CENTRO UNIVERSITÁRIO DOM BOSCO
CURSO ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PAULO GIOVANNY SIPAÚBA MAGNO

CONTRASTES ENTRE A ATUAL SITUAÇÃO DA SEGURANÇA DA INFORMAÇÃO NACIONAL E AS MEDIDAS GOVERNAMENTAIS TOMADAS: uma análise dos mais recentes ataques cibernéticos no Brasil

São Luís
2022

PAULO GIOVANNY SIPAÚBA MAGNO

CONTRASTES ENTRE A ATUAL SITUAÇÃO DA SEGURANÇA DA INFORMAÇÃO NACIONAL E AS MEDIDAS GOVERNAMENTAIS TOMADAS: uma análise dos mais recentes ataques cibernéticos no Brasil

Monografia apresentada ao Curso de Análise e Desenvolvimento de Sistemas do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.
Orientador: Prof. Esp. Francisco de Assis Silva Moura Junior.

São Luís
2022

Dados Internacionais de Catalogação na Publicação (CIP)
Centro Universitário – UNDB / Biblioteca

Magno, Paulo Giovanny Sipaúba

Contrastes entre a atual situação da segurança da informação nacional e as medidas governamentais tomadas: uma análise dos mais recentes ataques cibernéticos no Brasil. / Paulo Giovanny Sipaúba Magno. __ São Luís, 2022.

43 f.

Orientador: Esp. Francisco de Assis Silva Moura Junior.

Monografia (Graduação em Sistemas de Informação) - Curso Tecnológico de Análise e Desenvolvimento de Sistemas - Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB, 2022.

1. Segurança da informação. 2. Ataques Cibernéticos.
3. Orçamento público. I. Título.

PAULO GIOVANNY SIPAÚBA MAGNO

CONTRASTES ENTRE A ATUAL SITUAÇÃO DA SEGURANÇA DA INFORMAÇÃO NACIONAL E AS MEDIDAS GOVERNAMENTAIS TOMADAS: uma análise dos mais recentes ataques cibernéticos no Brasil

Monografia apresentada ao Curso de Análise e Desenvolvimento de Sistemas do Centro Universitário Dom Bosco como requisito parcial para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Aprovada em: 27 de junho de 2022.

BANCA EXAMINADORA:

_____

Prof. Esp. Francisco de Assis Silva Moura Junior (Orientador)

Especialista em Ciência de Dados

Centro Universitário Dom Bosco (UNDB)

_____

Prof. Me. Alysson Marquezelli Simeao Almeida

Mestre em Engenharia da Computação e Tecnologia da Informação

Centro Universitário Dom Bosco (UNDB)

_____

Prof. Dr. Giovanni Lucca França da Silva

Doutor em Engenharia Elétrica, Visão Computacional e Machine Learning

Centro Universitário Dom Bosco (UNDB)

Dedico a minha esposa, pais, irmãos, amigos e *pets*.

AGRADECIMENTOS

Agradeço a minha esposa por me forçar a aceitar quem eu sou, por ter aceitado caminhar comigo pelas pedras, e por ser um exemplo inatingível e incansável de dedicação e excelência em praticamente tudo, menos cantar e brincadeira com bola.

Aos meus pais, por terem me apoiado enormemente na segunda graduação e por me ajudarem sempre.

Ao meu irmão, por ser meu melhor amigo e um ideal de ser humano e por ter me incentivado a perseguir esse futuro.

Aos meus amigos André, Felipe, Henrique e Rafael por serem muito mais do que isso.

Aos meus amigos e colegas da faculdade, que agradeço na pessoa de Paulo Marques e Yuri Ageme por terem me acolhido no grupo, por termos compartilhado juntos as alegrias e desabores dessa jornada.

Aos professores da UNDB, que agradeço na pessoa de Pedro Henrique, Maurícios Morais, Alessandro Miranda, Allan Cruz, Giovanni Lucca, Alysson Almeida, Alysson Marquezelli pelos transmissão dos ensinamentos técnicos e empíricos.

Ao professor Igor Cavalcanti, por ter se tornado para mim um modelo de desenvolvedor a alcançar e por ser um poço inesgotável de conhecimento e experiência.

Ao coordenador do curso de Análise e Desenvolvimento de Sistemas Rodrigo Monteiro, por acreditar no meu potencial e pelo apoio constante.

Ao meu orientador Francisco Moura, pela ajuda nesse trabalho de conclusão de curso.

Só existem dois tipos de empresas: as que foram hackeadas e as que ainda serão.

Robert S. Mueller

Eu não sou um excelente programador; eu sou somente um bom programador com excelentes hábitos.

Kent Beck

LISTA DE FIGURAS

SUMÁRIO

CONTRASTES ENTRE A ATUAL SITUAÇÃO DA SEGURANÇA DA INFORMAÇÃO NACIONAL E AS MEDIDAS GOVERNAMENTAIS TOMADAS: uma análise dos mais recentes ataques cibernéticos no Brasil[1]

DISPARITIES BETWEEN THE CURRENT SCENARIO OF THE NATIONAL SECURITY OF INFORMATION AND GOVERNMENTAL MEASURES: an analysis of the recent cyber-attacks perpetrated against Brazilian state agencies

Paulo Giovanny Sipaúba Magno[2]

Prof. Esp. Francisco Moura[3]

RESUMO

O presente artigo discute o tema da segurança da informação e descreve a maneira como é tratado no Brasil. O cenário atual é o do aumento da relevância da informação, a interconectividade trazida pela internet, pela proliferação de dispositivos eletrônicos e pelo número crescente de novas redes sociais e os riscos à segurança da informação que surgem em meio a isso. Assim, objetiva-se analisar qual a postura do governo sob os aspectos orçamentário e normativo em cotejo ao que se experiencia na prática. Para tanto, faz-se uma análise sobre o termo informação, entendendo sua importância atualmente. Em seguida, examina-se o tema da segurança da informação e o aumento de sua relevância para as organizações. Por fim, relacionam-se os ataques cibernéticos desde 2019 até 2022, a plataformas da Administração Pública Federal, aos dados concernentes ao orçamento público na área da tecnologia da informação e opiniões de especialistas e profissionais da área. Conclui-se que a despeito do aumento no número de incidentes de segurança, os investimentos públicos diminuíram, o que demonstra um contraste em relação à gravidade da questão, a propostas do próprio governo e às ações efetivamente tomadas. Para tanto, utiliza-se o método hipotético-dedutivo para chegar a conclusões obtidas a partir dos dados, sendo estes provenientes de pesquisa bibliográfica e documental.

Palavras-chave: Segurança da Informação. Ataques Cibernéticos. Orçamento Público.

ABSTRACT

[1] *Paper* apresentado à disciplina Trabalho de Conclusão de Curso do Curso de Análise e Desenvolvimento de Sistemas do Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB.

[2] Graduando do 5º Período do Curso de Análise e Desenvolvimento de Sistemas do Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB. E-mail: pgs.magno@gmail.com.

[3] Professor Especialista. Docente do Curso de Análise e Desenvolvimento de Sistemas do Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB. E-mail: francisco.junior@undb.edu.br.

The following paper discusses the topic of security of information and describes the way in which it is addressed in Brazil. The main objective is to analyze the government's position when it comes to public budget and legislation, which is then compared with the incidents of security and the opinions of professionals and specialists of the field. To do so, an analysis of the term information and what it entails is performed. Then, an examination of security of information and its current rise in prominence is made. Finally, a collection of the all the nation-wide security incidents from 2019 to 2022, perpetrated against federal agencies, is assembled and contrasted against the investments made. The conclusion is that, although the number of incidents tend to increase, the investments show a decrease, which demonstrate a discrepancy between governmental planning and theory, and experience.

Keywords: Security of Information. Cyber attack. Public budget.

1 INTRODUÇÃO

Sabe-se que a informação é hoje um dos ativos mais valiosos para toda sorte de organizações, sejam elas privadas, com ou sem fins lucrativos, sejam elas públicas, cujos fins se materializam na realização de políticas públicas. No caso das empresas privadas, há mercados que lidam especificamente com a compra e venda de informações. Quando a informação não é o produto a ser comercializado, ela também se apresenta na forma de informação privilegiada acerca dos mais diversos temas, conferindo vantagem ao seu detentor e se tornando, em muitos casos, a diferença entre fortuna e ruína de um negócio (SZCZEPANSKI, 2020, p. 4).

Isso ocorre pois, em mundo absolutamente conectado, no qual as relações se dão de modo instantâneo e em nível global, a indisponibilidade da informação, por poucas horas que seja pode representar resultados catastróficos para os balanços de empresas[4], seja na perda de clientes seja em danos causados a pessoas que vão de danos materiais a até físicos e, no limite, a morte, quando se leva em consideração a queda de serviços hospitalares ou aeroportuários[5], por exemplo.

Por esses motivos, o elevado valor conferido à informação traz não somente vantagens competitivas, mas também ameaças àqueles que a possuem, manipulam ou são de algum modo compelidos a entregar a terceiros. Basta considerar que o cadastro mais simples em um aplicativo de refeições exige várias informações

[4] As Lojas Americanas S/A estimam perda de 250 milhões por site fora do ar: https://www.tecmundo .com.br/Mercado/234286-americanas-acumula-prejuizo-r-250-milhoes-sites-offline.htm

[5] O desastre áereo do Voo Gol 1907 se deu, em parte, pela falta de comunicação entre as aeronaves e as torres: https://g1.globo.com/mt/mato-grosso/noticia/2021/09/29/voo-1907-tragedia-que-matou-154-pessoas-em-mt-completa-15-anos.ghtml

críticas à segurança do cliente como CPF, endereço, telefone ou dados de cartões de créditos, sendo todas estas informações que poderiam gerar sérios prejuízos se utilizadas de forma descuidada ou de algum modo captadas por indivíduos mal-intencionados.

Desta forma, sendo a informação assim tão estimada, certamente um conjunto de medidas devem ser desenvolvidas para salvaguardá-las. Esse é precisamente o objeto de estudo da área de segurança da informação.

Assim, ao se reconhecer a importância desse tema para as pessoas, tanto físicas quanto jurídicas, e neste último caso, as de direito público, unindo-se ao campo de segurança, é feito o recorte deste trabalho, o qual terá como objetivo precisamente analisar como o Estado brasileiro vem lidando com o tema da segurança da informação (ou falta dela), considerando o que se prevê na teoria e o que se experiencia na prática, cotejando as políticas de segurança e os incidentes e ataques cibernéticos que vêm ocorrendo cotidianamente nos últimos anos contra plataformas públicas das mais diversas entidades públicas federais.

Partindo-se desse recorte, indaga-se se o Brasil está no rumo correto no que tange o resguardo da informação de que tem posse enquanto detentor de imensos cadastros de brasileiros. A hipótese que se levanta é que a segurança da informação é atualmente o elo mais fraco da corrente quando se fala em garantia de do sigilo de dados, o que implica dizer que a não implementação de robustos sistemas de gestão da segurança, a redução dos investimentos em material e pessoal representam ameaças imensuráveis àqueles que são, pela natureza da relação jurídica, obrigados a confiar suas informações ao Estado, como se poderá observar pelo relato dos casos de falhas de segurança que vêm sido registrados de forma cada vez mais numerosa nos últimos tempos.

Esta hipótese é submetida a teste por meio do desenvolvimento de uma análise que parte da construção de objetivos que são cumpridos no decorrer deste trabalho. Propõe-se, como objetivo geral, analisar, sob os aspectos legais, orçamentários, empíricos e técnicos, como se encontra o tema da segurança da informação no Brasil em nível federal em vista dos mais recentes ataques cibernéticos.

Para a consecução deste objetivo, são traçados os objetivos específicos que se seguem: na primeira subseção, apresentar o conceito de informação e demonstrar sua importância nos dias atuais; na segunda, examinar o tema da

segurança da informação, o que significa em termos práticos e como alcançá-la; e, por fim, na terceira, investigar como, na realidade, a segurança da informação se dá no Brasil, relacionando leis, notícias e análises de especialistas.

Pelo exposto, torna-se evidente que a avaliação mais detida sobre os riscos de segurança da informação para a coletividade justifica a produção deste artigo. Os impactos do apagão de dados sobre a COVID-19, os inúmeros casos de incidentes de segurança, os ataques cibernéticos e os vazamentos de dados de milhões de brasileiros revelam a necessidade de se analisar mais profundamente o tema e reavaliar se as recentes e vertiginosas reduções de investimentos na área de tecnologia da informação e comunicações, dos setores principalmente da saúde, representam um passo na direção de remediar esse cenário.

O método utilizado é o hipotético-dedutivo, porquanto se parte de uma hipótese proposta como possível solução de um problema, a qual é submetida a teste por meio da análise de argumentos retirados da bibliografia especializada a fim de confirmá-la ou refutá-la. A técnica de pesquisa, como previamente aludido, é a bibliográfica e documental, pois foi realizada ampla coleção de documentos, livros, revistas e notícias disponíveis na internet.

Dito isso, passa-se a analisar detidamente os tópicos elencados como alvo de cada objetivo específico, iniciando-se por um exame do termo informação e sua importância. Em seguida, trata-se do tema da segurança da informação e seus conceitos basilares. Por fim, realiza-se um apanhado sobre os aspectos mais importantes desse tópico no Brasil, relacionando orçamento público, legislação, prática, opiniões de especialistas e os incidentes de segurança.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 DADOS E INFORMAÇÃO: objeto, *commodity*, bem jurídico

Dados são o novo petróleo
Clive Humby

A informação possui hoje uma relevância tão grande na vida em sociedade que, como todo assunto que assume papel de destaque, ganhou um campo próprio de estudo. Esse campo, a ciência da informação, não é exatamente algo novo. Segundo Saracevic (2009), essa ciência cuida da coleta, armazenamento,

recuperação e uso da informação. A informação pode se revelar sob várias formas, porém a ciência da informação está interessada principalmente na informação que pode ser gravada e em conhecimento, além das tecnologias e os serviços relacionados que permitem e facilitam o seu gerenciamento e uso.

O mesmo autor relata o contexto no qual a informação enquanto objeto de estudo se formou citando o pós-Segunda Guerra Mundial como o marco histórico de transição entre a visão que se tinha sobre esse tema e os contornos que passou a ter, embora o uso do termo em si possa ser observado a partir do início dos anos 60 daquele século.

Dito isso, convém então tentar entender melhor qual é o objeto de estudo dessa ciência. Tuomi (1999) relembra a ideia tradicional de informação quando afirma que a percepção comum que se tem é de uma hierarquia entre dados, informação e conhecimento. Entende-se que, do menor para o maior, em termos de complexidade, temos dados, seguidos de informação e por fim conhecimento. O autor vai além ao dizer que a análise que se faz normalmente envolve dizer que os dados são fatos simples, a informação é uma estruturação desses dados e o conhecimento se revela ao aplicar sobre elas interpretação, contextualização e significado.

Assim, na visão tradicional do que se entende por informação, este termo faz parte de um conceito mais amplo. A informação entendida como uma amálgama de dados. Os dados são a menor unidade possível no qual algo mais pulverizado do que informação pode ser armazenado. Dados são então como átomos dispersos e que por si, nas palavras de Corea (2019), não possuem nenhum significado se não lhe forem feitas as perguntas corretas.

É por isso que quando se fala em dado não se fala ainda em informação. A informação é o produto de um processamento exercido sobre os dados, o que representa no mínimo uma consideração de vários dados em conjunto; informação é, portanto, uma soma que representa algo maior e mais complexo do que a mera junção das partes. Neste ponto abandona-se uma visão atômica para partir para uma visão molecular. Essa molécula possui um significado, utilidade ou propósito relevante que é dado pela organização e ordenação de seus átomos e que constitui um consenso para um determinado público-alvo (SORDI, 2015, p. 48-50).

Por fim, na etapa final, tem-se que informações se misturam e são posicionadas, ordenadas e estruturadas, analisadas em um determinado contexto, interpretadas sob uma determinada perspectiva, para então ser proposta uma

afirmação sobre a realidade ou tomada alguma decisão. É aquilo a que se dá o nome de conhecimento e finalizando a alegoria dos átomos e moléculas, é como se aqui surgisse um organismo (CASTRO; FERRARI, 2016, p.42).

Feitas essas considerações, deve-se tentar entender qual o problema que esse campo pretende resolver e as soluções por ele propostas. Segundo Saracevic (2009), o problema se trata da explosão da informação e a tecnologia da informação como uma solução para ele. Essa explosão é observada já no início do século XX por meio do aumento exponencial do número de publicações e registros de toda natureza e continua hoje de forma ainda mais acelerada por conta das novas formas através das quais a informação pode ser criada e consumida. Luciano Floridi (2010, p. 9) comentando a dependência das atuais sociedades da informação desse tipo de matéria-prima, afirma que no mínimo 70% do PIB de todos os países que compõem o G7 é formado por ativos intangíveis de informação, em contraste a ativos materiais fruto da manufatura ou agricultura, e que o crescimento e funcionamento desses países está intimamente ligado à constante produção de enormes volumes de dados, a qual a humanidade jamais presenciou nessa escala no decorrer de sua história.

Essa aceleração pode ser analisada inclusive em tempo real por meio de projeções. Acessando-se plataformas como o *website Internet Live Stats*[6], é possível observar diversas métricas como o número de *e-mails* enviados, buscas realizadas no motor de buscas Google, número de sites criados, *tweets* (mensagens escritas na plataforma Twitter), dentre vários outros, todos eles dados gerados por segundo. Somente na data deste escrito (10 de abril de 2022), para se ter uma ideia do volume de dados, estima-se que foram enviados mais de 237 bilhões de *e-mails*.

Assim, em vista desse surpreendente número de dados, de forma mais recente na história, surge o campo de *Big Data*. Esse por sua vez é caracterizado pela análise de coleções de dados que diante de seu imenso volume, velocidade de criação e variedade, torna-se difícil demais para armazenar, gerenciar, processar e analisar utilizando técnicas e ferramentas tradicionais (BAHGA; MADISETTI, 2019). Já Corea (2019, p. 13) define esse campo como uma nova abordagem definida pelo uso de tecnologias diversas com o intuito de extrair algum tipo de entendimento de dados pulverizados, ou seja, em sua maior granularidade, o que ele chama de dado de baixo valor. Além disso, uma característica relevante seria a incapacidade desses dados de

[6] https://www.internetlivestats.com

serem abarcados pelos sistemas de bancos de dados tradicionais. A existência dessa área de estudo se deve precisamente pela forma como a informação é vista, que segundo o autor (2019, p. 14), trata-se de um novo tipo de capital, uma moeda de troca diferente das demais, ou mesmo uma nova fonte de valor e que hoje permeia uma pletora de áreas de interesse e estudo tais como saúde, biologia, governo, mercado financeiro, controle de energia, detecção de anomalias, previsão de crimes, gerenciamento de riscos, entre outros.

Mayer Schonberger e Cukier (2013) corroboram com esse argumento. Os autores contam a história da primeira empresa de *Big Data* a lidar no mercado de aviação comercial, Farecast, fundada pelo cientista da computação Oren Etzioni e como houve uma mudança acerca do uso dos dados e da informação. A empresa, que ajudou milhões de consumidores a economizar nos preços das passagens, seria posteriormente vendida à Microsoft por 110 milhões de dólares, e sua tecnologia incorporada ao motor de buscas Bing, com isso contribuindo para uma nova perspectiva sobre os dados como a matéria-prima dos negócios e contribuindo para um tipo novo de valor econômico, um acelerador da inovação e serviços originais.

Um outro tipo de manipulação de dados se materializa no campo da inteligência artificial. Para Corea (2019, p. 26-30), essa é uma área de estudos multifacetada, que congrega aspectos de robótica, processamento de linguagem natural, internet das coisas e/ou visão computacional para produzir um sistema que aprenda a aprender. A ideia em si não é nova, tendo seu nascedouro em 1950 com a publicação de Alan Turing, que propunha a existência de uma máquina que pudesse pensar. A proposta, no entanto, esbarrou em muitos obstáculos relativos à quantidade de dados que os algoritmos tinham disponíveis e podiam receber como entrada, e a tecnologia dos equipamentos da época. Hoje, o cenário é totalmente diferente: houve avanços significativos relativos ao armazenamento, poder de processamento dos computadores, redução do custo dos equipamentos, aumento largura e qualidade de banda de conexões com a internet, além da possibilidade de trabalhar com computação em paralelo provida por GPUs (processadores gráficos).

Além deste, também se vê emergir o campo da mineração de dados (*Data Mining),* que lida especificamente com a extração em larga escala de grandes quantidades de dados desorganizados e desestruturados, fazendo parte de um campo mais amplo chamado Descoberta de Conhecimento em Bancos de Dados (KDD - *Knowledge Discovery In Databases*), como explicam Castro e Ferrari (2016, p.38-42).

O nome mineração perfeitamente se adequa à importância e status que esse minério tem nos dias atuais. Os autores apresentam o surgimento dessa área de atuação como um processo sistemático, interativo e iterativo, que busca preparar grandes bases de dados (minas) a fim de retirar-lhes algum tipo de conhecimento (minerais preciosos), fazendo uso de aprendizagem de máquina e técnicas de análise.

Por fim, também se deve citar um campo ainda mais abrangente, a ciência de dados (*Data Science*), que incorpora os conhecimentos da estatística, elencando princípios, metodologias e orientações para que se possa transformar, validar e criar significados a partir de bases de dados. Isto é possível pois a ciência de dados é entendida como multidisciplinar, fazendo uso de 5 aspectos, os 5Ps da ciência de dados: propósito, pessoas, processos, plataformas e programabilidade (FILATRO, 2020, p. 31-35).

De posse dessa contextualização sobre o que se entende informação e as áreas em que ela é utilizada atualmente, faz-se necessário também ilustrar com exemplos algumas das diversas aplicações específicas desses conhecimentos. Eles vão desde utilizar uma inteligência artificial para detectar casos de COVID analisando imagens de pulmões saudáveis, infectados pela doença ou outras similares (WU et al, 2020), a treinar um modelo para detecção de fraude de cartões de crédito, analisando desta vez o uso do cartão em busca de atividades que fujam do padrão do usuário (PARUCHURI, 2017).

Por outro lado, empresas podem utilizar informações de pesquisas de mercado, ou mesmo os dados acerca do seu próprio negócio para tomar decisões fundamentadas e extrair o máximo potencial de sua atividade. Para tanto, podem utilizar sistemas de *Business Intelligence* (BI) para traçar linhas de tendência, identificando os produtos mais e menos vendidos, por exemplo, a fim de dar início a campanhas específicas de *marketing* ou mesmo abandonar determinados segmentos, especializar-se em outro etc., como neste estudo cujos resultados afirmam uma melhora na manutenção de equipamentos laboratoriais de uma indústria de celulose (FARIA; LONGHINI, 2017). Podem ainda considerar a criação de ferramentas internas específicas, que auxiliem na tomada de decisão (*Decision Support Systems*). Essas mesmas ferramentas são também usadas por órgãos governamentais para justificar a criação de políticas públicas, a exemplo desse estudo direcionado ao setor de agricultura familiar do estado da Paraíba (CARVALHO; FARIAS, 2017).

É possível também configurar um sistema de controle de anúncios a fim de disparar determinados tipos de divulgação publicitária a partir do uso que membros de uma rede social fazem de seu status, a exemplo de direcionar propagandas de vestidos de casamento ao detectar a troca de um status de solteira para noiva (DIETRICH, DAVID, et al., 2015, p.3).

Os primeiros exemplos, sobre o uso médico para o auxílio no diagnóstico de doenças e detecção de fraudes, desfrutam de um status privilegiado e estável no que tange o uso ético das informações. Certamente pode ser argumentado que visam alcançar um bem maior ou benefício direto do detentor da informação, o que reduz as tensões sobre o uso das informações dos pacientes ou clientes. Contudo, quando se trata do direcionamento de anúncios, passa-se a tratar mais seriamente sobre o uso das informações pessoais dos usuários, que em número esmagador tendem a ignorar completamente os acordos de uso, aquiescendo a tudo, como aponta um estudo elaborado por Obar e Oeldorf-Hirsch (2020). Assim, esses usuários se tornam alvos potenciais de formas de controle, criação de perfis comportamentais, cerceamento da autonomia e ataques a sua privacidade, que ocorreriam, para efeitos legais, em conformidade com o acordo assinado ou sob a forma de cessão espontânea das informações (TEFFÉ; MORAES, 2017, p.14).

Ademais, se por um lado existem formas de uso dos dados que operam nas fronteiras relativas da ética, por outro há registros inequívocos de crimes que jamais poderiam ser cometidos senão com o auxílio desses dados, como ocorre nos casos de fraudes perpetradas após vazamentos de dados, conforme indicam os especialistas após aquele que ficou conhecido como “vazamento do fim do mundo” (LEMOS, 2021).

Em vista disso, a questão do uso indevido de informação se torna um ponto central de análise e uma preocupação que levou inclusive ao surgimento da lei 12.965/2014, o Marco Civil da Internet, uma legislação que visou estabelecer regras gerais, princípios, garantias, direitos e deveres dos usuários e provedores de internet a fim de que regulamentar a maneira como as relações jurídicas se dão no seio da internet (BRASIL, 2014). Não somente ela, mas mais recentemente, em 2021 é promulgada a Lei Geral de Proteção de Dados, de inspiração europeia, cujo objetivo foi tratar de modo específico a coleta e uso de dados (BRASIL, 2021).

Levando isso em consideração, a questão sobre o valor da informação, o estado atual de ampla conectividade e dependência de sistemas informatizados

tornam possível afirmar que um ativo como esse deve ser protegido e controlado. É o que se analisa a seguir.

2.2 SEGURANÇA DA INFORMAÇÃO: conceitos elementares

> Segurança da informação é muito mais do que um assunto de tecnologia da informação
> *Stephane Nappo*

Dada a importância da informação, a sua segurança é hoje uma das maiores preocupações dos usuários de sistemas informatizados. Como foi dito, a informação é sem dúvida o ativo mais valioso atualmente e a sua proteção tornou-se um dos aspectos mais importantes nas relações entre as pessoas que compartilham e usam informações umas das outras.

Dito isso, para entender o conceito de segurança da informação, primeiro se deve compreender o que são sistemas de informação. Segundo Kim e Solomon, um sistema de informação é um agregado que contém *hardware*, um sistema operacional e um *software* aplicativo que juntos trabalham para coletar, processar e guardar informações de indivíduos e organizações (2018, p. 12). Deste modo, quando falamos em sistemas de informação, estamos tratando justamente da forma a partir da qual esses valiosos dados serão manuseados.

Os sistemas de informação não existem no vácuo: para que haja um sistema de informação é necessário um conjunto de três elementos, o qual se dá o nome de tripé dos sistemas de informação e que é composto de pessoas, processos e tecnologia. As pessoas são os atores que criam e manuseiam os sistemas. Os processos são as formas que os dados e as pessoas utilizam para manipular a informação. A tecnologia é o meio pelo qual essa relação se dá, e que pode ser dividida em *software*, *hardware*, dados e redes (WHITMAN; MATTORD, 2018, p. 22-23).

Assim, na ligação desses três elementos, muitas ameaças, riscos e vulnerabilidades estão à espreita e o alvo, voluntária ou involuntariamente, são precisamente os dados previamente mencionados. As estratégias para mitigar esses problemas é o objeto de estudo da segurança da informação. De acordo com Kim e Solomon (2018, p.12), a segurança de informação é um conjunto de atividades que

visam proteger um sistema de informações e os dados nele contidos. Já Whitman e Mattord (2018, p.10) a conceituam como a manutenção da confidencialidade, integridade e disponibilidade, seja em fase de armazenamento, processamento ou transmissão, e essa manutenção se dá por meio da aplicação de políticas, educação, treinamentos e conscientização, além de tecnicamente, por meio da tecnologia.

Mencionou-se acima os termos disponibilidade, confidencialidade e integridade. Estes termos são a conhecida tríade da segurança da informação, que Whitman e Mattord (2018, p. 15 e 16) conceituam da seguinte forma: disponibilidade é a característica do sistema de permitir que os usuários autorizados (sejam pessoas ou máquinas) tenham acesso à informação sem interferência ou obstrução; confidencialidade é a característica da informação que consiste em estar protegida da divulgação ou exposição não autorizada; por fim, integridade é característica da informação que a descreve como completa, íntegra e sem corrupções.

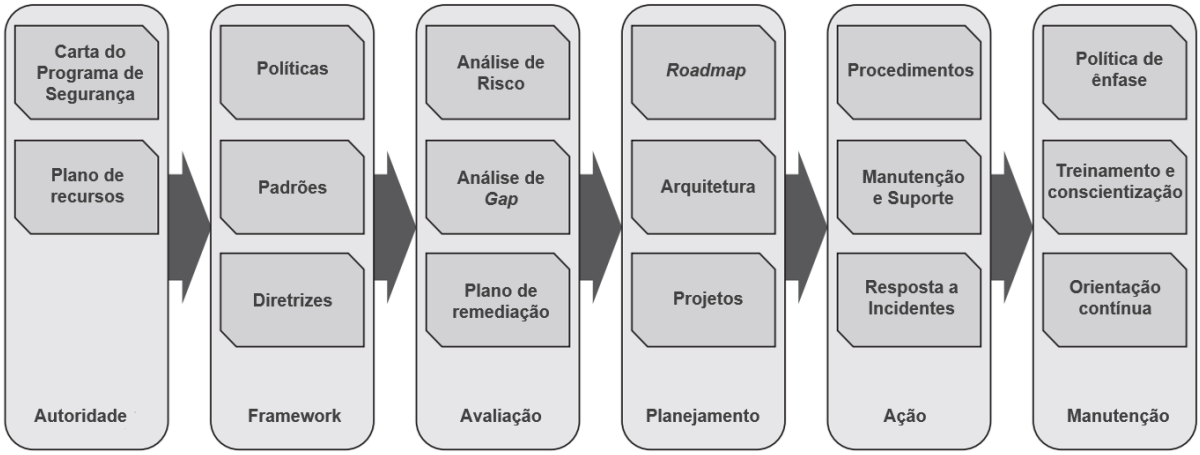
Os mesmos autores identificam que esse conceito se encontra atualmente defasado em vista dos numerosos novos tipos de ameaças que impactam os sistemas de informação, a exemplo de dano acidental ou intencional, destruição, furto, modificação não intencional ou não autorizada (2018, p. 11). Deste modo, o modelo deve ser atualizado a fim de abarcar outras características, chamadas de características críticas da informação, que incluem: acurácia ou precisão, que descreve um dado sem erros, cujo valor é aquele que o usuário espera que seja; autenticidade, que consiste na originalidade, em contraste a ter sido fabricado ou copiado; informação identificável relativa à pessoa, que engloba os conjuntos de dados que podem identificar uma pessoa de forma única; posse, a característica que define como o controle ou a posse de um dado reflete a sua legitimidade ou autorização; e, por fim, utilidade, que descreve como o dado possui valor ou utilidade para um determinado fim (2018, p. 15 e 16).

Assim, pode-se notar que a segurança da informação trabalha no equilíbrio. Um sistema sem acesso seria plenamente seguro no que tange a integridade e a confidencialidade do conteúdo nele guardado, porém os titulares desse conteúdo não poderiam usufruir dele. Do mesmo modo, um sistema de acesso irrestrito, até poderia garantir que o conteúdo fosse mantido em sua forma original, mas não asseguraria o segredo de informações sensíveis. Por fim, um sistema que garantisse o acesso de informação sigilosa somente àqueles autorizados, mas não garantisse a integridade, jamais seria confiável pois não se saberia se a informação foi ou não adulterada.

Reforçando, portanto, é necessário um balanço absoluto entre estar disponível e acessível somente para aqueles que possuem as credenciais necessárias a acessar e garantir que a informação não foi modificada sem o aval dos titulares, mas que possa sê-lo se assim for necessário (WHITMAN; MATTORD, 2018, p. 23).

Em teoria, um sistema de informação é considerado seguro se consegue manter esse equilíbrio. Na prática, a implementação desses tipos de sistema exige que sejam realizadas várias etapas, que permeiam todos os envolvidos, para a consecução desse fim. Rhodes-Ousley (2013, p. 14) relaciona seis aspectos que devem ser considerados minuciosamente: autoridade, *framework* (estrutura de trabalho), avaliação, planejamento, ação e manutenção. Na figura 1, é possível observar uma esquematização desses seis pilares:

Figura 1 – Implementação de Segurança da Informação



Fonte: Road-Ousley, 2013.

O aspecto da autoridade diz respeito à formalização de uma carta de programa de segurança, que deverá descrever o propósito, escopo e responsabilidades do setor de segurança. Esse setor normalmente é responsável pela proteção da informação, análise de riscos, monitoramento e resposta. Em algumas situações esse setor engloba segurança física, recuperação de desastres e continuidade do negócio. Também é incluído um plano de recursos que visa justamente quantificar as necessidades para a implementação da segurança, pessoal, terceirização, entre outros (RHODES-OUSLEY, 2013, p. 15).

Quando se fala em *framework*, analisamos a política de segurança, padrões e diretrizes. Nesse aspecto são desenhados o que a organização deve fazer ao ser apresentada a situações e incidentes e que tecnologias devem ser usadas. Os padrões indicam os produtos em si, versões e configurações, recursos de rede. Por

essa razão, como dizem respeito a especificidades dos equipamentos e *softwares*, devem ser revisados regularmente. As diretrizes indicam como os equipamentos devem ser usados para se conformar à política de segurança (RHODES-OUSLEY, 2013, p. 15).

Avaliação ou análise trata de análise de riscos, análise de *gap* e planejamento de remediação. A análise de riscos visa avaliar o grau de abertura dos ativos da organização frente a ameaças já antecipadas. Essa análise ajuda a alocar esforços e investimentos nas áreas mais críticas, além de também definir que riscos devem ser aceitos, mitigados ou transferidos. A análise de *gap* procura definir o estado atual da segurança e o local aonde se quer chegar. O planejamento de remediação diz respeito à ordenação dos passos necessários para alcançar esse status ideal (RHODES-OUSLEY, 2013, p. 16).

O planejamento é subdividido em *roadmap*, arquitetura de segurança e planos de projeto. O *roadmap* é um plano de ação para executar o planejamento de remediação. É importante para quando as etapas forem ser implementadas. A arquitetura de segurança pode ser vista como uma esquematização de alto nível de como as tecnologias de segurança são implementadas, como se encaixam. Os planos de projeto detalham como as implementações de segurança serão realizadas e por quais colaboradores individuais (RHODES-OUSLEY, 2013, p. 16).

A ação diz respeito a procedimentos, manutenção e suporte, e planos de resposta a incidentes. Os procedimentos ditam a forma como o trabalho deve ocorrer no dia a dia. Manutenção e suporte se referem a ações que visam dar continuidade às operações do programa de segurança, relacionando-se com um ciclo normal de planejamento, atualização, revisão e melhoria. Os planos de resposta a incidentes se referem a ações específicas já programadas que buscam reduzir o tempo de resposta e diminuir os danos eventualmente causados (RHODES-OUSLEY, 2013, p. 17).

A manutenção é composta por ênfase da política de segurança, programas de conscientização de segurança e orientação contínua. O primeiro se refere a salientar diariamente a política de segurança a fim de que as pessoas da organização não se esqueçam de que esse deve ser um esforço constante. Os programas de conscientização constituem momentos de treinamento que visam educar parceiros e colaboradores sobre o que se espera deles, medidas que devem tomar e em que circunstâncias e que consequência poderão advir de ignorá-las. A orientação contínua diz respeito a disponibilização constante de um canal para que os responsáveis por

segurança possam ser consultados e tirem dúvidas, evitando incidentes (RHODES-OUSLEY, 2013, p. 17).

É possível perceber pela explanação acima que a distância entre a teoria e a prática é longa. A segurança da informação é um assunto extremamente complexo justamente porque não é possível assegurar o isolamento completo dos riscos. Eles podem, em sua grande maioria, ser apenas minimizados. Bastará, porém, uma falha nessa cadeia de eventos para que um incidente ocorra, prejudicando um número por vezes imensurável de interessados.

Por conta deste fato, a implementação da segurança da informação requer não somente uma criação de documentos que prevejam o que deve ser feito, mas sim que seja elaborada toda uma cadeia de ações, cultura, conscientização, diretrizes formando uma visão total que perpassa, senão todos, mas uma considerável parte dos processos que compõem o dia a dia de uma determinada corporação e daqueles que com ela dialogam, o que inclui redes, sistemas, serviços, infraestrutura, compondo um ecossistema de competências e responsabilidades. É o que se dá o nome de governança de segurança da informação (HUREL, 2021, p.7).

Dito isso, torna-se relevante mencionar as potenciais consequências de não seguir esses passos. Os chamados incidentes de segurança revelam as brechas dos sistemas, que podem ser exploradas por indivíduos mal-intencionados através de ataques dos mais diversos tipos e que inclusive foram utilizados contra várias das plataformas públicas que serão mencionadas nas páginas seguintes. Alguns exemplos são: *defacement, Distributed Denial of Service (DDoS), ransomware*. Como consequência desses ataques, pode haver a captura das informações de usuários, o que posteriormente poderá resultar em outros tipos de ataques como *phishing* e engenharia social.

Website defacement ou *web graffiti* (em tradução livre, “pichação *web*”) constitui a invasão de um servidor e, após adquirir direitos de administrador, e a substituição do conteúdo do site por outro. De modo geral, é considerado não mais que um incômodo, um ato de vandalismo. Contudo, em determinadas vezes pode ser utilizado como fachada para instalação de outros códigos maliciosos no sistema (KIM; SOLOMON; 2018, p.374-375).

Negação de serviços distribuída (*Distributed Denial of Service - DDoS*) é um tipo de ataque que visa sobrecarregar de chamadas um servidor a ponto de esse sistema não ser capaz de atender a nenhum outro tipo de chamada, tornando o

serviço indisponível. Esse tipo de ataque pode ser vislumbrado quando se tenta acessar um *website* e é exibido na tela o erro 503 que indica um serviço temporariamente indisponível (MACHADO, 2014, p.104).

Ransomware é um tipo de ataque em que a vítima tem seu sistema invadido e encriptado (os dados são embaralhados e impossíveis de acessar) com a exigência do pagamento de quantias de dinheiro pelo resgate dos dados e a ameaça de divulgação dos dados ou destruição deles (JOHNSON, 2015, p. 297).

Engenharia social é uma conduta que se configura como uma espécie de fraude em que o criminoso se passa por uma pessoa a fim de obter informações confidenciais ou algum tipo de vantagem de uma vítima que acredita estar lidando com um amigo, parente, colega de trabalho ou até mesmo um representante real de uma empresa com a qual a vítima tenha algum tipo de contrato ou relação (MACHADO, 2014, p.80; FONTES, 2007, p.203-206).

Phishing é um tipo de ataque de engenharia social que ocorre principalmente no envio de e-mails e mensagens que simulam empresas e usuários reais e solicitam o envio de alguma informação relevante do usuário, como nomes, senhas, informações de cartões de crédito, CPF, entre outros, por meio de *websites* falsos que perfeitamente imitam a página oficial de um serviço real (JOHNSON, 2015, p. 312).

Feitas essas considerações acerca do tema de segurança da informação, analisar-se-á o contexto brasileiro sob esse prisma.

2.3 A SEGURANÇA DA INFORMAÇÃO NO BRASIL: teoria e prática

> São necessários 20 anos para construir uma reputação e alguns segundos de cyber-incidentes para arruiná-la.
>
> *Stephane Nappo*

No Brasil, os esforços governamentais para a salvaguarda da segurança da informação podem ser encontrados sob a forma de várias normativas e decretos, entre as quais se destaca a Política Nacional de Segurança da Informação (PNSI), instituída de forma mais recente pelo Decreto Nº 9.637/2018, que traz objetivos, diretrizes e princípios acerca da implementação do tema em todos os órgãos da

Administração Pública Federal, determinações sobre a criação de comitês de verificação do estado de implementação da PNSI e disposições sobre a instituição de políticas específicas para cada órgão e planos de abrangência nacional (BRASIL, 2018).

O próprio PNSI prevê, em seu art. 5º, inc. I, a criação de um de seus instrumentos: a Estratégia Nacional de Segurança da Informação, cujo objetivo é o de estabelecer um diálogo entre os vários *stakeholders*, dentre eles órgãos públicos e entidades privadas, para convergir sobre ações estratégicas a serem tomadas no Brasil para melhorar o cenário bastante precário no qual se insere o país, o que é reconhecido pelo próprio documento em sua "Parte I - Diagnóstico". Essa estratégia deverá ser construída em módulos, devido à extensão do tema, sendo o primeiro, instituído pelo Decreto Nº 10.222/2020, o módulo Estratégia Nacional de Segurança Cibernética (ENSC). Os seguintes, ainda não instituídos, contemplarão a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados.

É possível citar também as POSIC (Política de Segurança da Informação e Comunicação), que devem ser aprovadas no âmbito de cada órgão, segundo determinações do art. 2º, inc. I da Instrução Normativa GSI/PR nº 1/2008, art. 15, inc. II da PNSI e art. 2º da ENSI, a fim de se adequar às particularidades de cada instituição. Cita-se como exemplo a POSIC-IPHAN[7], instituído pelo Instituto do Patrimônio Histórico e Artístico Nacional e a POSIC-MS[8], relativa ao Ministério da Saúde. Pela leitura dos documentos, nota-se que o primeiro leva em consideração as recomendações preconizadas pela ISO 27002/2005 acerca de boas práticas para gestão de segurança da informação; o segundo, por outro lado, vai além e cita não somente essa, como também as 27001:2013, 27003:2011, 27004:2010, 27005:2011 e 27014:2013.

Assim, ambas se revelam normativas mais técnicas e específicas, mais direcionadas à implementação prática de segurança, e que se assemelham aos documentos de políticas de segurança citados anteriormente e propostos por Rhodes-Ousley (2013). Contudo, também chama atenção o fato de haver disparidade nos padrões de segurança, já que a referência às ISOs não são as mesmas, o que

[7] https://www.gov.br/iphan/pt-br/acesso-a-informacao/dados-abertos/POSICV220180315.pdf
[8] https://datasus.saude.gov.br/wp-content/uploads/2019/12/portaria.pdf

contrasta com a determinação da Estratégia de Segurança de Cibernética que propunha padronização dos critérios adotados. Uma possível explicação é o fato de que ambos entraram em vigor em data anterior à Estratégia, não tendo sido ainda atualizados a fim de refletir as mais recentes modificações.

Ademais, inobstante esses inúmeros instrumentos normativos, todos os órgãos brasileiros, enquanto detentores das maiores bases de dados sobre os cidadãos, devem também se adequar aos ditames da Lei Geral de Proteção de Dados (Lei Nº 13.709/2018), que já em seu art. 1 os submete expressamente ao mencionar “pessoa jurídica de direito público”, e dirime qualquer dúvida a esse respeito em seu parágrafo único, ao declarar ser de interesse de todos os entes federativos, citados por nome, a observância do diploma legal referido (BRASIL, 2018).

Assim, se esses órgãos e entes públicos estão obrigados a cumprir as determinações da LGPD, então é possível afirmar que o Estado não só pode sofrer as sanções previstas naquela lei, como também pode ser demandado a reparar danos causados aos usuários desses cadastros na ocorrência de algum evento que ponha em risco as suas informações. É isso o que se depreende do arts. 42 e 52 da LGPD, o que é corroborado por Marini e Silva (2021), ao analisar a responsabilidade civil do Estado nesses casos.

Outro ponto relevante diz respeito à cooperação internacional. A Convenção de Budapeste, que trata sobre o combate ao cibercrime internacional foi ratificada pelo Brasil em 2021, abrindo margem para a cooperação entre as nações. A convenção foi resultado de um acordo celebrado em 2001 (BRASIL…, 2021).

É possível perceber, no entanto, que a despeito de todo o arcabouço de leis, decretos e instrumentos normativos de modo geral, a situação real do Brasil apresenta problemas e inúmeros casos de incidentes de segurança.

Novaes Neto et al. (2020) relatam que o Brasil teve um aumento de 493% nos casos de vazamentos de dados somente no ano de 2019. O número de incidentes passou de 3 para 16, com o vazamento de dados na ordem de 205 milhões de pessoas afetadas. Esse número engloba casos ocorridos no setor público e privado. Nas linhas seguintes, a análise se restringirá apenas ao setor público e em âmbito federal.

A começar por 2019, relatou-se que em abril daquele ano houve o vazamento de dados de 2,4 milhões de usuários do SUS (Sistema Único de Saúde), por uma brecha identificada entre os sistemas que fazem interface com SUS, neste

caso um sistema de cadastro, o que gerou a exposição de nomes completos, nomes da mãe, endereços, CPF e datas de nascimento (PADRÃO, 2019).

O Detran do Rio Grande do Norte permitiu uma brecha que dava acesso ao sistema nacional de dados, expondo aproximadamente 70 milhões de usuários, a partir da informação de CPF, o que incluiu endereço residencial completo, telefone, operadora, dados da CNH (categoria, validade, emissão, restrição, registro), foto, RG, data de nascimento, sexo e idade (NAKAGAWA, 2019).

Afirmou-se anteriormente que a segurança da informação envolve o treinamento do pessoal que fará a manipulação de informações sigilosas. Essa constatação se confirma no caso do vazamento que afetou 16 milhões de pessoas, tendo os seus dados acessados pelo descuido de um funcionário do Hospital Albert Einstein. O funcionário publicou uma planilha com dados de acesso do SUS na plataforma GitHub (VAZAMENTO..., 2020).

Já em dezembro de 2020, houve o relato de vazamento de 243 milhões de brasileiros por meio de uma falha de segurança no aplicativo E-SUS Notifica, que deu acesso a, entre outras informações, CPF, nome completo, endereço e telefone dos afetados (NOVA..., 2020).

Em 15 de janeiro de 2021, o Tribunal Regional do Trabalho da 3ª Região foi vítima de um ataque DDoS (*Distributed Denial of Service*) o que resultou em instabilidade dos serviços prestados pelo tribunal. A equipe técnica agiu rápido e isolou os sistemas e dados a fim de minimizar os danos (TRF-3..., 2021).

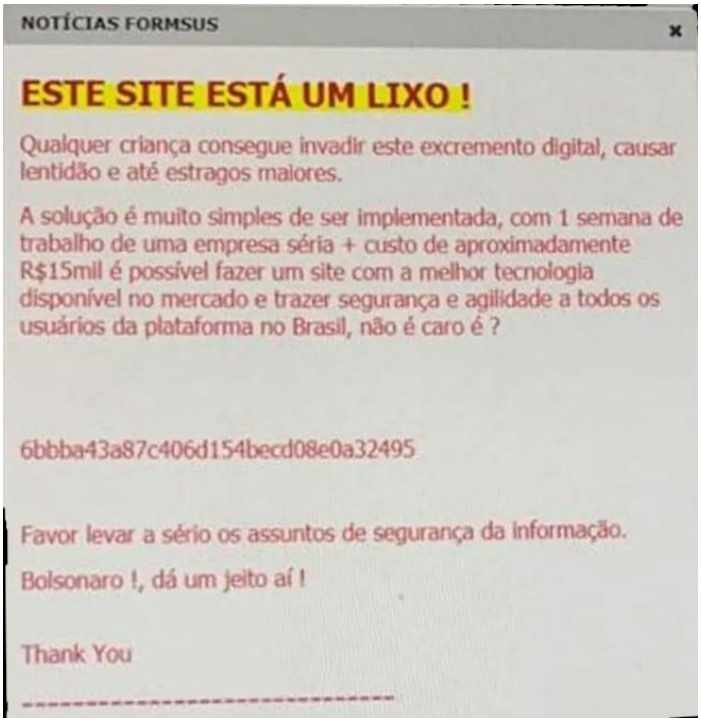
Em 19 de janeiro, foi detectado um enorme vazamento de dados, pertencente a pessoas físicas (inclusive falecidas) e jurídicas, até mesmo de grandes autoridades nacionais como ministros do Supremo Tribunal Federal, somando aproximadamente 223 milhões de afetados. A Polícia Federal então deflagrou a operação *Deepwater*, que resultou na prisão de Marcos Roberto Correia da Silva, conhecido por Vandathegod, nos fóruns em que ocorre a venda dos dados. Menciona-se esse caso pois o *hacker*, em uma postagem num fórum onde ocorre a venda dos dados em *bitcoin*, declarou que os dados foram obtidos de uma empresa privada ligada ao governo. Ademais, o mesmo *hacker* alega que invadiu também o sistema do Tribunal Superior Eleitoral e Senado Federal (CIBERCRIME..., 2021).

Em 3 de fevereiro de 2021, uma tentativa de ataque *ransomware* aos serviços administrativos de uma subsidiária da Eletrobrás, Central Nuclear Almirante

Álvaro Alberto, causou o desligamento desses serviços para proteger os dados da organização (NISZ, 2021).

Em fevereiro de 2021, houve o ataque *hacker* ao site do Ministério da saúde. O ato de *defacement* (espécie de pichação digital) foi perpetrado em uma página de formulário do ministério. Curiosamente, o atacante em sua mensagem pedia que a segurança da informação fosse levada à sério, e que até mesmo uma criança invadiria aquele sistema (FormSUS) (RIGUES, 2021). É o que se vê na figura 2:

Figura 2 – *Defacement* 1



Fonte: Olhar Digital, 2021.

Em 9 de setembro de 2021, o site da ANVISA foi alvo também de *defacement* em uma página de formulário destinada a registrar dados de saúde de turistas que desejem adentrar o território nacional (Declaração de Saúde do Viajante – DSV). A página ficou fora do ar por algumas horas no período da tarde. A mensagem deixada pelos *hackers* novamente zomba dos níveis de segurança e mostra ligação direta com um fato ocorrido na semana anterior, em que a seleção brasileira de futebol enfrentava a seleção argentina nas eliminatórias da Copa do Mundo, em São Paulo. Na ocasião, a ANVISA encerrou a partida por conta do descumprimento de jogadores argentinos sobre regras de quarentena impostas pela agência. A mensagem pode ser conferida na figura 3 (DEPOIS..., 2021):

Figura 3 – *Defacement* 2

Fonte: Security Report, 2021.

Em 30 de outubro de 2021, o Tribunal Regional do Trabalho da 4ª Região detectou acessos suspeitos em sua infraestrutura tecnológica, não tendo havido dano em vista de medidas rápidas tomadas pela equipe técnica da Secretaria de Tecnologia da Informação e Comunicações do TRT4 (SETIC), que isolaram e contiveram o ataque (TRT-RS..., 2021).

No final do mesmo ano, no dia 10 dezembro houve uma das falhas mais sérias, que ficou conhecida como o “Apagão de Dados do Covid” e que afetou vários sistemas do Ministério da Saúde, deixando-os fora do ar até o dia 14 de janeiro. Os sistemas afetados foram: e-SUS Notifica, o Sistema de Informação do Programa Nacional de Imunização (SI-PNI), ConecteSUS, a emissão do Certificado Nacional de Vacinação Covid-19 e da Carteira Nacional de Vacinação Digital. A falha foi provocada por um ataque *hacker*, de autoria do grupo LAPSUS$ e, inicialmente, foi reportado como um tipo de *ransomware* já que os atacantes publicaram uma mensagem no site do Ministério na qual se lia que dados da ordem de 50 terabytes haviam sido capturados e que se houvesse interesse em recuperá-los, que fosse feito contato através de dados do Telegram e Whatsapp contidos na mesma imagem. A imagem original pode ser vista na figura 4 (PF..., 2021):

Figura 4 – *Defacement* 3

Fonte: Poder 360, 2021.

Posteriormente, no entanto, foi constatado que não houve perda dos dados pois havia *backups* e que também os dados não haviam sido criptografados, mas que aplicativos do Ministério haviam sido deletados pelos *hackers*, o que tornou necessária a reconstrução dessas aplicações (MINISTÉRIO…, 2021).

Após o ataque ao Ministério da Saúde, no dia 23 de dezembro o mesmo grupo assumiu autoria de um ataque contra o Correios (Empresa Brasileira de Correios e Telégrafos), que deixou indisponível o portal da organização. Em nota, a empresa declarou que houve instabilidade e indisponibilidade em seu portal, mas que já operava praticamente na totalidade de sua capacidade (HACKERS..., 2021).

Já no ano de 2022, no dia 20 de fevereiro, a equipe técnica do Tribunal Regional do Trabalho da 17ª Região detectou uma atividade suspeita nos sistemas que integram a infraestrutura de tecnologia do tribunal. Por conta disso, o expediente presencial, as sessões de julgamento, audiências e os prazos processuais, regimentais e administrativos foram todos suspensos. O site oficial e o Balcão Virtual de atendimento estiveram fora do ar naquela data, tendo sido reportado o fato por meio da conta oficial do tribunal no Instagram (RIBEIRO, 2022).

O acesso ao portal do tribunal e o sistema de processo judicial eletrônico foram restabelecidos somente no dia 7 de março. Após 20 dias, alguns sistemas permaneceram foram do ar, como o serviço de telefonia fixa e o Balcão Virtual. Os prazos continuaram prorrogados até o dia 18 de março (RIBEIRO, 2022).

Em 28 de março, o site oficial do SEBRAE (Serviço Brasileiro de Apoio às Micro e Pequenas Empresas) sofreu um ataque cibernético que o tirou do ar. O órgão utilizou seu perfil oficial no Twitter para atualizar os usuários do serviço da situação ocorrida. Não foram dados mais detalhes, além de que a empresa seguia atendendo os clientes por meio de Whatsapp e canal 0800 (SITES..., 2022).

Somente dois dias após esse incidente, o Tribunal Regional Federal da 3ª Região registra ataque *ransomware* que deixou parte de seus serviços indisponíveis por 12 dias. Os sistemas afetados incluíram, dentre outros, o sistema de Processo judicial eletrônico (Pje) e o sistema de transmissão de precatórios (TRF-3..., 2022).

Em 6 de abril de 2022, a Justiça Federal de Pernambuco sofreu ataque cibernético que tornou inacessíveis os serviços prestados pelo órgão, o que resultou na criação de uma página provisória para a utilização de serviços que não faziam parte do sistema afetado. Também nesse caso, os transtornos forçaram a suspensão de prazos processuais, reduzindo a efetividade da prestação jurisdicional (JFPE..., 2022).

Em 27 de abril de 2022, foi a vez da Escola Superior do Ministeŕio Público da União, o ataque *ransomware* afetou os sistemas da instituição, o que ocasionou a decisão pelo desligamento das máquinas afetadas, deixando todo o portal *off-line*. No dia 3 de maio, os serviços voltaram a ser restabelecidos parcialmente, concluindo-se no dia 6 de maio (SISTEMAS..., 2022).

Em 17 de maio, novamente o Ministério da Saúde é afetado e mais uma vez nos mesmos sistemas (Conecte SUS, e-SUS Notifica e SI-PNI). As tentativas de acesso indevido ocasionaram a manutenção do sistema, que ficou fora do ar durante aquele dia (SILVA, 2022).

Considerando os elementos que constituem a teoria e a realidade da segurança da informação no Brasil, passa-se a análise das informações expostas.

3 RESULTADOS E DISCUSSÃO

O *ranking* mundial *Global Cybersecurity Index* (Índice de Cibersegurança Global) é uma pesquisa que tem por finalidade calcular uma pontuação dos países membros relativamente ao seu comprometimento com a cibersegurança. A pontuação obtida por cada país se baseia em um questionário respondido ou validado por representantes daquele país acerca de cinco pilares: legal, técnico, organizacional,

construção de capacidade e cooperação. Após a aferição das informações, o país participante recebe uma pontuação entre 0 e 1 (UNION, 2017, p. 1).

Do ponto de vista legal, o índice aponta a existência de normas tratando sobre cibersegurança e cibercrime; a partir da perspectiva técnica, o objetivo é avaliar a existência de instituições técnicas sobre o mesmo tema; sob o prisma organizacional, a pontuação analisa a existência de instituições destinadas à coordenação de políticas nacionais sobre cibersegurança; já sobre a construção de capacidade, mede-se a existência de pesquisa, desenvolvimento, educação e treinamentos, além de profissionais certificados e agências públicas de incentivo ao aumento da capacidade; por fim, coordenação se refere a existência de redes de parceria, modelos de cooperação e compartilhamento de informações (UNION, 2017, p. 4).

No relatório de 2017, o Brasil obteve a pontuação 0.593, figurando entre outros 76 países que se enquadraram na categoria “em amadurecimento”, nomenclatura que indica o engajamento e adoção de políticas e iniciativas complexas acerca da cibersegurança. No *ranking* das Américas, ocupou a 5ª posição, ficando atrás de EUA, Canadá, México e Uruguai; no *ranking* mundial, ficou na 38ª colocação (UNION, 2017, p. 14-15, 52).

No relatório de 2018, a pontuação caiu para 0.577. No *ranking* regional, caiu para a 6ª colocação, dando lugar ao Paraguai; no *ranking* mundial caiu para a 70ª posição (FERNMELDE-UNION, 2018, p. 56).

No relatório de 2020, após a mudança na forma de calcular a pontuação, mudando para um intervalo de 0 a 100, o Brasil obteve a pontuação 96.6, colocando-o no *ranking* regional em 3º lugar, somente atrás de EUA e Canadá. No *ranking* global, subiu para a 18ª colocação, sendo apontado como ponto forte o pilar legal, e os pilares técnico e organizacional com potencial de crescimento (FERNMELDE-UNION, 2020, p. 28; 57; 136).

Um estudo realizado pelo instituto Igarapé visou elencar as maiores ameaças constatadas pelos profissionais de vários setores da sociedade. Ao analisar as respostas enviadas pelos participantes do setor público, os profissionais que responderam ao questionário da pesquisa relataram que as três maiores ameaças que experienciam eram: cibercrimes, ameaças à infraestrutura física e falta de capacitação (IGARAPÉ, 2021, p. 10).

Essas respostas se refletem na ampla coleção de incidentes de segurança listados anteriormente. Em praticamente todos os casos foi constatada a prática de um crime cibernético, afetando a infraestrutura tecnológica dos órgãos vítimas do ataque, sendo que em pelo menos um deles, foi registrado expressamente um erro de um operador do sistema, o que dá enfoque à questão da capacitação.

Em uma matéria do Poder 360, o veículo de imprensa relata a redução específica do orçamento do sistema DATASUS, constatado por meio da utilização do sistema SIOP (Sistema Integrado de Planejamento e Orçamento), havendo redução de 53% (287 milhões em 2018 para 136 milhões em 2021) nos valores efetivamente pagos, sendo este o menor desde 2013. Além disso, relata pelo menos 7 ataques ao Ministério da Saúde, apesar de seu diretor, Merched Cheheb, alegar que não houve impacto e que a área de segurança recebeu aumento de recursos (MALI, 2022a).

Relativamente aos recursos humanos, concordam tanto o diretor do DATASUS, quanto a Associação Nacional dos Analistas de Tecnologia da Informação (ANATI), que se pronunciou em entrevista ao Poder 360 por meio de seu presidente Thiago de Aquino, informando que a redução de pessoal de 664 analistas para 446 – o que representa uma queda de ⅓ no corpo técnico – se dá por conta dos salários incompatíveis com a função, resultando em sobrecarga de trabalho nos remanescentes (MALI, 2022b).

Aprofundando o aspecto orçamentário, realizou-se uma pesquisa no painel de gastos com TI do Sistema Integrado de Planejamento e Orçamento (SIOP), cujo intuito foi extrair informações acerca do investimento público no decorrer dos anos com a área de tecnologia da informação, analisando o empenho, a liquidação e o que foi efetivamente pago. O primeiro gráfico (figura 5) mostra que o máximo de recursos públicos que essa rubrica recebeu ocorreu no ano de 2021. No ano de 2022, ano da escrita deste trabalho, o empenho foi o menor da série histórica desde 2013, representando este valor menos da metade do empenho do ano anterior (44,98%) (BRASIL, 2022).

Figura 5 – Orçamento Público – Despesas X Anos

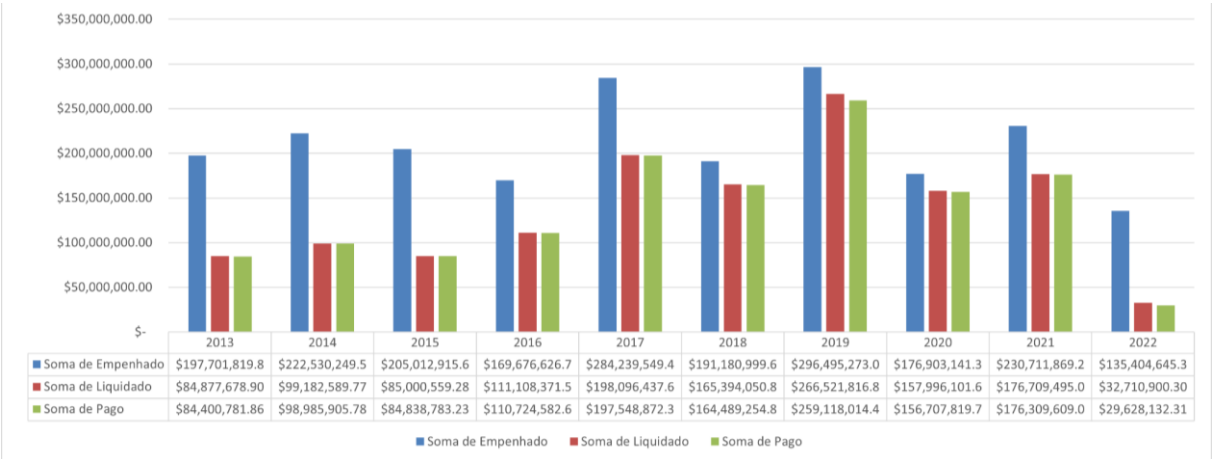
	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Soma de Empenhado	$7,779,208,05	$8,366,081,88	$7,734,577,95	$8,584,073,03	$9,004,017,18	$9,481,360,61	$9,502,907,77	$10,227,364,2	$11,334,604,2	$5,098,102,20
Soma de Liquidado	$4,658,078,43	$5,314,607,81	$5,137,341,19	$6,062,875,82	$6,101,696,18	$6,088,972,45	$6,473,732,02	$6,435,537,90	$6,539,250,21	$1,215,767,63
Soma de Pago	$4,509,072,16	$5,150,131,95	$4,673,159,44	$6,010,895,33	$6,060,354,41	$6,010,189,81	$6,419,164,72	$6,361,564,41	$6,454,163,91	$1,167,347,02

Fonte: elaborada pelo autor.

Grande parte dos casos relatados de incidentes de segurança ocorreram na Justiça Federal, Justiça do Trabalho e Ministério da Saúde, razão pela qual extraiu-se um gráfico seguindo a mesma metodologia, porém segmentando por órgão.

O segundo gráfico (figura 6), da Justiça Federal, mostra uma relação similar ao primeiro gráfico. O maior empenho ocorre em 2019, sendo o mais baixo também em 2022:

Figura 6 – Orçamento Público – Despesas X Anos – Justiça Federal

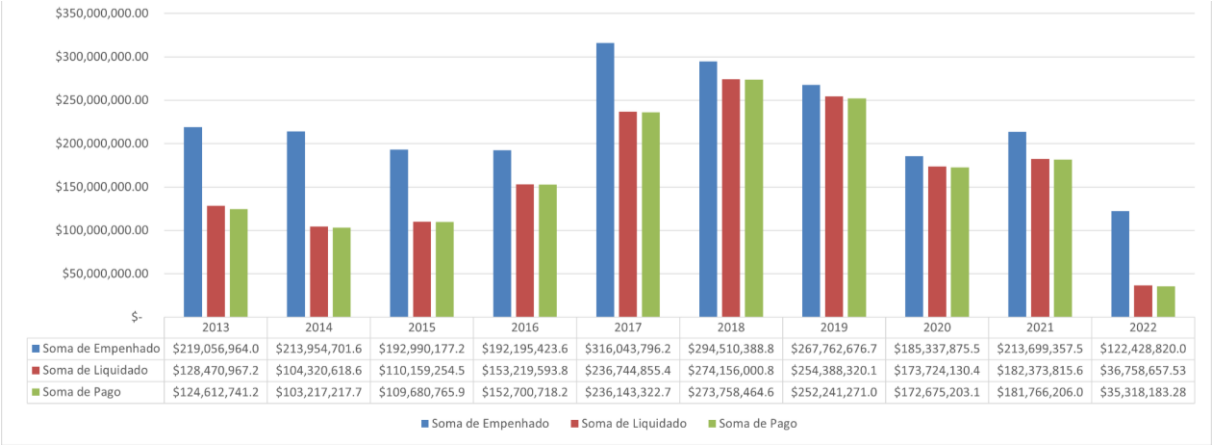


	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Soma de Empenhado	$197,701,819.8	$222,530,249.5	$205,012,915.6	$169,676,626.7	$284,239,549.4	$191,180,999.6	$296,495,273.0	$176,903,141.3	$230,711,869.2	$135,404,645.3
Soma de Liquidado	$84,877,678.90	$99,182,589.77	$85,000,559.28	$111,108,371.5	$198,096,437.6	$165,394,050.8	$266,521,816.8	$157,996,101.6	$176,709,495.0	$32,710,900.30
Soma de Pago	$84,400,781.86	$98,985,905.78	$84,838,783.23	$110,724,582.6	$197,548,872.3	$164,489,254.8	$259,118,014.4	$156,707,819.7	$176,309,609.0	$29,628,132.31

Fonte: elaborada pelo autor.

O terceiro gráfico (figura 7), da Justiça do Trabalho, segue a mesma linha dos anteriores:

Figura 7 – Orçamento Público – Despesas X Anos – Justiça do Trabalho

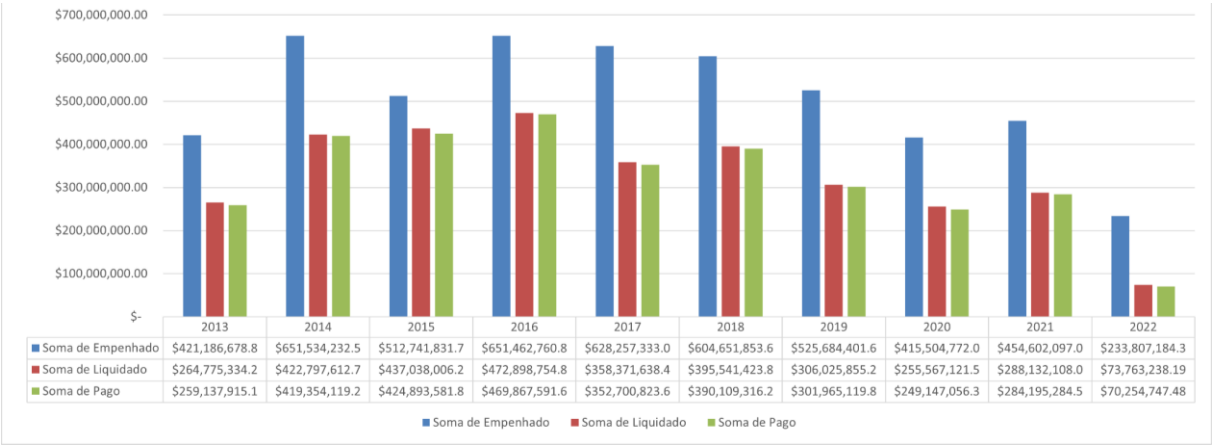


	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Soma de Empenhado	$219,056,964.0	$213,954,701.6	$192,990,177.2	$192,195,423.6	$316,043,796.2	$294,510,388.8	$267,762,676.7	$185,337,875.5	$213,699,357.5	$122,428,820.0
Soma de Liquidado	$128,470,967.2	$104,320,618.6	$110,159,254.5	$153,219,593.8	$236,744,855.4	$274,156,000.8	$254,388,320.1	$173,724,130.4	$182,373,815.6	$36,758,657.53
Soma de Pago	$124,612,741.2	$103,217,217.7	$109,680,765.9	$152,700,718.2	$236,143,322.7	$273,758,464.6	$252,241,271.0	$172,675,203.1	$181,766,206.0	$35,318,183.28

Fonte: elaborada pelo autor.

O quarto e último gráfico (figura 8), do Ministério da Saúde, também exibe o decrescimento no investimento público:

Figura 8 – Orçamento Público – Despesas X Anos – Ministério da Saúde

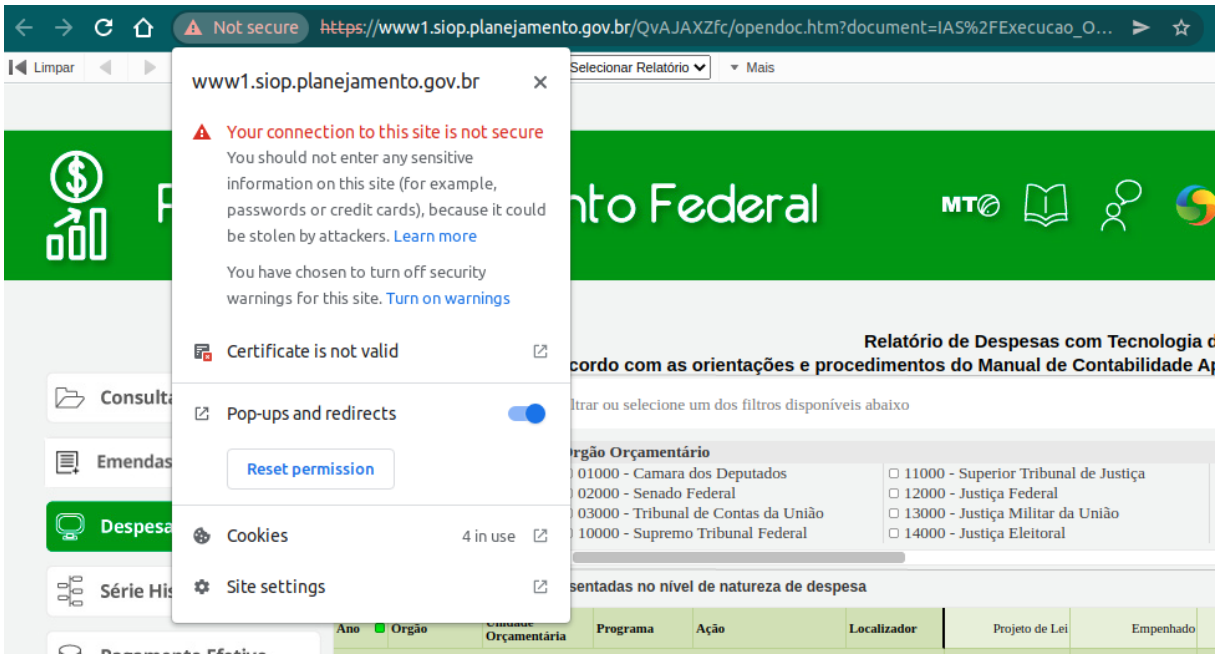


	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Soma de Empenhado	$421,186,678.8	$651,534,232.5	$512,741,831.7	$651,462,760.8	$628,257,333.0	$604,651,853.6	$525,684,401.6	$415,504,772.0	$454,602,097.0	$233,807,184.3
Soma de Liquidado	$264,775,334.2	$422,797,612.7	$437,038,006.2	$472,898,754.8	$358,371,638.4	$395,541,423.8	$306,025,855.2	$255,567,121.5	$288,132,108.0	$73,763,238.19
Soma de Pago	$259,137,915.1	$419,354,119.2	$424,893,581.8	$469,867,591.6	$352,700,823.6	$390,109,316.2	$301,965,119.8	$249,147,056.3	$284,195,284.5	$70,254,747.48

Fonte: elaborada pelo autor.

Registre-se que ao acessar o portal do SIOP, em 7 de junho de 2022, o navegador Chrome acusa a conexão com o portal como insegura, estando o portal sujeito a ataques e que não recomenda a inserção de informações sensíveis. O certificado digital é tido como inválido, como se observa abaixo na figura 9:

Figura 9 – Certificado Inválido do SIOP



Fonte: elaborada pelo autor.

Considerando a abrangência da análise, que perpassa perspectivas normativas, orçamentárias e empíricas, um extenso apanhado de incidentes de segurança da informação em contraste a importância desse tema nos dias atuais, passa-se às considerações finais.

4 CONSIDERAÇÕES FINAIS

Ante o exposto, é possível perceber que a informação se tornou um bem extremamente valioso e digno de proteção. Mais ainda, diante das novas formas de interconectividade experienciados pela sociedade, a produção e consumo de dados nunca aconteceu de forma tão massiva como se tem nos dias atuais. Esse cenário então abre margem para oportunidades e ameaças, do ponto de vista do indivíduo, organizações, empresas, e até mesmo nações.

Diante dessa realidade, nota-se uma preocupação cada vez maior com a salvaguarda da informação em vista da produção de normativas, leis e planos, aumento de investimentos, treinamento, especialização e, paralelamente, um influxo constante de incidentes de segurança que tornam indisponíveis serviços básicos e caros à coletividade.

O Brasil então se divide: de um lado, é percebida uma atenção especial que se consubstancia na elaboração de amplo aracabouço legal e de planos; de outro, o governo corta despesas, investindo menos no ano seguinte a grandes vazamentos de informações e ataques cibernéticos, e sofrendo com pouco pessoal para dar conta de uma área que se mostra cada vez mais crítica.

Assim, novamente surgem oportunidades e ameaças, basta que a Administração Pública ponha em prática o extenso e elogiado conjunto de planos que tem lhe conferido posição de destaque em nível global no que tange a preocupação com a segurança da informação.

Se, por outro lado, a tendência referente aos investimentos percebida em 2022 for mantida, então é provável que os numerosos incidentes comecem a se multiplicar de modo ainda mais descontrolado, o que acarretará danos cada vez mais graves, alargando ainda mais o abismo entre teoria e realidade.

Findo este trabalho, os próximos passos tratarão de relacionar os conteúdos aqui expostos às mesmas espécies de dados encontrados em países que estão mais bem colocados no *ranking* do Índice de Cybersegurança Global. Fazendo isso, ter-se-á em mãos um estudo comparado, cujo intuito será descobrir como obtiveram os resultados que lhes logram o prestígio das primeiras posições.

REFERÊNCIAS

ATAQUE hacker deixa sistemas da Justiça Federal em PE fora do ar. **Revista Consultor Jurídico**, 6 abr. 2002. Disponível em: https://www.conjur.com.br/2022-abr-06/ataque-hacker-deixa-sistemas-justica-federal-pe-fora-ar. Acesso em: 10 abr. 2022.

BAHGA, Arshdeep; MADISETTI, Vijay**. Big Data Analytics**: A Hands-On Approach. 1ª ed. [S.l.]: VPT 2019.

BRASIL aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. **Ministério Público Federal**, 23 de dez. de 2021. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 8 de jun. de 2022

BRASIL. **LEI Nº 12.965 de 23 de abril de 2014**. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 15 abr. 2022.

BRASIL. **LEI Nº 13.709 de 14 de agosto de 2018**. Lei geral de proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 abr. 2022.

BRASIL. **Política corporativa de segurança da Informação e Comunicação (POSIC)**. Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN). Brasília, mar. De 2018. Disponível em: https://www.gov.br/iphan/pt-br/acesso-a-informacao/dados-abertos/POSICV220180315.pdf Acesso em: 10 abr. 2022.

BRASIL. **Portaria Nº - 271, de 27 de janeiro de 2017**. Política corporativa de segurança da Informação e Comunicação (POSIC). Ministério da Saúde. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/12/portaria.pdf Acesso em: 10 mai. 2022.

BRASIL. **Sistema integrado de Orçamento e Planejamento (SIOP)**. Disponível em: https://www1.siop.planejamento.gov.br/QvAJAXZfc/opendoc.htm?document=IAS%2FExecucao_Orcamentaria.qvw&host=QVS%40pqlk04&anonymous=true&sheet=SH06 Acesso em: 6 jun. 2022.

CASTRO, L. N. D.; FERRARI, D. G. **Introdução à mineração de dados**. São Paulo: Saraiva, 2016. E-book.

CIBERCRIME: Polícia Federal prende hacker suspeito de vazar dados de 223 milhões de brasileiros. **Security Report**, 19 de mar. De 2021. Disponível em: https://www.securityreport.com.br/destaques/cibercrime-policia-federal-prende-hacker-suspeito-de-vazar-dados-de-223-milhoes-de-brasileiros/ Acesso em: 10 abr. 2022.

COREA, Francesco. **An Introduction to Data: Everything You Need to Know About AI, Big Data and Data Science**. 1ª ed. 2019, Springer International Publishing: Suíça, 2019.

DEPOIS de ataque hacker, serviço da Anvisa é normalizado. **Poder 360**, 8 de set. de 2021. Disponível em: https://www.poder360.com.br/tecnologia/depois-de-ataque-hacker-servico-da-anvisa-e-normalizado/ Acesso em: 10 abr. 2022.

FARIA, Gustavo Názaro Lopes De; LONGHINI, Tatielle Menolli. Ciclo PDCA, com auxílio do power bi, aplicado à gestão da manutenção de equipamentos laboratoriais de indústria de celulose. **Produto & Produção**, vol. 22, no 2, junho de 2021. DOI.org (Crossref), https://doi.org/10.22456/1983-8026.101859. página 143-152

FERNMELDE-UNION, Internationale (ITU). **Global Cybersecurity Index 2018**. Open WorldCat. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf Acesso em: 15 mai. 2022.

FERNMELDE-UNION, Internationale (ITU). **Global Cybersecurity Index 2020. 2021. Open WorldCat**. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf Acesso em: 15 mai. 2022.

FILATRO, A. C. **Data Science Na Educacao**. São Paulo: Saraiva, 2020. E-book.
FLORIDI, Luciano. **Information: a very short introduction**. Nova Iorque: Oxford University Press, 2010.

FONTES, E. L. G. **Segurança da informação**. São Paulo: Saraiva, 2007. E-book.

HACKERS que invadiram Ministério de Saúde atacam Correios. **Poder 360**, 23 de dez. de 2021. Disponível em: https://www.poder360.com.br/brasil/hackers-que-invadiram-ministerio-de-saude-atacam-correios/ Acesso em: 10 abr. 2022.

HUREL. Louise Marie. **CIBERSEGURANÇA NO BRASIL: uma análise da estratégia nacional**. Rio de Janeiro. ISSN 2359-0998. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf Acesso em: 10 abr. 2022.

IGARAPÉ, Instituto. **MAPEAMENTO DE RISCOS DIGITAIS: Uma Agenda Multissetorial Para A Segurança Digital No Brasil**. ISSN 2359-0998. Rio de Janeiro. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/Agenda-Seguranca-Digital.pdf Acesso em: 5 jun. 2022.

JFPE disponibiliza site provisório aos usuários após ataque cibernético. **Securtiy Report**, 7 de abr. de 2022. Disponível em: https://www.securityreport.com.br /destaques/jfpe-disponibiliza-site-provisorio-aos-usuarios-apos-ataque-cibernetico/ Acesso em: 24 mai. 2022.

JOHNSON, Thomas A., organizador. **Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare**. Editora: CRC Press, 2015.

KIM, David; SOLOMON, Michael. **Fundamentals of information systems security**. 3ª ed. Burlington, Massachusetts: Editora: Jones & Bartlett Learning, 2018.

LEMOS, Ronaldo. O Vazamento do fim do mundo. **Folha UOL**. 31 de jan 2021. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml Acesso em: 10 abr. 2022.

MALI, Tiago. Apagão de dados: governo cortou gasto do Datasus pela metade. **Poder 360**, 3 de fev. de 2022. Disponível em: https://www.poder360.com.br/coronavirus/apagao-de-dados-governo-cortou-gasto-do-datasus-pela-metade Acesso em: 10 abr. 2022a.

MALI, Tiago. Diretor do Datasus nega que corte de gasto fragilizou sistema. **Poder 360**, 3 de fev. de 2022. Disponível em: https://www.poder360.com.br/coronavirus/diretor-do-datasus-nega-que-corte-de-gasto-fragilizou-sistema/ Acesso em: 10 abr. 2022b.

MARINI, Bruno; SILVA, Jéssica Oshiro. **Da responsabilidade civil do poder público e dos agentes de tratamentos de dados no contexto da Lei Geral de Proteção de Dados**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 27, n. 6765, 8 jan. 2022. Disponível em: https://jus.com.br/artigos/95555. Acesso em: 12 jun. 2022.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: a revolution that will transform how we live, work, and think**. Houghton Mifflin Harcourt, 2013.

MINISTÉRIO da Saúde anuncia restabelecimento dos sistemas afetados por ciberataque. **Security Report**, 14 de jan. de 2021. Disponível em: https://www.securityreport.com.br/destaques/ministerio-da-saude-anuncia-restabelecimento-total-dos-sistemas-afetados-por-ataque-hacker/ Acesso em: 10 abr. 2022.

NAKAGAWA, Liliane**.** Detran vaza dados pessoais de quase 70 milhões de brasileiros. **Olhar Digital**, 8 out. 2019. Disponível em: https://olhardigital.com.br/2019/10/08/noticias/exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/. Acesso em: 10 abr. 2022.

NISZ, Charles. Eletrobras desliga sistemas da Eletronuclear por causa de ataque hacker. **Security Report**, 5 de fev. de 2021. Disponível em: https://www.securityreport.com.br/destaques/eletrobras-desliga-sistemas-da-eletronuclear-por-causa-de-ataque-hacker/ Acesso em: 10 abr. 2022.

NOVA falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. **G1**, 2 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 10 abr 2022.

NOVAES NETO, Nelson; MADNICK, Stuart; DE PAULA, Anchises Moraes, e BORGES, Natasha Marala. Developing a Global Data Breach Database and the Challenges Encountered. **ACM Journal of Data and Information Quality,** v. 13, n.

1, p. 1-33, jan. 2021. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3439873. Acesso em: 10 abr. 2022.

OBAR, Jonathan A., OELDORF-HIRSCH, Anne. **The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, Information, Communication & Society**, 23:1, 128-147, DOI: 10.1080/1369118X.2018.1486870, 2020.

PADRÃO, Márcio. Dados pessoais de 2,4 milhões de usuários do SUS são vazados na internet. **UOL**, São Paulo, 11 abr. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm. Acesso em: 10 abr 2022.

PARUCHURI, H. **Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review**. ABC Journal of Advanced Research, 6(2), pp. 113-120. doi: 10.18034/abcjar.v6i2.547, 2017.

PF apura ataque em nuvem nos sistemas do Ministério da Saúde. **Security Report**, 10 de dez. de 2021. Disponível em: ttps://www.securityreport.com.br/destaques/ministerio-da-saude-segue-trabalhando-para-o-reestabelecimento-de-plataformas-afetadas/ Acesso em: 10 abr. 2022.

RHODES-OUSLEY, Mark. **Information Security The Complete Reference**, ed 2. Editora: McGraw-Hill, Nova Iorque, 2013.

RIBEIRO, Isaac. PF investiga ataque hacker ao TRT-ES; alguns serviços seguem suspensos. **A Gazeta**, 11 de mar. de 2021. Disponível em: https://www.agazeta.com.br/es/economia/pf-investiga-ataque-hacker-ao-trt-es-alguns-servicos-seguem-suspensos-0322 Acesso em: 10 abr. 2022.

RIBEIRO, Isaac. Justiça do Trabalho no ES sofre ataque hacker e suspende atendimentos. **A Gazeta**, 21 de fev. 2021. Disponível em:https://www.agazeta.com.br/es/economia/justica-do-trabalho-no-es-sofre-ataque-hacker-e-suspende-atendimentos-0222 Acesso em: 10 abr. 2022.

RIGUES, Rafael. Hacker invade site do Ministério da Saúde e debocha da segurança. **Olhar Digital**, 4 de fev. de 2021. Disponível em: https://olhardigital.com.br/2021/02/04/noticias/hacker-invade-site-do-ministerio-da-saude-e-debocha-da-seguranca/ Acesso em: 10 abr. 2022.

SARACEVIC, Tefko. **Information Science**. Encyclopedia of Library and Information Science. New York: Taylor & Francis, 2009 pp. 2570-258. Disponível em: https://tefkos.comminfo.rutgers.edu/SaracevicInformationScienceELIS2009.pdf Acesso em: 10 abr. 2022.

SZCZEPANSKI, Marcin**. Is data the new oil? Competition issues in the digital economy**, 2020. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf Acessado em: 7 de julho de 2022

7 DIAS após ataque hacker, sistemas do TRF-3 continuam fora do ar. **Revista Consultor Jurídico**, 6 abr. 2002. Disponível em: https://www.conjur.com.br/2022-abr-06/ataque-hacker-sistemas-trf-continuam-fora-ar. Acesso em: 10 abr. 2022.

SILVA, Bruno. Ministério da Saúde identifica tentativa de ataque cibernético em sistemas. **Securtiy Report**, 15 de mai. de 2022. Disponível em: https://www.securityreport.com.br/destaques/ministerio-da-saude-identifica-nova-tentativa-de-ataque-cibernetico-em-sistemas/ Acesso em: 10 abr. 2022.

SISTEMAS acadêmicos já estão liberados aos usuários. **Escola Superior do Ministério Público da União**, 6 de mai. de 2022. Disponível em: https://escola.mpu.mp.br/a-escola/comunicacao/noticias/sistemas-academicos-ja-estao-liberados-aos-usuarios Acesso em: 10 abr. 2022.

SITE da Anvisa volta à normalidade após ataque cibernético. **Security Report**, 9 de set. de 2021. Disponível em: https://www.securityreport.com.br/destaques/site-da-anvisa-volta-a-normalidade-apos-ataque-cibernetico/ Acesso em: 10 abr. 2022.

SITES do Sebrae ficam indisponíveis após incidente cibernético. **Securtiy Report**, 30 de mar. de 2022. Disponível em: https://www.securityreport.com.br/destaques/sites-do-sebrae-ficam-indisponiveis-apos-incidente-cibernetico/ Acesso em: 11 de jun. de 2022.

SORDI, J. O. D. **ADMINISTRAÇÃO DA INFORMAÇÃO - Fundamentos e práticas para uma nova gestão do conhecimento**. 2. ed. São Paulo: Saraiva, 2015. E-book.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes sociais virtuais: privacidade e responsabilidade civil Análise a partir do Marco Civil da Internet**. p 108 a 146. e-ISSN:2317-2150 DOI: 10.5020/2317-2150.2017.v22n1p108. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272/pdf Acesso em: 10 abr. 2022.

TRF-3 comunica restabelecimento dos sistemas após 12 dias indisponíveis. **Securtiy Report**, 12 de abr. de 2022. Disponível em: https://www.securityreport.com.br/destaques/trf-3-comunica-restabelecimento-dos-sistemas-apos-12-dias-indisponiveis/ Acesso em: 25 abr. 2022.

TRF-3 sofre ataque cibernético do tipo DdoS. **Security Report**, 18 de jan. 2021. Disponível em: https://www.securityreport.com.br/destaques/trf-3-sofre-ataque-cibernetico-do-tipo-ddos/ Acesso em: 10 abr. 2022.

TRT-RS comunica que foi vítima de incidente cibernético. **Security Report,** 5 de out. de 2021. Disponível em: https://www.securityreport.com.br/overview/trt-rs-comunica-que-foi-vitima-de-incidente-cibernetico/ Acesso em: 10 abr. 2022.

TUOMI, Ilka**.** Data is more than knowledge: Implications of the reversed knowledge hierarchy for knowledge management and organizational memory. **Journal of Management Information Systems** (JMIS), v. 16, n. 3, 103–117, 1999.

UNION, International Telecommunication (ITU). **Global Cybersecurity Index 2017**.Open WorldCat. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf Acesso em: 15 mai. 2022.

VAZAMENTO de senhas do Ministério da Saúde expõe informações de pacientes de Covid-19, diz jornal. **G1**, 26 nov. 2020. Disponível em: https://g1.globo.com/bem estar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml. Acesso em: 10 abr. 2022.

WHITMAN, Michael E.; MATTORD, Herbert J.. **Principles of information security**. 6ª ed. Boston, Massachusetts: Editora: Cengage Learning, 2018.

WU X., HUI H., NIU M. et al., **Deep learning-based multi- view fusion model for screening 2019 novel coronavirus pneumonia: a multicentre study**. European Journal of Radiology, vol. 128, Artigo 109041, 2020.