Trabalho de Conclusão de Curso

# PÓS-GRADUAÇÃO EM SEGURANÇA DIGITAL, GOVERNANÇA E GESTÃO DE DADOS

**ALUNO: Henrique Oliveira da Rocha**
**ORIENTADOR: Leonardo Baltazar da Silveira**

PUCRS online uol edtech

# Sumário

**ARTIGO CIENTÍFICO**

# PRINCIPAIS AMEAÇAS DE SEGURANÇA ENCONTRADAS NO AMBIENTE VIRTUAL NAS ORGANIZAÇÕES

**RESUMO:** Em um mundo pós-pandêmico, a sociedade se encontra em um processo de digitalização cada vez mais acelerado. A utilização de novas tecnologias, que se alimentam de grandes bases de dados, é sucessiva e as informações tornam-se um ativo cada vez mais valioso em diferentes seguimentos. Neste cenário, surgem riscos e vulnerabilidades que ameaçam desestabilizar a efetividade e a segurança no ciberespaço das instituições. Diante destas inseguranças, este trabalho tem como objetivo apresentar as principais ameaças de segurança encontradas no ambiente virtual nas organizações. De um ponto de vista metodológico, o estudo limita-se a uma revisão bibliográfica composta por pesquisas acadêmicas e documentos oficiais sobre o tema. Como resultado, observou-se uma crescente insegurança relacionada aos crimes cibernéticos. Logo após, foram destacadas as principais vulnerabilidades encontradas no ambiente virtual pelas organizações de maneira atualizada. O estudo apresentou como conclusão que a proteção de dados deve fazer parte da cultura organizacional, havendo planejamento estratégico específico para segurança da informação. Além disso, observou-se a necessidade da realização contínua de estudos sobre o tema.

**PALAVRAS-CHAVE: Ameaças digitais, Crime cibernético, Proteção de dados, Segurança digital, Segurança da Informação.**

# 1. INTRODUÇÃO

Somos surpreendidos frequentemente com notícias de ataques a grandes corporações e vazamentos de dados. O rápido avanço do processo de digitalização da sociedade fez com que empresas de seguimentos e dimensões diferentes se inserissem no mundo digital, criando bases de dados e sistemas para dar suporte aos negócios.

Com isso, crimes e ataques cibernéticos se intensificaram nos últimos anos. Segundo o site Psafe.com: “3 em cada 4 empresas já tiveram dados vazados” (PSAFE.COM, 2021). Por sua vez, o estudo elaborado pela Ernst & Young, “*How Covid-19 is impacting future investment in security and privacy*”, em que mais de 130 companhias globais foram ouvidas, aponta que a pandemia de Covid-19 triplicou o número de ataques cibernéticos a empresas privadas no mundo todo em comparação aos meses pré-pandemia (ERNST & YOUNG, 2020).

Diante de tal cenário, o tema segurança digital ganha relevância para organizações e a inobservância de cuidados representa risco à manutenção da operação e até mesmo da existência dessas empresas. Isto posto, é preciso inicialmente compreender que qualquer empresa é um potencial alvo para a ação de criminosos, até mesmo pequenas instituições, ainda que nem sempre percebam que seus ativos e dados são valiosos.

Deve-se reconhecer também que diversas áreas são alvo de ataques. O Relatório de Defesa Digital da *Microsoft* aponta que os cibercriminosos estão visando e atacando diversos setores de infraestrutura, incluindo saúde, informações tecnológicas, serviços financeiros e setores de energia (MICROSOFT, 2021, p.8, tradução nossa). Em virtude da crescente relevância da segurança da informação para as organizações e diante das inúmeras ameaças que surgiram nos últimos anos, propõe-se neste estudo identificar e brevemente explanar as principais ameaças de segurança encontradas no ambiente virtual em organizações, tendo como base uma revisão bibliográfica.

# 2. REFERENCIAL TEÓRICO

No referencial a seguir apresentam-se conceitos de segurança da informação, seguido de uma explanação sobre os pilares da segurança digital. Posteriormente, apresenta-se a definição de ameaças, sua subdivisão em grupos e dados referentes às ameaças são exemplificados. Por último, comenta-se sobre a governança relacionada às ações de segurança nos sistemas de informação.

Um dos maiores desafios para as empresas encontra-se na coleta, armazenagem e proteção dos dados disponibilizados em suas bases de dados. A informação tornou-se um ativo valioso e determinante para o sucesso das organizações. Salvaguardar estes ativos ganhou protagonismo, uma vez que falhas de segurança prejudicam governos, empresas e sites a atingir suas missões.

Inicialmente, é imperativo conceituar “segurança da informação”, segundo Laudon e Laudon (1999, p. 270), visa “garantir a segurança dos dados, proteger os PCS e redes e desenvolver os planos de recuperação dos desastres que afetam os sistemas de informação”. Para a ABNT (2001, p. 2) conforme NBR ISO/IEC 17799 “é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades”.

Em seguida, são identificados como pilares da segurança da informação a garantia da integridade, confidencialidade e disponibilidade das informações processadas pela instituição. Integridade de dados relacionada com a exatidão da informação, sua continuidade e dos métodos de processamento; Confidencialidade sendo a propriedade de dar acesso às informações apenas para pessoas autorizadas; Disponibilidade sendo o atributo que garante que os usuários autorizados tenham acesso à informação quando for necessária (FONTES, 2006). O TCU traz ainda a Autenticidade como um quarto pilar, consistindo na garantia da veracidade da fonte das informações (TCU, 2012).

Depreende-se que a informação é o elemento chave para o sucesso ou

fracasso de uma organização. Porém, muitas empresas possuem limitações em desenvolver políticas para proteger seus dados, apesar do potencial para resultados desastrosos. Desta forma, o ponto de partida para elaborar uma estratégia de segurança de informação é identificar as principais ameaças que possam prejudicar a organização de qualquer forma.

Sêmola (2014), conceitua “ameaças” como sendo “agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização”. O autor aponta ainda, que as ameaças podem ser subdivididas em três grupos: “Naturais”, aquelas decorrentes de fenômenos da natureza; “Involuntárias”, aquelas inconscientes, quase sempre causadas pelo desconhecimento (acidentes, erros, falta de energia); e “Voluntárias”, aquelas propositais, causadas por agentes humanos como hackers, invasores, espiões, etc.

Segundo o relatório anual desenvolvido pela empresa de pesquisa e segurança Tenable, de 2016 a 2021, o número de CVEs (*Common Vunerabilities and Exposures* - uma lista de registro de ameaças e vulnerabilidades encontradas em *softwares*), aumentou em média 28.3% a cada ano. A pesquisa aponta ainda a existência de mais de 40,4 bilhões de vazamentos de dados em 2021, sendo 815 milhões apenas no Brasil (TENABLE, 2022). Estes números demonstram alerta quando se trata de segurança em ambientes digitais. A implementação da governança da segurança cibernética, em que uma visão abrangente e integralizada da segurança de redes, dos sistemas e serviços se torna vital para o sucesso das corporações.

Para Rosenau e Czempiel (2000), a governança é um conceito que transcende o escopo de governo e abraça mecanismos informais, não governamentais dentro de um sistema (nacional ou internacional). De uma maneira abrangente, governança abarca políticas, cultura, normas, boas práticas e procedimentos relacionados à segurança digital.

Após a obtenção dos conceitos apresentados pelos estudiosos, buscou-se realizar, em contrapartida aos trabalhos apresentados, a identificação de relevantes vulnerabilidades observadas no ambiente organizacional, em um

cenário pós-pandêmico, relacionadas à segurança da informação, principalmente em se tratando de ambientes virtuais.

# 3. PROPOSTA

Segundo o relatório anual de segurança de *Cybersecurity Ventures* (2022), danos relacionados a crimes virtuais devem custar ao mundo 7 trilhões de dólares. Em 2025, a estimativa é que os prejuízos ultrapassem 10,5 trilhões. O relatório acrescenta ainda, que em 2021, o prejuízo causado por crimes digitais foi de 6 trilhões de dólares, o equivalente a 11,4 milhões por minuto.

Diante de tal cenário, este estudo tem como objetivo apresentar as principais ameaças a serem analisadas pelas organizações no ambiente virtual, a fim de elaborarem uma estratégia de segurança da informação. Para tal fim, realizou-se uma pesquisa documental, entre os meses de julho a setembro de 2022, através da investigação da materialidade textual de pesquisas acadêmicas, documentos oficiais e sites especializados. A pesquisa se deu majoritariamente através da Internet, havendo como complemento pesquisa da literatura indicada em bibliotecas e sites especializados como ABNT, CERT.br, IPEA, *Microsoft*, PSAFE.com e *Tenable*. Com relação aos termos utilizados nas pesquisas, pode-se citar: “segurança digital”, “ameaças digitais”, “cibersegurança”, “crimes digitais”, “proteção de dados”, “segurança da informação”, “ataques virtuais”, além de outros semelhantes. Dentre os resultados obtidos na pesquisa, destacou-se como ameaças críticas às organizações:

- **Falta de uma Política de Segurança de Informações**: Segundo o TCU, a Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos (TCU, 2012). Trata-se da elaboração de um conjunto de regras e princípios a serem adotados com o objetivo de salvaguardar as informações, para que sejam utilizadas apenas a quem se destinam e ao propósito da organização.

A elaboração da Política deve envolver a alta gestão da empresa, a área responsável pela segurança das informações, bem como responsáveis pelos

sistemas informatizados. Dentre os tópicos a serem abordados pela Política destacam-se: objetivos de segurança da instituição; gestão de riscos; controles de acesso; tratativas relacionadas aos diversos vírus; capacitação de pessoal; definições de requisitos de qualidade de sistemas; entre outros.

- **Falta de conscientização sobre segurança de informações por parte do grande escalão**: A participação e conscientização da importância do desenvolvimento de uma Política de Segurança de Informações por parte da alta administração é um elemento crucial para o planejamento da segurança. Para Gil (1998, p. 192), um bom planejamento de segurança é a base para um programa de segurança abrangente e efetivo em relação ao investimento efetuado, entretanto, o principal requisito para o planejamento é o contínuo apoio e participação da alta administração.

Dessa forma, é necessário compreender que mesmo uma empresa que tenha desenvolvido uma Política de Segurança de Informações de alta qualidade possa não conseguir implementá-la devido à falta de recursos disponibilizados pela diretoria. A segurança cirbernética não deve ser considerada um problema da área de tecnologia da informação (TI) apenas, mas sim um foco central da organização como um todo.

- **Não admitir que a organização possa ser um alvo de cibercriminosos**: Mesmo com a existência de uma política de segurança implementada e ainda que não sejam apresentados dados recentes de ataques, é imprescindível que as organizações estejam conscientes, constantemente, que podem se tornar objeto de criminosos virtuais. Por conseguinte, atualizações em ações voltadas a àrea de segurança devem ser frequentes e uma preocupação continuada.

- **Não implementar uma estratégia de *backup* de dados**: Segundo Faria (2014) “o *backup* consiste na cópia de dados específicos para serem restaurados no caso da perda dos originais”. *Backups* podem ser utilizados tanto para restauração de dados como restauração de sistemas, caso venha acontecer um desastre ou um ataque de *cracker* contra o sistema, pode-se fazer a recuperação de versões anteriores dos dados perdidos (CERT.br,

2012).

Ainda que os sistemas de informações tenham uma política de segurança robusta implementada, deve-se manter um plano de *backup* de dados como proteção contra falhas. A falta da realização de *backup* pode fazer com que dados desapareçam para sempre, comprometendo a continuidade do negócio.

- **Falta de informação aos colaboradores relacionada a segurança e ameaças**: Uma das principais brechas de vulnerabilidade em sistemas de segurança são os funcionários das organizações. Mesmo diante de procedimentos e plano de segurança bem estruturados, é imprescindível capacitar e convencer os colaboradores como se protegerem e identificarem as vulnerabilidades. A organização deve elaborar um plano de conscientização contínuo utilizando ferramentas como palestras, seminários, simulação, gamificação, treinamentos e e-mails educativos.

Isabela Drago (2004, p. 7) afirma que: “Uma política de segurança da informação deve ser composta por regras claras, praticáveis e sintonizadas com a cultura e o ambiente tecnológico da empresa. Deve não apenas proteger as informações confidenciais, mas também motivar as pessoas que as manuseiam, mediante a conscientização e envolvimento de todos. Garantir a segurança organizacional é um grande desafio, que passa por todas as pessoas direta e indiretamente envolvidas”.

- **Falta de atualização de *patches* de segurança**: Para a FC BRASIL (2020), *patch* é “uma solução rápida para atualizar ou corrigir softwares. Os *patches* são criados por empresas de *softwares*, quando sabem de uma vulnerabilidade existente em computadores, dispositivos móveis ou outras máquinas em uma rede. Eles garantem que os *hackers* não usem essa fragilidade para invadir redes corporativas. *Patches* de segurança são correções em linhas de código de softwares que aumentam a segurança de um programa ou reduzem alguma vulnerabilidade encontrada. É preciso instalar as correções o quanto antes a fim de proteger os ativos da organização de riscos.

De acordo com a ABNT (2001. p. 43) *software* de fornecedores usado em sistemas operacionais deve ser mantido em um nível suportado pelo fornecedor. Assim, qualquer decisão de atualização para uma nova versão deve

levar em conta a segurança da versão, por exemplo a introdução de uma nova funcionalidade de segurança ou o número e a severidade dos problemas de segurança que afetam esta versão.

- **Ataques *Ransomware***: *Ransomware* é um tipo de malware que tem como objetivo bloquear ou prejudicar o acesso a arquivos. É preciso inicialmente compreender o que são malwares. O CERT.br (2012) os define como códigos maliciosos inseridos em programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Malwares podem infectar ou comprometer um computador através da exploração de vulnerabilidades existentes nos programas instalados; pela auto-execução de mídias removíveis infectadas; pelo acesso a páginas *Web* maliciosas; pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos; pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web*; ou diretamente de outros computadores (através do compartilhamento de recursos).

No cenário atual, *ransomwares* são usados para sequestrar os dados das organizações até que os usuários afetados paguem uma quantidade específica de dinheiro para sua liberação. Estes ataques podem usar e-mails para invadir um sistema, podem ser iniciados ao visitar sites, ao clicar em anúncios online ou através de vulnerabilidade exploradas por *hackers* em redes. Este tipo de malware pode encriptar arquivos, tornando-os inacessíveis ou inaproveitáveis.

Segundo o site Convergência Digital (2022), *hackers* de *ransomware* roubaram mais de 30 *terabytes* (TB) de dados pessoais e outros dados confidenciais em mais de 300 ataques somente em 2022. Por sua vez, segunda edição do recente estudo publicado pela *Microsoft* (2022), "*Cyber Signals*" - que apresenta os principais ameaças cibernéticas e tendências de segurança -, aponta que ataques *ransomware* estão em ascensão em 2022.

- **Ameaça *Bring Your Own Device* (BYOD)**: Para Perini (2017, p. 22) , BYOD é "a preferência pela utilização de dispositivos pessoais para exercer tarefas profissionais". O funcionário acessa dados corporativos para a realização de tarefas profissionais utilizando um dispositivo pessoal (celular,

computador, *tablet*, etc). Apesar de facilitar o rendimento do trabalho, os dispositivos pessoais podem se tornar uma porta de entrada para falhas de segurança, expondo assim os dados organizacionais. BOATEN e OSEI (2016) apontam quatro categorias de vulnerabilidades BYOD: 1 - associadas a malwares; 2 - de permissão de usuário; 3 - de encriptação; e 4 - do usuário desatento.

- **Vulnerabilidades causadas pelo trabalho remoto**: durante o período da Pandemia da Covid-19, o número de pessoas trabalhando remotamente aumentou consideravelmente. Segundo estudo realizado pelo Instituto de Pesquisa Econômica Aplicada - IPEA (2020), entre maio e novembro de 2020, a população brasileira ocupada e não afasta no País era de 74 milhões, sendo que 8,2 milhões passaram a trabalhar remotamente. Com mais pessoas trabalhando de casa e outras localidades que não o escritório, aumentaram as vulnerabilidades e brechas a ataques virtuais.

Durante o trabalho remoto, com a operação descentralizada das empresas, houve um aumento de armazenagem de informações em nuvens, com isso, funcionários foram expostos a conexões em redes não seguras; uso de dispositivos não aprovados; e padrões de segurança reduzidos, em comparação ao fornecido pelas empresas. Isto posto, tornou-se relevante adotar alguns cuidados durante o trabalho remoto, quais sejam: treinar os funcionários sobre questões de segurança; configurar equipamentos de trabalho ou pessoais com *softwares* de confiança; adotar um modelo seguro de comunicação entre os funcionários; e fornecer ferramentas de segurança adequadas aos acessos à rede da organização.

- **Outras ameaças**: Apesar de não serem pormenorizados neste trabalho, merecem citação ainda como vulnerabilidades encontradas no ambiente virtual os ataques em nuvem; ataques *phishing*; ataques de Inteligência Artificial (IA) e *machine learning*; utilização de *hardware* ultrapassado; e ataques internos às empresas.

# 4. RESULTADOS E DISCUSSÕES

Ao realizar a pesquisa sobre os principais ameças de segurança no ambiente virtual, observou-se uma tendência crescente de ataques e gastos relacionados à cibersegurança. Os prejuízos estimados com ataques superaram a marca de trilhões de dólares mundialmente. Ademais, o estudo apontou que a preocupação das organizações relacionadas à segurança digital ganhará protagonismo, principalmente nos próximos anos.

Em relação às ameaças, destacou-se em primeiro lugar a falta de uma polícita de segurança de informações como ponto crítico de vulnerabilidade aos ataques. Entre os estudos, foi possível destacar um consenso na importância da elaboração da estratégia de segurança pelas empresas e no tratamento do tema como vital para manutenção das atividades.

Como causas da falta de planejamento estratégico relacionada à segurança digital no ambiente virtual, notou-se a necessidade de conscientização por parte do grande escalão e a não admissão de que a organização possa ser um alvo de cibercriminosos. A consequência da falta do programa de segurança é a não elaboração de uma estratégia de *backup* de dados; desinformação dos colaboradores; falta de atualização de *patches* de segurança; possíveis ataques *Ransomware*; ameaças causadas por dispositivos não protegidos; e vulnerabilidades trazidas pelo trabalho remoto. Por fim, outras ameaças foram mencionadas neste trabalho, exemplificando que o rol aqui apresentado não é taxativo, mas sim abarca pontos comuns observados na maioria dos estudos e documentos encontrados.

# 5. CONSIDERAÇÕES FINAIS

Este artigo teve como objetivo - através da consolidação e revisão bibliográfica de pesquisas acadêmicas, documentos e sites especializados -, identificar as principais ameaças de segurança do ambiente virtual nas organizações. É importante destacar que esta pesquisa limitou-se a identificar as principais ameaças de uma maneira genérica, sem particularizar casos específicos de ataques e vírus. No desenvolver da pesquisa, foram destacadas as principais ameaças encontradas no ambiente virtual pelas organizações de maneira atualizada. A falta de uma política de segurança de informações, falta de conscientização sobre segurança por parte do grande escalão, falta de estratégia de *backup* de dados, ataques *ransomware* e falta de informação aos colaboradores, merecem destaque. Ademais, foi possível identificar uma deficiência em relação à segurança, uma vez que o número de ataques encontra-se crescente.

Observou-se que novas pesquisas precisarão ser realizadas uma vez que o tema segurança digital está em constante evolução e as ameaças se renovam juntamente com o avanço tecnológico e virtualização do negócio por parte das empresas. A conscientização sobre segurança e privacidade pelas organizações e população em geral necessitará de protagonismo de políticas públicas e privadas, a fim de evitar que novos prejuízos possam ser causados pela ação de cibercriminosos.

# REFERÊNCIAS


ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 17799**: tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

BRASIL PAIS DIGITAL. ***Ransomware* - Sequestro de Dados**. Disponível em: https://brasilpaisdigital.com.br/seguranca-e-cidadania-no-mundo-digital/ransomware/. Acesso em: 29 ago. 2022.

*CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES*. ***Significant Cyber Incidents Since 2006***. Disponível em: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Acesso em: 16 ago. 2022.

CERT.BR. **Cartilha de Segurança para Internet**. 2012. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 17 de ago. 2022.

CONVERGÊNCIA DIGITAL. ***Ransomware* cresce, soma 320 ataques e 30 TB de dados sequestrados em 2022**. Agosto, 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Ransomware-cresce%2C-soma-320-ataques-e-30-TB-de-dados-sequestrados-em-2022-61030.html?UserActiveTemplate=site. Acesso em: 29 ago. 2022.

*CYBERSECURITY VENTURES*. ***Boardroom Cybersecurity 2022 Report***. 2022. Disponível em: https://content.secureworks.com/-/media/Files/US/Reports/Secureworks_NC2_BoardroomCybersecurityReport.ashx?modified=20220809161846. Acesso em: 31 ago. 2022.

DRAGO, Isabela. **Segurança da Informação**: Estudo Exploratório em

Organizações de Grande Porte do Município de Curitiba. Curitiba, 2004.

*ERNST & YOUNG*. **COVID-19: *How future investment in cybersecurity will be impacted***. Julho, 2020. Disponível em: https://www.ey.com/en_gl/consulting/how-the-covid-19-pandemic-is-impacting-future-investment-in-security-and-privacy. Acesso em: 17 ago. 2022.

FARIA, Heitor Medrado de. **Bacula**: Ferramenta livre de *backup*. 2.ed. - Rio de Janeiro: Brasport, 2014.

FC BRASIL. **O que é *patch* e para que serve esse programa?** 2020. Disponível em: https://www.fcbrasil.com.br/blog/o-que-e-gerenciamento-de-patch-e-como-ele-funciona/. Acesso em: 26 ago. 2022.

FONTES, Edison. **Segurança da informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

GIL, Antonio de Loureiro. **Segurança em informática**. 2. ed. São Paulo: Atlas, 1998. 192 p.

HUREL, Louise Marie. **Cibersegurança no Brasil**: Uma Análise da Estratégia Nacional. 2021. Disponível em: https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/. Acesso em: 16 ago. 2022.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). **Trabalho remoto no Brasil em 2020 sob a pandemia do Covid-19**: quem, quantos e onde estão? 2021. Disponível em: https://www.ipea.gov.br/portal/images/stories/PDFs/conjuntura/210714_nota_trabalho_remoto.pdf. Acesso em: 30 ago. 2022.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação com**

**Internet.** Rio de Janeiro: LTC, 1999.

*MICROSOFT*. ***Cyber Signals****: Defend against the new ransomware landscape*. Agosto, 2022. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v. Acesso em 29 de ago. 2022.

*MICROSOFT*. ***Microsoft Digital Defense Report***. Outubro, 2021. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi. Acesso em 17 de ago. 2022.

OSEI, Ezer; BOATEN, Francis. ***Bring-YourOwn-Device*** **(BYOD)**: An Evaluation of Associated Risks to Corporate Information Security, 2016. Disponível em: https://arxiv.org/ftp/arxiv/papers/1609/1609.01821.pdf. Acesso em: 29 ago. 2022.

PERINI, Vinícius Lahm. **Integração de Ferramentas de Administração e Segurança BYOD**. Caxias do Sul, 2017. Disponível em: https://repositorio.ucs.br/xmlui/bitstream/handle/11338/3735/TCC%20Vin%c3%adcius%20Lahm%20Perini.pdf?sequence=1&isAllowed=y. Acesso em: 29 ago. 2022.

*PSAFE.COM*. **Verificador de vazamentos**: 3 em cada 4 empresas já tiveram dados vazados. Junho, 2021. Disponível em: https://www.psafe.com/blog/verificador-de-vazamentos-ferramenta-gratis-mostra-a-empresas-se-seus-dados-ja-foram-vazados/. Acesso em: 17 ago. 2022.

ROSENAU, James N.; CZEMPIEL, Ernst-Otto (Org.). **Governança sem governo**: ordem e transformação na política mundial. Tradução de Sérgio Bath. Brasília: Universidade de Brasília, 2000.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma Visão Executiva. 2. ed. Rio de Janeiro, 2014. Elsevier.

*Tenable Research*. ***Tenable's 2021 Threat Landscape Retrospective***: A guide for security professionals to navigate the modern attack surface. Disponível em:

https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective. Acesso em: 25 ago. 2022.

Tribunal de Contas da União. **Boas práticas em segurança da informação**. 4. ed. Brasília, 2012. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B226095120B. Acesso em: 24 ago. 2022.