ARTIGO

DOI: https://doi.org/10.21721/p2p.2022v9n1.p206-221

Submetido em: 26/05/2022 Aceito em: 28/09/2022 Publicado em: 29/09/2022

GESTÃO DA SEGURANÇA DA INFORMAÇÃO:

análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira

Paulo Ricardo Silva Lima[1]
Universidade Federal de Pernambuco - UFPE
pauloricardo.admpublic@gmail.com

Leonardo Matheus Marques Ferreira[2]
Universidade Estadual de Alagoas - UNEAL
leonardomarques033@gmail.com

Ana Lydia Vasco de Albuquerque Peixoto[3]
Universidade Estadual de Alagoas - UNEAL
analydia.peixoto@uneal.edu.br

Resumo

As tecnologias são importantes ferramentas para o alcance da eficiência e qualidade dos serviços prestados pela administração pública brasileira. Uma prática comum que tem se alastrado no ciberespaço é a violação da privacidade, o acesso e a apropriação indevida de dados e informações públicas, causando prejuízos aos órgãos e a sociedade. O objetivo desta pesquisa é analisar as normas brasileiras de proteção de dados e informações no âmbito da administração pública brasileira, bem como as estratégias que podem ser adotadas para uma maior gestão da segurança de dados e informações públicas. Quanto à metodologia, trata-se de uma pesquisa de revisão bibliográfica e documental, de cunho qualitativo, utilizando a abordagem descritiva. A aplicação de leis como a Lei Geral de Proteção de Dados, Lei de Acesso à Informação, o seguimento das diretrizes do Marco Civil da Internet, atrelados aos serviços de *Pentests* e criação de equipes de cibersegurança com profissionais com perfil hacker ético, potencializam a criação de políticas e técnicas de segurança, garantido assim a proteção de dados e informações públicas.

Palavras-chave: Cibersegurança. Gestão da segurança da informação. Proteção de dados e informações.

INFORMATION SECURITY MANAGEMENT:

analysis of cyber defense policies and strategies for the protection of data and information of the Brazilian public administration

Abstract

Technologies are important tools for achieving the efficiency and quality of services provided by the Brazilian public administration. However, a common practice that has spread in cyberspace is the violation of privacy, access and misappropriation of public data and information, causing damage to agencies and society. In this sense, the objective of this research is to analyze the Brazilian data and information protection standards within the Brazilian public administration, as well as the strategies that can be adopted for a greater management of the security of data and public information. As for the methodology, it is a research of bibliographic and documental review, of a qualitative nature, using the descriptive approach. The application of laws such as the General Data Protection Law, the Access to Information Law, compliance with the guidelines of the Marco Civil da Internet, linked to Pentests services and the creation of cybersecurity teams with professionals with an ethical hacker profile, enhance the creation of of security policies and techniques, thus guaranteeing the protection of public data and information.

Keywords: Cybersecurity. Information security management. Data and information protection.

[1] Mestrando em Ciência da Informação pela Universidade Federal de Alagoas- UFAL.
[2] Graduando em Administração Pública pela Universidade Estadual de Alagoas (UNEAL).
[3] Mestre e Doutora em Medicina Veterinária pela niversidade Federal Rural de Pernambuco.

1 INTRODUÇÃO

Os sistemas informacionais e as tecnologias digitais têm contribuído significativamente para a prestação de serviços realizados pela administração pública brasileira com qualidade, alcançando assim o princípio constitucional da eficiência. Através de *sites* e aplicativos, o cidadão pode obter certidões, emitir boletos e realizar procedimentos de agendamento de consultas médicas, atendimento em departamentos administrativos, dentre outros, o que traz comodidade e praticidade. A exemplo disso, pode-se citar os portais de transparência, os quais foram instituídos com o advento da Lei de Acesso à Informação (LAI), nos quais estão disponíveis informações relativas aos investimentos em educação, saúde, segurança, dentre outros.

Apesar de todos os benefícios trazidos pelas tecnologias para a administração, observa-se que muitos órgãos públicos brasileiros não possuem sistemas de segurança e proteção de dados e informações, os quais podem ser utilizados ilicitamente por qualquer indivíduo qualificado em *hackear softwares*, trazendo prejuízos à instituição, bem como a violação de direitos fundamentais dos cidadãos, como à privacidade e à imagem.

Buscando inibir essas formas de uso indevido, o legislador brasileiro tem criado algumas normas legais que visam a segurança de dados e informações, as relações no ciberespaço de forma ética, e penalidades para violações ilegais de dados de terceiros. São exemplos dessas normas a Lei Geral de Proteção de Dados (LGPD) de 2018, a Lei de Acesso à Informação (LAI) de 2011, o Marco Civil da Internet (MCI) de 2014, e a ISO 27000.

Diante do exposto, o objetivo desta pesquisa é analisar as normas brasileiras de proteção de dados e informações no âmbito da administração pública brasileira, bem como as estratégias que podem ser adotadas para uma maior gestão da segurança. Quanto à metodologia, trata-se de uma pesquisa de revisão bibliográfica e documental, de cunho qualitativo, utilizando a abordagem descritiva.

2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO E ATAQUES CIBERNÉTICOS

A segurança da informação está relacionada à proteção de dados e informações, seja de um indivíduo, seja de uma organização, podendo esta ser do setor privado ou órgão da administração pública. Necessário esclarecer que os dados das organizações podem ser reconhecidos como ativos valiosos que precisam ser protegidos e preservados contra invasões cibernéticas e uso indevido de terceiros. Pensando na importância dos dados e informações no âmbito público, os gestores precisam garantir a defesa de seus ativos com estratégias e

medidas de segurança utilizando políticas e áreas especializadas em cuidar dos três pilares da informação conhecidos como confidencialidade, integridade e disponibilidade (CID).

Nessa perspectiva, Bruno Fraga (2019, p. 14) esclarece que

> A Tríade CIA (Confidentiality, integrity and availability) - confidencialidade, integridade e disponibilidade - representa os principais atributos que, atualmente orientam, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger.

No que diz respeito a confidencialidade, Oliveira, Moura e Araújo (2012) explicita que este atributo se refere a autorização de acesso às informações apenas a pessoas autorizadas, as quais também têm a incumbência de impedir o acesso de estranhos sem prévia indicação. Essa atuação do gestor previne a perda e a divulgação de dados e informações sensíveis ou sigilosas.

A integridade da informação ocorre sem que haja alteração em seus dados, são confiáveis, atualizadas e sem erros. De acordo com Neto e Araújo (2019, p.28) "Toda informação deve ser mantida na mesma condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais." As organizações pensando nessa característica da informação têm estabelecido algumas estratégias para que o conteúdo não seja manipulado ou violado, como por exemplo, converter documentos em formatos não modificados, solicitar assinatura digital nos documentos, dentre outras.

Para Bruno Fraga (2019, p. 14), quando se trata da disponibilidade da informação, esta deve estar sempre disponível com o uso legítimo daqueles usuários autorizados a terem acesso à informação pelo proprietário. No contexto da administração pública, existem os conhecidos Portais de Transparência, espaços no ambiente digital, nos quais estão disponíveis informações quanto aos investimentos em saúde, educação, lazer, dentre outros em prol do coletivo, esse é o exemplo mais claro dessa disponibilidade da informação, a qual pode ser acessada por qualquer cidadão interessado e com acesso à internet. Mesmo sendo uma obrigação da administração disponibilizar informações à sociedade nos portais de transparência, o gestor também precisa pensar em estratégias de forma que esse pilar não seja derrubado e evitando os prejuízos ao cidadão e a própria administração. Existem ataques como o DDoS (*Distributed Denial of Service*) ou o DoS (*Denial of Service*) que são ferramentas de Negação de Serviços muito usadas por *crackers* para deixar o serviço indisponível e como consequência a quebra do pilar.

De acordo com Santos e Silva (2021, p. 9) "[...] a Gestão da Segurança da Informação baseia-se na interação entre processos, procedimentos, controles, melhores práticas e tecnologias para nortear os modelos atualmente utilizados". Segundo Marcondes (2020) existem quatro funções da gestão de segurança da informação que podem ser adotadas pelas organizações, sendo elas o Planejamento, Organização, Direção e Controle. O planejamento trata-se de realizações de processos administrativos com ações e medidas preventivas para reduzir as vulnerabilidades e possíveis invasões. A organização está relacionada aos procedimentos internos de recursos humanos, dos *hardwares*, procedimentos, políticas e outros. A direção contempla a capacidade de os gestores de liderar as equipes e motivar através de uma boa comunicação em alcance dos objetivos estabelecidos, ou seja, coordenando e orientando as equipes. E além desses, o controle de identificar as falhas e por fim corrigi-las.

Contudo, torna-se importante a presença de profissionais especializados para cuidar com qualidade dos ativos da organização ou instituição. O mercado de *hacking*, da segurança digital ou da informação tende a crescer bastante por razões das intrusões por criminosos em sistemas vulneráveis e, consequentemente, ocorrendo a exploração do alvo. O Brasil está começando agora a desenvolver ações preventivas, fazendo estudos de políticas de segurança, análises de riscos, entre outros. De acordo com o Governo Federal (2021), o "Brasil subiu 53 posições e passou do 71º para o 18º lugar no Índice Global de Segurança Cibernética 2020, divulgado nesta semana pela União Internacional de Telecomunicações (UIT)". É provável que o Brasil venha a ter mais invasões, principalmente nos órgãos públicos apresentando uma maior vulnerabilidade pela falta de investimento na segurança dos ativos. Conforme com a Boletim Sec (2022) "Com base em uma pesquisa conduzida de forma independente, os governos locais são os menos capazes de impedir ataques de *ransomware* e recuperar *backups*, e muitas vezes pagam o resgate para recuperar os dados."

Desta forma a gestão da informação é trabalhada através de normas e princípios em políticas de segurança com o objetivo de evitar o vazamento de dados sigilosos e de invasões cibernéticas. Atualmente observa-se com mais frequência ataques *hackers* conhecidos como *crackers*, que buscam organizações vulneráveis para organizar um ataque direcionado em um alvo específico (ou não), nesse caso o atacante está buscando qualquer organização que tenha qualquer tipo de vulnerabilidade para se explorar e ganhar com isso, seja exigindo um determinado valor de *bitcoins* ou vendendo os ativos na *dark web* que é um local anônimo e descentralizado.

Um acontecimento bem recente ocorrido em 2021, de ataque cibernético pelo grupo *Lapsus$*, foi no sistema do Conecte SUS deixando o site indisponível para os usuários que fossem acessar o serviço de vacinação. Com isso, solicitando resgate de pagamento para devolução dos dados roubados. Esse tipo de ataque é conhecido de *Ransomware* que após infectar o computador ou servidor faz uma encriptação dos dados armazenados e depois resgatando em Bitcoins de moeda descentralizada e não rastreável. Por isso, é essencial que o órgão público trabalhe na segurança da informação e cibernética com profissionais especializados e na qualificação através de treinamentos dos servidores públicos.

Muitas invasões ocorrem na modalidade chamada de Engenharia Social que manipula a vítima em apenas do benefício do invasor. Um exemplo bem comum é o *hacker* criminoso enviando um *e-mail* com gatilhos mentais para que a vítima clique em um *link* malicioso e infectando a máquina, até podendo ganhar acesso a um servidor e também sendo possível a escalação de privilégio *Root* com permissão total. Diante disso, pode fazer o que quiser com aqueles dados como deletando, encriptando e pedindo resgate para devolver os dados, porém em muitos casos acontece que mesmo pagando o *cracker* não devolve e vai vender em outros locais interessados.

Buscando minimizar os ataques, o legislador brasileiro desenvolveu algumas normas específicas que versam sobre a proteção de dados (Lei nº 13.709/2018 - Lei Geral de Proteção de Dados), sobre comportamento ético na rede mundial de computadores (Lei nº 12.965/2014 - Marco Civil da Internet), sobre disponibilização de dados públicos em portais de transparência (Lei nº 12.527/2011 - Lei de Acesso à Informação), como também relacionado a certificação de segurança na internet (ISO 27000).

3 ANÁLISE DAS NORMAS DE SEGURANÇA E PROTEÇÃO DOS DADOS E INFORMAÇÕES DA ADMINISTRAÇÃO PÚBLICA NO CIBERESPAÇO

A Política de Segurança da Informação (PSI) é um conjunto de normas e princípios que devem ser implementados e atualizados em conformidade com a LGPD. Para o Tribunal de Contas da União – TCU (2012, p. 14) “Cabe destacar que a PSI pode ser composta por várias políticas inter-relacionadas, como a política de senhas, de backup, de contratação e instalação de equipamentos e softwares”. Além disso, analisar em práticas claras e objetivas de forma que fique de fácil entendimento e sempre atuando em diretrizes e regras de melhoria da segurança da informação da administração pública.

3.1 LEI DE ACESSO À INFORMAÇÃO (LAI)

A Lei nº 12.527/2011 intitulada de Lei de Acesso à Informação, regulamenta o direito dos cidadãos do acesso à informação de interesse particular ou geral nos órgãos públicos, previsto no artigo 5º da Constituição Federal que altera a Lei nº 8.112 de 11, de dezembro de 1990 e revoga a Lei nº 11.111, de 5 de maio de 2005.

No artigo 1º da referida é explicada o seguinte:

> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
> Parágrafo único. Subordinam-se ao regime desta Lei:
> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2011).

Com essa Lei o povo brasileiro tem o direito de solicitar através de meios legítimos como via *e-mail* com a identificação do requerente e das especificações do acesso à informação conforme o artigo 10, aqueles dados e informações públicos de seu interesse. Além disso, no artigo 11 alude que se deve ser disponibilizada a informação de acesso imediato e caso não seja possível será entregue um prazo de 20 dias, podendo ser prorrogado por mais 10 dias mediante uma justificativa. Contudo, há exceção em dados sigilosos que não serão concedidos o acesso. Esse direito é fundamental para que o cidadão também possa fiscalizar e analisar a administração pública (BRASIL, 2011).

Segundo o Art.31 da lei que versa sobre Informações Pessoais, o legislador brasileiro cristalizou que o tratamento das informações deve ser trazido de forma transparente com cuidados em dados sensíveis que residem na proteção dos direitos fundamentais, tais como a intimidade, honra e imagem das pessoas, em liberdades e os direitos individuais. Diante disso, é necessário que os órgãos públicos tenham ética com esse tratamento desses dados e informações.

3.2 MARCO CIVIL DA INTERNET

A Lei nº 12.965/2014, Marco Civil da Internet (MCI), está interligada ao respeito à liberdade, aos direitos humanos e às políticas de privacidade dos dados. Qualquer tipo de

aplicação ou serviço na *Web* precisa de um consentimento do usuário para que deixe claro a forma que irá tratar seus dados. Nessa perspectiva, no uso comum de *sites* e aplicativos, ao iniciar a criação de um perfil para ter acesso aos serviços e produtos ofertados naquele ambiente, que os proprietários dos direitos daquela plataforma solicitem o aceite das políticas de privacidade deles, e através disso, o usuário precisa ler e posteriormente, se estiver de acordo aceitando os seus termos, aceitar. Para Lucas Badesco (2018) "a lei veta o uso e fornecimento dos dados para finalidades às quais o usuário não consentiu."

Dentro do artigo 3º do MCI, entende-se como seus principais princípios sendo a garantia da liberdade de expressão, privacidade, proteção dos dados pessoais e a preservação da neutralidade na rede ou internet. Logo, torna-se fundamental essa garantia da privacidade e da proteção dos dados compartilhados pela internet e essa lei veio para dar uma maior segurança para os usuários, pois, informações inseridas e cadastradas nas plataformas precisam estar asseguradas que estão sendo mantidas com seguranças.

No artigo 7º são assegurados os seguintes direitos abaixo:

> I. inviolabilidade da intimidade e da vida pessoal[...];
> II. inviolabilidade e sigilo do fluxo de suas comunicações pela internet [...];
> III. inviolabilidade e sigilo de suas comunicações privadas armazenadas [...];
> IV. não suspensão da conexão à internet [...];
> V. manutenção da qualidade contratada da conexão à internet;
> VI. informações claras e completas constantes dos contratos de prestação de serviços [...];
> VII. não fornecimento a terceiros de seus dados pessoais [...];
> VIII. informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais [...].

Esses princípios estão relacionados a uma entrega de garantia da segurança da informação de enfoque a proteção com criptografia de ponta dos dados coletados que mesmo com vazamento ainda não consiga visualizar a leitura dos dados armazenados nos bancos de dados, da privacidade sem o compartilhamento dos dados a terceiros e todas informações objetivas sobre a coleta e dos tratamentos de dados.

Entretanto, mesmo com todas as recomendações da LAI quanto do MCI, observa-se que as plataformas e bancos de dados públicos possuem fragilidades quanto à segurança das informações organizacionais e dos cidadãos, o que reforça a necessidade de práticas computacionais que fortaleçam esses ambientes.

3.3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Na Lei nº 13.709/2018, denominada de Lei Geral de Proteção de Dados (LGPD), que passou a ser validada em 2021, são apresentadas uma série de direitos e obrigações das organizações públicas e privadas que focalizem na regularização da proteção e segurança de dados. “A LGPD visa proteger os direitos de liberdade e de privacidade, criando normas a serem seguidas por empresas e governos para a coleta e o tratamento de dados pessoais [...]” (OLIVEIRA; TILT, 2021). Diante do exposto, a referida norma encontra-se também fundamentada na liberdade, privacidade e no livre desenvolvimento da personalidade da pessoa natural.

Pode ser entendido no artigo 1º na relação dos tratamentos de dados pessoais, seja em pessoa natural ou jurídica de direito privado em empresas particulares e estatais ou pública tais como a União, estados, Distrito Federal, territórios, municípios e autarquias. Através dessa norma, toda empresa tem o dever e a obrigação de estar regulamentada com a LGPD em tratar os dados pessoais com privacidade, criptografia, liberdade de expressão sem a violação da intimidade, da honra e da imagem do cidadão.

No atual contexto sócio histórico, marcado pela Pandemia da Covid-19, verificou-se ataques cibernéticos direcionados aos bancos de dados públicos e as informações em ambientes digitais de empresas privadas, organizados pelos *hackers*. O que se observa também paralelo a isso, é que a nova geração está se tornando cada vez mais digital e conectada na internet em muitos dispositivos como computadores, celulares, lâmpada smart, TV smart e tantos outros que já estão inseridos na rede. Estes dispositivos conhecidos de *Internet of Things* (IoT) ou a Internet das Coisas, são alvos de cibercriminosos.

Na administração pública é mais suscetível a invasões e como há diversas falhas que podem serem encontradas mais facilmente por *hackers,* uma vez que é comum não haver análises de riscos, análise de vulnerabilidades e serviços como *Pentest* - teste de intrusão ou até mesmo em uma equipe de *Red Team* que em português significando Time Vermelho, o qual atua de forma mais ofensiva, realizando, por exemplo, ataques simulados de alguma brecha de *software* vulnerável e até mesmo com exploração da vulnerabilidade humana com técnicas de engenharia social, manipulando vítimas direcionadas que possuem uma maior chance de serem exploradas.

Além disso, há o *Blue Team* - Time Azul, e o seu foco principal é a defesa em ciberataques, monitorando logs de acessos, *firewalls*, gerenciamento de riscos, resposta de incidentes e identificar possíveis ameaças. Logo, para se adaptar melhor a LGPD é importante

que os órgãos públicos mantenham em suas estruturas um setor especializado em cibersegurança com equipes traçadas com funções específicas de *Red Team* e de *Blue Team*.

Na administração brasileira, as falhas de segurança podem tornar o órgão vulnerável a diversas investidas de terceiros mal intencionados, o que pode resultar em incidentes de invasões, vazamentos de dados confidenciais, deixando os serviços indisponíveis, alterando a integridades dos arquivos e isso quebra os pilares que devem ser mantidos com segurança e consequentemente violando a LGPD.

De acordo com Bruna Souza (2020) "Ao que tudo indica, a invasão aos sistemas do STJ na última semana usou o ransomware, um programa malicioso que sequestra dados e exige resgate para devolvê-los". Essa invasão do STJ é um dos muitos exemplos de casos de vítimas em ciberataques.

Apesar do gestor da Tecnologia da Informação (T.I.), muitas vezes, se preocupar apenas em aderir softwares com uma melhor segurança, é perceptível a falta de investimento em treinamentos e capacitações das equipes, o que privilegia uma maior vulnerabilidade e consequente ocorrência de invasões.

Em muitos setores públicos há vulnerabilidades de segurança pelo fato haver muitos usuários que sequer cadastram uma senha segura com letras maiúsculas, minúsculas, números e caracteres especiais, colocando genericamente uma senha como 123456, data de nascimento, e que por muitas vezes nem altera a senha provisória que é lhe entregue.

Oportuno se faz destacar que nenhum sistema é totalmente seguro, sempre vai ter falhas para serem corrigidas, assim como os próprios profissionais da tecnologia podem serem alvos de ataques, como por exemplo, enviando um e-mail com a mesma identificação de seu superior e inserindo no título da mensagem de URGÊNCIA, um gatilho mental da urgência. Esse tipo de informação, faz com que a vítima acesse tal link sem pensar que pode ser um hacker no outro lado esperando apenas ter o acesso a máquina, servidor ou até mesmo comprometendo vários dispositivos na rede, com o usuário baixando algum backdoor malicioso como o Cavalo de Tróia (em inglês *Trojan*), que é um tipo de exploit para explorar vulnerabilidades.

Desta forma, é muito importante analisar cada uma dessas etapas e planejar como será feito o tratamento de dados através de um mapeamento de dados com monitoramento de logs de acessos, coleta de dados, análises de vulnerabilidades, explorar falhas com técnicas de invasão, PoC em inglês *Proof of concept* (Prova de conceito) com um relatório de todas os procedimentos realizados.

3.4 ISO / IEC 27001

A ISO 27001 é uma norma internacional apresentada pela *International Standardization Organization* (ISO) com o seu enfoque na gestão da segurança da informação através de políticas de segurança e gestão de riscos com finalidade de adequar organizações com ou sem fins lucrativos, empresas privadas e públicas. Teve colaboração na criação da norma vários especialistas com o objetivo de padronizar uma norma internacional com metodologia de implementação. Além disso, uma empresa ou pessoa física pode obter certificação da ISO 27001.

Para proteção dos pilares da segurança da informação é uma boa prática esta implementação quanto para se adequar a Lei Geral de Proteção de Dados (LGPD). Tornou-se a norma mais reconhecida pelas organizações internacionais e muito usada na obtenção da certificação.

3.4.1 Como implementar a ISO/IEC 27001

A implementação como forma também de maior adequação da LGPD com a ISO 27001 usada internacionalmente no quesito da segurança da informação e na defesa cibernética. Conforme Mesquita (2020) é explicada as seguintes etapas de implementação da ISO 27001:

1. Obter apoio da alta direção e realizar o planejamento de todas atividades necessárias;
2. Definir o escopo do Sistema de Gestão de Segurança da Informação.;
3. Definir a metodologia de identificação, avaliação e tratamento de riscos;
4. Escrever a declaração de aplicabilidade que contenha os controles necessários;
5. Escrever o plano de tratamento de riscos;
6. Definir como será mensurado o nível de eficácia dos controles;
7. Implementar todos os controles e procedimentos aplicáveis de acordo com a declaração de aplicabilidade;
8. Implementar programas de treinamentos e conscientização;
9. Executar todas as atividades diárias definidas pela documentação do Sistema de Gestão de Segurança da Informação;
10. Monitorar e avaliar o Sistema de Gestão de Segurança da Informação;
11. Realizar auditoria interna e análise crítica;
12. Implementar ações corretivas caso seja necessário.

Diante disso, o benefício da implementação torna-se reconhecido internacionalmente através de seu controle na gestão da segurança da informação. Com sua aplicação, é possível

haver uma redução de riscos como a minimização de incidentes na organização como em invasões e consequentemente na redução de custos.

Trata-se de uma prioridade na segurança dos ativos do órgão público e planejar estrategicamente em planos de mitigação de riscos como uso de softwares mais seguros, podendo como também em sistemas livres (Gratuitos), possibilitando adaptação da organização no time de desenvolvimento de tecnologia da informação e qualquer falha que seja encontrada corrigindo-a.

Tendo em vista que a certificação pode ser obtida por uma organização com a finalidade de estar em conformidade com as cláusulas mandatórias de norma de segurança da informação. Também a pessoa física ou indivíduo, poderá realizar o exame pela *Exin* e obter a certificação. Isso contribui bastante no desenvolvimento e dos avanços da cibersegurança tanto no órgão público quanto nas empresas.

3.5 PRINCIPAIS ESTRATÉGIAS PARA TORNAREM OS SISTEMAS INFORMACIONAIS SEGUROS NA ADMINISTRAÇÃO PÚBLICA BRASILEIRA

A cibersegurança é uma prioridade em qualquer organização, contudo, não é visto isso tanto na administração pública brasileira, pois, nos órgãos públicos o que se tem muitas vezes é apenas um setor da Tecnologia da Informação (T.I.), com vários tipos de funções, incluindo os cuidados de segurança da informação.

Na perspectiva de Kaspersky (2022) a cibersegurança tende a proteger computadores, servidores,dispositivos móveis, redes e dados dentre outros que viram alvo dos atacantes. Nesse sentido, sugere-se a criação de um setor exclusivo para o tratamento de dados e das análises de vulnerabilidades.

Logo, também é preciso a contratação em serviço de *Pentest* - Teste de Intrusão, simulando realmente ataques e buscando falhas em aplicações web (sites), estudando os comportamentos da empresa e dos colaboradores com a possibilidade da exploração da técnica da engenharia social, verificando se estão tendo treinamentos ou capacitações para identificar imediatamente a tentativa de invasão. Para Bruno Fraga (2019, p. 19) as etapas de invasão são:

- **Conhecer:** A coleta de informações do alvo, como e-mails, funcionários, usuários, telefones, tecnologias e o uso da técnica de *Google Hacking* muito utilizada por *hackers*.

- **Analisar:** Após a coleta das informações como uma das etapas mais importantes para uma invasão bem sucedida, serão analisados os endereços IPs, serviços, Sistema Operacional (S.O.), versões de serviços e entre outros.
- **Explorar:** É a exploração das informações analisadas como exploits, ataques de força bruta ou em inglês *Brute Force* que foca na quebra de senhas, engenharia social e entre outros.

3.5.1 Políticas de segurança da informação

A implantação de políticas de segurança da informação deve ser estabelecida através de normas e regras como forma de controle e proteção dos ativos, com a aprovação pelo conselho administrativo. Segundo Rodrigo Pionti e Daniel Ferreira (2013, p. 4):

> A política de segurança define normas, procedimentos, ferramentas e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação para garantir o controle e a segurança da informação na empresa. É formalmente o documento que dita quais são as regras aplicadas dentro da empresa para uso de recursos tecnológicos e descarte de informações.

Torna-se recomendado no momento da admissão de um colaborador um termo ou contrato de confidencialidade para assegurar que não seja vazado nenhuma informação e mesmo que aconteça, o responsável pelo vazamento poderá ser punido pelo descumprimento com as normas da instituição e legislação penal brasileira.

3.5.1.1 Política de senhas

É visto de imensa importância a política de senhas de prevenção e maior segurança contra ataques de quebra de senhas, assim, definindo um mínimo de 8 caracteres, com variação em letras maiúsculas, minúsculas e caracteres especiais. De acordo com a Microsoft (2022) recomenda-se uma política de senha com mínimo de 8 caracteres em muitos ambientes utilizando esse meio de segurança, por não ser muito grande e fácil de se lembrar, além de reduzir a chance de ataques de força bruta.

Uma boa prática é o uso de programas com gerenciador de senhas com alta criptografia. Este serviço vai armazenar, criar, copiar e colar as senhas de maneira mais produtiva no trabalho. Tudo que será preciso vai ser um cadastro de uma senha mestre para ter acesso a todas senhas cadastradas e para aumentar a segurança o usuário pode optar por uma Autenticação de dois fatores ou em inglês *Two-Factor Authentication* (2FA), funcionando através de Tokens gerados por aplicativos ou programas como o *Google Authenticator*. É uma

camada maior de segurança para casos de vazamentos de senhas e se o usuário tiver com esse 2FA ativado, o cibercriminoso mesmo que tenha a senha ainda não conseguirá acessar.

Há alguns programas muito recomendados para cofre de senhas com criptografia de ponta. Veja alguns abaixo:

- ***1Password*:** É um *software* pago com uma alta criptografia conhecida de AES-256 bits para fornecer seguranças para seus usuários com senha mestre cadastrada pelo usuário para acessar seu gerenciador de senhas. Mesmo que ocorra vazamento de dados ainda estará criptografado. Além disso, alerta sobre vazamentos de senhas e qualquer tipo de problema relacionado a segurança.
- ***Birtwarden*:** É um *software free* (Gratuito) porém pode optar por um upgrade com mais benefícios. Possui também uma alta criptografia de AES-256 e senha mestre cadastrada pelo usuário para acessar seu gerenciador de senhas. Também é um sistema de código aberto.
- ***LastPass*:** É um *software free* (Gratuito) porém pode optar por um upgrade com mais benefícios. Possui também uma alta criptografia de AES-256 e senha mestre cadastrada pelo usuário para acessar seu gerenciador de senhas.

Basicamente é uma excelente tática para implementar na administração pública, fazendo a adesão em alguns desses softwares de gerenciamento de senhas com as melhores criptografias. Uma camada enorme de proteção contra vazamento de senhas é evitando o armazenamento das senhas em navegadores que não é nenhum um pouco recomendado, pois, qualquer hacker pode capturá-las e acessar muitos sistemas que estão com a mesma senha cadastrada. Torna-se uma grande vulnerabilidade para a organização, com isso é aconselhável a prática de treinamentos aos colaboradores para o uso dessas ferramentas tanto no ambiente de trabalho quanto no pessoal.

3.5.1.2 Política de criptografia

A criptografia tornou-se uma obrigatoriedade em todos sistemas que contém dados confidenciais e para isso o gestor precisa organizar com os seus programadores sobre o tipo de criptografia de ponta que será utilizado. Bem como, é imensamente essencial também nos órgãos públicos para proteção das informações coletadas dos cidadãos em banco de dados, inserir dentro desses *softwares* caso ainda não possua, implementar a criptografia *Advanced Encryption Standard* (AES-256 bits). Conforme Zanani (2021) Trata-se de uma criptografia mais segura da atualidade que até pelo Governo dos Estados Unidos (EUA) e outras grandes

organizações é utilizada com criptografia de 128 bits, podendo ser aplicadas de 192 e 256 bits, deixando extremamente difícil o ataque de força bruta ou *brute force* em inglês na quebra da chave em um ciberataque.

4 CONCLUSÃO

Por meio deste estudo explanou-se a importância das tecnologias principalmente na administração pública brasileira em base na sua eficiência, praticidade e de produtividade em seus processos. Desta forma, os gestores da Tecnologia da Informação na maioria das vezes também desenvolvem atividades relacionadas à cibersegurança. Assim, sugere-se que nos órgãos públicos, visando maior segurança e proteção, deva existir um setor especializado na temática, o qual possa realizar estudos de defesa de ciberataques, segurança ofensiva, *Pentest*, dentre outras modalidades, como também desenvolver medidas de proteção contra as invasões realizadas por cibercriminosos.

Em virtude da realidade atual das ocorrências de invasões que são cometidas, este artigo reflete na urgência de capacitação e contratação de profissionais especializados na área de segurança da informação, especificamente na defesa dos pilares da Confidencialidade, Integridade e Disponibilidade. Nesse sentido, o Brasil, os gestores têm a obrigação de seguir as normas da Lei de Acesso à Informação (LAI) com total transparência ao público, com ética como prevê o Marco Civil da Internet, e implementar as diretrizes da Lei Geral de Proteção de Dados (LGPD), bem como aplicar a norma internacional de padronização na ISO/IEC 27001, definindo normas, políticas de segurança da informação, metodologia da certificação tanto para a organização quanto para pessoa física em foco na adequação e reconhecimento internacionalmente.

Desse modo, esse estudo mostra estratégias de segurança nos sistemas informacionais com o intuito de aumentar as camadas de segurança com uso em serviços de *Pentests* e na criação de equipes de cibersegurança com profissionais com perfil hacker ético (em inglês, ethical hacker). Enfim, todos colaboradores necessitam de um mínimo de conhecimento com objetivo de evitar ataques de exploração humana através de técnicas de engenharia social, sendo um dos responsáveis principais pelas invasões no mundo.

REFERÊNCIAS

BOLETIMSEC. **FBI alerta para ataques de ransomware direcionados a governos locais.** 2022**.** Disponível em: https://boletimsec.com.br/fbi-alerta-para-ataques-de-ransomware-direcionados-a-governos-locais/ .Acesso em: 06 maio de 2022.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. TCU. Brasília, Ed. 4, p. 1-108, 2012. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B226095120B . Acesso em: 08 maio de 2022.

BRASIL. Governo Federal. **Brasil melhora posição no ranking mundial de cibersegurança**: País sobe 53 posições, saindo da 71ª para a 18ª colocação no mundo, conforme a União Internacional de Telecomunicações, agência especializada da ONU. Gov.br. 2022. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2021/julho/brasil-melhora-posicao-no-ranking-mundial-de-ciberseguranca . Acesso em: 06 maio de 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm . Acesso em: 09 maio de 2022.

BRASIL. **Lei nº 12.965 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: 11 maio de 2022.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014**. 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: 10 maio de 2022.

CRUZ, Bruna Souza. Segurança: ataque hacker no STJ: peritos temem vazamento em massa de dados copiados**.** São Paulo: **UOL**. 2020**.** Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/11/09/ataque-no-stj-hacker-continua-com-o-controle-de-documentos-sigilosos.htm .Acesso em: 14 maio de 2022.

FRAGA, B. **Técnicas de Invasão**: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019. p. 296.

FRAGA, B. **Técnicas de Invasão**: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019. p. 296.

KASPERSKY. **O que é cibersegurança?**. 2022. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security#:~:text=Ciberseguran%C3%A7a%20%C3%A9%20a%20pr%C3%A1tica%20que,ou%20seguran%C3%A7a%20de%20informa%C3%A7%C3%B5es%20eletr%C3%B4nicas. .Acesso em: 17 maio de 2022.

MARCONDES, J. S. **Gestão de Segurança da Informação**: O que é, o que faz, processos. Disponível em Blog Gestão de Segurança Privada. 2020. https://gestaodesegurancaprivada.com.br/gestao-de-seguranca-da-informacao-conceitos-processos/ .Acesso em: 05 maio de 2022.

MESQUITA, M. O que é a ISO-27001 e o que ela agrega para sua empresa. Minas Gerais: **Triplait**. 2020. Disponível em: https://triplait.com/o-que-e-a-iso-27001/ .Acesso em: 17 maio de 2022.

MICROSOFT. **Tamanho mínimo da senha**. 2022. Disponível em: https://docs.microsoft.com/pt-br/windows/security/threat-protection/security-policy-settings/minimum-password-length .Acesso em: 18 maio de 2022.

NETO, M.; ARAÚJO, J. **Segurança da informação**: uma visão sistêmica para a implantação em organizações. João Pessoa: Editora da UFBP, 2019. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1 . Acesso em: 04 maio de 2022.

OLIVEIRA, G. D.; MOURA, R. K.; ARAÚJO, F. A. Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação (t.i.). In: ENCONTRO REGIONAL DOS ESTUDANTES DE BIBLIOTECONOIA, DOCUMENTAÇÃO, GESTÃO E CIÊNCIA DA INFORMAÇÃO, 15, 2012, Cariri, CE. **Anais...** Cariri, CE: UFCA, 2012. p. 1-12. Disponível em: https://brapci.inf.br/index.php/res/download/81231 . Acesso em: 03 maio de 2022.

OLIVEIRA, V. **LGPD**: Entenda tudo sobre a lei que protege seus dados**.** São Paulo: UOL. 2020**.** Disponível em: https://www.uol.com.br/tilt/faq/lgpd-entenda-tudo-sobre-a-lei-que-protege-seus-dados.htm .Acesso em: 14 maio de 2022.

PIONTI, R.; FERREIRA, D. **Políticas de Segurança da Informação**. São Paulo. 2013. Disponível em: https://s.profissionaisti.com.br/wp-content/uploads/2013/07/politica-de-seguranca-da-informacao.pdf .Acesso em: 18 maio de 2022.

SANTOS, R. B.; SILVA, T. B. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. **RDBCI: Rev. Dig. Bibliotec e Ci. Info**., Campinas, São Paulo, v. 19, p. 1-31, 2021. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/download/8665529/27400/109334 . Acesso em: 05 maio de 2022.

ZANANI, M. Tipos de criptografia: descubra as mais importantes para a sua empresa. **Inova Globalweb**. 2021. Disponível em: https://inova.globalweb.com.br/post/tipos-de-criptografia-descubra-as-mais-importantes-para-a-sua-empresa .Acesso em: 19 maio de 2022.