Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.186-197, 2023.
DOI: 10.18762/1982-4920.20230012

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DE SAÚDE

Emanuele Fátima Moreira, Leonardo da Silva, Wdson de Oliveira

RESUMO

A Segurança da Informação é de grande importância para os ambientes de saúde para garantir a segurança e a privacidade de pacientes, familiares, ativos da instituição, entre outros dados considerados sensíveis. Estes locais são responsáveis por armazenar e manipular informações sensíveis, bem como dados críticos que estão relacionados aos diagnósticos e aos tratamentos de patologias que envolvem os pacientes. A violação dessas informações pode ocasionar danos irreparáveis à privacidade, bem-estar financeiro e até mesmo à vida dos pacientes. Há regulamentações específicas que impõem a proteção adequada desses dados, tais como a HIPAA nos Estados Unidos e a LGPD no Brasil. Pensando na necessidade de conscientização de pessoas que atuam no ambiente interno ou externo dessas instituições, para que os mesmos tenham conhecimento da importância de garantir a segurança dos dados, quais seriam as boas práticas para que o objetivo seja atingido com maestria.

Palavras-chave: Segurança; Informação; Dados; Privacidade.

ABSTRACT

Information Security is of great importance for healthcare environments to ensure the security and privacy of patients, families, institution assets, and other sensitive data. These locations are responsible for storing and manipulating sensitive information as well as critical data related to diagnoses and treatments of patient pathologies. Violation of this information can cause irreparable harm to patients' privacy, financial well-being, and even their lives. There are specific regulations that impose adequate protection of this data, such as HIPAA in the United States and LGPD in Brazil. Considering the need for awareness of people who work in the internal or external environment of these institutions so that they are aware of the importance of ensuring data security, what would be the best practices for achieving this goal with mastery.

Keywords: Security; Information; Data; Privacy.

1 INTRODUÇÃO

A Segurança da Informação visa realizar a proteção de ativos que possam causar algum problema financeiro, jurídico ou ainda mais grave, como a integridade física de profissionais. Entende-se como ativos tudo aquilo que possui valores, créditos ou que sejam de direito da instituição, podendo ser uma instituição corporativa ou não. A análise criteriosa dessas informações pode resultar no prognóstico do

paciente, incluindo informações clínicas, pessoais, de acolhimento e procedimentos realizados dentro do ambiente hospitalar.

Os dados coletados como nome, números para contato, prontuários médicos, entre outros, podem representar uma vulnerabilidade aos pacientes se acabarem nas mãos de indivíduos mal-intencionados. Eles podem ser armazenados por meio de um Sistema de Informação em Saúde (SIS) ou mesmo em arquivos, especialmente em regiões ou instituições com pouco acesso à internet ou que não possuem estrutura física adequada para receber máquinas de exame ou computadores.

A segurança da área da saúde está diretamente ligada à proteção geral e individual das possíveis vítimas que podem ser alvo de técnicas de engenharia social usando informações relacionadas a diagnósticos ou possíveis tratamentos. Os engenheiros sociais podem se apropriar dos dados de um paciente terminal e usar as informações pessoais adquiridas para contatá-lo, assim como persuadir, se beneficiar e realizar extorsões de várias maneiras. Essa técnica pode ser usada não apenas com pacientes, mas também com funcionários e visitantes do ambiente hospitalar. Sendo assim, eles conseguem realizar inúmeras táticas para persuadir, conseguir se beneficiar e realizar extorsões de formas diversas.

O principal objetivo é apresentar os riscos associados às tentativas de ataques ao sistema e ao acesso indevido a prontuários e dados de pacientes, estabelecendo métricas para manter a segurança das informações nos ambientes de saúde e ajudar a reduzir os problemas causados por falhas de segurança que podem prejudicar a instituição e os pacientes.

2 REFERENCIAL TEÓRICO

O objetivo desse tópico é fornecer uma visão geral dos conceitos relacionados à segurança da informação em ambientes de saúde.

Com o foco na importância da proteção da informação em uma organização e como isso pode resultar em benefícios para o negócio, tanto na minimização de perdas, como defendia Mandarini (2004).

Foi destacado que as informações são um ativo valioso para a organização e, por esse motivo, requerem proteção adequada, segundo Williams (2001), que também ressalta os desafios enfrentados pelas organizações em ambientes confidenciais.

Além de que, buscou-se a existência de um plano de ação para a implementação da ISO 27799, que deve incluir um conjunto de controles para garantir a segurança da informação com o respeito à privacidade das informações dos indivíduos, defendida por MOREIRA (2001).

Por fim, discutiu-se como a ausência de medidas efetivas de segurança da informação pode acarretar impactos prejudiciais tanto no contexto do ambiente de saúde quanto na esfera pessoal dos pacientes e seus familiares.

2.1 Segurança da Informação

A Segurança da Informação visa proteger toda e qualquer informação contra ameaças ou riscos que podem acabar comprometendo a integridade, disponibilidade ou confidencialidade, sejam elas armazenadas ou transmitidas em sistemas computacionais utilizando redes de comunicação.

Essa área de estudos pode abranger outros meios, como a segurança física, segurança lógica, segurança de rede, gestão de incidentes, conformidade regulatória, entre outras.

Cada uma dessas áreas corresponde a uma etapa do processo de segurança das informações e juntas se complementam para garantir o bom funcionamento de normas - estabelecidas por organizações como a ISO -, leis - estabelecidas pelo poder legislativo -, e diretrizes - orientações que devem estabelecer os princípios das tomadas de decisões para determinadas áreas. Estas normas devem ser estabelecidas conforme a LGPD - Lei Geral de Proteção de Dados -, que tem como objetivo a regulamentação do uso, proteção e transferência de dados pessoais no Brasil. A LGPD visa garantir a privacidade e a proteção dos direitos fundamentais de liberdade e de privacidade dos usuários. Ainda é importante destacar que sua importância se soma às normas estabelecidas por organizações, como a ISO e às diretrizes orientadoras para a tomada de decisões desta área, buscando sempre um ambiente cada vez mais seguro e confiável para todos.

Para as organizações, a Segurança pode ajudar de diversas formas, como com a proteção de ameaças cibernéticas, preservação da reputação, cumprimento das conformidades regulatórias, redução de custos e melhoria nas tomadas de decisões.

Segundo Mandarini (2004), a principal finalidade da Segurança da Informação é buscar a proteção da informação em um conjunto de ameaças com o intuito de garantir melhorias para seu negócio, minimizar as perdas e potencializar o retorno.

Dessa forma, Williams (2001) aborda sobre como as informações de qualquer organização são valiosas. Por isso, a Segurança da Informação é a responsável pela proteção, perdas e exposição delas. O autor revisita os desafios de atuar em um ambiente totalmente confidencial, onde cada informação armazenada pode causar consequências.

Publicada em 2008, a norma internacional ISO 27799 trata das orientações específicas do setor de saúde, no âmbito da segurança das informações. Ela apresenta controles e normas específicas do setor de saúde a fim de garantir a confidencialidade, integridade e a disponibilidade das informações por meio de controle de Segurança da Informação.

Composta por duas partes, ela apresenta o plano de ação de implementação do sistema de gestão da Segurança da Informação (SGSI) e traz o código de prática, conjunto de controles a serem implementados (LEITE, 2013).

O objetivo da norma e resoluções existentes é ressaltar a importância da Segurança da Informação e garantir a sua integridade, disponibilidade e autenticidade das informações nas instituições hospitalares.

> A privacidade de um indivíduo e de suas informações é um direito de cada cidadão e a ele pertence. Dessa forma, nenhuma organização deve negligenciar essa responsabilidade nem descuidar de nenhuma informação que lhe for confiada (MOREIRA, 2001, n.p; FONTES, 2006, n.p.)

2.2 Segurança do Trabalho

A Segurança do Trabalho visa garantir a segurança dos trabalhadores no ambiente em que atuam, podendo assim, realizar de forma preventiva que acidentes ou outras formas de risco à saúde dos trabalhadores aconteçam.

O cumprimento de algumas normas como a NR-35 e NR-12, entre outras, é necessária para a garantia da segurança dos trabalhadores em atividades como trabalho em altura, operação de máquinas e equipamentos, manipulação de produtos químicos, entre outros.

Essa área está associada à Segurança da Informação e deve ser mencionada durante treinamentos, pois as informações sobre equipamentos, procedimentos e protocolos de emergência podem ser cruciais para a prevenção de acidentes e a garantia da segurança dos trabalhadores. Dessa forma, a Segurança da Informação é indispensável para garantir que essas informações sejam mantidas em sigilo e possam estar disponíveis apenas para profissionais autorizados.

"É também definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (SÊMOLA, 2003, p).

2.3 Ambientes de Saúde

Os ambientes de saúde são espaços que oferecem cuidados médicos, diagnósticos e terapêuticos aos pacientes. Esses locais possuem diversos setores e podem ser divididos com base em suas especificações, como hospitais, clínicas, consultórios e laboratórios, cada um possui particularidades.

Os hospitais são os locais mais abrangentes e oferecem uma ampla variedade de serviços médicos, sendo emergências, atendimentos, exames médicos ou internações prolongadas. Geralmente as equipes de funcionários são formadas por médicos, enfermeiros, técnicos de enfermagem, fisioterapeutas, psicólogos, entre outros profissionais que atuam juntos para garantir o bem-estar de seus pacientes.

Todos os ambientes de saúde devem seguir normas rigorosas de higiene e segurança, com o intuito de evitar a propagação de doenças e infecções. Para isso, os profissionais que atuam nestes locais devem estar devidamente capacitados e atualizados para oferecer o melhor atendimento possível aos pacientes.

3 METODOLOGIA

Com o propósito de dar um embasamento teórico dos conceitos aqui apresentados, foi realizada uma pesquisa descritiva que atua com a ajuda de sites, livros e revistas procurando destacar ocorrências dentro de instituições em que foram utilizados métodos de engenharia social para a obtenção de dados de nível sensível

para o benefício de atacantes mal-intencionados. A partir desse ponto foi analisado o levantamento para a construção de respostas, para as respectivas perguntas sobre o que é, como ocorre, qual o propósito e a melhor forma de conseguir evitar o problema em questão. O método utilizado visa elevar o conhecimento de casos que ocorrem dentro do âmbito de saúde para o leitor, quais são os perigos que podem ocorrer e as formas como o atacante pode se beneficiar da obtenção desses dados, além de estabelecer quais ações podem ser tomadas para que o problema seja mitigado.

Para a compreensão de fatos em âmbito de saúde que afetam a vida de pessoas que atuam na área ou que precisam dos serviços prestados pelas instituições, foi realizada a pesquisa descritiva.

4 RESULTADOS E DISCUSSÃO

De acordo com o site “ProDoctor” (2021), o relatório divulgado pela empresa FortiGuard Labs no ano de 2020, aponta que cerca de 8,4 bilhões de tentativas de ataques cibernéticos ocorreram no Brasil, sendo que 5 bilhões ocorreram nos últimos 3 meses daquele ano.

Estes dados exemplificam a enorme quantidade de ameaças e crimes que podem acometer as empresas, incluindo a área da saúde como hospitais, clínicas e consultórios médicos.

Com base nesses acontecimentos, as organizações da área da saúde passaram a investir em ferramentas de softwares ou profissionais que possam combater ou identificar ataques dentro da área de tecnologia. Dessa forma, o desenvolvimento de plataformas de segurança que auxiliam no combate aos ataques cibernéticos e que possam ser utilizados de forma automatizada, passou a ser um dos requisitos para os estabelecimentos de saúde.

Os ataques podem ocorrer de diversas maneiras e dentre elas, está a engenharia social. Esta técnica é utilizada para conseguir informações sensíveis e relevantes de forma não virtual, para conseguir realizar o acesso de computadores, celulares ou outros dispositivos utilizando malwares. A técnica ainda pode induzir a

vítima a realizar o acesso a conteúdos ou sites infectados para a realização da manobra de dados.

Alguns exemplos citados pelo site “ProDoctor” sobre o uso da engenharia social, é o golpe do whatsapp que consiste em enviar uma mensagem em nome de outro indivíduo, se passando por ele, pedindo “favores financeiros”. Dessa forma, o atacante pode utilizar a lista de contatos e as conversas disponíveis a partir do próprio aplicativo da vítima. Mesmo sendo uma técnica muito utilizada e muito conhecida, ainda há um grande número de pessoas que acabam caindo neste golpe.

Pensando no uso da engenharia social podemos encontrar algumas situações que podem ocorrer no dia a dia dentro dos ambientes de saúde, tais como:

- Após atender um paciente, o médico acaba saindo de seu consultório e deixa sua estação de trabalho disponível para acesso - computador desbloqueado. Dessa forma, torna possível o acesso de um usuário não autorizado aos prontuários dos pacientes.
- O colaborador de uma clínica acaba expondo situações financeiras de um paciente em um ambiente com diversas pessoas presentes no mesmo ambiente.

Situações como as que foram citadas acima podem causar o interesse de um criminoso para tirar proveito dos pacientes e em alguns casos podendo se aproveitar da família ou até mesmo da organização e seus funcionários.

O uso bem sucedido desta técnica indica a falta de conhecimento da vítima sobre o assunto abordado neste artigo.

Outros dados importantes sobre o uso da engenharia social nos ambientes de saúde durante as pesquisas foram os casos divulgados em mídia social e redes televisivas que envolvem o uso da técnica para a manipulação e obtenção de informações sensíveis de pacientes.

Em 2022, o site ACIDADEON divulgou o caso de um golpe contra a família de um paciente com o uso de engenharia social. Durante uma ligação recebida por familiares do paciente que estava hospitalizado, o golpista propôs a realização de um procedimento de urgência, fingindo se passar por um médico.

A família acabou perdendo um valor de R$ 3,8 mil. Durante a ligação, o golpista demonstrou saber sobre o quadro clínico do paciente e acabou citando aos familiares sobre o estado de saúde do homem de 60 anos, que estava internado na Unidade de Terapia Intensiva de um hospital particular localizado na cidade de Araraquara, interior de São Paulo. A filha do paciente afirma que o golpista possuía informações precisas sobre o estado de saúde do pai, que estava internado há 15 dias.

O site “EXAME” (2022) faz menção aos comunicados realizados no ano de 2022 pelo Sindicato dos Hospitais, Clínicas e Laboratório do Estado de São Paulo (SindHosp), que realizou um alerta aos hospitais privados sobre os golpes aplicados por estelionatários e que envolviam o uso de informações privadas sobre pacientes que se encontravam internados. No alerta emitido pela organização, é solicitado aos hospitais que eles revejam os processos de segurança interna utilizados para que possam prevenir a invasão e o manuseio indevido de dados, deixando claro a importância da Segurança da Informação dentro dos ambientes de saúde.

Uma matéria publicada no site “Security Report” (2022), apresenta dados informando que o setor de saúde é um dos mais atacados do mundo. Em setembro de 2022, de acordo com o Índice Global de Ameaças, a saúde é o terceiro setor que sofre ciberataques. Este setor, lidera o ranking nacional no Brasil. Estima-se que uma empresa tenha sido atacada em média 1.613 vezes por semana entre os meses de abril e setembro de 2022, no País.

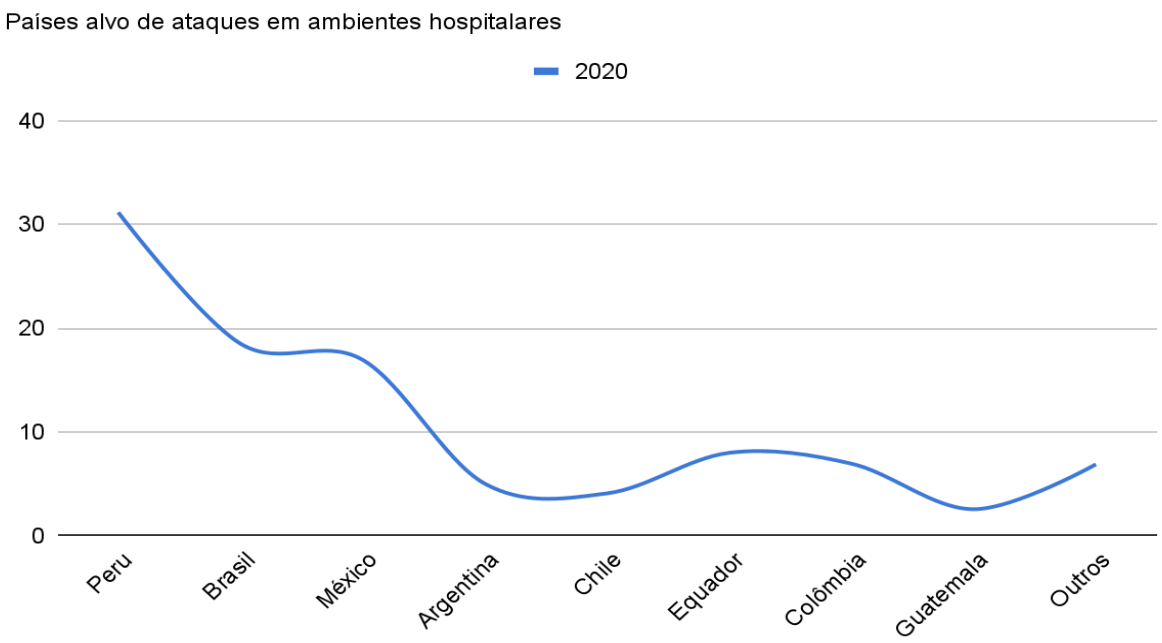
Durante o início da pandemia da Covid-19, o número de tentativas de ataque reduziu durante um curto período para que os serviços não ficassem indisponíveis. Dessa forma, os hospitais tornaram-se ainda mais visados, pois os ataques passaram a ser ainda mais lucrativos para os atacantes, tendo como princípio que a sua motivação se dá porque o cibercrime tem como prioridade o lucro que provém das informações roubadas.

De acordo com informações encontradas no site “WeLiveSecurity” (2021), no ano de 2020 um relatório foi divulgado pela empresa de segurança ESET na América Latina. Informações sobre o uso da engenharia social para a obtenção de dados durante o período de pandemia foram divulgadas para que as pessoas ficassem atentas com emails ou mensagens recebidas via whatsapp, onde as vítimas eram

levadas a acreditar que algumas marcas estavam dando “presentes” após o fornecimento de algumas informações pessoais, como uma espécie de troca.

Após análise das informações fornecidas a partir do site “WeLiveSecurity” (2021), foi possível identificar que na região na América Latina, o país que registrou o maior percentual de casos sucedidos do uso dessa tática de engenharia foi o Peru com cerca de 31%, seguido pelo Brasil com cerca de 18% e o México com aproximadamente 17%.

Figura 1 - Detecções de ataques de engenharia social por país na América Latina durante 2020.



Fonte: WeLiveSecurity

Os dados foram coletados a partir da realização da pesquisa descritiva utilizando revistas, artigos, sites e jornais para reunir casos que pudessem destacar a importância da Segurança da Informação em ambientes de saúde.

A análise dos casos foi crucial para revelar que a maioria das ocorrências envolvendo o vazamento de informações nos ambientes de saúde provém da falta de conscientização que pode ocorrer dentro das empresas ou pode ser praticada pela falta de implementação da proteção de dados.

O uso de engenharia social para obter informações que possam ser usadas em benefício próprio é uma prática que esteve presente nos casos estudados durante a etapa de desenvolvimento do artigo e é o motivo pelo qual se faz necessária a

conscientização e a implementação de uma política de Segurança da Informação nesses ambientes.

Os resultados da pesquisa indicam que a questão citada- a importância da Segurança da Informação em ambientes de saúde -, é uma questão crítica e precisa ser abordada de forma séria e rigorosa.

Os casos estudados revelam que parte das instituições de saúde não possuem políticas claras de Segurança da Informação ou softwares que possam auxiliar na garantia da proteção dos dados, podendo ser apontado também a falta de treinamento eficaz para a conscientização de funcionários sobre as medidas de proteção de dados que podem e devem ser consideradas durante a rotina de trabalho.

Além disso, muitas instituições fazem o uso de programas legados, que possuem tecnologias desatualizadas e vulnerabilidades conhecidas, o que faz com que as informações corram um risco maior em relação à integridade e confidencialidade dos dados dos pacientes e familiares.

Embora muito tenha sido feito para a melhoria desses casos, como a implementação de firewalls e o uso da criptografia de dados, há muito trabalho que ainda deve ser feito para garantir a segurança de dados sensíveis dos pacientes contra ameaças internas e externas desses ambientes.

É crucial destacar que a ausência de investimentos na Segurança da Informação pode prejudicar não só a privacidade dos pacientes e familiares, mas também a qualidade do atendimento e a reputação das instituições de saúde. Para isso, é sugerido que as organizações de saúde invistam mais em tecnologias de segurança avançadas e programas de treinamento para a conscientização de seus funcionários.

5 CONSIDERAÇÕES FINAIS

Neste artigo foi discutida a importância da Segurança da Informação em ambientes de saúde. Foi demonstrado como a falta dela pode impactar negativamente os pacientes, familiares e a organização como um todo.

A partir da pesquisa realizada, foi possível identificar que existem diversas ameaças que comprometem a integridade da Segurança da Informação em ambientes de saúde, como ataques cibernéticos, falhas na proteção de dados, perda de equipamentos eletrônicos, uso de engenharia social para a obtenção de dados

sigilosos, entre outros. Além disso, destacou-se a importância dos profissionais da área terem conhecimentos sobre as boas práticas de Segurança da Informação durante sua rotina de trabalho para evitar possíveis violações.

Em conclusão, trouxemos a importância da garantia de segurança dos dados para o bem-estar dos pacientes, além de prevenir possíveis danos financeiros e reputacionais às organizações. Sendo assim, é imprescindível que todos os envolvidos estejam comprometidos em garantir um ambiente seguro e confiável.

REFERÊNCIAS

A Importância Da Gestão E Armazenamento De Dados Na Área Da Saúde. Fala Universidades, 14 de jun. de 2022. Disponível em: <https://falauniversidades.com.br/a-importancia-da-gestao-e-armazenamento-de-dados-na-area-da-saude/#:~:text=O%20controle%20de%20informa%C3%A7%C3%B5es%20dos,eficiência%20e%20seguran%C3%A7a%20nos%20atendimentos>. Acesso em: 20 de ago. 2022.

ISO 27799:2016. Thales. Disponível em: <https://cpl.thalesgroup.com/pt-pt/compliance/iso-277992016-compliance>. Acesso em: 20 de ago. de 2022.

ISO 27799: Health informatics — Information security management in health using. Geneva, 2008.

Como garantir a Segurança da Informação na saúde. cmtecnologia, São Paulo, jan. 2017. Disponível em: <https://blog.cmtecnologia.com.br/garantir-seguranca-informacao/>. Acesso em: 27 de ago. 2022.

Como manter a Segurança da Informação na área da saúde. morsh telemedicina, 08 de set. 2019. Disponível em: <https://telemedicinamorsch.com.br/blog/seguranca-da-informacao#:~:text=Conseguir%20a%20prote%C3%A7%C3%A3o%20dos%20dados,softwares%20e%20sistemas%20operacionais%20atualizados>. Acesso em: 27 de ago. 2022.

Engenharia Social e Seu Impacto Para o Avanço Dos Crimes Virtuais. ProDoctor, Minas Gerais, 14 de out. 2021. Disponível em: <https://prodoctor.net/imprensa/engenharia-social-e-seu-impacto-para-o-avanco-dos-crimes-virtuais/>, Acesso em: 06 de jun. 2023.

Golpe do falso médico faz família de Araraquara perder R$ 3,8 mil. acidadeon, São Paulo, 15 de set. 2022. Disponível em: <https://www.acidadeon.com/araraquara/cotidiano/Golpe-do-falso-medico-faz-familia-de-Araraquara-perder-R-38-mil-20220915-0015.html>. Acesso em: 16 de set. 2022.

Hospitais de SP alertam contra série de golpes em famílias de pacientes. Exame, São Paulo, 12 de ago. 2022. Disponível em: <https://exame.com/brasil/hospitais-de-sp-alertam-contra-serie-de-golpes-em-familias-de-pacientes/>. Acesso em: 03 de set. 2022.

LEITE, V., **Segurança da Informação em Instituições de Saúde.** Business Protection Services & Solutions. Disponível em:<http://www.defenda.com.br/> Acesso em: novembro de 2022.

MANDARINI, M. **Segurança Corporativa Estratégica.** São Paulo: Manole, 2004.

MOREIRA, N. S. **Segurança Mínima: Uma visão corporativa da Segurança da Informação**, Rio de Janeiro: Axcel Books, 2001.

Número de Ciberataques a Instituições da Saúde no Mundo Bate Recordes. Security Report. Disponível em: <https://www.securityreport.com.br/overview/numero-de-ciberataques-a-instituicoes-da-saude-no-mundo-batem-recordes/> Acesso em: 06 de jun. 2023

QUINTELLA, H. L. M. M.; GONÇALVES, A. L., **Fatores críticos de sucesso da Segurança da Informação em uma organização hospitalar analisados através da cultura organizacional.** Revista Carioca de Produção. Disponível em: <http://www.recap.eng.uerj.br/doku.php> Acesso em: novembro de 2022

SÊMOLA, M. **Gestão de Segurança da Informação – uma visão executiva.** 8ª ed, Rio de Janeiro: Elsevier, 2003.

REDAÇÃO. **Brasil é o segundo país da América Latina com mais detecções de ataques de engenharia social.** We Live Security, 12 de jan. 2021. Disponível em: <https://www.welivesecurity.com/br/2021/01/07/brasil-e-o-segundo-pais-da-america-latina-com-mais-deteccoes-de-ataques-de-engenharia-social/>. Acesso em: 06 de jun. 2023

WILLIAMS, P. A. **Information Security Governance, Information Security Technical Report.** v. 6, n. 3 p.60-70, 2001.