Universidade de Brasília

Faculdade de Administração, Contabilidade, Economia e Gestão de Políticas Públicas

Departamento de Administração

VITOR MAGALHÃES FERREIRA

OS IMPACTOS ORGANIZACIONAIS CAUSADOS PELOS INCIDENTES DE ATAQUES CIBERNÉTICOS *RANSOMWARE* NOS TRIBUNAIS DE JUSTIÇA BRASILEIROS.

Brasília – DF

2023

VITOR MAGALHÃES FERREIRA

OS IMPACTOS ORGANIZACIONAIS CAUSADOS PELOS INCIDENTES DE ATAQUES CIBERNÉTICOS RANSOMWARE NOS TRIBUNAIS DE JUSTIÇA BRASILEIROS.

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador:
Dr., Rafael Rabelo Nunes

Brasília – DF

2023

OS IMPACTOS ORGANIZACIONAIS CAUSADOS PELOS INCIDENTES DE ATAQUES CIBERNÉTICOS RANSOMWARE NOS TRIBUNAIS DE JUSTIÇA BRASILEIROS.

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do aluno

Vítor Magalhães Ferreira

Dr., Rafael Rabelo Nunes
Professor-Orientador

Dr., Carlos André de Melo Alves
Professor-Examinador

Dr. Aldery Silveira Júnior
Professor-Examinador

Brasília, fevereiro de 2023

AGRADECIMENTOS

Agradeço ao Professor Dr. Rafael Rabelo Nunes, meu orientador, por toda a ajuda e direcionamento na orientação deste trabalho. Agradeço também a minha família por me ajudar em toda minha trajetória educacional, provendo tudo que era necessário para ter a melhor educação possível. Agradeço também às pessoas que compartilharam essa trajetória comigo na UnB.

*“*Educação não transforma o mundo. Educação muda as pessoas. Pessoas transformam o mundo.” Paulo Freire.

RESUMO

Com os recentes incidentes causados por ataques cibernéticos de *ransomware* ao setor Judiciário Brasileiro, este estudo se propôs a entender quais foram os impactos organizacionais sentidos em termos financeiros, de pessoas, processos e infraestrutura, em uma amostra de tribunais de justiça. Como meio de coleta de dados foram aplicados questionários com gestores de TI dessas organizações com perguntas abertas voltadas aos tópicos já mencionados, sendo também levantados dados de notícias, notas oficiais, relatórios, pesquisas, entre outras fontes de informações. Os resultados do estudo demonstraram que as organizações seguiram às recomendações acadêmicas de defesa contra esse tipo de incidente, tendo planos claros de recuperação e tendo sucesso em realizá-los, o que resultou em poucas perdas em termos de informação e infraestrutura de TI, porém, analisando outros tópicos organizacionais, é possível notar impactos relevantes na área financeira, de pessoas e processos que prejudicaram os tribunais. A maior contribuição deste trabalho é demonstrar que esses tipos os incidentes geram efeitos que vão além da área de TI, impactando outras áreas e comprometendo a produtividade da organização afetando a entrega de serviços à sociedade.

Palavras-chave: Segurança Cibernética; Incidentes; Ataques Cibernéticos; *Malware; Ransomware*; Judiciário; Tribunais.

SUMÁRIO

INTRODUÇÃO

1.1. Contexto

O uso de computadores e da internet vem crescendo muito nos últimos anos devido a possibilidade de proporcionar o rápido e prático acesso à informação, comunicação, realização de compras, entretenimento, trabalho, trazendo diversos benefícios as pessoas. De acordo com Castells (1999) estes proporcionaram transformações sociais, econômicas e políticas em todo mundo no começo do século. Santos (2012) complementa que a ascensão econômica e social brasileira permitiu uma maior penetração dessas tecnologias no dia a dia da sua população e empresas.

Este rápido e difuso uso da internet fizeram com que questões voltadas à segurança e bem-estar neste meio se tornassem um tema de atenção, caracterizando e reforçando à atuação da área de segurança cibernética. Segundo Chaves (apud SILVA, 2003, p.19) Cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação”, logo, o entendimento do que seria a segurança cibernética está de acordo com o Estado Brasileiro (2011) onde o objetivo da segurança cibernética é a busca pela garantia da proteção de ativos e de informações estratégicas por meio de um conjunto de ações defensivas, exploratórias e ofensivas, principalmente relacionadas às infraestruturas críticas da informação como redes de comunicação e computadores.

Por outro lado, existem pessoas mal-intencionadas que buscam se aproveitar de forma ilegal das vulnerabilidades do espaço cibernético para praticar crimes em busca de algum tipo de benefício próprio. Juntamente com o conceito de crime, os “crimes cibernéticos” são todas as condutas “típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática” (SCHMIDT, 2014. p.4).

1.2. Formulação do problema

Um dos principais tipos de incidentes cibernéticos são os ataques cibernéticos do tipo *ransomware, o* qual é considerado pelo artigo 158 do Código Penal Brasileiro

um crime de extorsão, o qual objetivo é constranger a fazer, tolerar ou deixar de fazer algo, sob violência ou grave ameaça para obter vantagem indevida. (BRASIL, 1940).

Com diversos incidentes gerados por ataques de *ransomware* às empresas e pessoas em um panorama global e nacional, surgem dúvidas sobre quais são os impactos sentidos pelas vítimas, e no campo da administração, surgem diversas dúvidas sobre como esses incidentes afetam a produtividade das empresas envolvendo tópicos como finanças, pessoas e processos.

Incidentes cibernéticos gerados a partir de ataques contra o Governo Federal são frequentes, tendo em vista que as organizações públicas possuem dados de milhões de brasileiros, portanto, a necessidade garantir a segurança dessas informações é essencial. Um dos setores mais afetado é o Poder Judiciário que é responsável por resolver conflitos entre cidadãos, entidades e Estado, administrando uma grande quantidade de dados sigilosos de diversos processos judiciais decisórios (MOURA, 2022).

E dessa forma, é possível delimitar o problema de pesquisa o qual esse estudo irá desdobrar: quais são os impactos que os tribunais brasileiros sofrem em termos financeiros, de pessoas e de processos em relação aos incidentes causados por ataques cibernéticos do tipo *ransomware?*

1.3. Justificativas

No processo de estruturação do tema, foi verificado que já existem diversos tipos de estudos realizados com o enfoque na parte técnica dos incidentes de ransomware, focando nos aspectos que envolvem a área da Ciência da Computação, porém, poucos estudos continham um enfoque na Ciência da Administração, focando em questões gerenciais como finanças, pessoas e processos.

Além deste ponto, não foram encontrados trabalhos acadêmicos que focassem nos impactos sentidos pela área Jurídica em específico em decorrência deste tipo de incidente de ataque cibernético.

Portanto, observa-se a oportunidade de desenvolver uma pesquisa que busque entender de forma profunda como os incidentes de ataques cibernéticos do tipo ransomware impactam os tribunais e o setor judiciário.

1.4. Objetivo Geral

Analisar os impactos organizacionais de incidentes cibernéticos gerados por ataques do tipo *ransomware* aos tribunais de Justiça brasileiros levando em consideração aspectos financeiros, de processos e pessoas.

1.5. Objetivos Específicos

a) Levantar e colher dados sobre o histórico de incidentes cibernéticos de ataques de *ransomware* em um panorama global, nacional e nos tribunais brasileiros.

b) Coletar dados e informações nos tribunais para entender quais foram os impactos causados pelos incidentes, levando em consideração aspectos financeiros, de processos e pessoas.

c) Analisar e discutir os resultados encontrados na busca de entender padrões e boas práticas no que tange a defesa e gerenciamento contra esse tipo de incidente.

2. REFERENCIAL TEÓRICO

2.1. Segurança da Informação

A norma internacional ISO/EIC 27002 define a segurança da informação como:

> O conjunto de medidas técnicas e gerenciais que visam proteger informações contra ameaças, garantindo sua confidencialidade, integridade e disponibilidade. Ela fornece uma abordagem abrangente para a gestão de segurança da informação, incluindo a identificação de ameaças, avaliação de riscos, implementação de controles de segurança e monitoramento contínuo (ISO/IEC 27002, 2013, p. 21).

O Instituto de Engenheiros Elétricos e Eletrônicos, por sua vez, discorre que segurança da informação é a disciplina que trata da proteção de informações confidenciais, da integridade dos dados e da disponibilidade dos sistemas de informação (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 2015), através de medidas técnicas, gerenciais e organizacionais. (INFORMATION SYSTEMS SECURITY ASSOCIATION, 2016).

De acordo com a Associação Internacional de Profissionais de Segurança de Computadores (2013), a segurança da informação é o processo de proteção de informações valiosas de ameaças internas e externas, incluindo vazamentos, roubo, destruição e uso não autorizado.

A segurança da Informação é um campo de estudo e atuação o qual busca assegurar três princípios essenciais dos dados e informações: a disponibilidade, confidencialidade e integridade (BRASIL, 2014), desde seu armazenamento até a transmissão através da educação, conscientização e normas (WHITMAN; MATTFORD, 2012), orientações, procedimentos, políticas e demais ações que tem por objetivo proteger a informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada (FONTES, 2017).

A segurança da informação é caracterizada pela aplicação adequada de proteção sobre um conjunto de ativos visando preservar o valor que esses possuem. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade” (BASTOS; CAUBIT, 2009, p. 17).

Pode-se observar certa uniformidade no entendimento sobre o papel da segurança da informação. Será explicado de forma mais aprofundada quais são os três pilares mais comentados pelos autores, Integridade, Disponibilidade e Confidencialidade.

Integridade

De acordo com Mittal “A integridade dos dados é uma propriedade importante da segurança da informação que garante que os dados não sejam alterados, corrompidos ou excluídos de forma não autorizada”, sendo uma propriedade fundamental de segurança da informação. (MITTAL, 2019, p. 4). Chang (2019) conecta o tema com o conceito com o de ataque cibernético, trazendo que a integridade dos dados é uma preocupação crescente em sistemas de informação devido a ameaças cada vez mais sofisticadas, como ataques cibernéticos e vírus de computador. É crucial para garantir a confiabilidade e a precisão dos dados em sistemas de informação, especialmente em aplicações críticas, como saúde e financeiro (XIAO, 2018).

Segundo Sommerville, integridade é a garantia de que os programas e os dados dos sistemas não serão danificados, ou seja, diz respeito à garantia de que a informação realmente é o que deveria ser. Integridade significa garantir a existência dos dados, não corrompidos, íntegros, concluindo que aos dados originais nada foi acrescentado, retirado ou modificado (SOMMERVILLE, 2007).

A informação tem integridade quando é completa, inteira e incorrupta. A integridade da informação é ameaçada quando a informação é exposta a corrupção, danos, destruição ou outras perturbações do seu estado autêntico. Também indicam que a integridade é a base dos sistemas de TI, pois a informação não tem valor ou não é utilizada se os usuários não puderem verificar sua integridade (WHITMAN; MATTORD, 2012).

Disponibilidade

Para Kim, a disponibilidade é “Uma medida da capacidade de um sistema de informação ser usado para atender às necessidades de negócios e operacionais de seus usuários" (KIM, 2018, p. 123).

De acordo com a disponibilidade é uma propriedade fundamental da segurança da informação que garante que os usuários tenham acesso aos dados e sistemas quando precisam (GOLLMAN, 2017).

Beal (2008) complementa que a disponibilidade é como a garantia de que a informação e seus dados associados estejam disponíveis para os usuários legítimos, em um momento desejado. Isso implica no funcionamento da rede e do sistema nessa solicitação (FERREIRA, 2003).

Confidencialidade

Kim afirma que a confidencialidade “é o pilar da segurança da informação que impede que informações confidenciais sejam acessadas ou divulgadas por indivíduos não autorizados” (KIM, 2018, p. 124).

Sandhu (2016) traz que a confidencialidade é um pilar crítico da segurança da informação, que protege contra a exposição não autorizada de informações confidenciais. Sua manutenção busca garantir que indivíduos não tenham acesso acidental ou intencional a informações quando não autorizados (CAIÇARA, 2007).

Segundo Whitman e Mattord (2021), a informação tem confidencialidade quando apenas os usuários que possuem os direitos, privilégios e necessidades conseguem acessar as informações e dados disponíveis. Quando pessoas não-autorizadas também conseguem esse acesso, se pode dizer que informação teve sua confidencialidade quebrada, podendo acontecer através de ataques cibernéticos, por exemplo.

2.2. Segurança Cibernética

O National Institute of Standards and Technology explica que “A segurança cibernética é a proteção de tecnologias de informação e sistemas contra ameaças maliciosas ou não autorizadas que possam prejudicar a integridade, confidencialidade ou disponibilidade desses sistemas" (NIST, 2014. p.4).

Já a universidade Carnegie Mellon, define a segurança cibernética como:

> A segurança cibernética é um campo amplo que inclui a proteção de dados sensíveis, sistemas e redes, bem como a prevenção de ameaças e ataques cibernéticos. Isso inclui medidas técnicas, como criptografia e autenticação, bem como práticas de gerenciamento de segurança, como treinamento de funcionários e políticas de segurança (CARNEGIE MELLON UNIVERSITY, 2016, p.8).

"A segurança cibernética envolve o uso de tecnologias, processos e práticas para proteger sistemas, redes e dados sensíveis contra ameaças externas, incluindo hackers, vírus, spyware, *malware*, ataques de negação de serviço e roubo de informações confidenciais." (SYSTEM ADMINISTRATION, NETWORKING AND SECURITY, 2015, p. 6).

A segurança cibernética tornou-se uma questão de interesse e importância global. Mais de 50 nações já publicaram oficialmente algum tipo de documento estratégico delineando sua posição oficial sobre ciberespaço, cibercrime e/ou cibersegurança (KLIMBURG, 2012).

A União Europeia define o “conceito de segurança cibernética como o conjunto de salvaguardas e ações que se podem empregar para proteger o domínio cibernético, tanto no âmbito civil quanto militar, frente às ameaças vinculadas com suas redes interdependentes e sua infraestrutura de informação, ou que possam afetá-las” (EUROPEAN COMISSION, 2013, p.6).

Para o governo brasileiro, “Segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas” (BRASIL, 2015, p.5).

Pode-se observar que os objetivos da segurança da informação são parecidos com o da cibersegurança, quais seriam as diferenças entre as duas áreas?

Solms e Niekerk (2013) explicam que a segurança da informação é a proteção da informação, que é um ativo não exclusivo de sistemas de informação eletrônicos. Já a segurança cibernética, por outro lado, trata da segurança da informação no próprio ciberespaço, além de também se preocupar com a proteção dos atores que atuam nele, incluindo pessoas, máquinas, redes e as informações.

Buriti (2018) complementa, dizendo que a segurança da informação atua em qualquer forma possível de segurança a dados, seja em máquinas ou arquivos físicos em papel, por exemplo. Já a segurança cibernética lida com a proteção de máquinas, dados e informações especificamente no ciberespaço ou na Internet.

A segurança cibernética é de grande relevância à medida que as atividades governamentais, empresariais e do dia a dia em todo o mundo migram para o ambiente on-line. Mas especialmente nas economias emergentes, em qualquer organização que digitalize suas atividades carece de recursos organizacionais, tecnológicos e humanos, e outros ingredientes fundamentais necessários para garantir o seu sistema, que é a chave para o sucesso a longo prazo (KSHETRI, 2016).

Vulnerabilidade e ameaças

Beal define ameaça como sendo “a expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação” (BEAL, 2008, p. 14). Exemplos de ameaças acidentais são falhas de hardware, desastres naturais, erros de programação, entre outros, enquanto ameaças propositais podem entendidas por roubos, invasões, fraudes, extorsões, etc.

Chapple (2017), comenta que as vulnerabilidades são erros ou falhas em sistemas, aplicativos ou processos que podem ser explorados por ameaças para causar danos ou prejudicar o funcionamento. Incluindo ataques cibernéticos, para comprometer a segurança da informação (FERBRACHE, 2019).

A vulnerabilidade está intimamente ligada ao ponto fraco de um ativo, uma fragilidade. Trata-se de um erro na configuração, procedimento ou até de um agente

na segurança de sistemas e aplicativos, de maneira não proposital ou proposital (FERREIRA, 2003).

Uma das vulnerabilidades mais aproveitadas pelos criminosos é a humana, explorada pela engenharia social, método que consiste na aplicação de conhecimentos de manipulação social a fim de conseguir obter algum tipo de vantagem, acontecendo de forma não obvia e socializada (ROSA, 2012).

Ataques cibernéticos

O governo dos Estados Unidos da América define ataques cibernéticos como qualquer atividade desautorizada ou em desacordo com a lei dos EUA, que busca comprometer ou prejudicar a confidencialidade, integridade ou disponibilidade de computadores, sistemas de informação ou comunicações, redes, infraestrutura física ou virtual controlada por computadores (CEA, 2018).

O Ministério da Defesa do Brasil entende o conceito de forma parecida, considerando como o ataque cibernético “ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL, 2014, p. 23).

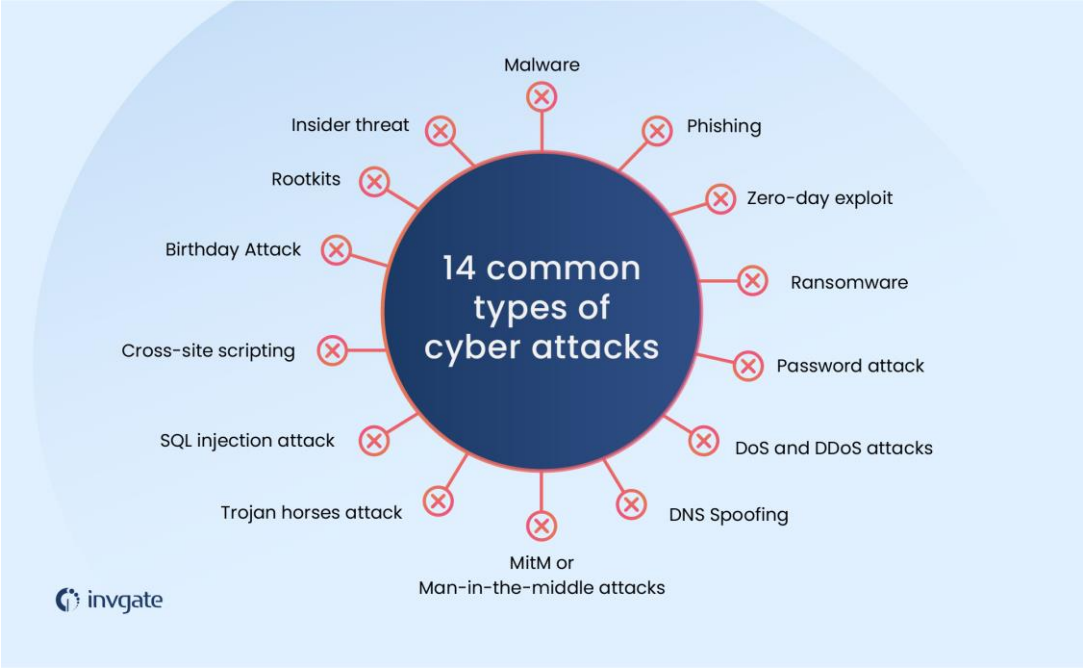
O ataque cibernético tem intenção de derrubar ou corromper redes, bancos de dados, sistemas, equipamentos e dispositivos relevantes, podendo para isso, fazer ou não uso de técnicas de invasão (FERREIRA, 2016).

Klinburg, por sua vez, contribui com uma visão sintetizada sobre o assunto, onde ataques cibernéticos seriam tentativas maliciosas de invasões para quebrar os princípios da segurança da informação em ambientes virtuais, como computadores ou redes computacionais (KLINBURG, 2018). Os princípios da segurança são quebrados com o comprometimento da confidencialidade quando o atacante tem acesso a dados que não lhe são permitidos; altera a integridade quando consegue meios de modificar os dados da vítima; e restringe a disponibilidade quando é capaz de tornar dados, informações e equipamentos indisponíveis a seus usuários legítimos (DA SILVA, 2018).

Woloszin (2009) apresenta que os ataques cibernéticos e o ciberterrorismo são uma tendência mundial sombria. A maior preocupação para o Brasil reside no fato de que os conhecimentos específicos sobre o tema ainda são do domínio de poucos, assim como, os recursos financeiros são insuficientes.

Existem diversos tipos de ataques cibernéticos diferentes, a Figura 1 ilustra alguns dos mais populares:

Figura 1 – Ilustração sobre alguns dos principais tipos de ataques cibernéticos



Fonte: InvGate (2022)

Incidentes Cibernéticos

De acordo com o National Institute of Standards and Technology, um incidente é

> Uma ocorrência que, real ou potencialmente, comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou das informações que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitável (NIST, 2023, p.1).

A natureza dinâmica dos ataques cibernéticos exige abordagens adaptativas, de forma flexível, e evolutivas para a detecção e resposta a esses incidentes (Garcia, 2016). Kshetri (2017) complementa dizendo que eles são inevitáveis, sendo a detecção e a respostas fundamentais para minimizar seus efeitos. Belanger, Rico e Gosselin afirmam que “Os incidentes cibernéticos representam um risco crescente para a segurança da informação e privacidade de dados, e exigem medidas proativas de prevenção e gestão de riscos." (BELANGER; GOSSELIN; RICO, 2019, p. 112).

Malware e Ransomware

De acordo com Caldas (2016), grande parte dos crimes cibernéticos são praticados com uso de programas computacionais maliciosos conhecidos por *malwares*, que tem como objetivo acessar sistemas de computadores de forma ilícita com intuito de roubar, alterar ou danificar esses equipamentos.

Um tipo de *malware* tem ganhado grande escala nos últimos anos e se tornando um problema epidêmico na área da segurança da informação, para governos, empresas e indivíduos, ferindo o princípio da disponibilidade dentro da segurança da informação, são os chamados *ransomware* (ARAUJO, 2019).

Ransomware é um malware que bloqueia seu computador ou impede que você acesse seus dados usando criptografia de chave até que você pague um resgate. Esse resgate geralmente é pago em Bitcoin. A extorsão baseada em dados tem existe desde cerca de 2005, mas o desenvolvimento de software de criptografia de resgate e Bitcoins (ZETTER, 2015).

R*ansomware* é um tipo de *malware* que impede o usuário de acessar seus arquivos ou sistemas, exigindo um resgate em troca da liberação daqueles dados, (ANTONOPOULOS, 2014), buscando lucrar com a vulnerabilidade dos usuários e organizações, criptografando seus arquivos valiosos (CHEN, 2019).

Souppaya (2015) traz uma visão gerencial a qual o *ransomware* é uma ameaça que pode prejudicar a disponibilidade de dados e sistemas críticos e causar interrupções de negócios e perdas financeiras significativas.

A Figura 2 demonstra como funcionam os ataques:

Figura 2 - Ilustração sobre como acontece o ataque de *ransomware*

Fonte: INFOB (2019)

Araújo (2019) acrescenta que o valor cobrado pelo resgate em dinheiro geralmente acontece em criptomoedas, e Richardson e North (2017) complementam que essas moedas são transferidas de forma descentralizadas e não dependem de um emissor central, podendo ser transacionada para qualquer pessoa em qualquer parte do planeta, sem intermediários, e inclusive, sem limitações relacionadas a valores. Dessa forma, esse tipo de transferência de dinheiro tem sido amplamente utilizado nesses tipos de ataque pela sua dificuldade de rastreio das transações e pela ausência de limitações, o que tornam as criptomoedas muito atrativas para esse tipo de crime.

Tipos de ataque de Ransomware

Existem 2 tipos de ataques de ransomware de acordo Savage, Coogan e Lau (2015), sendo eles:

i) *Ransomware Crypto*, mais comum, no qual criptografa arquivos e dados indisponibilizando o seu acesso.

ii) *Ransomware Locker*, no qual bloqueia o computador ou outro dispositivo, impedindo que as vítimas o utilizem.

De acordo com o *ransomware crypto* é um bloqueador de arquivos e dados que é implementado nos sistemas do usuário. O *malware* criptografa os dados e arquivos, tornando-os inutilizáveis, aproveitando deste momento para extorquir a vítima exigindo um resgate financeiro a ser pago em troca do desbloqueio (HANUMAT; AKASHDEEP; VINAY, 2016).

Já o *Locker*, funciona como um bloqueio de acesso ao sistema operacional, não havendo a criptografia de arquivos, softwares, entre outros nas máquinas. Pelo seu baixo nível de profundidade, acaba sendo um tipo de ataque fraco e relativamente simples de resolver, por isso, é menos utilizado pelos criminosos (HANUMAT; AKASHDEEP; VINAY, 2016).

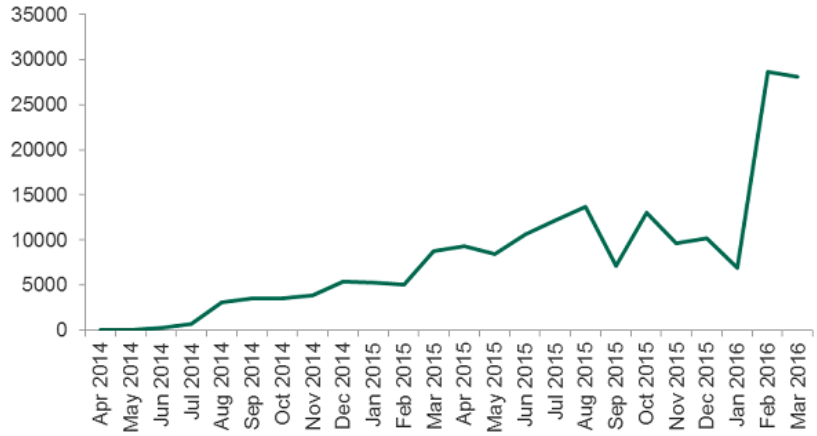
Ataques de ransomware em um panorama global

Os ataques de *ransomware* aumentaram de forma considerável nos últimos anos com o desenvolvimento do espaço cibernético, da informática e, principalmente, pelo maior número de usuários usando máquinas com fins voltados as suas vidas pessoais e profissionais. Uma das maiores empresas de segurança cibernética do mundo, a Kaspersky (2016), apontam que entre os anos de 2014 a 2016 houve um grande aumento em relação a ocorrência desse crime, o que está ilustrado pelo Gráfico 1.

De acordo com o Federal Bureau of Investigation, foram estimadas perdas de cerca de um bilhão de dólares americanos (US$ 1 bilhão) incorridas por ataques de ransomware no ano de 2016. Também foi visto que uma quantidade considerável de pessoas paga pelo resgate, o que pode ser evidenciado pelo fato de que aproximadamente 40% das vítimas de ransomware realizaram esse pagamento (FBI, 2016 apud DA SILVA, 2018).

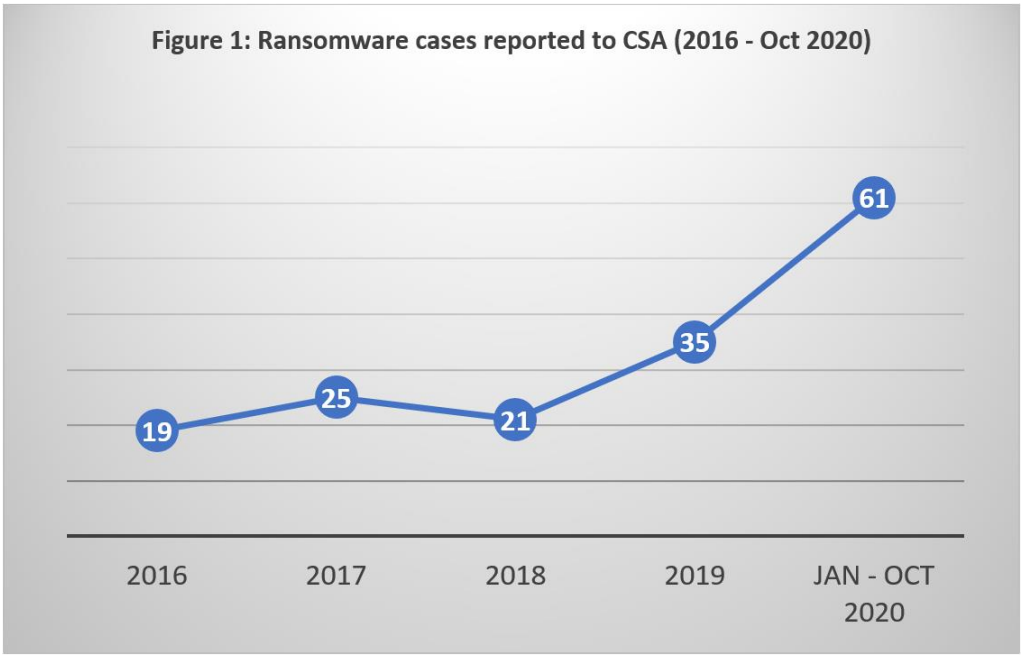
De acordo com a Agência de Segurança Cibernética de Singapura (2016), foi possível ver o crescimento da comunicação de casos de ataques de ransomware ao longo dos últimos anos, apresentado no Gráfico 2:

Gráfico 1 - Evolução dos ataques de *ransomware* de 2014 para 2016



Fonte: KARPERSKY (2016)

Gráfico 2 - Evolução da comunicação de casos de ataques de ransomware reportados.



Fonte: SingCert (Equipe de Emergência Computacional de Singapura).

No relatório de cenário de ameaças de 2020 da Bitdefender, empresa de software de cibersegurança, os ataques de *ransomware* estão aumentando e se tornando mais perigosos nos últimos anos. No primeiro semestre de 2020, o número total de relatórios globais de *ransomware* aumentou 715% ano a ano (BITFDEFENDER, 2020).

O *CryptoLocker*, foi um dos primeiros ataques de *ransomware* a ter grande sucesso. Ele se espalhou por meio de anexos a mensagens de *spam*, exigindo dinheiro em troca das chaves para descriptografia (FRUHLINGER, 2019).

Segundo Da Silva (2018), um dos ataques globais de *ransomware* que mais afetou computadores no mundo foi o *WannaCry* em 2017 afetando cerca de 300 mil dispositivos no ano de seu lançamento em aproximadamente 150 países. Dentre as vítimas, encontram-se infraestruturas críticas e empresas de energia. Mohurle e In (2017) complementam que empresas como FedEx, Nissan, empresas ferroviárias na Alemanha, Rússia, e empresas de telecomunicações como a megaforTelefonica e empresas do ramo de saúde no Reino Unido foram fortemente afetadas, estimando um custo de US$ 4 bilhões em perdas em todo o mundo.

De acordo com a Security Week (2021), site voltado a conteúdos e notícias de segurança cibernéticas, alguns dos principais ataques ocorridos nesse ano foram:

a. Colonial Pipeline, uma das principais redes de transporte de combustíveis dos EUA, sofreu um ataque de *ransomware*. O ataque resultou na interrupção do fornecimento de combustíveis ao longo da costa leste dos EUA, levando a preocupações de escassez e aumento nos preços da gasolina.

b. A JBS USA, maior processadora de carne bovina do mundo, foi vítima de um ataque de *ransomware*. O ataque interrompeu a produção da empresa em diversos locais e teve um impacto significativo na cadeia de suprimentos de carne bovina global.

c. A Garment manufacturer, uma fabricante de vestuário foi vítima de um ataque de *ransomware*, o que resultou na interrupção de suas operações. Além disso, os dados sensíveis da empresa, incluindo informações

financeiras e de clientes, foram ameaçados de serem divulgados publicamente

d. Ireland's Health Service Executive sofreu um ataque de *ransomware* que afetou seu sistema de informação, interrompendo as atividades clínicas e administrativas.

e. Leatherbee, uma empresa de consultoria de segurança cibernética, sofreu um ataque de *ransomware* que resultou na perda de dados sensíveis. O ataque foi notável porque a empresa é especializada em segurança cibernética e teve suas defesas violadas.

O mesmo site afirma que “No ano de 2022, 105 governos locais nos EUA foram atingidos por ataques de *ransomware*, junto com 44 universidades e faculdades, 45 distritos escolares e 25 provedores de assistência médica. Os ataques a esses distritos escolares afetaram mais de 1.900 escolas individuais, enquanto os incidentes com profissionais de saúde atingiram 290 hospitais” (SECURITY WEEK, 2023, p. 1).

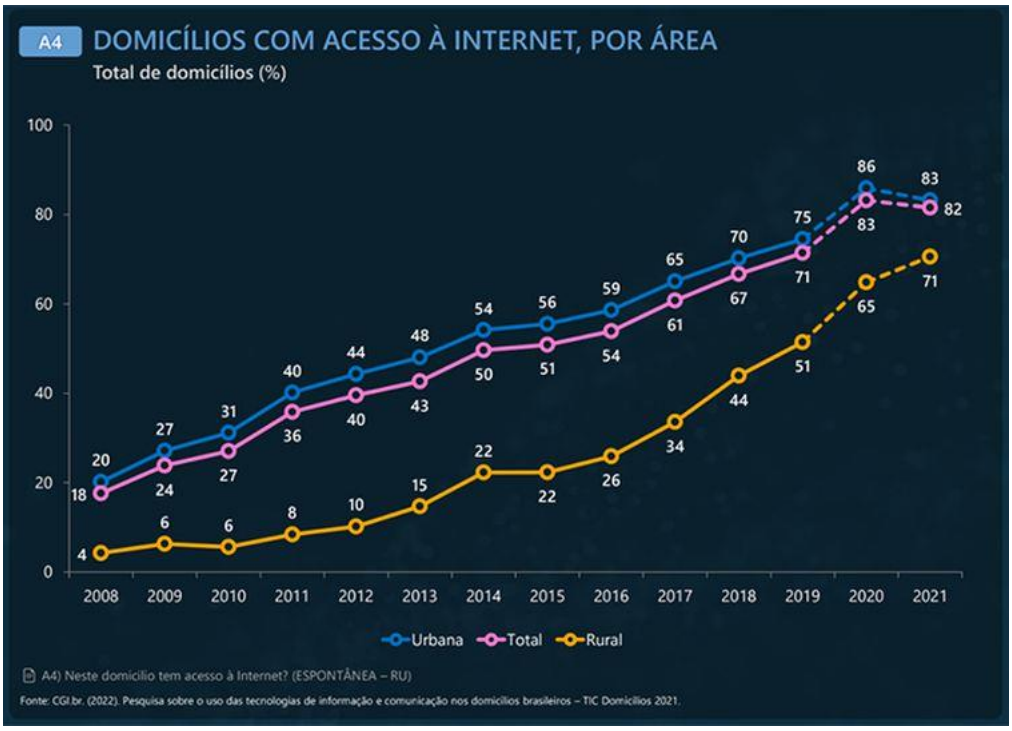
Ataques de ransomware em um panorama brasileiro

A população brasileira aumentou o acesso e uso da internet nos últimos anos, de acordo com o Comitê Gestor da Internet do Brasil (2021), o Brasil tem 152 milhões de usuários de Internet, o que corresponde a 81% da população do país com mais de 10 anos. O Gráfico 3, demonstra o aumento da porcentagem de domicílios que utilizam a internet ao longo dos anos.

Assim como na maioria dos países emergentes, o Brasil ainda está se estruturando mediante a esse crescimento acelerado do uso da internet e aos diversos desafios que vieram com ela, sendo uma das principais, a questão da segurança. E por outro lado, observa-se grupos que se organizam com intenções criminosas na busca de se beneficiar pela exploração desse ambiente que apresenta vulnerabilidades.

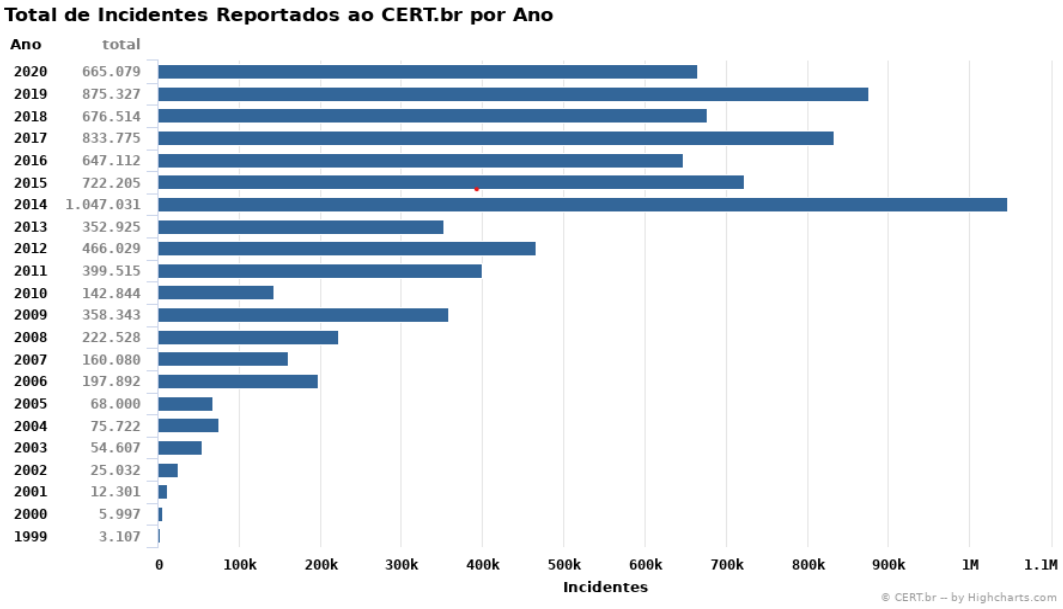
Segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (2020) foram reportadas, no ano de 2020, 665.079 notificações de ataques cibernéticos no país, ilustrado pelo Gráfico 4.

Gráfico 3 – Porcentagem de domicílios brasileiros com acesso à internet total e por área.



Fonte: CETIC.BR (2021)

Gráfico 4 - Total de incidentes de segurança cibernética em 2020



Fonte: CERT.BR (2020)

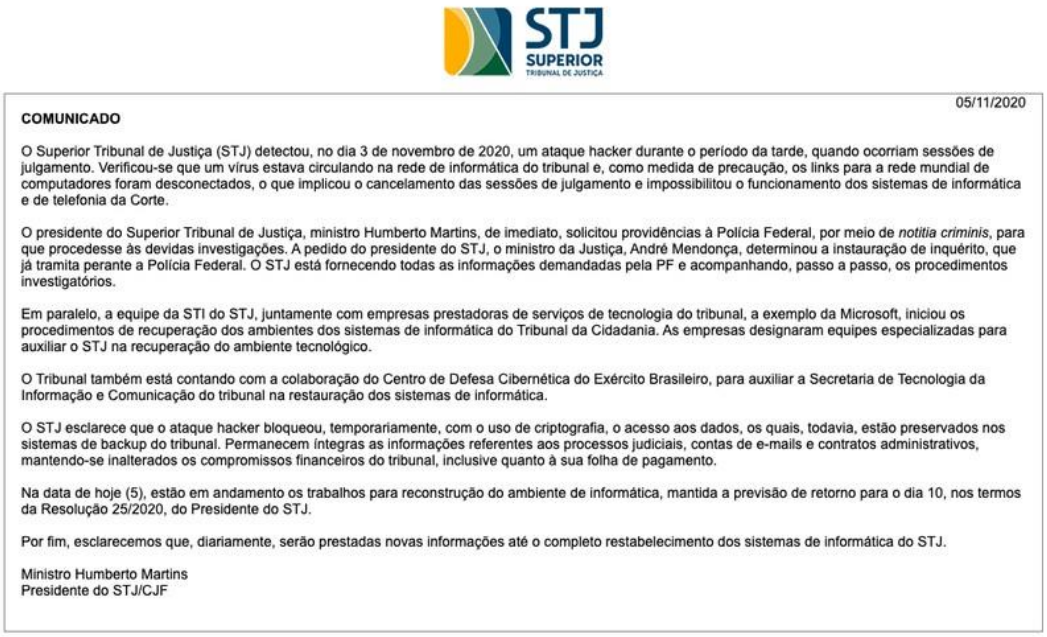
Entre o ano de 2021 e 2022, uma série de ataques utilizando o *ransomware* foram direcionados a pessoas e empresas no brasil. De acordo com a pesquisa Digital Defense Report, realizada pela Microsoft, foi registrado um aumento de 30% desse tipo de crimes cibernéticos no período, gerando um prejuízo de 32,4 bilhões de reais a empresas brasileiras, com ataques a dispositivos por meio de sites maliciosos, links, e-mails e programas maliciosos em sistemas e, principalmente, pessoas vulneráveis (MICROSOFT, 2022).

A partir desse contexto, serão evidenciados exemplos de ataques do tipo *ransomware* de forma mais segmentada para o tema deste estudo, organizações públicas e, principalmente, organizações da justiça brasileira.

No Brasil, um dos ataques mais preocupantes em 2020 foi o ataque de *ransomware* “RasomExx” direcionado ao Supremo Tribunal de Justiça (STJ). Os criminosos sequestraram dados e exigiram pagamento para liberá-los. Em nota, o presidente do STJ, ministro Humberto Martins, informou que todas as sessões de julgamentos foram suspensas até que a área técnica conseguisse restabelecer a segurança no sistema, com isso, o ataque afetou cerca de 12 mil julgamentos e o acervo dos processos da corte, que ainda geram preocupações referentes aos tipos de arquivos sigilosos que os criminosos tiveram oportunidade de aplicar o ataque. (STJ, 2020).

Imagem do pronunciamento do Presidente do STJ, Ministro Humberto Martins, sobre o ocorrido:

Figura 3 - Ilustração sobre como acontece o ataque de *ransomware*



05/11/2020

COMUNICADO

O Superior Tribunal de Justiça (STJ) detectou, no dia 3 de novembro de 2020, um ataque hacker durante o período da tarde, quando ocorriam sessões de julgamento. Verificou-se que um vírus estava circulando na rede de informática do tribunal e, como medida de precaução, os links para a rede mundial de computadores foram desconectados, o que implicou o cancelamento das sessões de julgamento e impossibilitou o funcionamento dos sistemas de informática e de telefonia da Corte.

O presidente do Superior Tribunal de Justiça, ministro Humberto Martins, de imediato, solicitou providências à Polícia Federal, por meio de *notitia criminis*, para que procedesse às devidas investigações. A pedido do presidente do STJ, o ministro da Justiça, André Mendonça, determinou a instauração de inquérito, que já tramita perante a Polícia Federal. O STJ está fornecendo todas as informações demandadas pela PF e acompanhando, passo a passo, os procedimentos investigatórios.

Em paralelo, a equipe da STI do STJ, juntamente com empresas prestadoras de serviços de tecnologia do tribunal, a exemplo da Microsoft, iniciou os procedimentos de recuperação dos ambientes dos sistemas de informática do Tribunal da Cidadania. As empresas designaram equipes especializadas para auxiliar o STJ na recuperação do ambiente tecnológico.

O Tribunal também está contando com a colaboração do Centro de Defesa Cibernética do Exército Brasileiro, para auxiliar a Secretaria de Tecnologia da Informação e Comunicação do tribunal na restauração dos sistemas de informática.

O STJ esclarece que o ataque hacker bloqueou, temporariamente, com o uso de criptografia, o acesso aos dados, os quais, todavia, estão preservados nos sistemas de backup do tribunal. Permanecem íntegras as informações referentes aos processos judiciais, contas de e-mails e contratos administrativos, mantendo-se inalterados os compromissos financeiros do tribunal, inclusive quanto à sua folha de pagamento.

Na data de hoje (5), estão em andamento os trabalhos para reconstrução do ambiente de informática, mantida a previsão de retorno para o dia 10, nos termos da Resolução 25/2020, do Presidente do STJ.

Por fim, esclarecemos que, diariamente, serão prestadas novas informações até o completo restabelecimento dos sistemas de informática do STJ.

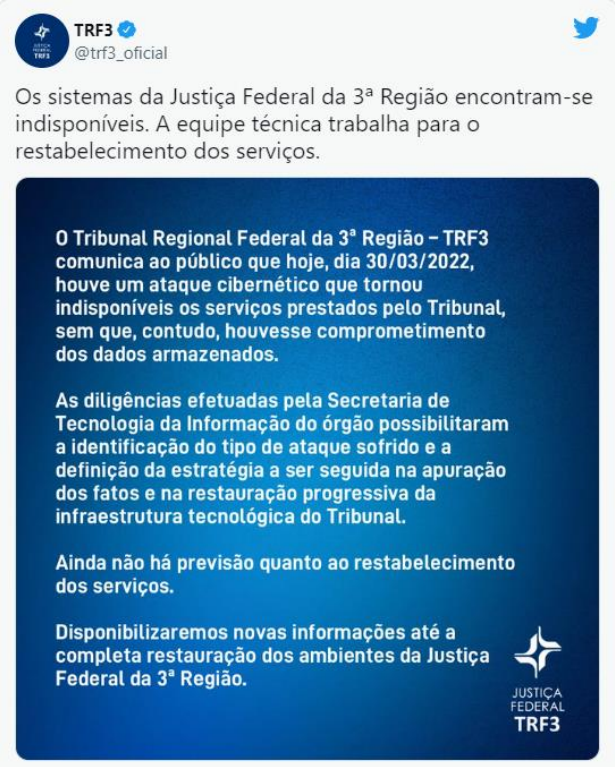
Ministro Humberto Martins
Presidente do STJ/CJF

Fonte: STJ (2020)

Ainda de acordo com a organização, os sistemas do STJ ficaram uma semana inoperantes e só foram completamente restabelecidos meses depois, gerando perdas consideráveis nas prestações de serviços à sociedade e ineficiência interna por grande parte dos colaboradores do órgão não terem conseguido trabalhar pela impossibilidade de uso dos sistemas.

Outro grande ataque de *ransomware* ocorreu em 2022 com o Tribunal Regional Federal da 3ª Região – TRF-3 que abrange São Paulo e Mato Grosso do Sul. O ataque cibernético impossibilitou o acesso aos sistemas utilizados para elaboração de minutas, conferência dos dados pelas partes e transmissão de ordem pagamento de precatórios, suspendendo atividades judiciais (UOL, 2022). Segue abaixo a nota emitida pelo TRF3 em uma das suas principais redes sociais, o Twitter:

Figura 4 - Publicação do TRF3 sobre ataque em seu perfil oficial no Twitter



Fonte: Twitter (2022)

O ataque gerou uma indisponibilidade de mais de 14 dias nos sistemas, tendo grande impacto na atividade-fim da empresa na entrega de serviços a sociedade, e novamente, gerando outras perdas causadas pela ineficiência da mão de obra ter ficado impossibilitada de trabalhar durante o período de reestabelecimento (UOL, 2022).

Outro caso de ataque de *ransomware* ao Judiciário Brasileiro foi direcionado ao Tribunal de Justiça do Estado do Rio Grande do Sul (TJ-RS) em 2021. A notícia foi dada pelo Desembargador Antônio Vinicius Amaro da Silveira, do Conselho de Comunicação. O tribunal percebeu que o sistema havia sido invadido na madrugada do dia, quando o site saiu do ar. A equipe de segurança orientou os colaboradores a não acessarem suas máquinas, os sistemas e os serviços de telefonia da organização, gerando uma interrupção no trabalho dentro da organização. (TJ-RS, 2021).

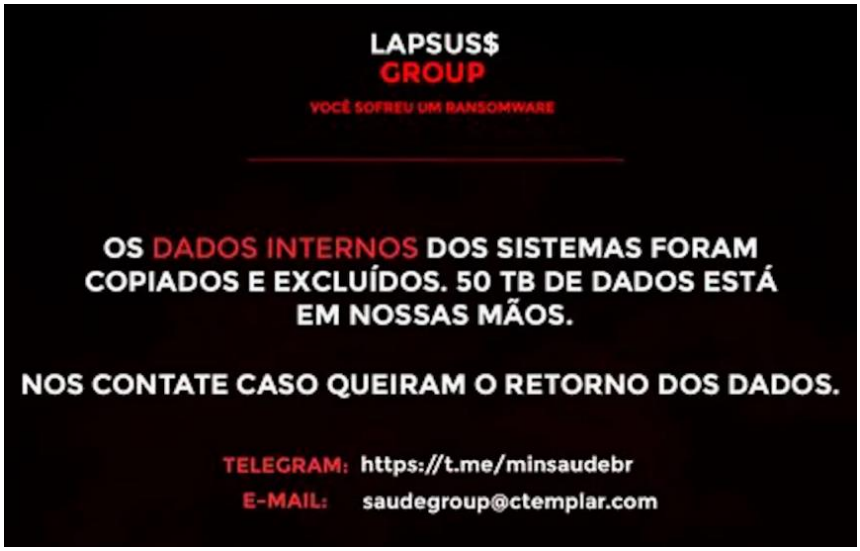
Outro ataque *ransomware* ocorreu com o Ministério da Economia, especificamente com a rede interna da Secretaria do Tesouro Nacional, a qual

declarou que foi vítima de ataque cibernético em agosto de 2021, o ministério divulgou em nota integra:

> Foi identificado na noite de sexta-feira (13/8) um ataque de ransomware à rede interna da Secretaria do Tesouro Nacional.
>
> As medidas de contenção foram imediatamente aplicadas e a Polícia Federal, acionada.
>
> Os efeitos da ação criminosa estão sendo avaliados, neste primeiro momento, pelos especialistas em segurança da Secretaria do Tesouro Nacional e da Secretaria de Governo Digital.
>
> Nesta primeira etapa, avaliou-se que a ação não gerou danos aos sistemas estruturantes da Secretaria do Tesouro Nacional, como o Sistema Integrado de Administração Financeira (SIAFI) e os relacionados à Dívida Pública. As medidas saneadoras estão sendo tomadas (MINISTÉRIO DA ECONOMIA, 2021, p.1).

E por fim a termos de exemplos, o Ministério da Saúde também sofreu um ataque cibernético em dezembro de 2021, que ao tentar entrar na página da organização, foi disposta a seguinte mensagem representada pela Figura 5:

Figura 5 – Mensagem disposta pelos Hackers na página do Ministério da Saúde



Fonte: ESTADÃO (2021)

Além do site do Ministério da Saúde, o funcionamento do Conecte SUS, que entre seus serviços, fornece o certificado nacional de vacinação, uma informação de grande importância na época devido a Pandemia do coronavírus, também foi afetado dificultando o acesso a diversos sistemas e informações importantes sobre a saúde dos brasileiros, usuários do sistema (ESTADÃO, 2021).

3. METODOLOGIA

Nesta seção será apresentada a metodologia utilizada para alcançar o principal objetivo preestabelecido na pesquisa, entender quais são os impactos organizacionais gerados pelos ataques cibernéticos de *ransomware* em tribunais de justiça brasileiros.

De acordo com Cervo e Bervian (2002, p. 23), o método corresponde a ordem que se deve impor aos diferentes processos necessários para atingir um certo fim ou um resultado desejado por meio de um conjunto de processos empregados na investigação e na demonstração da realidade.

3.1. Tipologia da Pesquisa

A pesquisa tem sua natureza aplicada, com o objetivo exploratório e descritivo. É qualificada como exploratória tendo como objetivo desenvolver, esclarecer, modificar conceitos e ideias buscando a formulação de problemas de pesquisa mais específicos para estudos futuros e proporcionar uma visão ampla sobre um fato (GIL, 2008). Também é caracterizada como descritiva, pois, a pesquisa descritiva busca entender as características de um fenômeno e para isso utiliza técnicas padronizadas de coleta de dados como a aplicação de questionários e a observação sistemática (SILVA & MENEZES, 2000).

Devido ao caráter de entender profundamente sobre o tema baseado na percepção de especialistas sobre o tema, a pesquisa é essencialmente qualitativa. Vieira e Zouain (2005), afirmam que a pesquisa qualitativa atribui importância fundamental aos depoimentos dos atores sociais envolvidos, aos discursos e aos significados transmitidos por eles. Nesse sentido, esse tipo de pesquisa preza pela descrição detalhada dos fenômenos e dos elementos que o envolvem.

3.2. Participante do Estudo

A escolha dos entrevistados foi feita por conveniência pois, foi considerado que para colher respostas aprofundadas sobre o tema da pesquisa, seria essencial escolher um grupo de colaboradores que possuíssem conhecimento técnico profundo sobre o tema, assim como conhecimentos gerenciais sobre sua área e a relação com às outras, portanto, foram selecionados gestores de TI desses tribunais para participar da pesquisa.

Foram escolhidas três Tribunais de grande atuação no Brasil, sendo um Federal, e dois a nível Estadual. Essa escolha foi feita por terem sido justamente tribunais que sofreram incidentes cibernéticos do tipo ransomware. Por questão de sigilo, não é possível a identificação delas. Em cada organização foi entrevistado o seu respectivo Gestor de TI responsável pela área de segurança cibernética.

Importante ressaltar que as entrevistas foram conduzidas em setembro a outubro de 2022, e o questionário utilizado está disponível para consulta na parte de apêndices, ao final do trabalho.

3.3. Instrumentos de Coleta

Em termos de instrumento de coleta de dados, foram aplicados questionários com perguntas abertas sobre os principais tópicos a serem estudados nesta pesquisa. O questionário pode ser definido “como a técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo por objetivo o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas, situações vivenciadas, etc.” (GIL,1999 p. 128).

3.4. Procedimentos de Análise de Dados

Buscando entender o fenômeno específico de ataques de *ransomware* aos tribunais, o procedimento técnico utilizado na pesquisa foi a pesquisa de campo e documental. Yin define este procedimento como:

> A pesquisa pode ser conduzida de diferentes maneiras, incluindo pesquisa experimental, levantamento, estudo de caso, etnográfica e pesquisa de arquivo. A pesquisa de campo, que envolve observação direta de indivíduos e grupos em seus ambientes naturais, é frequentemente usada em combinação com análise de a revisão sistemática e interpretação de documentos como registros governamentais, relatórios corporativos e cartas pessoais, para obter uma compreensão mais profunda do fenômeno em estudo (YIN, 2018, p. 5).

Em relação à análise de dados, foi aplicada a análise de conteúdo sobre os questionários, relacionando as repostas com o conteúdo teórico do trabalho, de modo a alcançar os objetivos desta pesquisa.

Conforme Bardin (2016), a análise de conteúdo segue as etapas:

1. Pré-análise: consiste na coleta de documentos de fontes oficiais, o que foi realizado em grande parte no referencial teórico, onde foram dispostas informações sobre os ataques em formato de notícias, notas oficiais, relatório, entre outros tipos de fonte que também serão resgatados nessa etapa.

2. Exploração do material: consiste na análise e agrupamento das informações dispostas nas entrevistas, de modo a caracterizar o conteúdo em tópicos para o entendimento do fenômeno em diferentes partes e relacioná-los.

3. Interpretação dos resultados: é realizada a interpretação dos dados levantados, de forma a levantar conclusões acerca do objetivo desta pesquisa.

4. ANÁLISE E DISCUSSÃO SOBRE OS RESULTADOS DAS ENTREVISTAS

4.1. Número de funcionários impactados

No Tribunal A, toda a organização, contando com mais de 5000 funcionários, foram prejudicados diretamente ou indiretamente pelo ataque, assim como os externos que compõem muitos usuários dos serviços prestados. No Tribunal B, com mais de 6000 funcionários, assim como Tribunal C com cerca de 15000 funcionários, também foram afetados da mesma forma.

Observa-se que as três empresas, de acordo com os seus gestores, tiveram a maioria de seus profissionais prejudicados pelos ataques cibernéticos, seja de forma direta, quando existe um impacto claro no próprio trabalho do colaborador, ou indiretamente, quando os acontecimentos influenciam de alguma forma em seus processos de trabalho, mas não envolvendo suas atividades diretamente. Foi possível observar alguns impactos com comentários relatados pelos gestores em relação a:

a. Indisponibilidade de acesso as máquinas, sistemas e até outros casos periféricos como telefones, entre outros;

b. Indisponibilidade de comunicação interna entre os funcionários;

c. Impossibilidade de tocar os processos de trabalho que dependem dessa estrutura tecnológica e de comunicação;

d. Impossibilidade de resolução do problema por parte de equipes não técnicas de TI, restando aguardar a área solucioná-lo.

Os gestores comentam que além dos tribunais, terceiros dependentes dos serviços prestado como advogados, assistentes jurídicos e administrativos, entre outros profissionais também foram prejudicados, pois a indisponibilidade dos sistemas e pela suspensão das atividades desses tribunais dificultaram a realização de seu próprio trabalho, que dependem dessas informações e decisões.

Discutindo-se sobre os resultados, é possível observar que as organizações perdem muito em termos de capacidade produtiva na realização dos serviços jurídicos

com os ataques, isso se deve principalmente pela capacidade de infecção em larga escala do vírus às máquinas, sistemas e redes de comunicação, as principais ferramentas de trabalho dos colaboradores (DA SILVA, 2018; SOUPAYA, 2018).

Parveen (2019) argumenta que os ataques de *ransomware* tem danos significativos às empresas, incluindo, a interrupção das atividades de negócio, que levam elas a terem gastos significativos para se recuperarem e voltarem a operar e, muitas vezes, contando com as perdas de receitas e de infraestrutura.

Pode-se observar que os efeitos negativos dos ataques vão além dos Tribunais, afetando também empresas privadas, profissionais autônomos e seus clientes que dependem dos serviços prestados por eles, impactando outros atores do setor Judiciário. De acordo com Dias (2020), que analisou os impactos que a interrupção do trabalho dos tribunais, alguns desses efeitos são:

a. Acúmulo de processos pendentes: um tribunal sem colaboradores para processar e julgar casos, as demandas pendentes tendem a ter sua solução atrasada, prejudicando os envolvidos.

b. Falta de acesso à justiça: Se um tribunal para de funcionar bem, as pessoas não possuem acesso a um bom mecanismo para resolver suas questões jurídicas, o que pode prejudicar a proteção de seus direitos, impactando negativamente a confiança da sociedade na justiça.

4.2. Indisponibilidade de softwares e hardwares.

Em termos de tempo de indisponibilidade dos softwares e hardwares utilizados nas organizações, na Tribunal A, todos foram impactados pelas ações de contenção e recuperação, o tempo de indisponibilidade variou entre 2 até 30 dias, tendo em vista que as infraestruturas e máquinas e colaboradores priorizados foram resolvidos primeiros. No Tribunal B, os funcionários tiveram uma média de 10 dias de indisponibilidade dos serviços e máquinas. E no Tribunal C, grande parte dos funcionários sofreram com a indisponibilidade do software operacional de suas

máquinas, a recuperação demorou cerca de 30 dias, porém, assim como o caso A, foi realizado uma análise de priorização para recuperar casos priorizados primeiro.

O tempo médio de indisponibilidade entre as organizações foi de cerca de 24 dias. Um ponto abordado, foi o processo de priorização, que obteve um papel importante de recuperar as máquinas e softwares mais essenciais proporcionando um retorno mais rápido de processos nas organizações em comparação as que não possuem tal planejamento.

Omar (2011) argumenta que situações de desastres e ataques vêm com a probabilidade de que dados importantes sejam perdidos de forma irrecuperáveis. A identificação de dados críticos e um plano claro de recuperação são essenciais para mitigar esse risco.

Vale ressaltar que o tempo médio de recuperação de backup de TI de uma grande empresa depende de vários fatores, incluindo seu porte, complexidade da rede, quantidade de dados a serem recuperados, a tecnologia de backup utilizada e a eficiência do processo de recuperação, por isso tão importante a definição de um plano claro como Omar afirmou no parágrafo acima.

4.3. Capacidade Produtiva da equipe de TI para lidar com o problema.

Foi questionado aos gestores se existiu a necessidade de ampliar a capacidade produtiva da equipe de TI para a recuperação do ataque, analisando se foram necessárias horas extras, contratação de serviços de terceiros como consultorias especializadas, entre outros serviços.

No Tribunal A, houve a contratação de uma consultoria técnica especializada em serviços de nuvem para ajudar com as políticas de segurança e trazer o conhecimento das melhores arquiteturas visando a recuperação mais segura possível, também ocorreu o aumento na carga-horária da equipe com horas extras. No Tribunal B, foram utilizados serviços externos, mas em contratos já existentes e com o apoio, sem custo, de empresas de TI. No Tribunal C, foi necessário o apoio de empresas terceirizadas especializadas em ataques cibernéticos e foi relatado a necessidade de

a equipe interna cumprir horas extras na busca de acelerar o processo de recuperação.

Observa-se que as organizações tiveram um impacto significativo em termos de necessidade de capacidade produtiva para lidar com ataques, relatando a necessidade de aumentar a carga horária da equipe de TI na própria organização e até mesmo de empresas terceirizadas contratadas. Tal necessidade de mão de obra, veio acompanhada com a demanda de pagamento de horas extras ou formação de banco de horas pelos colaboradores, despesas que refletem nas finanças das organizações.

Esses pontos vão de acordo com o estudo de Stanfill e Wall (2015) que investigou o impacto dos ataques cibernéticos na carga de trabalho da equipe de segurança de TI. Foi possível concluir que há:

a. Aumento da carga de trabalho: os ataques cibernéticos têm um impacto significativo na carga de trabalho da equipe de segurança de TI, aumentando o tempo e os recursos necessários para investigar e resolver os incidentes.

b. Aumento do desgaste da equipe: O estudo também destacou que os picos de exposição a incidentes de segurança cibernética podem levar ao desgaste da equipe, tornando-os mais propensos a erros e descuidos.

c. Necessidade de atentar-se à gestão da carga de trabalho: foi sugerido que a gestão eficaz dos colaboradores de TI é crucial para garantir a eficiência e a eficácia na resposta aos ataques cibernéticos.

De forma complementar, Knight, afirma que:

> de acordo com uma pesquisa da empresa de segurança Nominet, 88% dos Diretores de Segurança da Informação (CISOs) relataram sentir-se “moderadamente ou tremendamente estressados”. Esta é uma estatística preocupante em um trabalho de alta demanda, onde talento e habilidade são mais importantes do que nunca para manter as organizações seguras e fora da linha de fogo cibernética (KNIGHT, 2022, p.1).

4.4. Perda de dados

Foi questionado se as organizações tiveram perdas de dados relevantes da organização devido ao ataque cibernético.

No Tribunal A, não houve perdas de dados, softwares e máquinas. No Tribunal B, a maioria dos arquivos, sistemas possuíam backup, portanto, com a restauração, pouco foi perdido com o incidente. No Tribunal C, houve a perda de dados salvos localmente nas máquinas, que não faziam parte da política de backup, porém todos os outros arquivos que se localizavam na própria rede da organização, foram recuperados e sistemas e máquinas não foram prejudicados.

Portanto, de acordo com os gestores, as perdas foram mínimas, todas as organizações continham planos de restauração bem formulados e preparados que resultaram em perdas mínimas de dados.

Cada instituição possuí sua própria forma de restauração, algumas mais profundas, restaurando até mesmo dados locais das máquinas, já outras com um escopo de restauração menor, sendo elas as mais prejudicadas. O Tribunal C, foi o mais afetado, tendo em vista que arquivos salvos localmente nas máquinas foram perdidos e, como nem sempre os colaboradores salvam todos os arquivos em pastas da rede, houve a perda de um volume considerável de arquivos julgados pelos colaboradores como importantes.

Em termos de discussão dos resultados sobre a perda de dados, positivamente, a maioria das organizações conseguiram seguir as recomendações dadas pelas referências bibliográficas deste trabalho em relação ao plano de recuperação.

"As soluções de backup são essenciais para a proteção contra perda de dados em caso de incidentes cibernéticos, como ransomware, que podem criptografar ou excluir dados importantes." (CHOI, 2020, P. 240). Baryamureeba complementa que: "As soluções de backup devem ser implementadas como parte de uma estratégia de segurança cibernética abrangente, pois elas ajudam a minimizar o tempo de inatividade e a perda de dados em caso de incidentes cibernéticos" (BARYAMUREEBA, 2018, p. 128).

Apenas no caso do Tribunal C que, possivelmente, poderia ser planejado uma técnica de restauração mais ampla, também conseguindo salvar dados locais, ou principalmente, trazer mais ações de educação sobre a importância de todos os documentos serem salvos na rede, justamente para evitar sua perda nesses tipos de incidente.

4.5. Despesas oriundas dos incidentes

Foi questionado quais foram as despesas oriundas dos incidentes recebidos, em termos de manutenção de equipamentos, adquirir novos bens, contratações, horas extras, entre outros tipos de despesas.

No Tribunal A, não houve gastos com a aquisição e nem manutenção de bens, porém, houve a necessidade de contratação de equipe especializada externa e pagamento de horas extras (em caso de não conversão de banco de horas) para funcionários envolvidos na recuperação. Já no Tribunal B, além dos gastos já recorrentes com contratos existentes de apoio técnico, foram relatados gastos com novas soluções de segurança para a organização de alto valor agregado. No Tribunal C, não houve necessidade de gastos com equipamentos e manutenção de bens, porém houve a necessidade do pagamento de horas extras da equipe interna e com os serviços de empresas técnicas terceirizadas, inclusive, com o pagamento de horas extras para essas.

Quando perguntado sobre os valores gastos, os gestores afirmaram que não era possível repassar os gastos realizados especificamente com os incidentes de *ransomware* por questões de sigilo financeiro/contábil. Além disso, foi justificado que não é exatamente claro quais foram os gastos decorrentes apenas com os incidentes, pois já existem gastos recorrentes com salários, contratos com empresas terceiras já comuns à organização, não sendo uma tarefa fácil entender a porcentagem direcionada ao incidente.

Portanto, não foi possível realizar uma projeção de valor para as despesas durante e após o incidente, porém, observa-se que as organizações precisaram sim fazer investimentos, principalmente, de contratação de serviços técnicos para ajudar

com a restauração e com novas soluções de segurança para diminuir o risco de impacto em próximos incidentes, os gestores comentaram que esses gastos foram significativos para as organizações, principalmente em termos de aquisição de novas tecnologias e serviços.

Em termos de discussão, a coleta de dados financeiros é uma tarefa desafiadora, de acordo com Smith (2006), o sigilo financeiro pode ser uma questão fundamental para proteger a privacidade dos indivíduos e preservar a confiança nos sistemas financeiros.

Wilson (2009) complementa, trazendo que a proteção do sigilo financeiro é uma questão importante e crescente em todo o mundo, e que a obtenção de dados financeiros pode ser uma tarefa difícil devido às restrições legais e às barreiras técnicas enfrentadas.

4.6. Pagamento solicitado pelos criminosos

Em todos os casos, não foi realizado o pagamento solicitado pelos criminosos. Pelo fato das organizações possuírem um plano de defesa contra esse tipo de incidente, essa solução não foi levada em consideração pelos tomadores de decisões nessas empresas, sendo até mesmo comentado que não há aparato legal que possibilitassem a realização desse tipo de pagamento à criminosos.

As organizações agiram de forma correta tendo em vista o referencial teórico, de acordo com Hernandez, Cartwright, Stepanova (2017) pagar o resgate em incidentes de *ransomware* incentiva a continuação desses incidentes e sugere que eles são bem-sucedidos e lucrativos e não garante que os dados serão realmente restaurados, e pode até mesmo levar a futuros incidentes contra a mesma vítima.

E de acordo com uma pesquisa com 1.200 profissionais de segurança citados no estudo da Deloitte, não é recomendado que o resgate seja pago, especialmente porque não há garantias que os criminosos irão restaurar os dados, e a pesquisa indica que menos da metade das vítimas que decidiram pagar recuperaram o acesso aos seus dados. (DELOITTE, 2020).

5. CONCLUSÃO

No processo de estruturação do tema, foi verificado que já existiam diversos tipos de estudos já realizados com o enfoque na parte técnica direcionada as teorias que envolvem a área da Ciência da Computação, porém, poucos estudos continham um enfoque na ciência da Administração, principalmente, em termos de análise do impacto de produtividade da ocorrência deste tipo de incidente tendo em vista recursos financeiros, infraestrutura, pessoas e processos.

Dessa forma, este estudo objetivou explorar os impactos na produtividade dos tribunais brasileiros em decorrência de incidentes cibernéticos envolvendo ataques de *Ransomware*. Os resultados da pesquisa, permitiram cumprir, em parte, o objetivo, demonstrando de forma qualitativa quais são os impactos sentidos nos tópicos citados.

Além de entender os impactos nos Tribunais, o estudo permitiu uma amplificação do problema de pesquisa tendo em vista que os incidentes geraram, de forma temporária, a indisponibilidade da entrega dos serviços prestados pelos Tribunais para o setor Judiciário que envolve outras empresas públicas, privadas, profissionais e cidadãos.

É perceptível que este tema possui desafios significativos no que tange a coleta de dados e informações por ser um tema sensível e sigiloso. Isso acontece, pois o compartilhamento sobre a forma de pensar e agir em relação à cibersegurança podem ser um próprio motivo para comprometê-las. Como resultado desse fator, foram encontradas dificuldades de aprofundar em perguntas e respostas.

Dessa forma, um ponto de melhoria em relação à pesquisa seria a busca por mecanismos de coleta de dados que consigam aprofundar mais nas perguntas e respostas, garantindo a segurança dos entrevistados. Além disso, em futuras pesquisas poderiam ser incluídos gestores de outras áreas como a de Recursos Humanos, Financeiro/Contábil e áreas especificas que lidam com processos para responder sobre os impactos e ações tomadas em relação a esses incidentes.

Portanto, este estudo deixa uma abertura para a realização de novas pesquisas e trabalhos acadêmicos sobre o tema, principalmente, com o aprofundamento das perguntas em outras áreas das organizações, trazendo uma visão mais ampla e profunda ao mesmo tempo com dados qualitativos e quantitativos que possam ajudar a entender de forma mais completa os impactos dos incidentes gerados por ataques do tipo *ransomware*. Além disso, a oportunidade de pesquisar o tema em um contexto maior, macroeconômico, envolvendo também organizações externas que possuem relação com os serviços prestados pelos Tribunais.

Por fim, como contribuição maior, este estudo oferece, acima de todas conclusões e dificuldades, uma visão mais ampla e gerencial sobre os impactos que o tipo de incidente cibernético de *ransomware* podem gerar nas organizações, principalmente da justiça brasileira, mostrando que esse ataque é de preocupação por todos os colaboradores da organização, indo além de apenas uma questão técnica discutida pela área da Tecnologia da Informação.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação.** Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC27001. Rio de Janeiro, 2013.

ALMEIDA, J. DE J. et al. Crimes cibernéticos. **Caderno de Graduação - Ciências Humanas e Sociais - UNIT - SERGIPE**, v. 2, n. 3, p. 215–236, 25 mar. 2015.

ANTONOPOULOS, Andreas M. **Mastering Bitcoin: unlocking digital cryptocurrencies**. " O'Reilly Media, Inc.", 2014.

BARDIN, L. **Análise de Conteúdo**. São Paulo: Almedina Brasil, 2016.

BARYAMUREEBA, V. **Cybersecurity for businesses: Policy, technology, and culture**. International Journal of Information Management, 38(1), 123-135, 2018.

BASTOS, Alberto; CAUBIT, Rosângela. **ISO 27001 e 27002 Uma Visão Prática**. Porto Alegre: Modulo, 2009.

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas S.A., 2008.

BÉLANGER, F., GOSSELIN, É., & RICO, M. **Cybersecurity risk management: A review of literature**. Journal of Information Privacy and Security, 15(2), 103-131, 2019.

BITDEFENDER. **Bitdefender PR Whitepaper August Connect**, 2016.

BITDEFENDER. **Bitdefender Mid-Year Threat Landscape Report**, 2021. Disponível em: https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf. Acesso em: 14 de dezembro. 2022.

BRASIL. **Código Penal**. Planalto, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em: 8 de Setembro, 2022.

BRASIL. **Doutrina Militar de Defesa Cibernética**, Exército Brasileiro, 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf.

BRASIL. Portaria CDN nº14, de 11 de maio de 2015. **Homologa a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018**. Diário Oficial da União. Brasília, DF, 2015. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf . Acesso em: 14 dez. 2022.

BRASIL. **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos. Governo do Brasil**, Disponível em:: https://www.gov.br/pt-br/noticias/justica-eseguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso em: 9 Set. 2022.

BURITI, **Qual é a diferença entre segurança cibernética e segurança da informação?**, 2021. Recuperado de: https://burititecnologia.com.br/qual-e-a-diferenca-entre-seguranca-cibernetica-e-seguranca-da-informacao/. Acesso em: 24 dez. 2022.

CAIÇARA, J. **Informática, Internet e Aplicativos**. São Paulo: Editora não identificada, 2007.

CANONGIA, C., & MANDARINO Junior. **Segurança cibernética: o desafio da nova Sociedade da Informação.** Disponível em: http://www.campus-party.com.br/index.php/release. Acesso em: 7 Jan. 2023.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura**. Volume I: A sociedade em rede. 3ª Ed. São Paulo: Paz e Terra, 1999.

CEBROWSKI, A. K. **Transformation and the Changing Character of War? Transformation Trends, Office of Transformation, Department of Defense.**

Disponível em: www.hsdl.org/?view&did=448180 [Artigo em site]. Acesso em: 21 Jan. 2023.

CERT.BR**. Estatísticas de Incidentes 2020**, 2021. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 7 dez. 2022.

CERVO, Amado Luis BERVIAN, A. **Pesquisa em ciências humanas e sociais** (5ª ed.). São Paulo: Cortez Editora. [Livro], 2001.

CERVO, Amado Luiz, BERVIAN, Pedro Alcino. **Metodologia científica**. 5ª ed. São Paulo: Prentice Hall, 2002.

CHANG, Edward C. **Cryptographic protection of data integrity in cloud computing.** Information Sciences**,** n.497, p 93-104, 2019.

CHAPPLE, Mike. **CompTIA security+ study guide**. John Wiley & Sons, 2017.

CHEN, Wei. **Information security principles and practices**. Jones & Bartlett Publishers, 2019.

CHOI, J., LEE, D., LEE, Y., & KIM, K. **Developing a Framework for Ransomware Response and Recovery**. Journal of Cybersecurity, 6(1), 1-13, 2020.

CISO. **Superior Tribunal de Justiça travado por ataque cibernético**, 2020. Disponível em: https://www.cisoadvisor.com.br/superior-tribunal-de-justica-travado-por-ataque-cibernetico/. Acesso em: 12 nov. 2022.

CYNTHIA, J. **Security protocols for IoT. In: Ubiquitous computing and computing security of IoT**. 1-28, 2019.

DE ARAUJO, Fábio Lucena. Aspectos jurídicos no combate e prevenção ao *ransomware*. **Revista da pós-graduação lato sensu em direito da Estácio**, v. 1, n. 1, p. 67-93, 2019.

DIAS, Victor. **A covid-19 e seus impactos no processo civil**. Revista de Processo. p. 351-368, 2020.

EUROPEAN COMMISSION. **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. High Representative of the European Union for Foreign Affairs and Security Policy,** 2013. Disponível em: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667. Acesso em: 02 de abr. de 2022.

FERBRACHE, D. **A practical guide to cyber security risk management**. Kogan Page, 2019.

FERREIRA, Fabiano Santana. **A política de segurança da informação do tribunal de justiça da Paraíba: uma análise baseada na NBR ISO 27002**. 2015.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

FRUHLINGER, J. **Os 6 maiores ataques de *ransomware* dos últimos 5 anos.** IT Forum. Disponível em: https://itforum.com.br/noticias/os-6-maiores-ataques-de-ransomware-dos-ultimos-5-anos/, 2019.

GARCIA, J, HERRERA, J., LIVRAGA, G. **Cybersecurity threats, challenges, opportunities and vulnerabilities**. Security and privacy trends in the industrial internet industry (pp. 1-30). Springer International Publishing, 2016.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 5. ed. São Paulo: Atlas, 1999.

GOLLMANN, D. **Computer Security – ESORICS 2017**. Volume 10493. Springer. ISBN 978-3-319-66398-2. 2017.

HERNANDEZ-CASTRO, J.; CARTWRIGHT, E.; STEPANOVA, A. **Economic analysis of *ransomware***. arXiv preprint arXiv:1703.06660. 2017.

IEEE INSTITUTE, KHASHIROVA, T. Y.; MAMUCHIEV, I. I.; MAMUCHIEVA, M. I.; OZHIGANOVA, M. I.; KOSTYUKOV, A. D.; SHUMEIKO, I. **Assessment of information security in integrated systems**, 2016.

INTERNATIONAL CONFERENCE ON QUALITY MANAGEMENT, TRANSPORT AND INFORMATION SECURITY, INFORMATION TECHNOLOGIES (IT&QM&IS),

Yaroslavl. Proceedings. IEEE, p. 201-205. doi: 10.1109/ITQMIS53292.2021.9642824, 2021.

INTERNATIONAL ASSOCIATION OF COMPUTER SECURITY PROFESSIONALS (IACSP). [2013].

ISO/IEC. **ISO/IEC 27032:2012(E) information technology e security techniques e guidelines for cybersecurity**. Geneva, Switzerland: ISO/IEC. 2012.

KASPERSKY. **Top *ransomware* 2016, 2016.** Disponível em: https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2016. Acesso em: 23 dez. 2022.

KIM, W. **A survey on availability in cloud computing.** Journal of Network and Computer Applications, 116, 118-130, 2018.

KLIMBURG, A. **National Cyber Security Framework Manual**, 2012. Disponível em: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. Acesso em: 7 jan. 2023.

KNIGHT, K. **The Impact Of Cyberattacks On IT Security Professionals' Mental Health, 2022.** Disponível em: https://www.forbes.com/sites/forbestechcouncil/2022/08/17/the-impact-of-cyberattacks-on-it-security-professionals-mental-health/?sh=1298f1721bb9. Acesso em: 19 dez. 2023.

KSHETRI, N. **Blockchain's roles in meeting key supply chain management objectives**. International Journal of Information Management, 37(2), 123-135, 2017.

LONGHURST, R. **Key Methods in Geography: Semi-structured Interviews and Focus Groups**. SAGE Publications, 2010.

SCHMIDT, G. **Crimes cibernéticos**. Jusbrasil, 2014. Disponível em: http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 20 nov. 2014.

SILVA, R**. Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

SILVA, E. L. da. & MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. Florianopolis: UFSC/PPGEP/LED, 23 p., 2000.

STAKE, R. E. **The art of case study research**. Thousand Oaks: SAGE Publications, 1995.

MANZINI, E. J. **A entrevista na pesquisa social**. Didática, São Paulo, v. 26/27, p. 149-158, 1991.

MERRIAM, S. B. Qualitative research and case study applications in education. San Francisco: Jossey-Bas, 1998.

MICROSOFT. **Microsoft Digital Defense Report 2022**, 2022. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us. Acesso em: 4 jan. 2023.

MITTAL, P. **Integrity protection of outsourced data in cloud computing**. ACM Computing Surveys (CSUR), v. 51, n. 4, p. 1-33, 2019.

MINAYO, M. C. de S. **O desafio do conhecimento: pesquisa qualitativa em saúde** (4th ed.). HUCITEC/ABRASCO, 1996.

MOHURLE, S. **A brief study of wannacry threat: Ransomware attack**. Sbgsmedia, 2017. Disponível em: https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf. Acesso em: 23 nov. 2022.

MOURA, R. **A impunidade dos hackers que colocaram o Judiciário de joelhos.** VEJA, 2022. Disponível em: https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/. Acesso em: 11 abr. 2022.

National Institute of Standards and Technology (NIST). Glossary. 2023, Disponível em: https://csrc.nist.gov/glossary/term/incident. Acesso em: 16 fev. 2023.

OMAR, Adnan; ALIJANI, David; MASON, Roosevelt. **Information technology disaster recovery plan: Case study**. Academy of Strategic Management Journal, 10(2), 127, 2011.

REVISTA CONSULTOR JURÍDICO, ConJur - **Após ataque hacker, sistemas do TRF-3 continuam fora do ar,** 2022. Disponível em: https://www.conjur.com.br/2022-abr-06/ataque-hacker-sistemas-trf-continuam-fora-ar. Acesso em: 23 out. 2022.

RICHARDSON, R, NORTH, M. ***Ransomware*: Evolution, Mitigation and Prevention**, 2017. Disponível em: https://digitalcommons.kennesaw.edu/facpubs/4276. Acesso em: 06 dez. 2022.

SANDHU, Ravi. **Access control models and technologies**. Springer, 2016.

SANTOS, G. **General detalha implantação do centro de defesa cibernética, novo órgão brasileiro**,. Folha de S. Paulo, 2012. Disponível em: URL. Acesso em: 23 dez. 2022

SASTRY & AKASHDEEP & VINAY. ***Ransomware* Digital Extortion**, 2016. Disponível em: https://doi.org/10.17485/ijst/2016/v9i14/82936. Acesso em: 17 out. 2022.

SAVAGE, K. **The evolution of *ransomware***. In Symantec SECURITY RESPONSE (Ed.), 2015.

SECURITY WEEK, **Artigos sobre ataques de *ransomware***, 2020. Disponível em: <https://www.securityweek.com/category/ransomware/>. Acesso em: 21 Jan. 2023.

SECURITY WEEK, ***Ransomware* Hit 200 US Gov, Education and Healthcare Organizations in 2022**, 2023. Disponível em: https://www.securityweek.com/ransomware-hit-200-us-gov-education-and-healthcare-organizations-2022/. Acesso em: 21 Jan. 2023.

SILVA, W. Rodrigues. **Análise econômica dos impactos de ataques cibernéticos**. 2018. Disponível em: https://repositorio.unb.br/handle/10482/34838. Acesso em: 5 dez. 2022.

SOMMERVILLE, I. **Engenharia de software**. 8. ed. Pearson Addison-Wesley, 2007.

SOMMERVILLE, Kerry L. **Hospitality employee management and supervision: concepts and practical applications**. John Wiley & Sons, 2007.

SOUPPAYA, Murugiah. **Cybersecurity for infrastructure protection**. NIST SP 800-82 R2, 2015.

STANFILL, John D.; WALL, Thomas J**. The impact of cyber attacks on the workload of IT security teams**. Journal of Cybersecurity, v. 1, n. 1, p. 31-40, 2015.

STJ. Comunicado: **Em razão de ataque cibernético, STJ funcionará em regime de plantão até o dia 9**. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx. Acesso em: 11 out. 2022.

SURESH, M. ***Ransomware*: current trends, challenges, target areas, and its prevention.** 2020. Disponível em: http://fir.ferris.edu:8080/xmlui/handle/2323/6941. Acesso em: 30 out. 2022.

TANG, Mincong; LI, Meng'gang; ZHANG, Tao. The impacts of organizational culture on information security culture: a case study. **Information Technology and Management**, v. 17, p. 179-186, 2016.

THE COUNCIL OF ECONOMIC ADVISERS. **The cost of malicious cyber activity to the U.S economy**. 2018. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Acesso em: 23 dez. 2022.

TILT. **Ministério da Saúde e Tesouro nacional sofre ataque hacker; entenda como ameaça ransomware age**. UOL, 2021. Recuperado de https://www.uol.com.br/tilt/noticias/redacao/2021/12/10/ministerio-da-saude-sofre-acao-hacker-entenda-como-a-ameaca-ransomware-age.htm.

Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT). **Extorsão x Extorsão mediante sequestro x Sequestro e cárcere privado. Tribunal de Justiça Do Distrito Federal e Dos Territórios,** 2020. Recuperado de https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/extorsao-x-extorsao-mediante-sequestro-x-sequestro-e-carcere-privado.

UOL. **TRF-3 segue fora do ar sete dias após ataque hacker; saiba o que rolou**. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2022/04/06/ataque-hacker-trf3-prazos-o-que-aconteceu.htm>. Acesso em: 12 out. 2023.

VIEIRA, M. M. F., & Zouain, D. M. **Pesquisa qualitativa em administração: teoria e prática**. Rio de Janeiro: Editora FGV, 2005.

VOLPI, M. T., & Volpi, M. A. ***Ransomware* no ordenamento jurídico brasileiro**. revistajudiciaria.com.br, 79, 2021.

WHITMAN, M. E., & MATTORD, H. J. **Roadmap to Information Security: For IT and Infosec Managers**. Cengage Learning, 2012.

WHITMAN, M. E., & MATTORD, H. J. **Principle of Information Security**. Thomson Course Technology, 2012.

WILSON, M. **Financial privacy and the challenges of data collection**. Journal of Financial Regulation and Compliance, 2009.

WOLOSZIN, A. L. A. **A ameaça invisível do terror cibernético**. Jornal do B. Internacional, 2009.

XIAO, J. **Data Integrity in Cloud Storage**. ACM Transactions on Storage, 14(2), 1-23, 2018.

YIN, R. K. **Case study research and applications: Design and methods**. Sage publications, 2018.

ZANELLA, Liane Carly Hermes et al. **Metodologia da pesquisa**. SEAD/UFSC, 2006.

ZETTER, K. **Hacker lexicon: A guide to Ransomware, the scary hack that's on the rise**. 2015.

7. APÊNDICE

7.1. Questionário utilizado nas entrevistas.

Descoberta do ataque e primeiras atitudes

Como foi descoberto o ataque cibernético?

Quais foram as ações tomadas ao ver que a organização estava sendo atacada?

Impactos sobre as pessoas e capacidade produtiva

Toda a organização foi impactada pelo ataque ou apenas áreas/colaboradores específicos?

Qual o número médio de funcionários que foram impactados?

Devido ao ataque, os colaboradores ficaram sem trabalhar devido à indisponibilidades de máquinas e sistemas? Quanto tempo?

Impactos nos sistemas e dados da organização

Existem softwares/serviços externos que são pagos e não puderam ser utilizados pelos funcionários em decorrência do ataque cibernético?

Algum software ou dados relevantes para o trabalho dos funcionários foram perdidos com a ocorrência do ataque?

Impactos financeiros na empresa

Quais foram as despesas que o ataque gerou? Existiram despesas com horas extras, contratação de serviços de terceiros como consultoria, recuperação de arquivos, cibersegurança, entre outros?

Houve aumentos de despesas na empresa em relação a manutenção de equipamentos ou até mesmo a necessidade de adquirir novos bens após o ataque?

Houve algum outro tipo de despesa não questionada? Caso não tenha sido comentado, foi realizado o pagamento solicitado pelos criminosos?