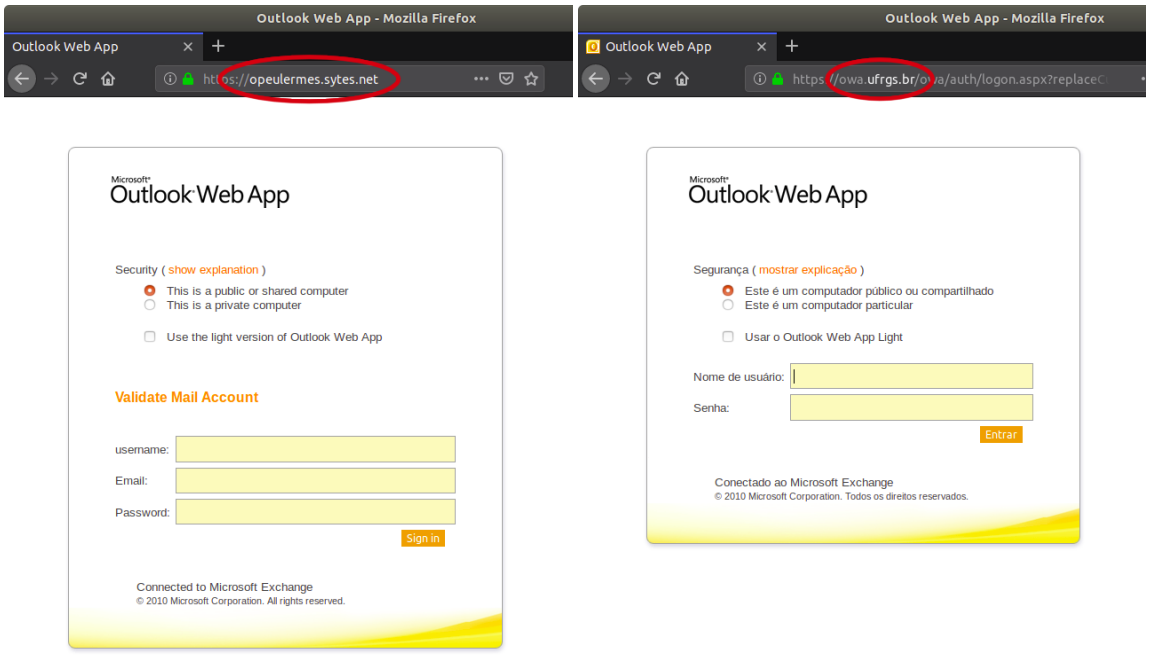
Não é recomendado que organizações façam o pagamento dos resgates na tentativa de retomar o acesso aos seus dados. Como em qualquer tipo de sequestro, o pagamento assume a boa fé do atacante que pode optar por não entregar a chave criptográfica que precisa ser usada pra decodificar os arquivos. Com o pagamento, a empresa também corre o risco de que o ataque se repita, e de que os atacantes tentem replicar o ataque bem-sucedido em outras empresas [Healthcare Information and Management Systems Society 2024]. Porém, não é raro que os responsáveis optem pelo pagamento na tentativa de diminuir o impacto do ataque. De acordo com relatório da Claroty, em 2024, 78% das empresas do setor de saúde entrevistadas relataram pagamentos. Em 39% delas, o valor dos resgates alcançou entre US$ 1 milhão e US$ 5 milhões. Cerca de um quarto dos participantes reportou perdas que chegaram a US$ 1 milhão ou mais, entre perda de receita, gastos com recuperação de sistemas e gastos legais [Claroty 2025].

Um dos ataques de ransomware mais proeminentes no setor da saúde ocorreu em 2024 e afetou a empresa estadunidense Change Healthcare. A Change Healthcare é uma subsidiária do grupo UnitedHealth, uma das maiores empresas de gerenciamento de receita, processamento de pagamentos e compartilhamento de informações de saúde do país. A empresa admitiu ter pago US$ 22 milhões em Bitcoins na tentativa de fazer o resgate dos dados [Claroty 2025], que não foram devolvidos pelos atacantes. Os dados expostos incluem informações de contato, detalhes de apólices de seguros de saúde, informações médicas e dados financeiros de pacientes. A empresa ficou fora de operação pelo período do ataque, o que ocasionou atrasos no pagamento de serviços prestados por profissionais da saúde. O gasto total da empresa com o ataque, somando implicações legais, técnicas e o pagamento do resgate, chegou a exorbitantes US$ 3,1 bilhões [Olsen 2025].

1.2.2. Phishing

Ataques de phishing são uma das maiores causas de vazamentos de dados no setor da saúde [Alder 2024], e um dos ataques de engenharia social mais efetivos contra organizações no setor [United States Department of Health and Human Services 2024a]. Engenharia social é o nome dado à técnica de manipular indivíduos a divulgar informações de acesso restritas ou a qualquer outra ação prejudicial a dispositivos e sistemas aos quais se tem acesso. Existem inúmeras estratégias de engenharia social usadas em golpes de phishing, e seus alvos são amplos e variados. De funcionários a clientes e fornecedores, qualquer informação divulgada por uma vítima de phishing tem potencial de causar danos a sistemas e expor dados sigilosos. Devido a isso, o phishing muitas vezes é o vetor de outros ataques [Adebukola et al. 2022]. Por exemplo, um usuário pode ser enganado a clicar em um link que realiza o download de um malware ou credenciais obtidas através de phishing podem ser usadas para obter acesso não autorizado a dados e sistemas. Também por esse motivo, é difícil precisar a real escala do impacto de ataques de phishing no setor da saúde, já que eventos de cibersegurança de impacto considerável podem ter tido origem em uma interação que começou com um simples e-mail de phishing.

As técnicas de engenharia social usadas em ataques de phishing são variadas e estão em constante evolução, e seus alvos em potencial são amplos e diversificados. Um e-mail de phishing pode ser encaminhado, por exemplo, para todos os funcionários de uma organização. Na Figura 1.2, temos o exemplo de uma campanha de phishing contra funcionários e alunos de uma universidade (ou seja, UFRGS). O ataque começa com um e-mail aparentemente legítimo demandando urgência, por exemplo, alguma situação precisa ser regularizada ou o usuário corre o risco de perder e-mails importantes ou ter sua conta suspensa. O corpo do e-mail de phishing geralmente apresenta um link malicioso que o alvo deve clicar para ser redirecionado e regularizar a situação. No caso da Figura 1.2, o cliente de e-mail Outlook é um dos recomendados para o acesso ao e-mail institucional. Ao clicar no link, o usuário é redirecionado a uma página falsa (ver Figura 1.2a). Caso o usuário não perceba o erro e informe suas credenciais de acesso, o atacante vai obter um *login* e senha que poderão ser usados tanto para prejudicar o indivíduo quanto para acessar áreas restritas do sistema da universidade. Dependendo do nível de permissão do usuário, inúmeros outros ciberataques podem ser executados uma vez obtido acesso.



(a) Ataque de phishing imitando o cliente de e-mails Outlook Web, hospedado em um domínio malicioso.

(b) A pagina verdadeira do cliente de e-mails Outlook Web, com o domínio legítimo da UFRGS.

Figura 1.2. Exemplo de um ataque de phishing direcionado ao e-mail institucional da UFRGS, para os usuários do cliente Outlook Web. Acervo pessoal.

Campanhas de phishing genéricas, como o exemplo da Figura 1.2, muitas vezes contêm erros de escrita e não são muito convincentes. Um tipo diferente de ataque de phishing é o phishing direcionado (ou *spear* phishing, em inglês). Esses ataques têm como alvo indivíduos específicos sobre os quais os atacantes têm alguma informação relevante, o que adiciona veracidade às informações falsas apresentadas no ataque e aumenta as chances de atrair as vítimas. Por ser menos genérico e elaborado de forma direcionada,

esse tipo de ataque tem uma eficácia muito mais alta e pode ser a primeira parte de um ataque mais complexo. Segundo um relatório sobre cibersegurança no setor da saúde [Healthcare Information and Management Systems Society 2024], o phishing permanece sendo o maior vetor de ataque e o principal meio pelo qual sistemas são comprometidos. Uma tendência preocupante que vem sendo observada por empresas no setor é o uso de *deepfakes*, uma técnica de Inteligência Artificial usada para gerar imagens falsas realistas, para aumentar a eficácia de golpes de phishing.

A principal forma de combater o phishing é através da conscientização e treinamento. Para isso, é necessária uma estratégia de treinamento implementada de forma contínua aplicada a funcionários, clientes, e quem mais tiver acesso a sistemas restritos de uma organização. Essa estratégia pode incluir cursos tanto online quanto palestras sobre tópicos de cibersegurança, boas práticas de cibersegurança e, principalmente, apresentar métodos de engenharia social usados em golpes de phishing e suas tendências. Devem ser abordados tópicos como, por exemplo, a falta de segurança em redes públicas, o uso de gerenciadores de senha, a necessidade de trocas de senha regulares, entre outros. Outra estratégia interessante é a simulação de cenários de phishing pelo próprio setor de Tecnologia da Informação (TI) da organização [Cartwright 2023]. Dessa forma, é possível manter o estado de atenção entre os usuários e também identificar os indivíduos que precisam de reforço em seus conhecimentos de cibersegurança. Esses métodos de combate ao phishing devem estar inseridos na estratégia de cibersegurança de empresas, o que demanda investimentos e a atenção de especialistas.

1.2.3. Negação de Serviço

Os ataques de negação de serviço (Denial of Service, DoS) são ataques onde um serviço é sobrecarregado com uma quantidade de tráfego ou requisições tão alta que resulta em um estado no qual os usuários legítimos não conseguem acessar o serviço [De Neira et al. 2023]. Assim, os ataques DoS não necessariamente exploram vulnerabilidades específicas na infraestrutura ou sistema. Em sua versão mais poderosa e distribuída (Distributed Denial of Service, DDoS), um grande número de hosts é utilizado para gerar o volume de tráfego ou requisições necessário ao ataque. Imagine uma estação de trem onde milhares de pessoas estão paradas em frente à porta do trem, fingindo estarem aguardando para entrar. Porém, na verdade, tais pessoas estão bloqueando que usuários legítimos (ou seja, quem realmente quer entrar no trem) acessem o serviço. Essa analogia nos permite compreender como funciona um ataque de tal magnitude.

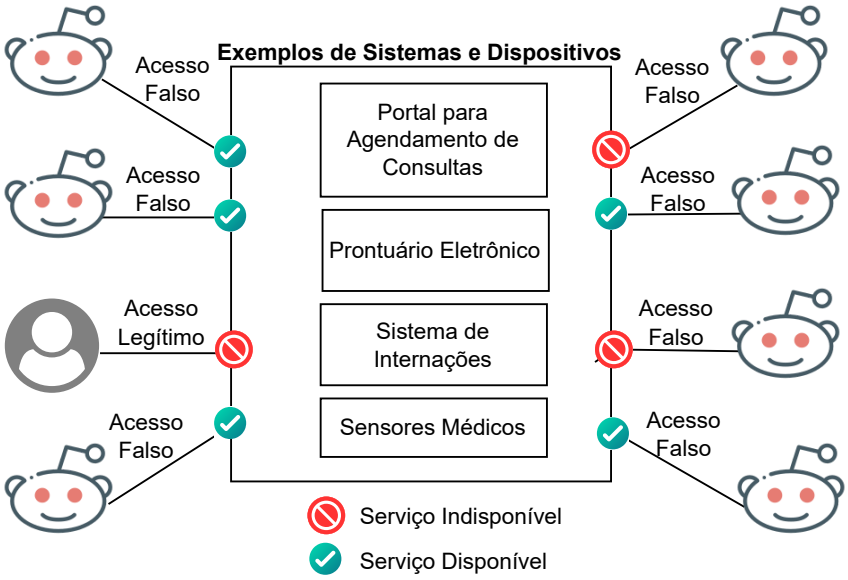


Figura 1.3. Exemplo de um DDoS, com um acesso legítimo a serviços sendo negado devido a uma grande quantidade de acessos falsos.

Para obter acesso a um grande número de dispositivos, outros tipos de ataque são empregados, como a distribuição de malware por e-mail (ver Seção 1.2.2). Decisões de projeto e processos de administração de sistemas que fornecem segurança fraca tornam ainda mais fácil comprometer uma grande quantidade de dispositivos [Navruzov and Kabulov 2022]. Tendências como a Internet das Coisas (*Internet of Things*, IoT) levaram a um aumento no número de dispositivos conectados à Internet. Muitas vezes, esses dispositivos não possuem mecanismos de segurança implementados, de modo que a simples verificação manual de serviços expostos publicamente é suficiente para obter acesso a eles. A existência de bilhões desses dispositivos com segurança fraca tem permitido que invasores criem ataques cada vez mais poderosos a cada ano. Por exemplo, o malware Mirai permitiu controlar cerca de 600 mil equipamentos infectados, criando assim uma rede de computadores zumbis conhecida como botnet [Gallopeni et al. 2020]. Dentre os dispositivos infectados estão câmeras de segurança, roteadores, geladeiras e até mesmo dispositivos médicos.

No setor da saúde, os ataques de DDoS podem impactar serviços com conectividade na Internet, causando a indisponibilidade para usuários legítimos. A Figura 1.3 apresenta uma representação de um ataque coordenado com zumbis enviando requisições falsas e impedindo que um usuário legítimo possa acessar os recursos (ou seja, os sistemas e dispositivos).

Por exemplo, sistemas de agendamento de consultas podem receber diversas requisições até que sejam sobrecarregados, de modo que fiquem muito lentos e os pacientes desistam de agendar uma consulta. Em outro exemplo, ataques a sistemas de prontuários eletrônicos podem sobrecarregar os servidores responsáveis pelo armazenamento e acesso às informações clínicas, tornando-os inacessíveis. Isso impede médicos e profissionais de

saúde de acessarem dados essenciais, como históricos de pacientes e resultados de exames, comprometendo a qualidade do atendimento e colocando vidas em risco. Portanto, tais ataques não só interrompem a operação dos serviços médicos, como também geram confusão e aumentam a insatisfação dos pacientes, com impacto direto na eficiência e na reputação das instituições de saúde.

1.3. Estado da Arte da Cibersegurança no Setor da Saúde

É inegável que a conectividade fornecida pela Internet traz inúmeros benefícios para o setor da saúde, como a interação em tempo real entre sistemas e o aumento na disponibilidade de serviços. A adoção de dispositivos de IoT para tarefas de diagnóstico e monitoramento de pacientes traz maior comodidade para equipes médicas e administrativas em unidades de saúde [He and Zeadally 2014]. Tecnologias como Inteligência Artificial (IA) têm grande potencial em diversas áreas relacionadas à saúde, podendo atuar, por exemplo, como ferramentas de diagnóstico [Chamberlaim et al. 2023], auxiliar no processo de tomada de decisões estratégicas hospitalares, e na cibersegurança [Nankya et al. 2024]. As mudanças nos padrões de trabalho possibilitadas pela Internet permitem que setores das organizações trabalhem, inclusive, de forma remota. Contudo, expor sistemas e serviços à Internet também pode levar a ataques cibernéticos, o que, por sua vez, pode causar disrupção de serviços, vazamento de Informações de Saúde Protegidas (*Protected Health Information*, PHI), perdas financeiras e ameaça até mesmo à saúde de pacientes.

Inúmeras estratégias para proteção cibernética de organizações de saúde são propostas todos os anos na indústria e na academia. Sistemas usando dispositivos IoT em contextos médicos (*Internet of Medical Things*, IoMT, ou Internet das Coisas Médicas) têm se mostrado particularmente vulneráveis, por se tratar de uma quantidade substancial de equipamentos continuamente gerando grandes volumes de dados, vindos de fabricantes diferentes e com pouca padronização em seus protocolos e atualizações de segurança [Soares et al. 2023]. Essas características levam ao aumento da superfície de ataque de organizações médicas e representam um desafio extra para as soluções de segurança no setor. Essas soluções precisam ser capazes de lidar com acessos não autorizados, perda, extravio e/ou descarte inapropriado de dispositivos IoMT [Cartwright 2023], além dos principais ciberataques discutidos na Seção 1.2.

Uma linha de pesquisa em alta na área de cibersegurança para o setor da saúde é o uso de soluções baseadas em blockchain. Existe um interesse crescente na literatura em usar tecnologias distribuídas de registro para resolver problemas tradicionais do setor, como falta de interoperabilidade, dificuldades de auditoria e vazamentos de dados [Santos et al. 2021]. Em particular, sistemas de saúde podem se beneficiar da descentralização, transparência e imutabilidade inerentes a sistemas de blockchain [Scheid et al. 2021b]. Esses sistemas podem facilitar o acesso e compartilhamento de registros médicos, além de contribuir para os esforços de padronização entre diferentes instituições [Abou Jaoude and Saade 2019]. Contudo, seu emprego também pode trazer desvantagens e novas complicações para sistemas de saúde. Além das preocupações com custo computacional e armazenamento, existe a preocupação com *compliance* e regulamentação, já que todos os dados de uma transação escritos em blockchain são permanentes e não podem ser apagados. Portanto, soluções empregando sistemas de blockchain para a área da saúde precisam empregar outras técnicas em conjunto para o armazenamento de dados pessoais e PHI.

Também em alta no mercado e na literatura estão soluções de segurança usando técnicas de Aprendizado de Máquina (*Machine Learning*, ML) e IA. Dentro do escopo de segurança cibernética, essas soluções contribuem principalmente para a detecção de ataques através do monitoramento de comportamento anômalo, vulnerabilidades de dia-zero e respostas automatizadas [Nankya et al. 2024]. Desafios para essa linha de pesquisa incluem principalmente o tratamento dos dados usados para treinamento, que podem incluir informações pessoais de pacientes. Técnicas de Aprendizado Federado (*Federated Learning*), em particular, permitem que vários clientes façam o treinamento de um modelo enquanto mantêm os dados usados de forma descentralizada, ou seja, sem compartilhar os dados entre si [Wen et al. 2023]. Também vale destacar o aumento do uso de ferramentas de IA para realizar ataques ou mesmo adicionar novas vulnerabilidades no setor. O uso de *deepfakes* (vídeos ou imagens falsas geradas artificialmente usando *deep learning*) tem o potencial de aumentar a eficácia de golpes de *phishing*, uma das principais ameaças do setor [Healthcare Information and Management Systems Society 2024]. A falta de regulamentação do uso de ferramentas de IA generativa por funcionários também põe organizações de saúde em risco, já que as principais ferramentas para esse fim (por exemplo, ChatGPT, Gemini e DeepSeek) são proprietárias e os dados são compartilhados com organizações externas.

O vazamento e/ou compartilhamento não autorizado de PHIs e dados pessoais de pacientes está entre os principais riscos do setor da saúde. De acordo com o relatório publicado pela IBM em 2024, o setor tem o maior custo associado a vazamento de dados: em média US$ 9,77 milhões por ataque [IBM Security 2024]. A maioria dos países possui ferramentas de regulação e *compliance* que lidam com empresas responsáveis por vazar dados pessoais de seus usuários. Na Europa, a *General Data Protection Regulation* (GDPR) se aplica a todos os indivíduos e organizações que lidam com dados pessoais de cidadãos europeus [GDPR.EU Horizon 2020 2021]. Em 2024, a GDPR aplicou 202 multas a hospitais, farmacêuticas, profissionais da saúde e fornecedores de equipamento médico em 26 países, totalizando 16,5 milhões de euros [Runte 2024]. Nos Estados Unidos, a *Health Insurance Portability and Accountability Act* (HIPAA) traz as diretrizes que organizações e provedores de seguros de saúde devem seguir para garantir que PHIs e informações pessoais identificáveis sejam protegidas de fraude ou roubo [U.S. Government 1996]. Em janeiro de 2025, um fornecedor de monitores de glicose, bombas de insulina e outros equipamentos para pessoas com diabetes foi multado em US$ 3 milhões [United States Department of Health and Human Services 2024b] depois de um vazamento que teve origem em um ataque de *phishing* direcionado. No Brasil, a Lei Geral de Proteção de Dados (LGPD) e a Autoridade Nacional de Proteção de Dados (ANPD) controlam a privacidade, uso e tratamento de dados pessoais. Em contramão ao restante das entidades regulatórias no mundo, a ANPD não aplicou multas em função de vazamento de dados em 2024 [Calegari 2025].

Diante de um cenário tão complexo quanto a computação no setor da saúde, as ferramentas de segurança precisam evoluir rapidamente para acompanhar inovações aceleradas, regulamentações complexas e, principalmente, demandas de sistemas críticos. Para isso, é necessário forte investimento em cibersegurança, já que a falta de orçamento é citada como um dos maiores desafios para pequenas empresas no setor da saúde nos Estados Unidos [HIMSS, FinThrive 2025]. Uma vez assegurado o investimento, é ne-

cessário que executivos, gestores e técnicos priorizem quais ameaças são mais urgentes em sua organização ou setor. Dispositivos IoMT têm grande potencial de serem explorados por adversários. Segundo relatório da Claroty, IoMT com vulnerabilidades críticas de segurança estão presentes em 89% das organizações de saúde pesquisadas [Claroty 2025]. Outra necessidade é a conscientização constante de funcionários sobre cibersegurança, através da aplicação de cursos, treinamento e até mesmo incidentes simulados. Por exemplo, em 2020, um funcionário do Hospital Albert Einstein publicou no GitHub de forma acidental uma planilha com senhas de funcionários do Ministério da Saúde (ver Seção 1.4.3), levando à exposição de dados de pelo menos 16 milhões de pacientes de Covid-19 [Cambricoli 2020]. Levando em consideração esses e outros fatores, essa seção apresenta um panorama da cibersegurança no setor da saúde, considerando a extensão dos desafios do setor.

1.3.1. Soluções

Alguns tópicos se destacam no estado da arte com aplicações de cibersegurança para a área da saúde. Dentre eles, soluções de controle de acesso e autenticação merecem atenção por garantir que dados sigilosos de saúde serão acessados apenas por pessoas autorizadas, sejam elas pacientes, profissionais de saúde ou de gestão. Em particular, sistemas utilizando dispositivos IoT em grande escala precisam de cuidados redobrados com seus mecanismos de segurança e privacidade. Também em alta estão soluções de segurança baseadas em blockchain, por fornecerem propriedades de segurança como autenticação e integridade de dados. Outra tecnologia emergente no estado da arte são algoritmos de ML atuando na detecção de ataques e respostas automatizadas a incidentes.

1.3.1.1. Segurança de Dispositivos de IoT em Saúde

IoT é uma área ampla que compreende diversas indústrias, como cidades inteligentes, monitoramento industrial, agricultura, entre várias outras. Dentro do escopo de saúde, dispositivos de IoMT têm potencial para trazer melhor qualidade de vida para pacientes com necessidade de monitoramento contínuo e maior comodidade para equipes médicas e de gerenciamento [He and Zeadally 2014]. Contudo, o emprego desses dispositivos aumenta consideravelmente os desafios de segurança enfrentados por organizações médicas e unidades de saúde. Algumas consequências do uso inadequado de dispositivos IoMT são, por exemplo, o vazamento de informações pessoais de pacientes e o atraso na detecção de eventos de saúde importantes devido a interrupções de serviço, entre outros [Sun et al. 2019]. Técnicas de segurança padrão em outros sistemas computacionais nem sempre podem ser aplicadas em sistemas IoMT, devido a restrições na capacidade computacional desses dispositivos, sendo que dispositivos sensores e vestíveis costumam ter ainda menos recursos.

Soluções de segurança visando sistemas de IoMT necessitam de técnicas de autenticação confiáveis, assim como esquemas de verificação e validação para manter a confiabilidade dos participantes, sejam eles pacientes, profissionais de saúde ou organizações médicas [Adil et al. 2024]. A autenticação é o processo que visa confirmar a identidade de um usuário e garantir que ele tem as permissões necessárias para acessar aquelas informações ou realizar determinada tarefa. No caso de dispositivos IoMT, por exemplo,

é necessário garantir que os dados de medição de sensores sejam acessados apenas pela equipe médica responsável e não por pessoas em outros cargos dentro da rede hospitalar. Um esquema de autenticação robusto garante vários requisitos de segurança desejáveis, como, por exemplo, controle de acesso, disponibilidade das informações e integridade de dados. Também existe a preocupação com a transmissão de dados médicos entre os dispositivos IoMT e seus respectivos *gateways* de acesso, já que esses dispositivos muitas vezes não têm poder computacional o suficiente para empregar técnicas de criptografia robustas que garantam que um adversário observando o tráfego de rede não será capaz de espionar os dados em trânsito [Sun et al. 2019].

[Gupta et al. 2019] propõe um mecanismo de autenticação para dispositivos IoT utilizando Disjunção Exclusiva (XOR) e funções *hash* criptográficas de mão única, com o objetivo de proteger a comunicação entre dispositivos de forma eficiente e com baixo custo computacional. Também lidando com o processo de autenticação, [Ostad-Sharif et al. 2019] propõe um sistema híbrido onde um algoritmo de criptografia mais leve é utilizado na primeira parte do processo, quando os participantes estão trocando as chaves criptográficas que serão usadas na comunicação, e, posteriormente, um algoritmo de Criptografia de Curva Elíptica (ECC) é usado para criptografar as mensagens contendo os dados. Já [Ding et al. 2019], por sua vez, propõe distribuir o custo computacional de algoritmos mais custosos usando dispositivos de borda (conhecidos em inglês como *Edge*), que têm capacidade computacional intermediária entre sensores IoMT e computadores tradicionais. Com isso, eles desenvolvem algoritmos de verificação de integridade para os dados armazenados, além dos mecanismos de controle de acesso, autenticação e privacidade.

1.3.1.2. Soluções Baseadas em Blockchain

Blockchain é uma tecnologia de registro distribuído que surgiu inicialmente para uso em sistemas de criptoativos [Scheid et al. 2021b]. Suas características incluem fornecer um ambiente descentralizado onde transações podem ser feitas sem a necessidade de supervisão por um terceiro. Em sistemas financeiros tradicionais, a supervisão é necessária para garantir não apenas a identidade dos participantes, mas também a ordem das transações realizadas, assim assegurando que, caso uma operação seja repetida, o mesmo valor não será debitado duas vezes de um dos participantes. Na blockchain, essa funcionalidade é replicada por meio de registros que são encadeados e mantidos por uma rede de nós que compartilham tarefas e arquivos entre si. Após sua proposta inicial em criptoativos, sistemas de blockchain sofreram um processo de generalização e passaram a ser aplicados nas mais diversas áreas [Abou Jaoude and Saade 2019]. Alguns dos benefícios em potencial do uso de blockchain são particularmente relevantes em sistemas de saúde [Scheid et al. 2021a]. A estrutura de blocos encadeados garante intrinsecamente a imutabilidade de registros, o que contribui para a integridade, confiabilidade e garantia de acesso aos dados. Além disso, a necessidade de autenticação dos participantes e a transparência das operações realizadas dentro da rede também são características de interesse dentro da área da saúde [Santos et al. 2021].

Com base em suas propriedades de cibersegurança em potencial, sistemas para gerenciamento de dados de saúde baseados em blockchain são amplamente estudados na

literatura acadêmica. A maioria das soluções foca nos desafios relacionados ao armazenamento e compartilhamento seguro de dados médicos [Arbabi et al. 2023]. Isso acontece pois não é possível remover ou apagar quaisquer informações uma vez armazenadas na blockchain. Ao mesmo tempo que essa característica tem potencial para contribuir com a integridade de registros, ela também representa um desafio para a implementação de sistemas que manipulam PHI. Essas informações estão sujeitas a leis de regulamentação que exigem, por exemplo, que seja possível remover informações pessoais e de saúde a pedido do usuário. Portanto, soluções usando blockchain precisam garantir que ou as informações armazenadas estão criptografadas de tal forma que não são recuperáveis sem a chave secreta, ou usam uma solução híbrida que armazena na blockchain apenas metadados e similares, enquanto os dados de saúde são armazenados em outro lugar.

MedShare [Wang et al. 2021], por exemplo, propõe um esquema usando criptografia baseada em atributos (Attribute-Based Encryption, ABE) para assegurar que os dados de saúde armazenados na blockchain são acessíveis apenas por partes autorizadas. De forma similar, [Zhang et al. 2022] também utiliza uma variante de ABE para permitir que seja feita a busca por palavras-chave nos dados criptografados, enquanto a blockchain é usada para garantir a imutabilidade das chaves e dos registros criptografados. Utilizando uma técnica de armazenamento híbrido, o EdgeMediChain [Akkaoui et al. 2020] usa uma rede de blockchain em dois níveis que salva os registros médicos criptografados separadamente, fora da blockchain. Uma blockchain privada intermediária gerencia a autenticação e os dados gerados por dispositivos geograficamente próximos. Depois dessa análise inicial, os dados relevantes são armazenados separadamente e seu endereço é colocado em uma blockchain pública global, garantindo o acesso a outros participantes do sistema. Isso permite que o sistema de blockchain em camadas funcione como um índice, oferecendo integridade de registros e gerenciabilidade de direitos de acesso.

1.3.1.3. Usos de ML e IA

Talvez um dos tópicos mais discutidos na atualidade, soluções de segurança usando IA e ML precisam de cuidado especial ao serem empregadas em sistemas de saúde. Além de atuar em funções diagnósticas e de monitoramento de saúde de pacientes, essas soluções também são usadas para detecção de ameaças e anomalias no tráfego de rede, o que pode indicar um incidente de segurança em andamento. As técnicas usadas nessa área podem ser divididas em modelos de aprendizado supervisionado e não-supervisionado. Modelos supervisionados necessitam de uma base de dados para treinamento, onde as vulnerabilidades e ameaças já conhecidas historicamente estejam devidamente identificadas e sinalizadas. Depois do treinamento, os modelos são capazes de reconhecer esses padrões com precisão em dados inéditos, como, por exemplo, durante o monitoramento da rede em tempo real. Já nos modelos de aprendizado não-supervisionado, não é feita essa sinalização prévia das vulnerabilidades conhecidas, e fica a cargo do modelo identificar sozinho as anomalias que se desviam do padrão de tráfego normal. Dessa forma, os modelos não-supervisionados são usados para identificar ameaças novas e desconhecidas, conhecidas como ameaças de dia-zero [Nankya et al. 2024].

Além da contribuição para a segurança de sistemas e redes de comunicação em organizações de saúde, técnicas de IA também têm aplicação na hora de proteger a pri-

vacidade de pacientes. No caso de ferramentas de IA que são usadas para diagnóstico, o treinamento dos modelos demanda grandes quantidades de informações médicas e de saúde de pacientes para que possam ser reconhecidos os padrões de doenças e anomalias. Nesses casos, é vital que os dados médicos usados no treinamento sejam anonimizados de alguma forma antes de passados para o modelo, visando manter a conformidade com as leis de proteção de dados vigentes. Para isso, técnicas como Encriptação Homomórfica e Privacidade Diferencial auxiliam na hora de garantir que os dados individuais de um paciente não possam ser identificados dentro de um conjunto maior de dados semelhantes. Dentro desse tópico, estão em destaque técnicas de IA como Aprendizado Federado. Ele permite que várias entidades façam o treinamento de modelos de IA localmente usando apenas os dados aos quais têm acesso, e depois compartilhem entre si apenas as atualizações do modelo [Aouedi et al. 2023]. Em outras palavras, elas compartilham "apenas o que o modelo aprendeu", e não os dados brutos de saúde de pacientes.

É importante ressaltar que ferramentas de IA também têm surgido como vetores e amplificadores de ameaças cibernéticas, chamando atenção negativamente na literatura e na mídia. Ataques de *phishing*, conhecidamente uma das maiores ameaças ao setor da saúde, dependem de técnicas de engenharia social para enganar funcionários com acesso a sistemas restritos com o objetivo de roubar credenciais válidas. *Deepfakes* e ferramentas de IA generativa têm contribuído para aumentar a eficácia desses ataques [Healthcare Information and Management Systems Society 2024], o que exige esforço e investimento cada vez maior na conscientização e educação cibernética de funcionários e colaboradores. Alguns exemplos das consequências desse tipo de ataque são o acesso não autorizado de adversários aos sistemas de organizações de saúde, podendo levar a vazamentos de dados pessoais e danos à estrutura de segurança do sistema. Ferramentas de *deep learning* também podem ser usadas para adulterar o resultado de diagnósticos por imagem, com o objetivos variando entre cometer sabotagem direcionada a indivíduos, fraude de seguros de saúde, ou até mesmo atentados [Mirsky et al. 2019].

1.3.2. Regulamentação, Compliance e Boas Práticas

Organizações em todo o mundo são obrigadas a obedecer à legislação vigente em suas áreas de atuação no que diz respeito ao tratamento de dados pessoais e identificáveis de seus usuários. No setor da saúde, a regulamentação e *compliance* são especialmente importantes por se tratar de uma área que manipula quase que integralmente dados sensíveis e de saúde de pacientes e usuários de serviços médicos. Diferentemente de outras categorias de dados pessoais, uma exposição de dados médicos pode revelar condições de saúde de um indivíduo [Sun et al. 2019]. Alguns dos principais regulamentos no tópico são o GDPR, da União Europeia, e o HIPAA atuante nos Estados Unidos. No Brasil, embora a LGPD tenha passado a valer em agosto de 2020, a autoridade responsável por vistoriar e aplicar sanções a organizações em descumprimento da lei ainda encontra dificuldades em sua atuação [O Globo 2024].

Se tratando da confidencialidade de informações médicas, a GDPR estipula que as informações médicas armazenadas devem ser apagadas depois de processadas e não mais necessárias, e que organizações devem obter o consentimento explícito dos pacientes para compartilhar seus dados com terceiros. A LGPD, fortemente baseada na GDPR, também estipula que os dados pessoais armazenados devem ser eliminados após o término

de seu uso, salvo circunstâncias específicas. Ela também exige que o usuário autorize o compartilhamento de dados com terceiros. Já a HIPAA não tem nenhuma restrição quanto a um período máximo de armazenamento dos dados, nem quanto à possibilidade de compartilhamento de dados entre diferentes provedores de saúde [Sun et al. 2019].

Outra característica relevante no âmbito do armazenamento de dados pessoais e de saúde é o direito do paciente de requisitar que seus dados armazenados junto a organizações de saúde sejam apagados, a qualquer momento. O Art. 17 do GDPR garante esse direito, conhecido como "direito ao esquecimento". Na LGPD, o mesmo direito é conhecido como "direito à eliminação de dados"e é previsto no inciso XIV do Art. 5º. Ele prevê que o titular dos dados pode solicitar a eliminação de suas informações pessoais armazenadas em banco de dados, independentemente do procedimento empregado para obtê-las. Essa regulamentação é particularmente relevante se tratando de sistemas de armazenamento de dados em blockchain, devido à imutabilidade dos registros. Portanto, qualquer implementação deve garantir que os dados armazenados (ou sua possibilidade de acesso) possam ser removidos da blockchain a pedido do paciente, garantindo assim a conformidade com a legislação. A HIPAA, por sua vez, não prevê nenhum equivalente do direito ao esquecimento.

Os regulamentos de proteção de dados pessoais também têm normativas tratando do vazamento de informações e suas consequências. A GDPR estipula que qualquer incidente que ocasione no vazamento de dados pessoais de saúde deve ser reportado dentro de no máximo 72 horas. As multas estipuladas para as infrações à GDPR são baseadas em sua gravidade. Para as menos severas, o valor da multa será o maior valor entre 10 milhões de euros ou 2% do faturamento anual da companhia. Para as infrações consideradas severas, o valor pode chegar a 20 milhões de euros ou 4% do faturamento [Wolford 2020]. Valores semelhantes de multas são estipulados pela LGPD. O Artigo 52 prevê uma multa de 2% do faturamento da pessoa jurídica, grupo ou conglomerado, limitada no total a 50 milhões de reais. Em julho de 2023, a Telekall Infoservice foi multada pela ANPD em 2% de seu faturamento anual, R$14.400,00 no total, por vender uma listagem de contatos de WhatsApp de eleitores para disseminação de material de campanha eleitoral [Autoridade Nacional de Proteção de Dados 2023]. Em contrapartida à GDPR, LGPD não estipula um prazo máximo para reportar um vazamento de dados, deixando essa definição a cargo da ANPD [Koch 2020]. Se tratando da HIPAA, organizações são obrigadas a reportar um vazamento de dados em no máximo 60 dias, caso ele afete mais de 500 pessoas [United States Department of Health and Human Services 2013]. As multas previstas na HIPAA são categorizadas por gravidade, variando de infrações civis a criminais. O valor máximo de cada categoria varia de US$ 25 mil a US$ 1,5 milhão, sendo aplicado a cada violação individual cometida [Edemekong et al. 2024].

1.3.3. Tendências, Desafios e Oportunidades

Segundo relatório [Claroty 2025], dispositivos IoMT são o ponto onde hospitais e organizações na área da saúde estão mais expostos a ciberataques, especialmente considerando dispositivos operando em sistemas operacionais legados que não recebem mais atualizações de segurança. 96% das organizações pesquisadas apresentavam nesses dispositivos vulnerabilidades relacionadas com campanhas de *ransomware* que podem comprometer a disponibilidade de serviços e, consequentemente, a saúde de pacientes. É importante

que dispositivos IoMT sejam atualizados com frequência para garantir que eles sejam capazes de lidar com as ameaças mais recentes. Em adição a isso, é urgente a necessidade de colaboração entre a indústria, a academia e agências de padronização para garantir a intercomunicabilidade, segurança e regulamentação de tecnologias emergentes no escopo de dispositivos IoMT.

Outra tendência importante diz respeito ao uso de IA de modo geral. Em todo o mundo, países se movimentam para desenvolver arcabouços regulatórios visando especificamente a IA, estimulados pela sua ampla adoção entre indivíduos e corporações. Essa movimentação é necessária tanto pelos benefícios da tecnologia, quanto pelos potenciais riscos de seu uso. Na União Europeia, o *EU AI Act* é um dos primeiros atos regulatórios visando especificamente o uso de IA [Lewis et al. 2025], adotado em junho de 2024 e efetivo a partir de fevereiro de 2025 . Ele usa uma estratégia baseada no risco da tecnologia aos usuários para estipular os requisitos necessários para que o uso de IA seja permitido. Por exemplo, tecnologias de identificação e categorização de características biométricas em larga escala são proibidas, enquanto o uso em serviços públicos essenciais é considerado de alto risco. Caso a adoção de uma estrutura regulatória pela União Europeia fortaleça a tendência de outras regiões a também adotarem regulações mais estritas no âmbito da IA, sistemas usando essas tecnologias precisarão se adaptar para garantir sua conformidade.

Outro desafio para o setor é a implementação de estratégias de treinamento, conscientização e preparação dos funcionários. Um dos maiores impactos da pandemia de COVID-19 foi a mudança nos padrões de trabalho nas mais diversas áreas. No setor da saúde em particular, essa mudança fez com que estratégias de segurança desenvolvidas ao longo dos anos deixassem de ser aplicadas no momento em que funcionários passaram a trabalhar de casa com nenhum ou pouco conhecimento em cibersegurança [Cartwright 2023]. Essa falta de treinamento torna uma organização especialmente vulnerável a ataques de phishing. Ataques de phishing direcionados a funcionários podem expor credenciais e levar a vazamentos de dados substanciais, como foi o caso da empresa Solara [United States Department of Health and Human Services 2024b], multada em US$ 3 milhões em 2025 nos Estados Unidos. Para prevenir esse tipo de ataque, as organizações precisam garantir o treinamento de cibersegurança de funcionários independentemente de papéis, o que requer investimentos consideráveis na área.

É vital que as ferramentas de cibersegurança sejam capazes de acompanhar o ritmo das inovações aceleradas que acontecem no setor da saúde. Porém, esse nem sempre é o caso. Os investimentos em cibersegurança costumam ser negligenciados no setor de forma global, o que resulta, por exemplo, na ausência de estratégias eficientes de proteção e no uso continuado de equipamentos obsoletos que nem sempre recebem *patches* de segurança e suporte [Cartwright 2023]. Devido às características próprias do setor, como o fato de os dados manipulados serem pessoais e sensíveis em sua maioria, tem-se que o custo médio de um vazamento de dados no setor da saúde ultrapassou o valor de US$ 10 milhões em 2024 [IBM Security 2024]. Historicamente, o setor é o que tem o custo mais elevado associado a esse tipo de ataque.

De acordo com o relatório produzido pela IBM, o setor de finanças está em segundo lugar com um custo médio por vazamento chegando a aproximadamente 53% do

custo do setor de saúde. Esse cenário demanda um investimento considerável do setor da saúde em ferramentas de cibersegurança para proteger equipamentos, sistemas e principalmente, dados. O valor de investimento necessário em cibersegurança é citado como um dos maiores desafios para pequenas empresas no setor da saúde nos Estados Unidos [HIMSS, FinThrive 2025]. Ainda nos Estados Unidos, o número de ataques cibernéticos no setor afetando 500 ou mais indivíduos está projetado para alcançar quase 700 incidentes em 2025. Esse número ultrapassa em mais de 10 vezes a média de ataques entre 2016 e 2022 [United States Department of Health and Human Services]. Nas próximas seções, serão abordados os impactos de ciberataques no setor da saúde e será apresentada uma metodologia para um planejamento eficiente de investimentos em cibersegurança, com casos de uso voltados para o setor da saúde.

1.4. Riscos e Impactos de Ciberataques

Organizações possuem diferentes riscos associados, como, por exemplo, os riscos de falha nos sistemas, ciberataques, incêndios e vazamentos de dados. Tais riscos podem ocasionar impactos com diferentes dimensões e magnitudes, que podem afetar diretamente as organizações, seus funcionários e usuários. A Figura 1.4 apresenta uma visão geral dos diferentes domínios de impacto de um ataque cibernético nas empresas. Primeiro, o domínio *Econômico* envolve todos os custos diretos e indiretos relacionados a um ataque cibernético. Como a perda financeira é uma das principais preocupações das empresas [Franco et al. 2023b], o foco das campanhas de segurança cibernética pode usar isso como um argumento poderoso para justificar a preocupação com a segurança cibernética. Em seguida, há o impacto *Legal* dos ataques cibernéticos, que transferem os casos de segurança cibernética para a esfera jurídica, as regulamentações e os aspectos de governança. Além disso, a esfera jurídica pode afetar diretamente os fatores econômicos, pois os efeitos colaterais envolvem os custos com advogados, compliance e multas aplicadas pelos órgãos reguladores.

Além disso, há diferentes impactos *Social*, pois os ataques cibernéticos podem interferir diretamente na vida das pessoas e nas estruturas sociais. Por exemplo, os ataques cibernéticos podem ser responsáveis por um colapso no sistema de saúde de um país, como no caso do Sistema Nacional de Saúde do Reino Unido [National Audit Office 2018], ou afetar a vida das pessoas, interrompendo serviços essenciais, como o fornecimento de alimentos [R. Mccrimmon and M. Matishak 2021] e a infraestrutura essencial dos países [J. R. Reeder, P. F. McQuade, S. A. Schipma 2021]. Além disso, o grande número de ataques cibernéticos que exploram a boa-fé dos seres humanos (por exemplo, técnicas de engenharia social e diferentes tipos de phishing) afeta a mudança de comportamentos sociais, o que faz com que as pessoas tenham muito mais medo, mesmo quando estão realizando interações legítimas [Parsons et al. 2013]. Por fim, o domínio *Técnico* de ciberataques descreve as principais disrupções e falhas de infraestrutura que podem também ocasionar um ou mais dos demais impactos descritos.

Em 2024, o custo médio global de uma violação de dados atingiu US$ 4,88 milhões, o maior valor já registrado, representando um aumento de 10% em relação a 2023 [IBM Security 2024]. Para pequenas e médias empresas (PMEs), os custos variaram entre US$ 120.000 e US$ 1,24 milhão, dependendo da gravidade do incidente [BigID 2024]. Empresas podem reduzir significativamente esses custos por meio de práticas efi-

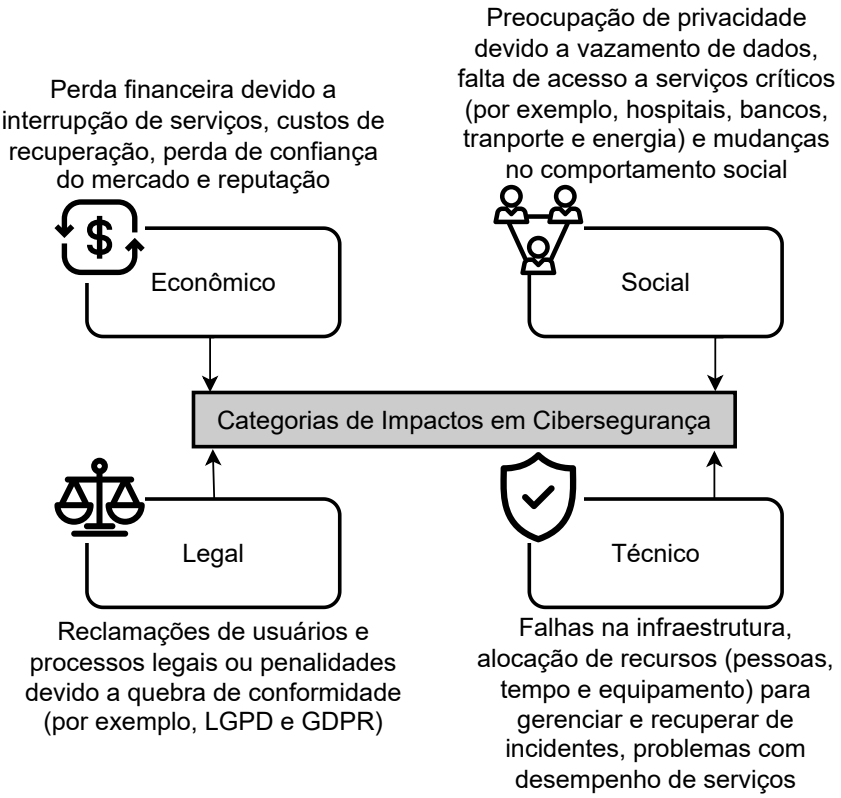


Figura 1.4. Impactos de Ciberataques

cazes de resposta a incidentes. Por exemplo, uma detecção rápida de violações pode reduzir substancialmente as perdas financeiras, e uma divulgação proativa aos clientes e partes interessadas pode atenuar os danos financeiros [IBM Security 2024]. As previsões mais recentes indicam que os custos globais do crime cibernético devem atingir US$ 9,5 trilhões por ano em 2024 [Secureworks 2024], enquanto os danos causados por ataques de ransomware podem ultrapassar US$ 275 bilhões até 2031 [Cybersecurity Ventures 2024].

Em relação aos custos, é importante mencionar que eles podem variar com base em diferentes características das empresas, como o país, setor, tamanho da organização e também configurações técnicas e proteções implementadas. Um estudo recente analisou diversos relatórios publicamente disponíveis de empresas de consultoria em cibersegurança para identificar os fatores que estão relacionados aos custos de um ciberataque e sua magnitude [Franco et al. 2024a]. Foi observado que o país, setor e o tamanho da organização estão diretamente relacionados aos custos de um ciberincidente. Fatores técnicos relevantes nos custos de um ciberataque também incluem o acesso remoto de funcionários, a utilização de computação em nuvem e a ausência de medidas de proteção básicas (por exemplo, antivírus, firewalls e autenticação multifator). A Figura 1.5 apresenta uma análise de cada fator e o seu impacto na variação dos custos de ciberataques. Por exemplo, organizações de um *País* específico podem reportar impactos financeiros até 100% maiores do que a média, enquanto organizações de outros países podem reportar impactos

75% menores que a média.

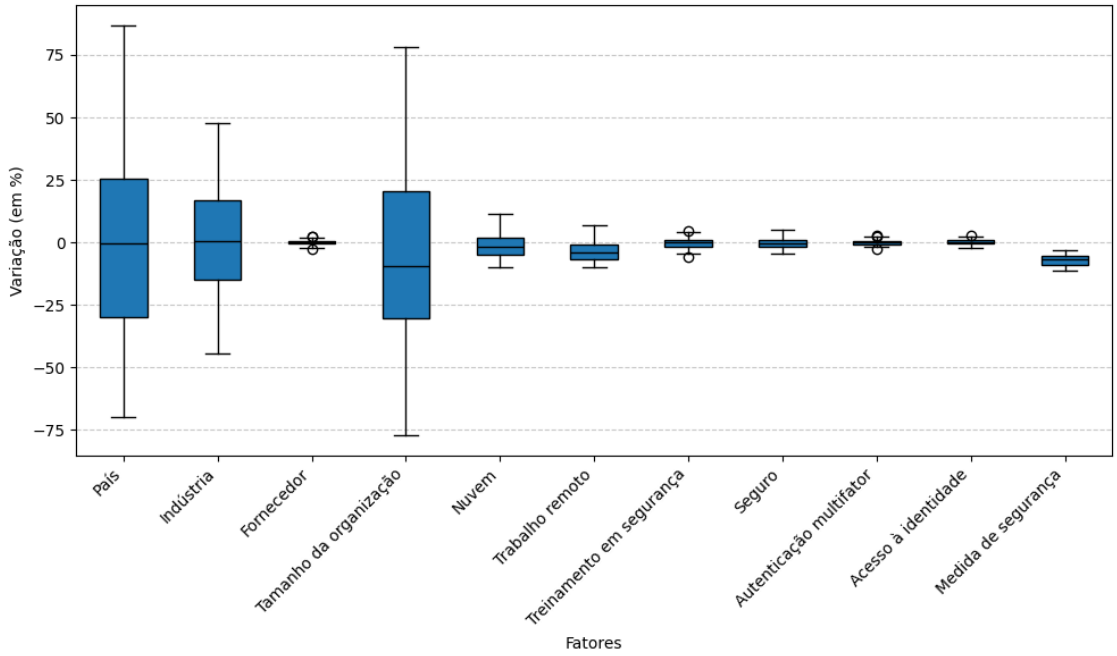


Figura 1.5. Distribuição de Variação de Impactos por Fatores

1.4.1. Ameaças e Impactos de Ciberataques no Setor da Saúde

De acordo com a Organização das Nações Unidas (ONU) e a Organização Mundial da Saúde (OMS), a quantidade de ciberataques no setor da saúde é uma ameaça global que não pode ser ignorada [Mishra 2024]. Relatórios de 2025 mostram que mais de dois terços das instituições de saúde entrevistadas sofreram ao menos um ataque de ransomware nos últimos anos [Arctic Wolf Labs 2025]. É possível observar o crescimento do interesse de cibercriminosos pelo setor da saúde, resultando em um aumento de ciberataques e colocando o setor como o segundo em número de ciberataques reportados [CheckPoint 2025]. Tal movimento vai também de encontro à falsa ideia de que cibercriminosos evitam o setor por questões éticas. Na verdade, a maior motivação de ciberataques ainda é econômica, tendo como alvo setores que possuem a maior quantidade de sistemas e informações críticas, o que significa uma maior propensão a obter lucros com o ciberataque.

O mercado de cibersegurança na área da saúde poderá atingir US$ 125 bilhões entre 2020 e 2025 [Cybersecurity Ventures, Herjavec Group 2021]. Esse crescimento é impulsionado pelo aumento acelerado dos ataques cibernéticos no setor, intensificados pela pandemia de COVID-19, iniciada no começo de 2020. A crise sanitária global desencadeou uma corrida não apenas pelo desenvolvimento de tratamentos, mas também por tecnologias de monitoramento de contato com infectados [Franco et al. 2021]. Como consequência, o setor de saúde tornou-se um dos principais alvos de criminosos cibernéticos como nunca antes na história. Por exemplo, de acordo com o relatório da Cybersecurity Ventures, 62% dos administradores hospitalares entrevistados se sentem inadequadamente preparados para planejar ou reagir a incidentes de cibersegurança que possam afetar suas instituições.

Embora o setor de saúde possua agilidade e interesse na adoção de novas tecnologias, o mesmo não se pode dizer em relação à ações para protegê-las contra ameaças de segurança cibernética. Apesar da reconhecida importância da cibersegurança nessa área, os dados sobre a situação atual são alarmantes. A escassez de profissionais de cibersegurança não é um problema exclusivo da área da saúde, mas, nesse setor, a dimensão do problema é particularmente preocupante diante dos riscos envolvidos. Segundo dados da pesquisa conduzida em [Thyagarajan et al. 2020], três em cada quatro hospitais não contam com um profissional designado especificamente para tratar de questões de cibersegurança.

Em um estudo de 2018 [Fuentes and Huq 2018], é possível observar diversos vetores de ataque em dispositivos médicos, inclusive nos protocolos para Comunicação de Imagens Digitais na Medicina (Digital Imaging and Communications in Medicine, DICOM) e Sistema de Arquivamento e Comunicação de Imagens (Picture Archiving and Communication System, PACS). Ataques simples, ainda hoje, são possíveis de serem executados, ocasionando vazamento de informações relevantes, como informações de pacientes e imagens de exames. Por exemplo, a Figura 1.6 nos mostra o total de 2.204 dispositivos (por exemplo, servidores PACS e equipamentos de imagens), encontrados através de um sistema de busca especializado que mapeia e rastreia dispositivos e sistemas conectados à internet, que estão expostos publicamente na Internet e respondendo a requisições do protocolo DICOM. Ao realizar requisições legítimas para tais dispositivos, podemos, por exemplo, ter acesso a dados pessoais e médicos de pacientes (por exemplo, quais exames foram realizados, data dos exames e até mesmo imagens dos exames). Portanto, ainda que as organizações de saúde invistam recursos significativos na integração de sistemas, os investimentos para manter os softwares atualizados e os sistemas protegidos ainda são insuficientes. Esse problema é agravado pela escassez generalizada de especialistas em cibersegurança, além das dificuldades enfrentadas para manter os poucos profissionais qualificados que existem, cujo custo é elevado e cuja demanda no mercado é intensa [Coventry and Branley 2018, US Health Care Industry Cybersecurity Task Force 2017].

As principais causas das violações de segurança no setor são malwares e as ameaças internas (por exemplo, auxílio de funcionários para campanhas de phishing e pacientes). Dado que malwares (por exemplo, como o ransomware [Neprash et al. 2022] e ataques direcionados a equipamentos médicos [Mirsky et al. 2019]) são recorrentes nesse contexto, o setor tem direcionado investimentos específicos para proteger-se dessas ameaças, especialmente aquelas que afetam dispositivos de IoT, cuja relevância tende a crescer significativamente nos próximos anos, como a utilização de sensores em monitores de sinais vitais, localização e monitoramento de equipamentos, controle de salas de emergência e cuidados ao paciente. Outro ponto importante é o processo de desenvolvimento e de inovação dentro do setor. Por exemplo, em uma análise de vulnerabilidades [Knight 2021] em 30 aplicativos de saúde, foi identificado que 77% possuíam exposição de dados sensíveis e potenciais ataques em suas APIs de comunicação. Esses números mostram que a velocidade de inovação e a necessidade de desenvolvimento de soluções têm sido realizadas sem o cuidado necessário com a cibersegurança desde a sua concepção.

Recentemente, em janeiro de 2025, a União Europeia definiu um plano para reforçar a cibersegurança no setor da saúde, incluindo iniciativas para prevenção, detecção

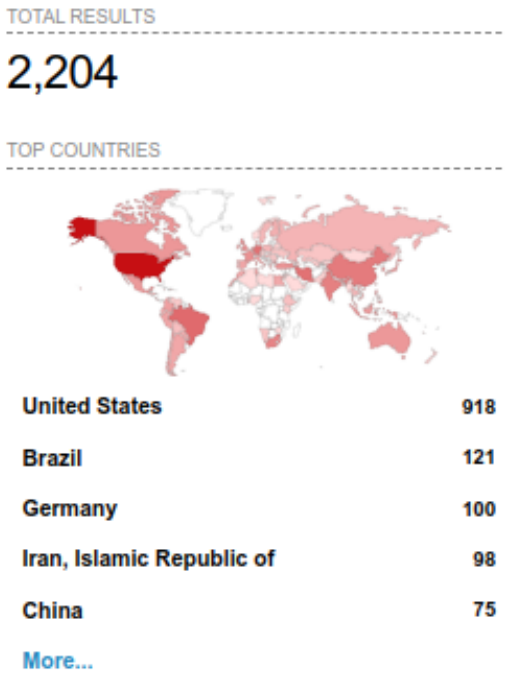


Figura 1.6. Resultado de Busca no Shodan por Dispositivos Expostos na Internet e Respondendo a Requisições DICOM

e resposta às ameaças [European Commission 2024]. Essa é uma ação necessária devido ao crescente aumento de ciberataques no setor. Somente os 27 países membros da União Europeia reportaram, juntos, 309 incidentes de grande magnitude no setor da saúde, resultando em atraso de procedimentos médicos, bloqueios de salas de emergência e disrupção de serviços essenciais para a gestão de serviços hospitalares. No Brasil, a situação ainda é alarmante, com uma grande quantidade de empresas do setor sendo alvos de ransomware e phishing, tornando o setor com a maior quantidade de ataques e com dados valendo até 50 vezes mais que os demais setores no mercado ilegal [Fonseca 2025, IBM Security 2024]. Além disso, legislações como a Lei Geral de Proteção de Dados (LGPD) podem afetar todos os setores com multas de até 2% do faturamento.

Os impactos de ciberataques no setor são extremamente preocupantes, já que envolvem dimensões que afetam diretamente a vida de pessoas, como é o exemplo da primeira morte resultante de um ciberataque, conforme reportado em [Associated Press 2020]. Além disso, existem também os impactos financeiros que causam para as organizações e profissionais que prestam serviços de saúde, o que pode levar até à falência de empresas que prestam serviços essenciais para a sociedade. No restante dessa seção, serão apresentados exemplos de dois casos de ciberataques que ocasionaram impactos sociais e econômicos relevantes no setor da saúde. Tais ciberataques tiveram como foco os dados e também sistemas críticos para a operação das organizações, resultando em interrupção de serviços e vazamentos de dados sensíveis. Embora os cenários apresentados sejam de grande magnitude, é importante que o setor compreenda que diversos ciberataques acontecem no setor, porém, em instituições menores, mas com um alto impacto para suas operações, funcionários e pacientes.

1.4.2. Estudo de Caso #1: Ataque de Ransomware no NHS-UK

Neste cenário, serão analisadas as causas e os impactos de um dos casos mais conhecidos de ciberataques no setor da saúde. O ataque do ransomware WannaCry, ocorrido em maio de 2017 no National Health System (NHS) do Reino Unido (United Kingdom - UK) [National Audit Office 2018] foi um marco em cibersegurança para o setor da saúde, resultando em impactos diretos na saúde de milhares de pacientes no Reino Unido. Discutiremos também boas práticas e o que poderia ter sido feito para evitar o ataque, bem como analisaremos as lições aprendidas, de nível técnico e administrativo, pós-ciberataque [NHS Foundation Trust 2023].

O ransomware conhecido como WannaCry infectou mais de 200 mil dispositivos em cerca de 156 países, tendo como foco a encriptação de arquivos de sistemas, planilhas eletrônicas e documentos importantes para a operação de negócios no mundo todo. Após a encriptação e indisponibilidade de sistemas, um valor em Bitcoin era solicitado como taxa de resgate dos dados. Tal ataque tinha como alvo dispositivos rodando o sistema operacional Microsoft Windows e explorava uma falha de segurança em sistemas de compartilhamento de arquivos para contaminar a maior quantidade de dispositivos possíveis. O NHS-UK, que possuía milhares de sistemas vulneráveis (por exemplo, com Windows XP e 7 sem atualizações recomendadas de segurança) foi alvo do ataque, tendo como resultado a disrupção de serviços de 80 das 236 unidades organizacionais que oferecem serviços de saúde à população (por exemplo, hospitais gerais, especializados ou serviços de ambulância).

Baseado em auditoria realizada [National Audit Office 2018], o ataque infectou e deixou totalmente fora de operação, ao menos, 34 unidades de saúde, enquanto outras 46 unidades reportaram disrupção de serviços devido à falta de recursos oferecidos pelas demais unidades infectadas. Por exemplo, funcionários dos serviços de saúde não puderam acessar dispositivos computacionais, gerando atrasos no processamento de informações de pacientes e nos resultados de exames médicos. Além disso, equipamentos médicos foram bloqueados ou isolados como forma de prevenção ao ciberataque, resultando em disrupção nos serviços de radiologia e análises clínicas que dependem de equipamentos digitais (por exemplo, diagnóstico por imagem e testes de sangue). O cronograma do ataque, baseado no relatório realizado pelo National Audit Office (2018), é apresentado abaixo.

- **12 de maio de 2017 (Início do Incidente):**
  - $\approx$11:00 horas: Primeiras unidades de saúde relatam problemas em sua operação.
  - 13:06 horas: Primeira notificação para as equipes de resposta a incidentes.
  - 16:00 horas: NHS-UK declara o ciberataque um incidente nacional.
  - 18:45 horas: Decisões estratégicas e coordenação para resposta ao incidente.
  - $\approx$22:00 horas: Especialista descobre como interromper (kill switch) o ransomware e consegue parar a propagação do ciberataque.
- **De 13 a 15 de maio de 2017:** Equipes do NHS-UK implementam soluções manuais para manter serviços essenciais ativos. A Microsoft divulga atualizações de segurança imediatas.

- **De 15 a 18 de maio de 2017:** O NHS-UK declara recuperação parcial dos sistemas, mas alerta sobre possíveis novos ataques. Atualizações de segurança são realizadas e proteções adicionais são implementadas (por exemplo, antivírus e atualização de sistemas).
- **19 de maio de 2017 (Fim do Incidente):** O incidente é contido pelo NHS-UK e os sistemas são restaurados.

Ao fim do ciberataque, foi identificado que, ao menos, 1220 equipamentos de diagnóstico foram infectados (≈1% de todos os equipamentos do NHS-UK), além dos computadores das unidades. Milhares de sistemas computacionais não foram infectados devido ao isolamento, o que evitou a propagação do ransomware, mas também ocasionou a interrupção dos serviços. Ao menos cinco hospitais necessitaram redirecionar todos os serviços de emergência e ambulância para outros hospitais, incluindo hospitais de referência como o Royal London Hospital e o Lister Hospital.

Os impactos do ciberataque podem ser divididos entre impactos aos pacientes e custos financeiros. A Tabela 1.1 apresenta um resumo dos principais impactos identificados e mensurados. Em relação aos pacientes, o ciberataque resultou em 6.912 consultas canceladas diretamente no período em que o NHS-UK estava enfrentando o ciberataque (ou seja, de 12 a 19 de maio de 2017). Tal número não inclui os impactos em consultas agendadas para o pós-incidente, o que pode chegar a cerca de 19.494 consultas canceladas. O NHS-UK reportou que, ao menos, 139 pacientes necessitando de diagnósticos urgentes em relação a câncer tiveram exames cancelados. Cirurgias e demais operações após o incidente foram afetadas, porém os números exatos não foram mensurados e reportados pelo NHS-UK. Em relação ao impacto financeiro, o NHS-UK não realizou estudos mais profundos em relação à redução de atendimentos no período do ataque. Porém, pesquisadores estimaram em torno de £ 5.9 milhões o impacto financeiro ao analisarem a redução das atividades durante o período [Ghafur et al. 2019]. Análises anteriores estimaram que o ataque WannaCry causou um prejuízo de £ 92 milhões ao NHS-UK, com base na suposição de que o ataque afetou 1% de todos os serviços do NHS, incluindo os cuidados primários (como os atendimentos em consultórios de médicos de família) [The Telegraph 2018]. No entanto, dados sobre cuidados primários não foram coletados na época. A pesquisa realizada, portanto, focou apenas nos cuidados secundários (hospitalares), utilizando mudanças reais observadas nas atividades.

As lições aprendidas com o ciberataque geraram diferentes reflexões e ações para embasar novas estratégias de cibersegurança e também ações diretas para evitar ciberataques futuros [Smart 2018, National Audit Office 2018]. Ficou claro para o NHS-UK e para o setor da saúde que a questão não é `se` mas sim `quando` o próximo ciberataque irá acontecer. Portanto, os principais desafios incluem estar preparado e capaz de responder rapidamente em caso de incidente. Como primeira lição, ficou evidente a necessidade de desenvolver um plano de resposta em caso de ciberataques, bem como definir papéis e responsabilidades em nível local e nacional dentro do NHS-UK. Além disso, é necessário garantir que todas as organizações processem e implementem alertas de cibersegurança, incluindo atualização de software para correção de vulnerabilidades e antivírus atualizados.

Porém, sem que organizações, líderes e equipes tratem ameaças digitais como um problema real, não será possível mitigar riscos de forma eficaz. Assim, é importante que

Tabela 1.1. Resumo e Principais Impactos em Pacientes e Econômicos do Ciberataque de Ransomware no NHS-UK

Tipo	Quantidade	Descrição
Equipamentos de diagnósticos infectados	1229 equipamentos	Atraso em exames e atendimentos
Unidades organizacionais de saúde afetadas	80 unidades (24.000 funcionários)	Impacto direto nos serviços de rotina e de urgência em diversas regiões do país
Consultas canceladas	6.912 consultas (19.494 pós-ciberataque)	Impossibilidade de realizar consultas por falta de acesso aos sistemas de agenda, exames e informações de pacientes
Diagnósticos urgentes afetados	139 pessoas	Pacientes em investigação de neoplasia foram diretamente afetados pela interrupção de serviços de patologia clínica e exames de imagem
Perda financeira devido a redução das atividades	£ 5.9 milhões	Redução na entrada de novos pacientes e nos atendimentos, bem como cancelamento de pacientes agendados
Impacto financeiro total estimado	£ 92 milhões	Custos relacionados ao impacto direto devido a redução das atividades, custos de TI e investimentos em infraestrutura adicional

os diferentes atores envolvidos no setor da saúde (por exemplo, políticos, gestores e os profissionais que lidam diretamente com pacientes) estejam cientes de riscos diretos aos serviços críticos e trabalhem proativamente para maximizar a resiliência da infraestrutura e minimizar o impacto ao cuidado aos pacientes. Por fim, todas as unidades organizacionais foram comunicadas para resolver e implementar todos os alertas de cibersegurança emitidos pelo NHS Digital entre março e maio de 2017. Também foram tomadas ações para garantir a proteção local através de firewalls.

Como consequência do ciberataque, houve uma priorização do orçamento de TI para aprimorar a cibersegurança nos principais centros traumatológicos e melhorias no sistema de alertas de segurança[1], além de uma lista com 21 recomendações de autoria da chefia do Departamento de Saúde e Assistência Social do UK [Smart 2018]. Desde então, diversos novos ciberataques aconteceram ao NHS-UK, e também ao redor do mundo, incluindo um recente vazamento de dados de pacientes e exames realizados em um laboratório de patologia que processa exames de sangue em nome de várias organizações do NHS[2].

1.4.3. Estudo de Caso #2: Vazamento de Dados no SUS

Em 2019, um atacante afirmou possuir dados de identificação de 205 milhões de usuários do Cartão Nacional de Saúde (CADSUS), incluindo nome, nome da mãe, endereço, CPF

[1]https://digital.nhs.uk/cyber-alerts

[2]https://www.england.nhs.uk/synnovis-cyber-incident/

e data de nascimento. Como prova, foram vazados 2 milhões dos dados em um website chamado *www.leaksus.com.br*. A Figura 1.7 apresenta um screenshot do website, que foi retirado do ar após alguns dias. O vazamento de dados ocorreu através de uma falha em uma API disponibilizada para consulta de dados de um usuário através do seu número do cartão SUS e senha. Porém, após realizar uma requisição legítima (ou seja, com um número de cartão e senha de um usuário real), foi possível realizar milhões de solicitações apenas alterando o número do CPF na chamada para a API. Por exemplo, a chamada *"consulta.php?cpf=xxx.xxx.xxx.xx"* retornaria todos os dados do CPF *xxx.xxx.xxx.xx* e poderia ser feita para qualquer CPF após realizar uma primeira consulta legítima. Tal vazamento ocorreu, portanto, não devido a um ciberataque sofisticado, mas sim como resultado de uma falha de implementação do sistema, conforme discutido na Seção 1.4.1 e reforçado por estudos sobre a segurança no desenvolvimento de aplicações para o setor da saúde [Knight 2021].

Figura 1.7. Website Criado em 2019 para Compartilhar Informações Vazadas do SUS devido a Exposição de API

Cerca de um ano após o vazamento devido à exposição de API, ocorreu um fato ainda mais curioso de exposição de dados. Informações sensíveis (por exemplo, CPF, endereço, telefone e doenças pré-existentes) de cerca de 16 milhões de pacientes ficaram expostas devido à exposição de senhas de usuários do Ministério da Saúde que possuíam acesso a tais informações. O vazamento das senhas aconteceu por erro humano e demorou cerca de 1 mês para a identificação da falha. De acordo com o levantamento do Jornal O Estadão de São Paulo [Cambricoli 2020], uma planilha com as senhas foi compartilhada no Github, uma plataforma para compartilhamento de códigos e trabalho colaborativo [3], juntamente com o código de um modelo estatístico sendo desenvolvido em uma parceria

[3]https://www.github.com

do Hospital Albert Einstein e o Ministério da Saúde; porém, o responsável pelo desenvolvimento não removeu o arquivo com as senhas do repositório público. Com as senhas publicadas, era possível acessar registros relacionados à COVID-19, incluindo casos suspeitos e internações por síndrome respiratória aguda grave. Tal falha mostra a importância da proteção de dados e também de políticas bem definidas para o gerenciamento de informações sensíveis em projetos na área da saúde [Todde et al. 2020].

Segundo o painel de Registro de Incidentes com Dados Pessoais [4], mantido como forma de conformidade com a LGPD, o Ministério da Saúde registrou três incidentes relatados desde a vigência da lei. O primeiro incidente relata o vazamento de credenciais do sistema CADSUS, que expôs dados demográficos e sensíveis de usuários, durante o período de abril de 2019 até junho de 2022. Também existe um incidente, em 2022, de venda ilegal de bases de dados administrativas vindas dos sistemas de saúde. Por fim, foi reportado o incidente referente a falha de API discutida anteriormente nesta seção, sendo comunicado o incidente aos titulares dos dados. Como lições aprendidas, foram adotadas estratégias de segurança adicionais, como autenticação multifator e a troca de senha a cada três meses como política obrigatória. Além disso, foi realizada verificação de vulnerabilidades utilizando ferramentas comerciais e teste de penetração. Os incidentes também foram comunicados às autoridades, como a Polícia Federal e a Secretaria de Governo Digital do Ministério da Economia.

Embora ações tenham sido tomadas em relação aos vazamentos, não é possível remover os dados já expostos de bases ilegais. Portanto, mesmo que informações como senhas e número de usuários possam ser alterados, os dados pessoais e sensíveis vazados continuam a ser válidos, afetando a vida de milhões de brasileiros e podendo resultar em discriminações, crimes financeiros ou mesmo exposição e chantagem. É importante adotar medidas de notificação aos titulares dos dados, como recomendado pela Autoridade Nacional de Proteção de Dados, mas também é fundamental que as organizações adotem medidas que evitem os vazamentos e não apenas medidas para remediar um incidente.

Diferentemente de impactos apenas técnicos ou econômicos, os vazamentos de dados podem ter um impacto contínuo e impossível de mensurar nas vidas das pessoas durante anos. Além disso, tais dados podem (e são) utilizados para fomentar o cibercrime, com campanhas de phishing cada vez mais eficientes, já que possuem dados que validam diversos cenários para induzirem usuários ao erro. Por exemplo, imagine um cenário onde um médico de um hospital próximo à sua residência entre em contato e solicite que você acesse um link para verificar possíveis tratamentos de uma doença crônica que você possui. Se os dados estiverem corretos, a chance de você clicar será aumentada. Essa ação pode resultar em potenciais riscos para a sua segurança cibernética e da empresa onde você trabalha. Tal cenário também pode acontecer de forma contrária: alguém entrando em contato com o hospital ou profissionais da saúde. Portanto, esse cenário analisado mostra a importância de estratégias de cibersegurança que auxiliem na proteção de dados sensíveis e, principalmente, na prevenção de vazamentos, incluindo possíveis falhas em aplicações, dispositivos móveis, sensores e sistemas de comunicação que são amplamente utilizados no setor da saúde para trazer inovação tecnológica e melhor acesso ao tratamento de pacientes.

[4]https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais

1.5. Planejamento em Cibersegurança: Análise, Priorização de Riscos e Investimentos

O planejamento e o investimento em cibersegurança devem ser encarados como componentes estratégicos essenciais à sustentabilidade operacional e econômica de organizações, independentemente do setor de atuação [Franco et al. 2023b]. À medida que as ameaças digitais se tornam mais sofisticadas e frequentes, torna-se indispensável adotar abordagens proativas de análise e gestão de riscos (sejam eles técnicos, econômicos, legais ou sociais), alinhadas às necessidades de proteção de ativos críticos, conformidade regulatória e resiliência cibernética. Essa necessidade é ainda mais pronunciada em setores que lidam com dados sensíveis ou operam serviços críticos à sociedade. A saúde, nesse contexto, destaca-se como uma área particularmente desafiadora [Thyagarajan et al. 2020], tanto pela criticidade das informações e sistemas envolvidos quanto pela complexidade de seus ambientes tecnológicos em constante evolução [Levina et al. 2022]. Assim, embora os fundamentos do planejamento em cibersegurança sejam aplicáveis de forma transversal, sua aplicação na área da saúde exige atenção adicional devido à sua importância para a sociedade, complexidade operacional e valor para cibercriminosos.

O planejamento de estratégias de cibersegurança no setor da saúde demanda uma abordagem com atenção em certos pontos, em virtude da natureza sensível dos dados tratados, da alta dependência tecnológica das atividades clínicas e das rígidas exigências impostas por marcos regulatórios. Dados clínicos, como prontuários eletrônicos, laudos diagnósticos e registros históricos de pacientes, são considerados informações pessoais sensíveis e, por isso, estão sujeitos a normativas como a LGPD, HIPAA e GDPR. Tais normativas impõem a implementação de mecanismos robustos de controle de acesso, rastreabilidade, governança e gestão do consentimento [Aragão and Schiocchet 2020]. Além disso, devido à sua importância e valor no mercado ilegal, tais dados têm sido alvo de ciberataques nos últimos anos [IBM Security 2024]. Portanto, devido à natureza crítica dos serviços oferecidos, é indispensável a elaboração de estratégias que garantam a resiliência de serviços críticos e sejam capazes de garantir a disponibilidade ininterrupta dos sistemas e resposta eficaz frente a incidentes, como ataques de ransomware e negação de serviço. O ambiente hospitalar, por exemplo, apresenta uma heterogeneidade tecnológica marcada pela convivência de sistemas legados, dispositivos médicos conectados e infraestruturas críticas de TI, muitas vezes sem atualizações regulares ou com vulnerabilidades conhecidas.

A avaliação de riscos e impactos nesse contexto deve considerar a singularidade de cada ativo digital e sua interdependência com processos clínicos, a fim de mitigar possíveis vetores de ataque. Além disso, o engajamento de profissionais da saúde no uso seguro das tecnologias exige a formulação de políticas e uma cultura organizacional alinhadas aos serviços de saúde que são a atividade principal, mas também que reduzam os riscos e potenciais vetores de ataques. Assim, a evolução constante das ameaças digitais, aliada às demandas por conformidade regulatória, auditorias e certificações institucionais, reforça a necessidade de um planejamento estratégico que integre dimensões técnicas, regulatórias, humanas e econômicas de forma coordenada. Tais esforços incluem, por exemplo, desde o treinamento em cibersegurança para evitar ciberataques com foco nos profissionais e usuários até a implementação de proteções robustas para mitigar os riscos em sistemas e dados críticos. Discutiremos como construir estratégias eficientes ao longo

desta seção, reforçando as nuances de setores como o da saúde frente a setores menos críticos.

1.5.1. Metodologia para Planejamento

A metodologia proposta em [Franco et al. 2023b] compreende cinco etapas que representam as tarefas sequenciais que os tomadores de decisão devem considerar ao planejar uma nova estratégia de segurança cibernética (ou atualizar uma estratégia já existente) [Franco et al. 2022]. A Figura 1.8 mostra a metodologia, incluindo todas as fases (de A a E) e exemplos de etapas críticas que devem ser executadas em cada uma dessas fases. Essa metodologia foi definida com base em uma análise aprofundada da literatura, em entrevistas com especialistas em segurança cibernética e tomadores de decisão do setor, das pequenas e médias empresas e do meio acadêmico, e com base em todo o conhecimento obtido e nas discussões realizadas pelo autor. É importante mencionar que as etapas destacadas para cada etapa são exemplos de etapas gerais comuns à maioria das empresas, mas não são exaustivas. A metodologia pode ser ampliada e adaptada para atender às demandas específicas de uma determinada empresa ou setor. Também, é fundamental observar que existem etapas que devem ser consideradas com maior cautela quando se considera a cibersegurança em setores críticos, como é o caso do setor da saúde.

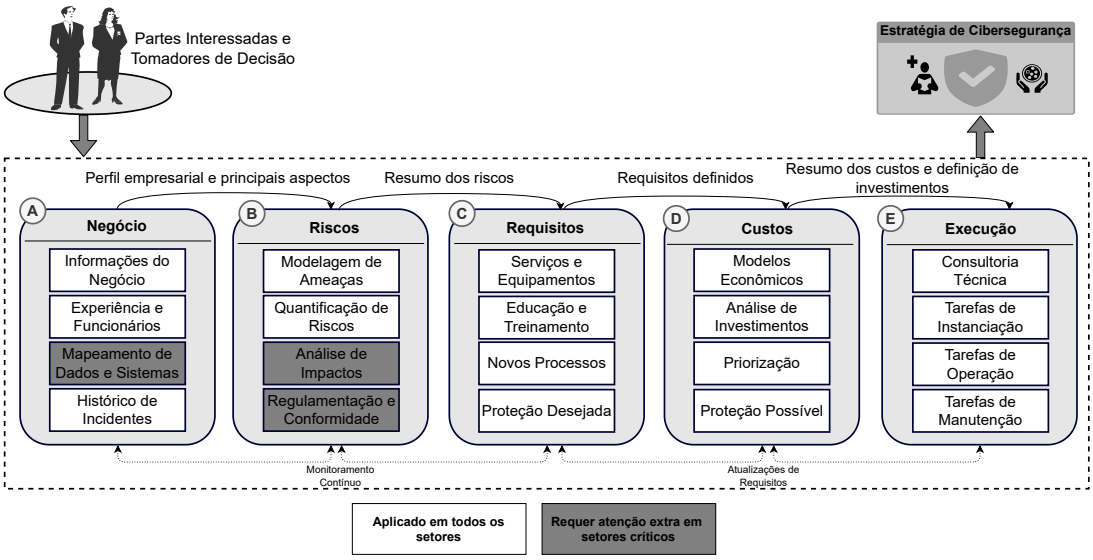


Figura 1.8. Etapas para Planejamento de Estratégias de Cibersegurança

O planejamento começa na **Etapa A** (ou seja, Negócio), na qual todas as informações relacionadas ao negócio devem ser coletadas e um briefing deve ser conduzido, considerando todas as partes interessadas envolvidas. Exemplos de partes interessadas no setor da saúde incluem a direção executiva e o conselho de hospitais e clínicas, profissionais de saúde, órgãos reguladores e governamentais, equipes de segurança da informação e os próprios pacientes. Para essa fase, as informações sobre o negócio são fundamentais, como a atuação da empresa, as tecnologias utilizadas, o número de funcionários, a receita e o portfólio. No caso da saúde, é essencial compreender os serviços fornecidos e sua criticidade.

Em seguida, a experiência do pessoal é um indicador importante para entender os possíveis desafios ou pontos fracos técnicos a serem considerados durante o planejamento de uma estratégia de segurança cibernética. Se a organização não possuir um elevado nível de conscientização sobre segurança cibernética, poderá tornar-se um vetor para diversos tipos de ataque (por exemplo, phishing e ransomware). Profissionais da saúde sem treinamento básico em cibersegurança, por exemplo, que tenham acesso a sistemas ou informações sensíveis, podem representar um elo fraco durante um ciberataque.

Além disso, o mapeamento de dados e sistemas é um aspecto que requer atenção especial no setor da saúde. Devido à necessidade de gerenciar dados sensíveis de pacientes, bem como ao uso da tecnologia como meio para cuidar da saúde, é fundamental mapear e compreender como cada dado e sistema está interconectado e configurado. Essa atividade, aliada à análise do histórico de incidentes anteriores, contribuirá para a avaliação de riscos e dos possíveis impactos decorrentes de ciberataques.

Na **Etapa B** (ou seja, Riscos), o foco é a análise de segurança e a modelagem de ameaças da organização. Para isso, podem ser consideradas ferramentas e soluções voltadas à avaliação de riscos, incluindo plataformas consolidadas no mercado E utilizadas para analisar dados relevantes à segurança e realizar testes de penetração (por exemplo, Nmap, Metasploit e Shodan). Além disso, durante essa fase, a modelagem de ameaças pode ser conduzida utilizando abordagens específicas, como a modelagem de ameaças utilizando STRIDE [Microsoft 2022] e a estrutura MITRE ATT&CK[5] para mapeamento de técnicas utilizadas por ciberataques. Um exemplo de mapeamento utilizando as metodologias STRIDE e DREAD [EC-Councl 2022] no setor da saúde está disponível em [Fuentes and Huq 2018], juntamente com uma análise dos principais sistemas médicos expostos. A análise de impactos também é uma etapa altamente relevante, especialmente em setores críticos. No caso do setor da saúde, além dos impactos técnicos e econômicos, há uma relação direta com a vida dos pacientes e com o bem-estar social. Além disso, devem ser consideradas as regulamentações e boas práticas específicas. Portanto, nessa etapa, é necessário realizar uma análise detalhada para compreender os riscos e os impactos de um ataque de forma individualizada, incluindo análises específicas para sistemas e dados sensíveis. Por exemplo, um DDoS em uma infraestrutura de cirurgia remota tem um impacto crítico, enquanto um ataque de ransomware em um sistema de pagamentos de uma clínica representa um impacto econômico relevante. Compreender tais riscos e impactos é essencial para, então, planejar estratégias eficazes de mitigação.

Já na **Etapa C** deve ser utilizado todo o conhecimento adquirido nas etapas anteriores para decidir quais requisitos de proteções são necessários. Por exemplo, caso, baseado na análise do negócio, riscos e impactos associados, tenha sido definido que ataques de phishing possuem alto risco de acontecer no corpo clínico de um hospital com o objetivo de propagar malwares ou acessar sistemas com informações sensíveis, é importante investir em treinamento para que os profissionais não sejam afetados. Além disso, proteções de endpoint (por exemplo, clientes de e-mails e estações de trabalho) podem ser contratadas para mitigar os riscos. Portanto, é nessa etapa que serão definidas quais proteções, treinamentos e novos processos podem ser implementados para mitigar os riscos e os impactos no contexto do negócio.

[5]https://attack.mitre.org/

Após a definição dos requisitos, na **Etapa D**, serão considerados os custos reais para implantação e operação das proteções e a definição ou ajuste do orçamento existente. Nessa etapa temos um dos principais desafios da cibersegurança: o baixo orçamento e os custos elevados das soluções. Considerando tal desafio, podemos utilizar modelos econômicos para a cibersegurança [L. A. Gordon, M. P. Loeb, L. Zhou 2021] que auxiliem na definição do orçamento e também na análise dos investimentos, seja de modo a otimizar o investimento ou fornecer fatos mensuráveis para angariar fundos adicionais para a cibersegurança junto à gestão (por exemplo, caso não seja investido X, podemos perder até 10 vezes o valor de X em um ano). Após a definição do orçamento, é necessário definir as prioridades (ou seja, reduzir os riscos de situações que possuam maior impacto) e, então, selecionar as proteções possíveis de serem implementadas dentro do orçamento e que sejam condizentes com o nível de cibersegurança almejado. Por fim, na **Etapa E**, a estratégia de cibersegurança definida será implementada e operada conforme especificada. Lembrando que toda estratégia deve ser testada, monitorada e atualizada com uma frequência apropriada (também definida baseado na análise do setor e ativos), já que os riscos e possíveis impactos são dinâmicos.

Para priorização, podemos utilizar desde métricas técnicas como o Exploit Prediction Scoring System (EPSS) [Jacobs et al. 2021], que auxilia na compreensão de quais vulnerabilidades possuem maior probabilidade de serem exploradas, ou abordagens que permitam a análise dos possíveis impactos financeiros, sociais e legais em caso de um ciberataque. Tais abordagens podem ser específicas para o setor da saúde ou adaptações de abordagens generalistas, mas levando em consideração a realidade de cada setor.

1.5.2. Quantificação e Priorização de Riscos

Ao realizar a análise de riscos, é importante quantificar os riscos de forma mensurável (por exemplo, compreender os reais riscos e seus impactos) de forma a possuir as informações necessárias para uma priorização baseada nos riscos, impactos e orçamento disponível. No entanto, essa quantificação é desafiadora, pois exige conhecimento profundo sob perspectivas técnica, econômica e jurídica em relação a uma empresa e ao cenário de ameaças existente [Franco et al. 2024b]. Além disso, em setores críticos como o da saúde, tal quantificação envolve também os impactos na sociedade e na vida humana. Portanto, as abordagens para quantificação de riscos e impactos devem lidar com esses desafios e encontrar maneiras eficazes de contornar as limitações existentes, incluindo a capacidade de lidar com *(i)* assimetria de informações entre as empresas, *(ii)* falta de comunicação entre os níveis de diretoria e *(iii)* falta de mapeamento quantitativo entre as ameaças e seus impactos reais.

Para a quantificação de riscos podemos utilizar modelos e simulações, como por exemplo o proposto em [Franco et al. 2024a] e [Nunes et al. 2024]. Ambos modelos utilizam dados estatísticos disponíveis em relatórios públicos de empresas de consultoria em cibersegurança para simular e prever possíveis riscos de ataques acontecerem e também seus impactos econômicos. Para isso, são utilizadas informações como o setor, tipo de ataque, localização geográfica e informações específicas dos serviços oferecidos. Esse tipo de abordagem permite reduzir a assimetria de informações e compreender quais riscos devem ser observados com maior atenção.

Por exemplo, uma clínica de exames médicos com sede no Brasil e uma filial na Alemanha deve ter em mente os principais ciberataques e riscos que têm como foco o setor da saúde (por exemplo, phishing, ransomware e vazamentos de dados). Além dos riscos dos sistemas específicos, precisamos estar atentos a informações estatísticas de forma global para encontrarmos um planejamento local eficiente. Por exemplo, o Brasil possui uma das maiores quantidades de ataques de phishing e a Alemanha possui impactos econômicos de ciberataques 4% acima do que a média global. Além disso, o impacto de vazamento de dados no Brasil é de ≈R$ 8 e na Alemanha é de ≈R$ 30 por cada registro vazado. Esse valor é uma média obtida por estudos realizados em 2024 [IBM Security 2024]. Porém, no setor da saúde, esses valores podem ser muito maiores, chegando a uma média global de ≈R$ 50. Apenas com essas informações, já seria possível compreender e quantificar alguns riscos e impactos que podem auxiliar na priorização.

Além disso, métricas técnicas podem ser utilizadas para compreender quais ciberataques e vulnerabilidades possuem a maior probabilidade de acontecer no mundo real. O EPSS, por exemplo, estima a probabilidade de que uma vulnerabilidade seja explorada na prática nos próximos 30 dias. Ele combina dados públicos, como Common Vulnerabilities and Exposures (CVE)[6] e histórico de exploração, para ajudar organizações a priorizarem a correção de falhas com maior risco real. Imagina que a clínica de exames mencionada acima possui diferentes sistemas com possíveis impactos técnicos, econômicos, legais e sociais em caso de um ciberincidente. É importante mapear os riscos de ciberataques específicos em cada sistema, além dos impactos para cada ciberataque em cada sistema. Na Tabela 1.2 é apresentada uma análise inicial dos principais sistemas da clínica e as vulnerabilidades encontradas. Para isso, foi utilizada a métrica EPSS para definir a probabilidade de uma vulnerabilidade (ou seja, CVE) ser explorada. Com essa informação, podemos definir o risco de cada vulnerabilidade para o sistema. Porém, além do risco de uma vulnerabilidade acontecer, precisamos correlacionar também com os impactos. Por exemplo, uma vulnerabilidade com alto risco de ser explorada, mas com um impacto baixo não deveria possuir uma prioridade alta.

Vulnerabilidade	**Sistema Impactado**	**EPSS**	**Probabilidade**
CVE-2025-Exemplo	Portal de Agendamento de Consultas	85%	Alto
CVE-2022-Exemplo	Servidor com Dados de Pacientes e Exames (PACS/RIS)	15%	Baixo
CVE-2023-Exemplo	Servidor de Laudos e Impressão de Exames	65%	Alto
CVE-2024-Exemplo	Portal Web da Clínica	5%	Baixo
CVE-2021-Exemplo	Página de Agendamento e Tabela de Exames	30%	Médio

Tabela 1.2. Exemplos de Vulnerabilidades e Riscos Mapeados para os Sistemas da Clínica de Exames

Ao analisar a Tabela 1.2, observamos que o Servidor com Dados de Pacientes e Exames (PACS/RIS) foi definido como risco Baixo, pois possui um EPSS de 15% (ou seja, possui 15% de chance de a vulnerabilidade ser explorada nos próximos 30 dias).

[6]https://www.cve.org/

Porém, como o servidor é um sistema crítico para a clínica, deveríamos alterar a prioridade para Alto, baseada nos possíveis impactos em caso de um incidente, enquanto a Página de Agendamento e Tabela de Exames poderiam ser alteradas para uma prioridade Baixa, por exemplo, já que o risco é Moderado, mas o impacto será Baixo nos sistemas e informações críticas da clínica. É possível usar outras métricas técnicas para compreender a gravidade dos riscos, porém, é fundamental ter em mente o contexto do setor e do negócio. No caso da saúde, por exemplo, precisamos priorizar a vida e também reduzir os possíveis impactos econômicos no negócio que podem surgir com falhas técnicas e questões de conformidade regulatória ou jurídicas.

Ao utilizar modelos econômicos, simulações e métricas técnicas disponíveis na indústria e academia, podemos priorizar a correção de problemas e a proteção de sistemas e informações críticas de forma a otimizar o planejamento e investimento em cibersegurança. Porém, tal tarefa não é simples, já que cada abordagem exige conhecimento técnico e possui diferentes curvas de aprendizagem. Tal fato é ainda mais crítico para setores que possuem usuários e profissionais com pouca experiência em TI, além de poucos profissionais dedicados à cibersegurança, como o caso do setor da saúde. Para isso, existem esforços para propor ferramentas que auxiliem no processo de compreensão dos riscos e aplicação automatizada de modelos, simulações e técnicas para quantificação de impactos e otimização de investimentos em cibersegurança. No resto desta seção, será conduzido um caso de estudo para o setor da saúde, permitindo assim o planejamento de uma estratégia de cibersegurança seguindo as etapas definidas ao longo da seção.

1.5.3. Caso de Estudo

Inicialmente, seguindo a abordagem definida na Figura 1.8, devemos compreender o negócio. Portanto, suponha um Laboratório de Análises Clínicas (LAC) situado no Brasil, com 50 funcionários e que atue diretamente como prestador de serviços para clientes privados e hospitais. O LAC possui cerca de 10% de seus funcionários atuando remotamente e com experiência básica na operação de TI. Além disso, embora o LAC não tenha sofrido nenhum ciberataque no último ano, alguns de seus funcionários já foram vítimas de ataques de phishing executados com sucesso.

Os sistemas disponíveis no LAC incluem um servidor de banco de dados para armazenamento de informações, exames e procedimentos de rotina, além de uma página web para agendamento de exames. Como o LAC já segmenta suas atividades, iremos focar apenas nesses dois ativos apenas, sem considerar os equipamentos médicos e de exames que estão sob cuidados de outro setor da empresa. A Figura 1.9 apresenta uma visão geral das proteções já implementadas na empresa.

Na segunda etapa, é necessária a modelagem das ameaças e a quantificação de riscos. Primeiramente, precisamos compreender os riscos inerentes ao cenário onde a empresa está situada e, então, conduzir a análise de riscos. Para isso, podemos utilizar histórico de incidentes no setor e em parceiros. Ao verificar os relatórios oferecidos pela plataforma *IMPACTO* (ver Figura 1.10), que foi desenvolvida no contexto do programa Hackers do Bem[7] para capacitação e planejamento em cibersegurança [8], verificamos que o setor da saúde possui uma alta taxa de phishing e também possui uma tendência de ataques

[7]https://hackersdobem.org.br

[8]https://www.inf.ufrgs.br/gt-impacto/

Figura 1.9. Proteções Implementadas de Forma Geral pelo LAC

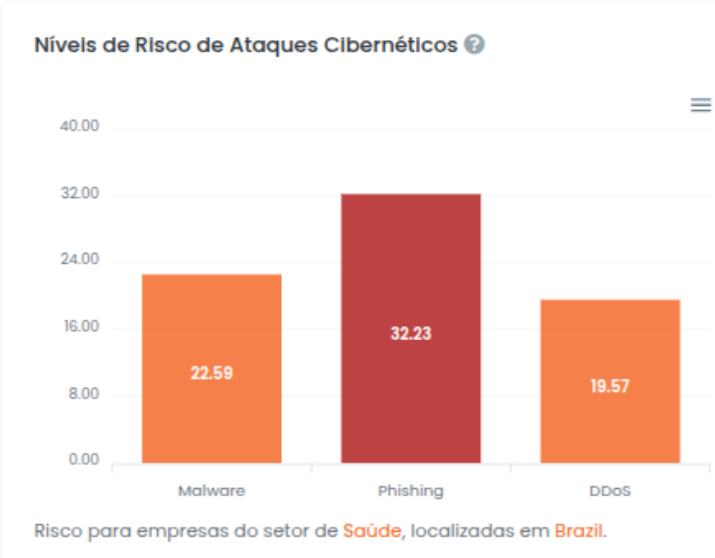


Figura 1.10. Exemplo de Média de Ataques no Setor da Saúde e no Brasil Conforme Relatórios Publicamente Disponíveis

de malware. Tais dados confirmam que precisamos ter uma estratégia clara para evitar problemas de malwares específicos (por exemplo, ransomware) e que possuem ataques de phishing como parte sua estratégia de propagação. Como diversos funcionários da empresa já foram vítimas de ataques de phishing com sucesso no passado, isso também

reforça a necessidade de proteção contra phishing. Por fim, observamos também uma incidência razoável de DDoS no setor, principalmente em empresas de saúde localizadas no Brasil.

Tais ameaças possuem impactos diretos nos ativos. Por exemplo, ataques de phishing e ransomware podem ser utilizados para tornar indisponíveis os sistemas de banco de dados e também utilizados como forma de vazamento de dados e extorsão. Já ataques de DDoS podem tornar inacessível o portal de agendamento de exames e consulta de resultados. Os possíveis impactos de cada ataque nos ativos são apresentados na Tabela 1.3.

Tabela 1.3. Exemplo de Mapeamento de Impactos e Ataques por Ativo

Impacto	Ativo	Ataque(s)	Descrição
Médio	Portal de Agendamentos	DDoS, Ransomware	Faturamento de R$ 200 mil por mês, disrupção do negócio afeta diretamente os agendamentos, perda de reputação
Alto	Banco de Dados	Ransomware	Disrupção do negócio, Multas por vazamento de dados, perda de reputação e extorsão
Alto	Funcionários e Clientes	Phishing	Roubo de credenciais e Acesso a sistemas e informações sensíveis, perda de reputação, inicio de outros ataques, como, por exemplo, o ransomware

Podemos quantificar os riscos econômicos utilizando estratégias de, por exemplo, verificar o quanto um ativo pode afetar os ganhos de uma empresa caso fique inacessível ou mesmo consultar relatórios que apresentam a média de perda financeira por cada dado vazado. Já os riscos aos pacientes e procedimentos precisam ser investigados com cautela, já que envolvem vidas e o apetite para risco não deve existir. Devemos também considerar nessa etapa demandas específicas da LGPD e do HIPAA, para garantir que não existem requisitos específicos não cumpridos. Nesse caso, identificamos que nem todo dado em trânsito está sendo criptografado, permitindo que ataques acessem dados de exames em alguns cenários, o que viola boas práticas.

Para identificar a real exposição aos riscos, é possível utilizar ferramentas para escanear a rede e sistemas, como o Nmap ou mesmo ferramentas pagas como o Nessus Tenable. Tais ferramentas auxiliam a mapear os ativos expostos e também possíveis vulnerabilidades que podem ser exploradas por atacantes. Além disso, métricas como o EPSS (ver Seção 1.5.2) auxiliam na identificação de quais vulnerabilidades são mais prováveis de serem exploradas e quais devem ser priorizadas.

Ao identificar os impactos e riscos, podemos definir quais proteções deverão ser priorizadas, levando em consideração aspectos técnicos (efetividade das proteções) e também econômicos (custos e orçamento disponível). Para definir o orçamento ideal, utilizaremos o modelo de Gordon-Loeb [Gordon et al. 2016], que pode ser utilizado como um benchmark para definir o investimento ótimo em cibersegurança. Ao adicionar os ativos, seu valor para o LAC e os riscos, o modelo de Gordon-Loeb define que o inves-

timento ótimo em cibersegurança deverá ser de R$ 87 mil para proteção contra malware, R$ 75 mil contra phishing e R$ 57 mil contra DDoS. Tais valores foram definidos através de simulações executadas utilizando a plataforma GT-IMPACTO e consideram como entrada valores hipotéticos como o lucro estimado da empresa e a importância de cada ativo para o faturamento e seus potenciais impactos financeiros. Além disso, são considerados os riscos de ataques com sucesso e potenciais impactos financeiros para definição do investimento ótimo. É importante lembrar que tal cálculo considera apenas os fatores econômicos e técnicos, desconsiderando especificamente os impactos sociais que são extremamente importantes no setor da saúde. Para isso, é importante levar em consideração os riscos para pacientes e vidas humanas durante a priorização dos investimentos. Encontrar um balanço entre o investimento ótimo e a redução de riscos críticos para a vida humana é fundamental para uma estratégia eficiente do ponto de vista técnico e econômico.

Tabela 1.4. Exemplos de Proteções baseado nos Requisitos de Cibersegurança Mapeados, incluindo Custos e Justificativas para os Investimentos

Tipo de Proteção	Custo Anual (R$)	Justificativa do Investimento
Proteção contra DDoS	R$ 15.000	Previne interrupções de serviço causadas por DDoS, garantindo disponibilidade dos sistemas críticos
Segurança de E-mail contra Phishing	R$ 6.000	Reduz o risco de comprometimento de credenciais e infecção por malware via e-mails maliciosos, protegendo dados sensíveis
Anti-Virus e Anti-Malware (Endpoints)	R$ 4.500	Garante a proteção dos dispositivos da empresa contra ameaças conhecidas e zero-day, reduzindo riscos de vazamento e interrupção
Gestão de Patches e Atualizações	R$ 10.000	Automatiza a aplicação de atualizações de segurança, corrigindo vulnerabilidades conhecidas e melhorando a postura de segurança
Treinamento e Conscientização em Segurança	R$ 30.000	Capacita os colaboradores para reconhecerem ameaças digitais, reduzindo riscos humanos e fortalecendo a cultura de segurança
Criptografia de Dados em Trânsito	R$ 20.000	Protege dados sensíveis durante a comunicação entre sistemas e banco de dados, garantindo confidencialidade e integridade
Conformidade com LGPD e HIPAA	R$ 30.000	Garante que os processos da empresa estejam alinhados com legislações de privacidade, evitando multas e prejuízos de reputação
Total Estimado	**R$ 115.500**	

Com o orçamento definido, podemos verificar quais proteções podem ser aplicadas no LAC para *(i)* reduzir os riscos de ransomware que têm como alvo o banco de dados e serviços críticos, *(ii)* diminuir a chance de funcionários e pacientes serem vítimas de phishing, *(iii)* mitigar os riscos de DDoS em serviços essenciais para o negócio e *(iv)* evitar problemas de conformidade e processos jurídicos devido a incidentes e vazamentos de dados. A Tabela 1.4 apresenta um planejamento inicial de investimento, totalizando R$ 115,5 mil de investimentos para proteção, sendo R$ 15 mil contra DDoS, R$ 50,5 mil contra phishing e malware e R$ 50 mil para adequação e verificação de conformidade. Tais valores são exemplos e ainda existe a possibilidade de aumentar proteções já que,

por exemplo, o valor para proteção contra DDoS está usando apenas 25% do valor ótimo sugerido por modelos econômicos.

Por fim, a última fase envolve a execução e a implantação da estratégia de cibersegurança. Se ainda não existir a experiência necessária na empresa, o suporte técnico pode ser obtido por meio da contratação de consultores. Além disso, é preciso definir um cronograma claro de implementação, pois alguns setores da empresa podem precisar interromper suas operações por algumas horas para implementar totalmente as soluções e os novos processos. Com isso, é possível compreender os diferentes fatores que devem ser considerados durante o planejamento e investimento em cibersegurança. É importante ressaltar que diversas ferramentas da indústria e da academia podem ser utilizadas para apoiar o processo de decisão, sendo fundamental priorizar também os elementos críticos para o setor e considerar os equipamentos e protocolos legados, como acontece no setor da saúde.

1.6. Conclusões e Lições Aprendidas

Neste capítulo, analisamos o cenário de cibersegurança no setor da saúde, um dos mais vulneráveis e visados para ação de cibercriminosos. A convergência entre a alta criticidade dos serviços prestados, o elevado valor dos dados sensíveis e a adoção acelerada de tecnologias digitais torna esse setor um alvo recorrente de ataques cibernéticos. A análise das ameaças, vulnerabilidades e estudos de caso evidencia um ponto crítico: a cibersegurança na saúde ainda não acompanha a velocidade da inovação tecnológica, e isso gera um risco sistêmico de grande impacto técnico, econômico, social e humano.

Portanto, assim como em outros setores críticos, os desafios enfrentados por hospitais, clínicas e demais instituições de saúde vão além da dimensão técnica. Existem gargalos estruturais relacionados à governança, escassez de profissionais especializados, cultura organizacional despreparada e falta de investimentos em cibersegurança. Além disso, embora as regulamentações, normativas e fiscalizações tenham evoluído, as boas práticas de segurança da informação ainda estão longe de ser uma realidade consolidada no setor da saúde.

O aumento de dispositivos conectados no setor, como por exemplo sensores, *wearables* e equipamentos médicos inteligentes, tem ampliado significativamente a superfície de ataque. Por exemplo, podemos observar diversos dispositivos médicos, servidores PACS e equipamentos de imagens publicamente vulneráveis. Os vazamentos de dados, sejam de órgãos públicos ou privados, e os ataques de phishing diretamente ao paciente estão cada vez mais frequentes no setor.

É importante que a tecnologia da informação e todos os envolvidos no setor da saúde compreendam que, em um setor onde vidas humanas estão diretamente em jogo, não há espaço para colocarmos os sistemas e dados em risco. A cibersegurança na saúde é, antes de tudo, uma questão de responsabilidade ética, social e profissional. Assim, esse capítulo tem como objetivo servir de ponto de partida para gestores, pesquisadores e profissionais que buscam transformar a cibersegurança em um aliado estratégico para a proteção e a sustentabilidade dos serviços de saúde.

Como caminhos futuros, entende-se que, em curto prazo, a conscientização e treinamento no setor serão cruciais e o principal componente para melhorarmos a cibersegu-

rança. Em médio prazo, será necessário um plano estratégico do setor para otimizar os processos já existentes, como a configuração básica de serviços visando à cibersegurança e também uma maior atenção para a proteção de dados. Também, será necessário adicionar camadas de proteção adicional em serviços legados, já que existem equipamentos e serviços antigos operando que não foram projetados para as ameaças do mundo atual, mas que cumprem muito bem suas aplicações na área da saúde. Por fim, em longo prazo, precisamos de políticas rígidas para incentivar o setor a investir em cibersegurança, bem como propor mecanismos que auxiliem a tornar os sistemas legados menos ossificados do ponto de vista de cibersegurança.

Referências

Abou Jaoude, J. and Saade, R. G. (2019). Blockchain applications–usage in different domains. *Ieee Access*, 7:45360–45381.

Adebukola, A., Navya, A., Jordan, F., Jenifer, N., and Begley, R. D. (2022). Cyber security as a threat to health care. *Journal of Technology and Systems*, 4(1):32–64.

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., and Jin, Z. (2024). Healthcare internet of things: Security threats, challenges, and future research directions. *IEEE Internet of Things Journal*, 11(11):19046–19069.

Akkaoui, R., Hei, X., and Cheng, W. (2020). Edgemedichain: A hybrid edge blockchain-based framework for health data exchange. *IEEE access*, 8:113467–113486.

Alder, S. (2024). Healthcare Data Breaches Due to Phishing. https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/.

Aljedaani, B. and Babar, M. A. (2021). Challenges With Developing Secure Mobile Health Applications: Systematic Review. *JMIR mHealth and uHealth*, 9(6):e15654.

Aouedi, O., Sacco, A., Piamrat, K., and Marchetto, G. (2023). Handling privacy-sensitive medical data with federated learning: Challenges and future directions. *IEEE Journal of Biomedical and Health Informatics*, 27(2):790–803.

Aragão, S. M. d. and Schiocchet, T. (2020). Lei Geral de Proteção de Dados: Desafio do Sistema Único de Saúde. *Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, 14(3).

Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygård, J. F., and Vitenberg, R. (2023). A survey on blockchain for healthcare: Challenges, benefits, and future directions. *IEEE Communications Surveys Tutorials*, 25(1):386–424.

Arctic Wolf Labs (2025). 2025 Cybersecurity Predictions. https://arcticwolf.com/arctic-wolf-labs-2025-cybersecurity-predictions/.

Associated Press (2020). German hospital hacked, patient taken to another city dies. https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

Autoridade Nacional de Proteção de Dados (2023). ANPD aplica a primeira multa por descumprimento à LGPD. https:

//www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd.

Beckers, K., Heisel, M., and Hatebur, D. (2015). Pattern and security requirements. *Pattern Secur. Requir. Eng. Establ. Secur. Stand*, pages 1–474.

Beerman, J., Berent, D., Falter, Z., and Bhunia, S. (2023). A review of colonial pipeline ransomware attack. In *IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW 2023)*, pages 8–15.

BigID (2024). A cost comparison of data breaches. https://bigid.com/blog/a-cost-comparison-of-data-breaches/.

Boritz, J. E. (2005). Is practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems*, 6(4):260–279.

Calegari, L. (2025). ANPD não multou empresas por violação da LGPD em 2024. https://valor.globo.com/legislacao/noticia/2025/01/29/anpd-nao-multou-empresas-por-violacao-da-lgpd-em-2024.ghtml.

Cambricoli, F. (2020). Nova falha do Ministério da Saúde Expõe Dados Pessoais de mais de 200 Milhões de Brasileiros. https://tinyurl.com/falha-sus-200milhoes.

Cartwright, A. J. (2023). The Elephant in the Room: Cybersecurity in Healthcare. *Journal of Clinical Monitoring and Computing*, 37(5):1123–1132.

Chamberlaim, A., de Azevedo Flor, B., da Silva Pereira, E., Almeida, L. S., Martins, L. D., Silva, Y. S., Siqueira, G. G., Maiczak, T., and Bovo, F. (2023). Inteligência artificial (ia) e suas aplicações em exames de imagem: uma nova era para diagnósticos na área da saúde. *Cuadernos de Educación y Desarrollo*, 15(12):17605–17624.

CheckPoint (2025). The State of Cyber Security 2025. https://engage.checkpoint.com/security-report-2025.

Coventry, L. and Branley, D. (2018). Cybersecurity in Healthcare: a Narrative Review of Trends, Threats and Ways Forward . *International Journal of Midlife Health and Beyond (MATURITAS)*, (113):48–52.

Cybersecurity Ventures (2024). Global ransomware damage costs predicted to reach $275 billion by 2031. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-

Cybersecurity Ventures, Herjavec Group (2021). The 2020-2021 Healthcare Cybersecurity Report. https://www.herjavecgroup.com/2021-healthcare-cybersecurity-report-cybersecurity-ventures/.

De Neira, A. B., Kantarci, B., and Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, 222:109553.

Ding, R., Zhong, H., Ma, J., Liu, X., and Ning, J. (2019). Lightweight privacy-preserving identity-based verifiable iot-based health storage system. *IEEE Internet of Things Journal*, 6(5):8393–8405.

EC-Councl (2022). DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/.

Edemekong, P., Annamaraju, P., Afzal, M., and Haydel, M. (2024). Health insurance portability and accountability act (hipaa) compliance. *StatPearls*.

European Commission (2024). EU Action Plan to Increase Healthcare Cybersecurity. https://healthcare-in-europe.com/en/news/eu-action-plan-increase-healthcare-cybersecurity.html.

Fonseca, F. (2025). Saúde é Setor que mais Sofre Ataque Cibernético. https://valor.globo.com/publicacoes/especiais/inovacao-na-medicina/noticia/2025/02/27/saude-e-setor-que-mais-sofre-ataque-cibernetico.ghtml.

Franco, M., Rodrigues, B., Killer, C., Scheid, E. J., De Carli, A., Gassmann, A., Schoenbaechler, D., and Stiller, B. (2021). WeTrace: a Privacy-preserving Tracing Approach. *Journal of Communications and Networks*, 1(1):1–16.

Franco, M. F., Granville, L. Z., and Stiller, B. (2023a). CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment. In *36th IEEE/IFIP Network Operations and Management Symposium (NOMS 2023)*, pages 1–6, Miami, USA.

Franco, M. F., Granville, L. Z., and Stiller, B. (2023b). CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment. In *36th IEEE/IFIP Network Operations and Management Symposium (NOMS 2023)*, pages 1–6, Miami, USA.

Franco, M. F., Künzler, F., von der Assen, J., Feng, C., and Stiller, B. (2024a). RCVaR: an Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports. *Computers & Security*, page 103737.

Franco, M. F., Lacerda, F. M., and Stiller, B. (2022). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. *Journal of Business and Projects (Revista de Gestão e Projetos)*, 13(3):1–25.

Franco, M. F., Mullick, A. R., and Jha, S. (2024b). QBER: Quantifying Cyber Risks for Strategic Decisions. https://arxiv.org/abs/2405.03513.

Fuentes, M. R. and Huq, N. (2018). Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks. https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf.

Gallopeni, G., Rodrigues, B., Franco, M., and Stiller, B. (2020). A Practical Analysis on Mirai Botnet Traffic. In *2020 IFIP Networking Conference (Networking)*, pages 667–668. IEEE.

GDPR.EU Horizon 2020 (2021). Complete guide to GDPR compliance. https://gdpr.eu/.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., and Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine*, 2:98.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, 9(2):49–61.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, 7:49–59.

Gupta, A., Tripathi, M., Shaikh, T. J., and Sharma, A. (2019). A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks*, 149:29–42.

He, D. and Zeadally, S. (2014). An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE internet of things journal*, 2(1):72–83.

IBM Security (2024). Cost of a data breach report 2024. `https://www.ibm.com/reports/data-breach`.

Islam, T., Sheakh, M. A., Jui, A. N., Sharif, O., and Hasan, M. Z. (2023). A review of cyber attacks on sensors and perception systems in autonomous vehicle. *Journal of Economy and Technology*, 1:242–258.

J. R. Reeder, P. F. McQuade, S. A. Schipma (2021). Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *Greenberg-Traurig Data, Privacy Cybersecurity*, 1:1–25.

Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., and Roytman, M. (2021). Exploit Prediction Scoring System (EPSS). *Digital Threats: Research and Practice*, 2(3):1–17.

Javaid, M., Haleem, A., Singh, R. P., and Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1:100016.

Knight, A. V. (2021). All That We Let In: Hacking 30 Mobile Health Apps and APIs . `https://approov.io/info/all-that-we-let-in-hacking-30-mobile-health-apps-and-apis`.

Koch, R. (2020). What is the LGPD? Brazil's version of the GDPR. `https://gdpr.eu/gdpr-vs-lgpd/`.

L. A. Gordon, M. P. Loeb, L. Zhou (2021). Information Segmentation and Investing in Cybersecurity. *Journal of Information Security*, 12:115–136.

Levina, A., Iliashenko, V. M., Kalyazina, S., and Overes, E. (2022). Smart hospital architecture: It and digital aspects. In Jahn, C., Ungvári, L., and Ilin, I., editors, *Algorithms and Solutions Based on Computer Technology*, pages 235–247, Cham. Springer International Publishing.

Lewis, D., Lasek-Markey, M., Golpayegani, D., and Pandit, H. J. (2025). Mapping the regulatory learning space for the eu ai act. *arXiv preprint arXiv:2503.05787*.

Microsoft (2022). Microsoft Threat Modeling Tool Threats. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats/.

Mirsky, Y., Mahler, T., Shelef, I., and Elovici, Y. (2019). CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. In *28th USENIX Conference on Security Symposium*, SEC'19, page 461–478, USA. USENIX Association.

Mishra, V. (2024). Cyberattacks on healthcare: A global threat that can't be ignored. https://news.un.org/en/story/2024/11/1156751.

Nankya, M., Mugisa, A., Usman, Y., Upadhyay, A., and Chataut, R. (2024). Security and privacy in e-health systems: A review of ai and machine learning techniques. *IEEE Access*, 12:148796–148816.

National Audit Office (2018). Investigation: WannaCry Cyber Attack and the NHS. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

Navruzov, E. and Kabulov, A. (2022). Detection and analysis types of ddos attack. In *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pages 1–7. IEEE.

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., and Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, 3(12):e224873.

NHS Foundation Trust (2023). NHS England business continuity management toolkit case study: WannaCry attack. https://www.england.nhs.uk/long-read/case-study-wannacry-attack/.

Nunes, J., Franco, M., Scheid, E., Kozenieski, G., Lindemann, H., Soares, L., Nobre, J., and Granville, L. (2024). SIM-Ciber: Uma Soluçao Baseada em Simulaçoes Probabilısticas para Quantificaçao de Riscos e Impactos de Ciberataques Utilizando Relatórios Estatısticos. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 570–585.

O Globo (2024). Em um mês, autoridade brasileira de dados abre mais investigações contra empresas do que em quatro anos. Acessado em 8 de maio de 2025.

Olsen, E. (2025). UnitedHealth hikes number of Change cyberattack breach victims to 190 million. https://www.healthcaredive.com/news/change-healthcare-cyberattack-affects-190-million-unitedhealth/738351/.

Ostad-Sharif, A., Abbasinezhad-Mood, D., and Nikooghadam, M. (2019). A robust and efficient ecc-based mutual authentication and session key generation scheme for healthcare applications. *Journal of medical systems*, 43(1):10.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., and Jerram, C. (2013). Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In *Security and Privacy Protection in Information Processing Systems*, pages 366–378, Berlin, Heidelberg. Springer.

R. Mccrimmon and M. Matishak (2021). Cyberattack on Food Supply Followed Years of Warnings. https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936.

Claroty (2025). State of cps security: Healthcare exposures 2025. https://claroty.com/resources/reports/state-of-cps-security-healthcare-exposures-2025.

Healthcare Information and Management Systems Society (2024). 2024 himss healthcare cybersecurity survey. https://cdn.sanity.io/files/sqo8bpt9/production/4f1c1968050411b8bf9335a187301881f9153b9f.pdf.

HIMSS, FinThrive (2025). Survey Reveals Cybersecurity Funding is a Top Challenge for Smaller Hospitals. https://tinyurl.com/finthrive.

Runte, C. (2024). GDPR Enforcement Tracker Report. https://cms.law/en/gbr/publication/gdpr-enforcement-tracker-report.

Santos, J. A., Inacio, P. R., and Silva, B. M. (2021). Towards the use of blockchain in mobile health services and applications. *Journal of Medical Systems*, 45(2):17.

Scheid, E. J., Knecht, A., Strasser, T., Killer, C., Franco, M., Rodrigues, B., and Stiller, B. (2021a). Edge2BC: a Practical Approach for Edge-to-Blockchain IoT Transactions. In *IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021)*, pages 1–9.

Scheid, E. J., Rodrigues, B., Killer, C., Franco, M., Niya, S. R., and Stiller, B. (2021b). *Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues*, pages 1–29. Number 1 in IFIP AICT Festschrifts. Springer, Cham, Switzerland.

Secureworks (2024). Boardroom cybersecurity report 2024. https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024.

Singer, P. W. and Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.

Smart, W. (2018). Lessons learned review of the WannaCry Ransomware Cyber Attack.

Soares, L. R., Nobre, J. C., and Kerschner, G. (2023). Design of a blockchain-based secure storage architecture for resource-constrained healthcare. In *2023 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6.

Sun, Y., Lo, F. P.-W., and Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access*, 7:183339–183355.

The Telegraph (2018). WannaCry cyber attack cost NHS £92m as 19,000 appointments cancelled.

Thyagarajan, C., S.Suresh, Sathish, N., and Suthir, S. (2020). A Typical Analysis And Survey On Healthcare Cyber Security. *International Journal of Scientific Technology Research*, 9(3):1–5.

Todde, M., Beltrame, M., Marceglia, S., and Spagno, C. (2020). Methodology and Workflow to Perform the Data Protection Impact Assessment in Healthcare Information Systems. *Informatics in Medicine Unlocked*, 19:100361.

United States Department of Health and Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

United States Department of Health and Human Services (2013). Breach Notification Rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

United States Department of Health and Human Services (2024a). Social Engineering Attacks Targeting the HPH Sector. https://www.hhs.gov/sites/default/files/social-engineering-targeting-the-hph-sector-tlpclear.pdf.

United States Department of Health and Human Services (2024b). Solara Medical Supplies, LLC Resolution Agreement and Corrective Action Plan. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/solara-ra-cap/index.html.

US Health Care Industry Cybersecurity Task Force (2017). Report On Improving Cybersecurity in the Health Care Industry. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

U.S. Government (1996). Health insurance portability and accountability act of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

Verizon Business (2025). 2025 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/.

Wang, M., Guo, Y., Zhang, C., Wang, C., Huang, H., and Jia, X. (2021). Medshare: A privacy-preserving medical data sharing system by using blockchain. *IEEE Transactions on Services Computing*, 16(1):438–451.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., and Zhang, W. (2023). A survey on federated learning: challenges and applications. *International Journal of Machine Learning and Cybernetics*, 14(2):513–535.

Wolford, B. (2020). What are the GDPR Fines? https://gdpr.eu/fines/.

Young, A. and Yung, M. (1996). Cryptovirology: Extortion-based security threats and countermeasures. In *Proceedings 1996 IEEE Symposium on Security and Privacy*, pages 129–140. IEEE.

Zhang, J., Yang, Y., Liu, X., and Ma, J. (2022). An efficient blockchain-based hierarchical data sharing for healthcare internet of things. *IEEE Transactions on Industrial Informatics*, 18(10):7139–7150.

Todos os links foram visitados em maio de 2025.

