Research, Society and Development, v. 10, n. 2, e40510212557, 2021
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v10i2.12557

A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional

Data protection and information security in the pandemic COVID-19: national context

Protección de datos y seguridad de la información en la pandemia COVID-19: contexto nacional

Recebido: 01/02/2021 | Revisado: 05/02/2021 | Aceito: 14/02/2021 | Publicado: 20/02/2021

Juliana Souza Barbosa
ORCID: https://orcid.org/0000-0002-3809-0908
Instituto Federal de Educação, Ciência e Tecnologia Goiano, Brasil
E-mail: ju.goiana@hotmail.com
Danihanne Borges e Silva
ORCID: https://orcid.org/0000-0002-9627-2929
UniAraguaia Centro Universitário, Brasil
E-mail: sublimefestas2017@gmail.com
Daniela Cabral de Oliveira
ORCID: https://orcid.org/0000-0002-9647-933X
Instituto Federal de Educação, Ciência e Tecnologia Goiano, Brasil
E-mail: danielacaboliveira@gmail.com
Dilça Cabral de Jesus
ORCID: https://orcid.org/0000-0002-8557-0429
Universidade de Rio Verde, Brasil
E-mail: dilcac@gmail.com
Wesley Flávio de Miranda
ORCID: https://orcid.org/0000-0003-1501-7967
Instituto Federal de Educação, Ciência e Tecnologia Goiano, Brasil
E-mail: wesley.miranda@ifgoiano.edu.br

Resumo
Durante o enfrentamento da pandemia pela COVID-19, os ataques cibernéticos se tornaram constantes. O objetivo do estudo foi apresentar a lei geral de proteção de dados, segurança da informação e os ataques cibernéticos durante a pandemia COVID-19 e refletir o impacto social dos ataques medidas na sociedade e nas organizações. Nessa revisão qualitativa os artigos, foram selecionados nas bases de dados Scielo e Google Acadêmico, também foram selecionados livros para o desenvolvimento do trabalho. Diante do cenário da pandemia da COVID-19 foi relatado alguns ataques realizados por hackers no Brasil.
Palavras-chave: Proteção de dados; Segurança da informação; Pandemia; COVID-19.

Abstract
During COVID 19's pandemic, cyber-attacks became constant. The aim of the study was to present the general law on data protection, information security and cyber-attacks during the COVID19 pandemic and to reflect the social impact of the measured attacks on society and organizations. In this qualitative review, the articles were selected from the Scielo and Google Scholar databases, and books were also selected for the development of the work. In view of the COVID-19 pandemic scenario, some attacks by hackers in Brazil were reported.
Keywords: Data protection; Information security; Pandemic; COVID-19.

Resumen
Durante la pandemia de COVID-19, los ciberataques se volvieron constantes. El objetivo del estudio fue presentar la ley general sobre protección de datos, seguridad de la información y ciberataques durante la pandemia COVID-19 y reflejar el impacto social de los ataques medidos em la sociedade y las organizaciones. Em esta revisión cualitativa, los artículos fueron seleccioandos de las bases de datos Scielo y Google Scholar, y también se seleccionaron libros para el desarrollo del trabajo. Em vista del escenario de la pandemia de COVID-19, se reportaron algunos ataques de piratas informáticos en Brasil.
Palabras clave: Protección de datos; Seguridade de la información; Pandemia; COVID-19.

1. Introdução

O grande volume de informações deve ser armazenado e trafegado de forma segura e assim deve ocorrer na internet, ou melhor, no chamado espaço cibernético. As pessoas e grupos, acobertados pela distância e anonimato, tentam burlar a segurança dos sistemas informatizados das organizações e extrair benefícios indevidos da exploração da bem chamada informação.

Diante desse contexto, as informações quanto aos dados pessoais para variadas atividades, tais como: identificação, classificação, autorização e tantas outras, transformou num elemento essencial para o mercado e, sobretudo, para que a pessoa consiga se mover, com autonomia e liberdade, nos corredores denominado sociedade da informação.

E assim, surge o conceito de segurança da informação sendo definida como área de conhecimento dedicada à proteção de dados contra acessos não autorizados, alterações indevidas ou indisponibilidade (Sêmola, 2003). Conforme descrito pela Academia Latino-Americana da Segurança da Informação (2006), a segurança da informação protege as informações registradas, sem importar onde estejam situadas: impressas em papel, discos rígidos dos computadores ou na memória das pessoas.

Devido a quarentena imposta pela COVID-19, a proteção de dados e a segurança da informação se tornaram vulneráveis. Às pressas, as pessoas e às organizações tiveram de se adaptar ao trabalho remoto, tendo que lidar com a logística de pessoal, dispositivos e outros equipamentos. E assim, surgiram os ataques cibernéticos na pandemia COVID-19.

2. Desenvolvimento

Este trabalho trata-se de uma pesquisa qualitativa, baseada em uma revisão exploratória, conforme metodologia proposta por Gil (2008).

Os artigos para compor este trabalho foram selecionados livros, leis e artigos das bases de dados *Scielo* e *Google* Acadêmico, publicados no ano de 2020, utilizando as palavras-chave: proteção de dados, pandemia, normativas, segurança da informação e ataques.

A busca foi realizada, em primeiro momento, de forma rápida e objetiva, com leitura dos títulos dos artigos e excluindo os artigos duplicados disponíveis em mais de uma base de dados. Em seguida, foi realizada a leitura dos artigos previamente selecionados, os quais incluíram todos os trabalhos que ratassem diretamente sobre proteção de dados e ataques cibernéticos durante o período de pandemia no Brasil. Na sequência, fez-se a ordenação das informações coletadas e realizou-se uma leitura crítica do referencial teórico.

3. Referencial Teórico

3.1 Quarta Revolução Industrial e o Impacto na Sociedade

Segundo Schwab (2016) a Quarta Revolução Industrial cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível. Isso permite a total personalização de produtos e a criação de novos modelos operacionais. Ela teve início na virada do século e baseia-se na revolução digital. É caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram baratos e pela inteligência artificial.

Ainda segundo os autores, a quarta revolução industrial:

> A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitas e biológicos (Schwab, 2016).

Sendo assim, é possível afirmar que a quarta revolução industrial é distinta das outras revoluções devido aos seguintes fatores: a velocidade evolui em ritmo exponencial e não linear, a amplitude e a profundidade são marcadas pela revolução digital como base, combinando várias tecnologias e o impacto sistêmico transformando os sistemas em organizações, indústrias e em toda sociedade.

Ainda segundo os autores, essa revolução digital:

> [...] fundamenta-se em utilizar a tecnologia da informação para implementar a *Internet of Things* (IoT) e serviços de forma que os processos e mecanismos de negócios sejam profundamente integrados, tornando o *modus operandi* operacionalmente flexível, eficiente e sustentável, elevando padrões de qualidade e reduzindo cusots de forma consistente (Cavazzini et al., 2018, p. 3).

Por sua vez, Schwab (2016) afirma que além da velocidade e da amplitude, a quarta revolução industrial é única por causa da crescente harmonização e integração de muitas descobertas e disciplinas diferentes. As inovações tangíveis resultam da interdependência entre tecnologias distintas não são mais ficção científica. Por exemplo, as tecnologias de fabricação digital interagem com o mundo biológico. Alguns designers e arquitetos misturam o design computacional, a fabricação aditiva, a engenharia de materiais e a biologia sintética criando sistemas pioneiros que envolvem a interação entre microrganismos, produtos e até mesmo os edifícios.

A quarta revolução industrial terá um impacto na economia global. Alguns economistas divide o crescimento econômico argumentando que o impacto da produtividade está acabando e outros afirmam que tecnologia e inovação estão num ponto de inflexão e, em breve, irão desencadear um aumento na produtividade e maior crescimento econômico (Schwab, 2016).

Segundo Transformação Digital (2018), a quarta revolução industrial também traz impactos na transformação da experiência do cliente, dos processos operacionais e dos modelos de negócio. Na transformação da experiência do cliente tópicos como o atendimento ao cliente, novas formas de engajamento, bem como maior atenção aos pontos de contato dele com a organização. No campo da transformação dos processos operacionais, tem-se digitalização de processos, mudanças na capacitação do colaborador e gerenciamento de performance. Por sua vez, na transformação dos modelos de negócios, tem-se a consolidação dos modelos de negócios digitais, a criação de novos negócios digitais e a globalização digital (Transformação Digital, 2018).

Schwab (2016) afirma que a quarta revolução industrial pode trazer impactos positivos ao mundo como: criar demandas adicionais para serviços e produtos, aumentar o potencial de crescimento econômico e a reformulação das estruturas organizacionais e econômicas oferecidas pelos recursos digitais.

Outro impacto, que vale ressaltar é o mercado de trabalho, pois as novas tecnologias irão mudar a natureza do trabalho em todos os setores e ocupações. A tecnologia produz um efeito destrutivo que ocorre quando as rupturas alimentadas pela tecnologia e a automação substituem o trabalho por capital, forçando os trabalhadores a ficar desempregados ou realocar suas habilidades em outros lugares. Outro efeito destrutivo vem acompanhado por um efeito capitalizador, em que a demanda por novos bens e serviços aumenta e leva à criação de novas profissões, organizações e indústrias.

Assim, redefinir o papel do indivíduo em uma sociedade em que o trabalho está em ampla transformação, é de vital importância, uma vez que novas modalidades de prestação de serviço surgem como por exemplo o trabalho utilizando plataformas digitais. Tudo isso, provoca o surgimento de novos conflitos ainda desconhecidos, exigindo assim, da ciência do direito da área jurídica conhecimento e regulamentações que venha possibilitar dirimir essas novas demandas da sociedade em virtude da transformação digital.

Segundo os autores Schwab e Davis (2019) destaca que a Quarta Revolução Industrial dever ser focada na humanidade, em que as tecnologias possam ser moldadas em prol de melhorar o bem com, assim promovendo desenvolvimento humano em seus mais variados contextos.

3.2 Proteção de dados

A primeira geração das normas de proteção de dados surgiu como reação ao processamento eletrônico de dados das organizações públicas e privadas, bem como às centralizações dos bancos de dados em gigantes bancos de dados nacionais (Mayer-Schönberger, 2001). São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o Fair Credit Reporting Act (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o Privacy Act (1974), aplicável à organização pública.

Às legislações nacionais seguiram importantes instrumentos internacionais e transnacionais que contribuíram para a consolidação do conceito de privacidade ligado à proteção de dados. Destacam-se, nesse contexto, a Convenção 108 do Conselho da Europa (1981), as Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados (1980) e a Diretiva Europeia 95/46/CE relativa à proteção de dados (1995).

Vale ressaltar, que a partir do momento em que a tecnologia permite o armazenamento e o processamento rápido e eficiente de dados, dá-se a associação entre proteção à privacidade e informações. Nesse contexto, percebe-se, uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada "privacidade informacional", "proteção de dados", "autodeterminação informativa", entre outros (Doneda, 2006).

Ao longo do desenvolvimento do conceito de privacidade como proteção de dados, estabeleceu-se, por meio de instrumentos internacionais e transnacionais, um consenso em torno de um quadro básico de princípios que devem nortear a atividade de tratamento de dados (Bennett, 1992, p. 95). Esses princípios têm como finalidade impor limitações ao tratamento de dados.

Outro princípio relevante é o da qualidade dos dados, exigindo que os dados constantes do banco sejam objeto de tratamento leal e lícito, adequados e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados. Tal princípio enseja cautela na formação do banco de dados, assim como constante atualização. No princípio da qualidade dos dados, incluem-se os direitos de acesso, retificação e cancelamento dos dados (Cueva, 1990, p. 187).

O princípio da segurança física e lógica refere-se à exigência de que o banco de dados esteja protegido contra extravios, destruições, modificações e desvios não autorizados (Doneda, 2006). Por fim, um importante princípio da matéria de proteção de dados é o princípio da responsabilidade, que visa assegurar a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade.

3.3 Lei Geral da Proteção de dados

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Defesa, 2020).

O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da

economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (Pinheiro, 2018).

Segundo Peixoto (2020) com sua entrada em vigor alguns de seus aspectos jurídicos começam a ser debatidos à luz do Marco Civil da Internet e, sobretudo, com o Código de Defesa do Consumidor (CDC), a exemplo do recente vazamento de dados da empresa Netshoes em que o MPDFT acordou um Termo de Ajustamento de Conduta (TAC) com a empresa.

Pensando nisso, a atuação das empresas no contexto digital trouxe consigo a necessidade de criação de mecanismos de regulação e proteção dos dados pessoais daqueles que utilizam serviços, compras ou realizam qualquer tipo de transação online que envolve o fornecimento de informações pessoais. Toda situação ou ação realizada no ambiente virtual faz parte da realidade de qualquer pessoa, portanto os direitos garantidos no "mundo *of line*" devem ser assegurados também no espaço virtual. Em virtude disso, é importante apontar que a lei brasileira não protege somente os dados pessoais nos meios digitais (Pinheiro, 2018).

Vale a pena ressaltar que, a Lei europeia (GDPR) está vigente, estabelecendo as regras atinentes ao tratamento de dados pessoais relativos a pessoas situadas na União Europeia. É bom lembrar que as empresas e órgãos estatais brasileiros que mantenham negócios com os países europeus terão a obrigatoriedade de garantir que suas políticas de tratamento de dados estão em conformidade com a GDPR, sob o risco de penalidades, bem como perda de clientela, valor de marca e credibilidade no mercado internacional (Peixoto, 2020).

A LGPD tem alcance extraterritorial, ou seja, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil. Desse modo, o dado pessoal tratado por uma empresa de serviço de *cloud computing* que armazene o dado fora do país terá que cumprir as exigências da LGPD (Pinheiro, 2018).

De acordo com Peixoto (2020), a LGPD terá um impacto dos mais significativos que uma legislação nacional já alçou.

A legislação é categórica: todos os dados tratados por pessoas jurídicas de direito público e privado, cujos titulares estejam no território nacional; ou a sua coleta se deu no país; ou ainda que tenha por finalidade a oferta de produtos ou serviços no Brasil, devem estar preparadas. Assim, não se trata de uma opção, mas de uma obrigação das empresas em se adequarem às normas brasileiras de proteção de dados pessoais (Peixoto, 2020).

Conforme Peixoto (2020), as medidas as serem tomadas para a proteção estarão no ranking de debates jurídicos, econômicos e sociais dos próximos anos, pois o tráfego crescente e os riscos de ataques e vazamentos de dados afetam praticamente toda a iniciativa pública e privada num país.

Milhões de informações pessoais circulam por redes virtuais diariamente. É cada vez mais frequente a exposição de dados em larga escala, mostrando as fragilidades de sistemas e protocolos, inclusive por parte de quem deveria fiscalizar a segurança das operações: o Estado (Peixoto, 2020).

Ao coletar dados, as empresas devem informar a finalidade. A lei previu uma série de obrigações para elas, que têm de manter registro sobre as atividades de tratamento, de modo que possam ser conhecidas mediante requerimento pelos titulares ou analisadas em caso de indício de irregularidade pela Autoridade Nacional. Quando receberem um requerimento do titular, a resposta às demandas tem de ser dada em até 15 dias (Valente, 2020).

Os negócios serão impactados profundamente, cabendo as empresas e instituições se protegerem de eventuais penalidades e, tão importante quanto, resguardarem-se da opinião pública negativa às que não se adaptarem, demonstrando ausência de confiabilidade ao mercado já que não conseguem garantir a proteção de seus bancos de dados (Peixoto, 2020).

Esses entes devem adotar medidas para assegurar a segurança das informações e a notificação do titular em caso de um incidente de segurança. Tal exigência vale para todos os agentes da cadeia de tratamento. Se um controlador causar dano a alguém por causa de uma atividade de tratamento, poderá ser responsabilizado e deverá reparar o prejuízo (Valente, 2020).

Existem diversos tipos de ataques cibernéticos e os bancos de dados conectados à internet estão em certo grau de vulnerabilidade. Um dos casos mais emblemáticos de negligência com informações foi o vazamento de dados de milhões de usuários do Facebook para a empresa britânica de marketing político, a Cambridge Analytica. No Brasil, tem-se a confirmação de dois casos recentes: o da Netshoes e do Banco Inter; e outro em apuração, o da empresa de proteção de crédito Boa Vista (Peixoto, 2020).

No caso do Poder Público, a lei dispensa o consentimento no tratamento de dados para políticas públicas previstas em leis, regulamentos e contratos. É permitido também o uso compartilhado de dados por entes públicos, desde que respeitados os princípios previstos na norma. Uma obrigação é que cada órgão informe as hipóteses de tratamento de dados, incluindo a base legal, a finalidade e os procedimentos empregados para tal (Valente, 2020).

Por sua vez, Peixoto (2020) relata que uma das ações mais imediatas em caso de exposição e vazamento é comunicar a Autoridade Nacional de Proteção de Dados (ANPD) em prazo razoável (que será definido pela própria autoridade).

A LGPD lista um conjunto de sanções para o caso de violação das regras previstas, entre as quais destacam-se advertência, com possibilidade de medidas corretivas; multa de até 2% do faturamento com limite de até R$ 50 milhões; bloqueio ou eliminação dos dados pessoais relacionados à irregularidade, suspensão parcial do funcionamento do banco de dados e proibição parcial ou total da atividade de tratamento (Valente, 2020).

Dessa maneira Peixoto (2020), destaca a importância de mencionar que já existem empresas que trabalham com certificação digital para sites empresariais e institucionais, como forma de melhorar a confiabilidade durante a navegação, ao atestar que o site está em conformidade com LGPD.

A fiscalização fica a cargo do Autoridade Nacional de Proteção de Dados (ANPD), órgão criado com vinculação à Presidência da República, com indicação no texto da lei de um estudo para um formato mais autônomo dois anos depois. Até agora, o Palácio do Planalto não instituiu a ANPD. No dia seguinte à derrota do adiamento do início da vigência proposto na Medida Provisória No 959, no fim de setembro, a Presidência editou decreto com a estrutura do órgão, mas, na prática, este ainda não existe (Valente, 2020).

3.4 Espaço Cibernético

O ciberespaço (ou espaço cibernético) é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a internet, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros. O termo foi criado por Willian Gibson em seu romance “Neuromancer”. (APDSI, 2005).

Segundo Vianna e Fernandes (2015) o espaço cibernético digital é constituído por sistemas de informação automatizados e redes de comunicação de dados, para provimento de informações a usuários e clientes em distintas organizações e para a sociedade.

Por sua vez, a ISO/IEC 27032 (2012), espaço cibernético é entendido como "um ambiente complexo resultante da interação de pessoas, *software* e serviços existentes na internet, conectados entre si por meio de dispositivos de tecnologia e redes, o qual não existe como forma física".

O espaço cibernético não se encontra restrito ao uso da internet ou dos computadores, como corrobora Klimburg (2012): o ciberespaço é mais do que a internet, incluindo não somente o *hardware*, *software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes.

Segundo Vianna e Fernandes (2015) os ataques cibernéticos simples ou individuais, causam males controláveis e prejuízos limitados, capazes de causar danos econômicos e de reputação significativos a vítimas dos setores público e privado, atingindo nações e grandes organizações mundiais.

Dessa forma, um ataque cibernético pode ocorrer sob diversas formas, sendo as mais relevantes: instalação de um programa ilícito como vírus, cavalos de troia ou spywares; negação de serviço disponibilizado (*Denial-of-Service* (DoS)); introdução de funcionalidades não autorizadas nos sistemas operacionais; inserção de vulnerabilidades em sistemas estratégicos, como os referentes a comandos não documentados que tornam possível a terceiros desabilitar ou alterar a operacionalidade desse sistema crítico; *hacking*: exploração das vulnerabilidades que manifestam em qualquer arcabouço de controles e sistemas integrados numa rede; infiltração de pessoas com objetivos diversos como: disponibilização de senhas que permitam o acesso externo de terceiros não autorizados e instalação prévia de programas hostis que produzam ou facilitem o ataque e modificações de *hardware* (Wallier Vianna, 2011).

Uma pesquisa do Fórum Econômico Mundial, mostra que uma grande parte das organizações tem consciência do aumento dos riscos cibernéticos nos últimos anos, entretanto, muitas dessas instituições acreditam que não estarem adequadas para gerenciar esses riscos, o que pode acarrear sérios prejuízos à marca, espionagem corporativa, bem com os custos dessas violações.

Schwab e Davis (2019) ressalta que eliminar a lacuna entre a ciência/condescendência de sua incapacidade frente aos crimes cibernéticos e promover meios capazes de impedi-los é essencial para a segurança e desenvolvimento das empresas, governos e organização da sociedade civil.

3.4.1 Segurança da Informação e a Segurança Cibernética

O termo cibernética se refere ao uso de redes de computadores e comunicações e a interação dentro de sistemas utilizados por exemplo por organizações digitais. Nesse sentido, Mandarino Júnior (2009), define segurança cibernética como a arte de assegurar a existência e a continuidade da sociedade da informação, garantindo e protegendo, no espaço cibernético, os ativos de informação e as infraestruturas críticas (IC).

De acordo com Vianna & Fernandes (2015) a segurança cibernética, também conhecida como segurança digital ou do espaço cibernético, é uma evolução de segurança da informação. A segurança cibernética está inserida no contexto amplo e multifacetado da segurança da informação, em consonância com o descrito pela Academia Latino-Americana da Segurança da Informação (2006)**:**

> A segurança da informação tem como propósito proteger as informações registradas, sem importar onde estejam situadas: impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem.

Já Coelho e Araújo define a Segurança da Informação como proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

A norma ISO/IEC 27032 (2012) *Guidelines for cybersecurity (*Diretrizes para a segurança cibernética*)*, alinhada com o "espírito" de segurança da informação inerente à família das normas internacionais 27000, define segurança cibernética como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético (ISO/IEC 27032, 2012).

Já a norma ISO/IEC 27002 (2005), afirma que a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e

as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software (Coelho & Araújo, 2013).

A Figura 1, extraída da ISO/IEC 27032 (2012) ilustra uma forma de inserção da segurança cibernética no campo da segurança da informação.

Figura 1 – Relacionamento entre segurança cibernética e outras seguranças.

Fonte: Adaptado de ISO/IEC 27032 (2012).

A NBR ISO/IEC 27002 (2013) afirma que a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios ou cumprimento da missão de uma organização e consequentemente necessita ser protegida, descreve também que segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao mesmo, maximizar o retorno sobre investimentos e as oportunidades de negócio.

Em relação aos eventos que possam comprometer a segurança das informações, a Norma Complementar n. 05/IN01/DSIC/GSIPR (Brasil, 2009), promovida pelo órgão responsável por normatizar a segurança da informação no estado brasileiro, define que um incidente de segurança "é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores". No trato com incidentes de segurança, devem ser observados os seguintes aspectos:

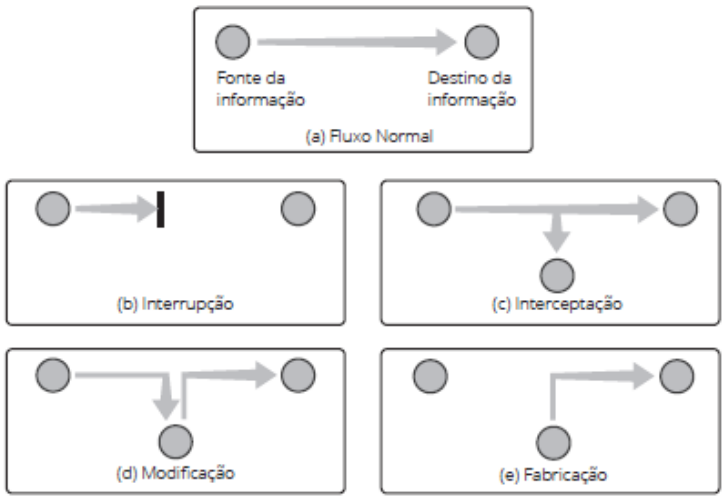
-Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a um sistema cibernético ou a seus dados;

- ✓ interrupção indesejada ou negação de serviço prestados pelo sistema;
- ✓ uso não autorizado de um sistema para processamento ou armazenamento de dados;
- ✓ furto de informação sigilosa em formato eletrônico digital;
- ✓ extorsão via o uso de computadores;
- ✓ modificações nas características de *hardware*, *firmware* ou *software* de um sistema, sem o conhecimento, instruções ou consentimento prévio do responsável pelo sistema;
- ✓ obtenção, guarda e preservação de evidências;
- ✓ detecção (monitoração de redes e sistemas para detecção de intrusão, ou da tentativa);

- ✓ violação ou quebra da Política de Segurança da Informação (PSI) de forma explícita ou implícita.

A Figura 2 ilustra quatro possíveis modelo de ataque, sendo eles: interrupção, interceptação, modificação e fabricação. A interrupção consiste quando um ativo é destruído ou torna-se indisponível, caracterizando um ataque contra a disponibilidade. A interceptação é quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), caracterizando um ataque contra a confidencialidade.

Figura 2 – Modelos de ataques.



Fonte: Coelho & Araújo (2013).

A modificação é quando um ativo é acessado por uma parte não autorizada é alterado, caracterizando um ataque contra a integridade. Já a fabricação é quando uma parte não autorizada insere objetos falsificados em um ativo, caracterizando um ataque contra a autenticidade (Coelho & Araújo, 2013).

3. 5 Ataques Cibernéticos na pandemia da COVID 19

Segundo o Correios Braziliense (2020) o número de vítimas de crimes praticados pela internet aumentou no período de pandemia. O aumento no período em que as pessoas passam conectadas e novos comportamentos impostos em função do novo coronavírus, como maior adesão da população às compras pela internet, têm contribuído para a ação de criminosos. Segundo registros da Polícia Civil do Distrito Federal (PCDF), entre março e junho de 2020, os crimes de estelionatos praticados pela internet aumentaram 198,95%. Já os de furto mediante fraude subiram 310,97%. De março a junho de 2019, foram 82 enquanto, no mesmo período de 2020, houve 337 ocorrências registradas.

Segundo o Jornal Daqui (2020) Em Minas, o número de crimes cibernéticos aumentou quase 50% em comparação ao ano passado. Segundo dados da Polícia Civil, de janeiro a maio deste ano, foram registrados 3.070 casos de crimes cibernéticos, quase 606 registros a mais que no mesmo período de tempo em 2019.

De acordo com Gatefy (2020) De acordo com a agência europeia, campanhas de phishing e spam têm sido muito utilizadas com o objetivo de coletar credenciais e outros dados pessoais e confidenciais. Além disso, e-mails são usados para infectar usuários com software malicioso, ou malware. Com o objetivo de extorquir dinheiro e roubar dados pessoais e sensíveis, os hackers se aproveitaram do cenário de pânico causado pela COVID para distribuir malware, ransomware e aplicativos maliciosos visando indivíduos, empresas e outras organizações. Sobre a dark web, no contexto da pandemia, a

agência europeia diz que a plataforma tem sido usada para a comercialização de produtos falsificados relacionados à COVID-19, como máscaras, produtos farmacêuticos e kits de testes. Segundo o relatório da Europol, casos e tentativas de exploração sexual infantil têm sido uma ameaça constante durante a pandemia. A agência diz, inclusive, que houve um aumentou na incidência de referências a sites ilegais envolvendo exploração sexual infantil (Gatefy, 2020).

4. Considerações Finais

A tecnologia está cada vez mais avançada, e durante a pandemia do COVID-19 onde as pessoas e as organizações tiveram que se reinventar os crimes virtuais ganharam espaço nas redes. Em consequência do isolamento social, as pessoas estão mais conectadas e acabam correndo mais riscos e assim surgiram diferentes ataques cibernéticos durante a pandemia COVID-19 no Brasil.

As tecnologias digitais exercem papel crucial nesses tempos de pandemia, tendo um aumento no acesso, bem como o aceleramento no uso de algumas ferramentas a Inteligência Artificial, a qual está sendo bastante aplicada na área da saúde, seja no monitoramento de pacientes infectados, na busca de desenvolver vacinas, para citar alguns. Nesse sentido, vale ressaltar que essas transformações provocadas no uso das tecnologias digitais trazem imensos desafios seja no campo ético na regulação de uso, na área de segurança e proteção dos dados, respeito aos direitos fundamentais de privacidade, na era pós-Covid-19.

Sendo assim, as premissas abordadas no objetivo final foram contempladas com sucesso, abordando os contextos da proteção de dados, a lei que rege a proteção de dados e alguns ataques que surgiu durante o contexto da pandemia COVID-19.

Referências

Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI). (2005). Glossário da Sociedade da Informação. Portugal: APDSI.

Academia Latino-Americana de Segurança da Informação. (2006). Introdução à Segurança da Informação. Microsoft TechNet. http://www.nerdbb.com/download/file.php?id=2618.

Brasil. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. (2009). "Norma Complementar n. 05/IN01/DSIC /GSIPR." Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Diário Oficial [da] República Federativa do Brasil (156), agosto. Seção 1.

Cavazzini, L. S., Cavalcanti, L. de L., Machado, A. R., Denny, D. M. T. & Saleme, E. R. (2018). Aplicabilidade da indústria 4.0 na cadeia produtiva agroindustrial: sonho ou realidade? VIII Congresso Brasileiro de Engenharia de Produção.

Coelho, F. E.S., Araújo, L. G. S. (2013). Gestão da Segurança da Informação NBR 27001 e 27002. Escola Superior de Redes.

Correio Braziliense. (2020). Registros de golpes na internet crescem 310% no DF durante a pandemia. https://www.correiobraziliense.com.br/cidades-df/2020/08/4868977-mais-golpes-na-pandemia.html. Acesso em: 01 de fevereiro 2021.

Doneda, D. (2006). *Da privacidade à proteção de dados pessoais*. Editora Renovar.

Gatefy. (2020). Como a Covid-19 impactou os crimes cibernéticos, segundo a Europol. https://gatefy.com/pt-br/blog/covid19-crimes-ciberneticos-relatorio-europol/. Acesso em: 01 de fevereiro 2021.

Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Socia*l. (6a ed.), Atlas.

International Organization for Standardization. (2012). ISO/IEC 27032: Information technology: Security techniques: Guidelines for cybersecurity. Geneva: ISO/IEC.

International Organization for Standardization. (2014). ISO/IEC 27000: Information technology: Security techniques: Information security management systems: Overview and vocabulary. Geneva: ISO/IEC.

Jornal Daqui. (2020). Crimes Cibernéticos Crescem Durante a Pandemia da Covid-19. https://www.daquibh.com.br/crimes-ciberneticos-crescem-durante-a-pandemia-da-covid-19/.

Schwab, K. (2016). *A Quarta Revolução Industrial.* Editora Edipro Edições Profissionais Ltda.

Schwab, K. (2019). Aplicando a Quarta Revolução Industrial. Prefácios de Satya Nadella, João Doria, Tradução: Daniel Moreira Miranda. Edipro, Título original: Shaping the fourt Industrial Revolution.

Sêmola, M. (2003). *Gestão da Segurança da Informação – uma visão executiva*. Campus.

Klimburg, A. (2012). *National cyber security framework manual*. Talinn: NATO CCD COE Publication.

Mandarino Júnior. R. (2009). Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. Brasília.

Pinheiro, P. P. (2018). Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) / Patrícia Peck Pinheiro. – São Paulo: Saraiva Educação. 1. Direito à privacidade - Legislação - Brasil 2. Direitos fundamentais 3. Proteção de dados - Legislação I. Título. 18-1667 CDU 342.7(81)

Transformação Digital. Página Inicial. (2018). http://transformacao.digital.

Vianna, E. W. & Fernandes, J. H. (2015). C. O Gestor da Segurança da Informação no Espaçop Cibernético Governamental: Grandes Desafios, Novos Perfis e Procedimentos.

Wallier Vianna, Eduardo. (2011). "Procedimentos para a gestão de incidentes de segurança nas redes de computadores da Administração Pública Federal." Monografia de Especialização, Universidade de Brasília. http://dsic.planalto.gov.br/documentos/cegsic/monografias_2009_2011/16_Eduardo_Wallier.pdf.