CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNOLÓGO EM
REDES DE COMPUTADORES

Hércules Vinícius Rodrigues Torres

A prevenção contra o roubo de dados - uma análise de sua relevância

RECIFE/2023

Hércules Vinícius Rodrigues Torres

A prevenção contra o roubo de dados - uma análise de sua relevância

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor(a) Orientador(a): Msc. Filippo César Guedes Régis

RECIFE/2023

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

T693p Torres, Hércules Vinícius Rodrigues.
A prevenção contra o roubo de dados - uma análise de sua relevância/ Hércules Vinícius Rodrigues Torres. - Recife: O Autor, 2023.
22 p.

Orientador(a): Msc. Filippo César Guedes Régis.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro - UNIBRA. Tecnólogo em Redes de Computadores, 2023.

Inclui Referências.

1. Segurança. 2. Ataques. 3. Proteção. 4. Crimes. I. Centro Universitário Brasileiro. - UNIBRA. II. Título.

CDU: 004

Dedico este trabalho à minha família.

AGRADECIMENTOS

Quero agradecer aos meus amigos mais queridos, Pedro, Adriano e Lívia por seu suporte emocional e técnico durante ao longo do ano de TCC. Eles sempre estiveram presentes com palavras de encorajamento e força e me ajudando com a pesquisa emprestando materiais e dando feedback. Vocês também fazem parte da minha jornada durante este tempo de minha vida.

“A vida nunca está completa sem seus desafios”
(Stan, Lee)

SUMÁRIO

1 INTRODUÇÃO.....09
1.1 OBJETIVO GERAL.....11
1.2 OBJETIVO ESPECIFICOS.....11
2 METODOLOGIA.....12
3 REFERÊNCIAL TEÓRICO.....14
4 DESENVOLVIMENTO.....15
5 CONCLUSÕES.....24
6 CONSIDERAÇÕES FINAIS.....25
7 REFERÊNCIAL.....25

A PREVENÇÃO CONTRA O ROUBO DE DADOS - UMA ANÁLISE DE SUA RELEVÂNCIA

Hércules Vinicius Rodrigues Torres

Filippo César Guedes Regis

RESUMO

Levando em consideração de que ao passar dos anos vem ocorrendo um crescimento de ataques cibernéticos ao redor do mundo, dentre tantos países o Brasil é um dos que se encontra entre os mais atingidos por este crime, a falta de aplicações de segurança dentro de empresas é grande. Caso sua rede esteja vulnerável e sofra um ataque, as pessoas por trás do ataque podem danificar o sistema e roubar diversos dados sigilosos e profissionais e também informações pessoais, tanto suas como de seus colegas trabalhadores, como, por exemplo, seu e-mail, cartões de créditos, senhas do banco, etc.

Palavras-chave: Segurança, ataques, proteção, crimes

- **1. INTRODUÇÃO**

Desde seu nascimento, a internet se tornou uma grande arma de conhecimento para a civilização, a partir de então, o volume de pessoas utilizando-a com os mais diversos propósitos aumentou cada vez mais. Segundo a pesquisa “TIC Domicílios 2020”, desenvolvida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, o uso da internet no Brasil chegou a 152 milhões de pessoas, representando 81% da população no país, entre 2020 e 2021 (UOL, 2021).

Apesar de todos os benefícios que a internet trouxe, ela também trouxe consigo riscos e perigos dentro de diversas áreas, incluindo uma das mais importantes, a área de segurança, com isso surgiram os crimes digitais e, por conta disso, surgiu também a demanda progressiva de manter as informações e os ativos organizacionais de modo seguro. A informação deve garantir três requisitos fundamentais, Dantas (2011) diz que: integridade, disponibilidade e confidencialidade são requisitos que devem ser mantidos por serem os princípios da segurança da informação.

O primeiro estudo sobre Cibersegurança aconteceu em 1949, em um estudo publicado por John von Neumann, o matemático que foi um dos responsáveis por criar o ENIAC, o primeiro computador militar. Embora na época fosse apenas um estudo teórico, aquela pesquisa foi o que levantou a possibilidade para a segurança nos computadores, porém, apenas em meados dos anos 1960, o assunto começou a ser percebido como algo indispensável. (BRANCO, 2021)

Jonh Von Neuman criou estudos nos quais abordavam a teoria de autômatos que se auto-reproduzem. Esses estudos mostravam que programas de computadores poderiam ser desenvolvidos para se espalharem por outras máquinas, as danificando, antes mesmo do termo “vírus” nascer dentro da área. Apesar de nunca ter sido colocada em prática, a teoria fez com que Neumann fosse considerado o pai dos “vírus de computador”, e seus estudos foram utilizados como base e expandidos em 1972, quando

Veith Risak, um pesquisador alemão, publicou seu artigo “Self-reproducing automata with minimal information exchange”. (BRANCO, 2021)

Em 1970, a IBM chamou alguns estudantes para testar seus novos computadores e acabaram percebendo que os alunos estavam conseguindo acessos a lugares que deviam estar restritos nas máquinas, fizeram isso com a intenção de melhorar o funcionamento dos dispositivos. Presentemente, isso é chamado de “hacking ético” onde os invasores têm intenções de aplicar melhoras em sistemas que eles não têm permissão para entrar. A segurança cibernética começou a entrar nos trilhos na década de 70, com os primeiros exemplos de proteção sendo criados pela ARPA em conjunto com a força aérea dos EUA, na forma de protocolos de segurança para o sistema operacional Honeywell Multics. (BRANCO, 2021)

A escolha deste tema teve seu principal fundamento na intenção de demonstrar como esta área de segurança precisa ser aprimorada e melhor desenvolvida, pois é considerada uma das mais importantes dentro da área de redes, ao pesquisar diversas condições sobre o tema foi percebido como faltam profissionais capazes de atuar na área vem gerando acidentes e inconveniências para as pessoas e as empresas. (SANTOS, 2020).

Segundo Sobers (2022) uma das causas para o aumento da demanda de proteção dados hoje em dia são os efeitos colaterais da pandemia, na qual durante seu período, causou um aumento nas estratégias de explorar pontos fracos dentro da rede, levando a um aumento de dados hackeados e violados de fontes cada vez mais comuns dentro do local de trabalho, como dispositivos móveis e IoT.

Assim como mencionado antes por Sobers (2022) durante o lockdown da pandemia, muitas empresas foram obrigadas a adotar massivamente o home office, e assim, a necessidade de segurança da informação cresceu ainda mais dentro das empresas. No decorrer dessa fase, diversos índices apontam que houve um grande aumento especialmente em ataques dos tipos phishing, spam, ransomware, esses tipos de ataque estão cada vez mais elaborados e contextualizados com para aumentar a eficiência dos golpes e evoluir com base na necessidade do criminoso por trás.

Foi identificada a escassez de pesquisas e discussões voltadas a temática, segundo Souza (2023) a nossa sociedade não foi educada o suficiente sobre ataques virtuais, o que acaba fazendo com que, as pessoas tenham dificuldades em diferenciar e-mails e com isso eles acabam clicando em anúncios de sites não conhecidos e assim, ocasionando em ataques conhecidos como phishing, assim então, caindo em golpes de roubo de dados, portanto, foi-se visto uma boa oportunidade de revisitar um assunto pouco explorado e visibilizado pelas pessoas.

De acordo, com Schuh (2022), ao sofrer as consequências da falta de cuidado com sua segurança de redes sofre com situações de invasão de privacidade, quebra de sigilo, perda de clientes e parcerias por fracasso ao proteger dados pessoais, financeiros e profissionais acarretando multas, transtorno e processos judiciais à empresa responsável. Sobers (2022) afirmou que recentes pesquisas de segurança revelaram que a maioria das empresas tem práticas de segurança fracas, assim as deixando vulneráveis. Diante das intenções determinadas, a pergunta de pesquisa que norteou o trabalho foi: “Quais as consequências de ter seus dados roubados e quais os benefícios de se precaver contra esses tipos de ataques mal-intencionados? Como essas situações ocorrem e por quê?”.

• 1.2 OBJETIVOS GERAIS E ESPECÍFICO

Objetivo Geral: Analisar os efeitos que sua rede sofre ao ter uma segurança aplicada de forma inadequada.

Objetivo específicos:

- Indicar formas de proteção integradas para combater ataques.
- Expor possíveis causas de roubos e vazamentos de dados.
- Apresentar como a transformação digital estimulou as organizações a evoluírem.
- Realçar a atual situação do mundo na área de segurança da informação.

• 2 METODOLOGIA

O presente trabalho tem como tema “Precauções e Perigos dos Roubos de Dados” com finalidade de mostrar dados que evidenciam como e por que as pessoas e as organizações facilmente sofrem golpes e ataques virtuais de “Phishing” e “Ramsomwares” e tem suas informações e dados pessoais roubados. Esse trabalho teve embasamento por meio de pesquisas bibliográficas.

Para o desenvolvimento foram utilizadas pesquisas acadêmicas e artigos científicos com relação aos diferentes tipos de ataques que podem ser utilizados para cometer o crime de roubo digital ou para explorar vulnerabilidades do software como: Ramsomware, vírus, worms, phishing, backdoor, assim como também foi pesquisado formas de proteção e precaução contra esses ataques que podem ser implementados como: firewall, antivírus, VPN, filtragem de conteúdo, detecção de intrusão.

Os principais materiais utilizados na elaboração da pesquisa para formar a pesquisa foram: Google Acadêmico, ScienceDirect e Google Livros, que são datados entre os anos de 2000 até 2022. Os termos de busca que foram mais usados para encontrar as fontes das pesquisas foram: “Roubo de Dados Digitais”, “Ramsomware”, “Transformação Digital”, “Prevenir Roubo de Dados”, “Vazamento de Dados”, “Segurança Cibernética” e entre outros, com os critérios de inclusão dos dados mais atuais que foram encontrados e que auxiliaram na construção de uma discussão teórico, metodológica, informativo e coerente.

- **3 REFERENCIAL TEÓRICO (Estudo da arte)**

A segurança da informação pode ser definida como a proteção da informação contra diversos tipos de ameaças, de uma forma na qual garanta a continuidade do negócio, minimize os riscos, maximize o retorno sobre o investimento e as oportunidades de negócio. Também existem outras diferentes propriedades tão importantes quanto as mencionadas anteriormente, nas quais também devem ser consideradas e implementadas no processo de segurança: a autenticidade, o não repúdio e a confiabilidade (NBR ISO/IEC 27002:2005).

As vulnerabilidades podem estar presentes em diversos lugares e de diferentes formas, como por exemplo: instalações físicas desprotegidas contra inundações, incêndios e outros desastres naturais; falta de políticas de segurança; falta de controles de acessos e utilização de materiais da empresa; equipamentos sem restrição para sua utilização. (COUTINHO, et al. 2017)

A informação pode existir em numerosas formas, entre elas temos: documentos físicos, sejam eles impressos ou escritos em papéis e até mesmo arquivos virtuais, independente da maneira da qual a informação é criada e armazenada, ela deve ser protegida da forma adequada (NBR ISO/IEC 27002:2005).

De acordo com Oliveira et al. (2021) Conforme o tempo passa mais tecnologias são criadas e as que já existem evoluem cada vez mais criando o conceito conhecido como IoT (Internet of Things), algumas vão ficando mais seguras, mas paradoxalmente nada é 100% seguro na área de tecnologia, quando algo é atualizado ou algo novo é criado pode significar que vai ficar mais seguro do que a versão antiga, mas também significa que novas fraquezas vão nascer, às vezes novas seguranças não são

implementadas e isso só piora ainda mais, dando mais chances a criminosos virtuais se aproveitarem da fraca segurança e acabar ganhando mais ainda com a situação.

Frequentemente ocorrem ataques cibernéticos, e mesmo nas maiores empresas os criminosos virtuais saem vitoriosos, pois, eles evoluem seus métodos constantemente, deixando as velhas e novas tecnologias para trás, e isso acaba causando uma série de eventos ruins que criam má reputação e perda da credibilidade das organizações, consequentemente também diminuindo a confiança dos clientes e até os perdendo, além de também, perder parceiros de negócios que podem sofrer do mesmo destino por estarem associados à organização, e isso provocando uma perda de espaço no mercado, afetando a competitividade da sua empresa, gerando custos fora do planejamento. (SANTOS, 2018)

Atualmente, existem diversos tipos diferentes de hackers, “os chamados de White Hats, Gray hats estes fazem pequenos ataques DOS para derrubar alguns sites, ou escrevem algum software para derrubar a licença de alguns programas, e por fim, os Black Hat.s.” (SKOUDIS & HAL, 2005)

Pela definição de Peltier (2010), ameaça é um evento indesejável que pode danificar um ativo, causando impacto nos resultados do negócio. Ele classifica as ameaças em três grupos básicos com base na natureza do agente causador: ameaças Naturais, que incluem eventos da natureza como enchentes, terremotos e tempestades elétricas; ameaças humanas, as quais englobam eventos que sejam causados ou facilitados por um agente humano, de forma voluntária ou não, tais quais malwares, eventos de fraude, e outros erros comuns na área de Tecnologia; e por fim, as ameaças ambientais, ação do tempo, poluição e umidade.

4 DESENVOLVIMENTO

> Segurança cibernética refere-se à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da administração pública federal (CRUZ, 2013).

Assim como mencionado anteriormente, a história com a segurança e os “hackers” começou desde cedo entre a década de 60 e 70, antes mesmo de muitos terem um computador, naquela época, o termo “hacker” não era algo negativo, na verdade, era um adjetivo positivo para pessoas que, na verdade, só queriam otimizar e inovar a área da tecnologia da informação, porém posteriormente, com a criação dos vírus e o surgimento dos ataques cibernéticos, essa reputação foi tingida de forma negativa uma década depois.

O primeiro hacker da história foi John Draper, que no seu tempo explorou os sistemas de telefone automatizados que usava frequências analógicas com um apito, usando para fazer ligações de longas distâncias gratuitamente. Mais atualmente, um dos primeiros hackers a ganhar visibilidade dentro da mídia foi Robert Morris, no final dos anos 1980, ele fez o primeiro ataque de negação de serviço (também conhecido como DDoS) usando worms, porém, foi dito pelo mesmo que ele não tinha más intenções e apenas queria destacar as falhas de segurança no sistema, mas infelizmente, suas ações teriam consequências, já que devido a uma falha no código, o worm se replicou desproporcionalmente e isso acabou causando danos severos que duraram por alguns dias. (STEFANELLO, 2021)

Avançando ao agora, as tecnologias evoluíram a patamares inacreditáveis, mas infelizmente a conduta da humanidade também evoluiu negativamente, diferentemente do jovem Robert que tinha boas intenções no tempo, atualmente, é raro achar alguém como ele, afinal, presentemente, apenas utilizam de seus talentos na tecnologia de forma que prejudique os outros e roubam seus dados pessoais, hackeando seus e-mails através de suas senhas fracas e conseguindo assim, acesso a cartões de créditos, contas bancárias, contas de redes sociais e consequentemente assim, roubando seu dinheiro e talvez até ameace não devolver seus dados por uma quantia específica, esses tipos de ataques se tornaram mais recorrentes durante o ano de 2020, na pandemia do vírus COVID-19, com a transformação digital. (BARBOSA et al., 2021)

Com o começo da pandemia em 2020, o mundo começou a se transformar rapidamente e se digitalizar mais, e isso fez com que a transformação digital ocorresse de forma mais rápida e isso teve alguns benefícios naquela situação de não poder sair de casa, ajudando as pessoas a terem acesso ao trabalho delas via home office, porém, hoje, em um período pós-pandemia, ficou mais difícil para se proteger de ataques, já que o foco das empresas agora é o trabalho por computadores. (BARBOSA et. al 2021). No ano de 2021, foi se constatado que o Brasil é uma das maiores população conectada do mundo e está na 44 ª posição no ranking de governos digitais, segundo a ONU (2021).

A pandemia obrigou as empresas a se adaptarem a situação e adotarem essa postura mais digital, dada a situação, a única forma de diminuir o impacto na produtividade das empresas era através do home office, era um tipo de serviço no qual já existia, mas se tornou comum agora, porém, isso não tornou as coisas mais fáceis de se adaptar para muitas pessoas, nas quais não estavam acostumadas com esse tipo de contato constante com a tecnologia, especialmente os idosos, que tem dificuldade em

trabalhar nesse formato por não estarem acostumados com computadores, essa transformação digital deixou as pessoas mais dependentes e apegadas às tecnologias (Microsoft, 2021).

No status quo presente no momento do país, o Brasil ainda tem um longo caminho pela frente para se desenvolver melhor em diversos pontos dentro da área de tecnologia, mas também tem qualidades a serem reconhecidas como a vantagem de estarmos inseridos em um contexto em que três a cada quatro brasileiros estão conectados à internet, 97% deles por meio de celulares, os principais desafios para a transformação digital de governo não são exatamente tecnológicos. A transformação digital exige, em primeiro lugar, uma mentalidade digital vinda pelas pessoas. (Monteiro, 2021)

Esse aumento de pessoas dentro da internet devido à pandemia causou com que mais pessoas se tornassem suscetíveis a ataques desse tipo, visto que, os cibercriminosos se acostumaram e se adaptaram rapidamente diante da situação pandêmica (Europol, 2020). É extremamente fácil cair em golpes online atualmente principalmente para os leigos em internet, apenas um deslize bobo pode trazer os maiores dos prejuízos. Casos assim, são os mais comuns dentro do dia a dia das pessoas, especialmente dos adultos e idosos, nos quais são mais suscetíveis a qualquer ataque dentro web. Com essa mudança drástica na vida das pessoas, começaram a ocorrer mais ataques cibernéticos ao redor do mundo todo. (Neves, 2022)

Hoje em dia, o crime mais popular no Brasil é o “Phishing” no qual consiste em e-mails, mensagens SMS, e até mesmo ligações visando atrair a vítima usando algum tipo de prêmio ou uma oferta ótima de algum tipo de marca, visando obter suas informações pessoais, sejam senhas, dados financeiros, dados bancários e até números de cartões de créditos (JUNIOR & LIMA, 2010). Por ser um ataque fácil de criar, ele acaba sendo o mais usado e mais comum de ser visto pelas vítimas dos ciber-criminosos. (NEVES, 2022)., Além disso, com o recente contexto pandémico, verificou-se uma adaptação dos

golpes de phishing, fazendo-se os criminosos passarem por entidades de saúde, resultando em um aumento na distribuição massiva de campanhas de cerca de 59% (Interpol, 2020)

O relatório Internet Crime Report 20214 do FBI reporta que tipos de ciberataques que mais ocorreram nos últimos cinco anos (2017- 2021) foram: phishing, vishing, smishing e pharming, registando-se cerca de 323.972 vítimas e que consequentemente tiveram perdas num valor de $44,213,707. (FBI, 2021)

Infelizmente, a situação no Brasil nesse quesito não é das melhores, muito pelo contrário, é, na verdade, uma das piores do mundo, visto que existem notícias sobre ataques cibernéticos todos os dias, além de diversas empresas famosas dentro da noticiarem e fazerem relatórios todos os anos sobre a situação mundial dentro da área, e trazer dados confiáveis tirados por eles próprios. Como já apresentado antes, os anos recentes têm sido os piores devido à influência da transformação digital dentro do país.

O ano de 2022 foi o ano que mais ocorreram ataques cibernéticos, ocorreram um total de 146 bilhões de tentativas de golpe registradas no mundo todo, aumentou cerca de 56% em relação a 2021, foi o maior número observado pela Trend Micro (2021), empresa multinacional de cibersegurança.

Em seu novo relatório a empresa citou os motivos para esse aumento de tentativas de crimes, a pandemia do covid-19, a adoção de regimes híbridos e o home office pelas empresas ao redor do mundo, além disso, a forma da qual os bandidos cometem os crimes também mudou, antes eram ataques dispersos a quaisquer indivíduos, mas agora se tornaram ataques direcionados a empresas ou pessoas específicas, os tornando ainda mais perigosos, mas em contraparte, menos comum, Candido, diretor-geral da Trend Micro apontou que a Segurança precisa ser tratada como prioridade por todas as companhias, que devem se antecipar a criminosos (CANDIDO, 2023).

De acordo com a 2ª Pesquisa Nacional BugHunt de Segurança da Informação**,** realizada pela Bughunt mais de 1/4 das empresas brasileiras sofreram ataques cibernéticos no último ano. (TELLES, 2023) De acordo com Telles (2023), chefe da Bughunt, recentemente, empresas como Americanas, Mercado Livre, Renner, sofreram ataques e invasões, sofrer um ataque pode causar prejuízos incalculáveis às companhias, tanto em relação ao roubo de dados, como no âmbito financeiro e até mesmo parar a operação por completo. A cibersegurança não é mais apenas um cuidado adicional, se tornou uma estratégia de negócios.

Segundo a Anatel (2021) em 2021 o Brasil sofreu mais de 2,6 bilhões de ataques cibernéticos, também segundo a Tenable Inc (2022), uma das empresas mais abrangentes atualmente no mercado de segurança, em 2022 o Brasil foi o país com o maior volume de dados expostos, durante esse ano 2,29 bilhões de registros foram expostos em escala global e mais de 800 milhões desses registros aconteceram por negligência na proteção dos bancos de dados, o relatório anual da companhia afirmou que em 2022 foram expostos 257 terabytes ao redor do mundo e o Brasil foi um dos países mais foram prejudicados, tendo 112 terabytes de dados vazados, conforme Capella (2021), diretor-geral da Tenable no Brasil afirmou, isso aconteceu devido à falta de estratégia, organização, e competência para se planejar quais ameaças deveriam ser prioritárias. Segundo Junior (2022):

> “Os crimes mais populares que estão presentes hoje em dia são: Fraudes por e-mail; Interceptação de informações pessoais de terceiros ou dados sigilosos de organizações e empresas; Roubo de dados financeiros, credenciais bancárias de terceiros.”

Outro tipo de ataque mais popular atualmente, são os “Ransomwares”, são ataques conhecidos por serem como um sequestro virtual, onde o agressor rouba os

dados da vítima e cobra uma taxa por eles, normalmente em bitcoins ou outros tipos de moedas virtuais. (BREWER, 2016)

Para deixar as organizações mais alerta com esse tipo de questão foi criada uma nova lei na qual foi inspirada na norma europeia de Proteção de Dados (GDPR-General Data Protection Regulation), em 14 de agosto de 2018 foi criada a Lei n.º 13.709 a Lei Geral de Proteção dos Dados Pessoais (LGPD) ou Marco Civil da Internet (BRASIL, 2018) que visa medidas preventivas, proativas na manutenção e privacidade dos dados de terceiros (GARCIA et al., 2020).

A LGPD é o resultado de um movimento da sociedade e das autoridades brasileiras, com empresas e pessoas procurando respostas para perguntas sobre segurança. Segundo a LGPD, a proteção deles “abrange qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Ou seja, ela protege os documentos mais importantes, como RG, CPF, telefone, data de nascimento, renda, hábitos de consumo, etc. (PINHEIRO, 2020).

O motivo que inspirou o surgimento desta lei de forma mais consistente foi o desenvolvimento do modelo de negócios da economia digital, tal qual passou a ter uma dependência maior de bases de dados digitais, especialmente relacionados as pessoas, providenciadas pelos avanços tecnológicos e pela globalização (PINHEIRO, 2020).

Pesquisa realizada pelo Grupo DARYUS, revelou informações sobre o quadro de adesão à LGPD no país. Conforme o estudo, 35% dos entrevistados afirmam que suas empresas estão parcialmente adequadas, enquanto outros 24% apontaram que estão na fase inicial do processo de adequação à lei. (DARYUS, 2021).

Essa lei começou a ser aplicada a partir de 2021 e ela trouxe consigo consequências e multas para quem não as seguir, como, por exemplo: advertências com indicação de prazo para adoção de medidas corretivas; bloqueio de dados pessoais; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, publicização da infração após devidamente apurada e confirmada a sua ocorrência (JUNIOR, 2022).

De acordo com Oliveira et al., (2021) Dentre os diversos artigos e parágrafos identificados no texto da LGPD, podemos citar como sendo os mais relevantes para este trabalho os seguintes itens:

- Uso da Informação: Especificar para o usuário qual a finalidade da coleta de seus dados, além de ser transparente em relação ao tratamento dessas informações e adotar medidas que garantam sua segurança;
- Acesso à Informação: O usuário deve ter acesso fácil as informações que estão sendo utilizadas sempre que desejar, podendo revogar seu consentimento de compartilhamento de dados posteriormente, sem maiores dificuldades;
- Titularidade e Responsabilidade: O “titular” dos dados e a pessoa a qual as informações se referem. No entanto, quando o titular concorda com o uso de ˜ suas informações, a empresa torna-se a responsável pela sua segurança e seu tratamento;
- Tratamento das Informações: O tratamento de dados deve ser finalizado quando o objetivo especificado for anteriormente alcançado (salvo casos específicos), quando as informações deixarem de ser necessárias ou quando o órgão regulador solicitar;

- Divulgação de Incidentes: Qualquer vazamento ou falha de segurança que comprometa os dados de algum usuário devem ser relatados imediatamente as autoridades competentes, para que o problema seja resolvido.

- **Formas de Proteção**

Dito isso, de acordo com Pinheiro (2017) existem diversas formas de se precaver e tomar contramedidas dentro dessas situações, a segurança integrada é uma delas, é um método no qual combina diferentes tecnologias de segurança com compatibilidade de políticas, gerenciamento e suporte, e pesquisa avançada para obter uma proteção mais eficaz. Através dessas combinações, é possível chegar em um resultado satisfatório de proteção da sua rede, assim conseguindo proteger contra uma grande variedade de ataques e ameaças e até minimizar os danos delas.

Apesar de individualmente, essas tecnologias serem inconvenientes de serem instaladas e geralmente serem difíceis e caras de se gerenciar e atualizar, elas são bastante vantajosas de se usar quando integradas em uma solução única, assim oferecendo uma proteção mais completa e eficaz, ao mesmo tempo que reduz os custos de manutenção e de operações (PINHEIRO, 2017). As principais tecnologias que podem ser integradas de acordo com Pinheiro (2017) são:

- Firewall: Controla todo o tráfego de dados através da verificação das informações que entram e saem da rede a fim de garantir que não ocorram acessos não autorizados;
- Detecção de Intrusão: Detecta o acesso não autorizado e fornece diferentes alerta e relatórios que podem ser analisados para políticas e planejamento da segurança;
- Filtragem de Conteúdo: Identifica e elimina o tráfego de pacotes não desejado na rede;

- Redes Privadas Virtuais (VPN): Asseguram as conexões além do perímetro da rede local, permitindo que redes locais se comuniquem com a segurança através da internet;
- Gerenciamento de Vulnerabilidade: Permite a avaliação da posição de segurança da rede descobrindo falhas de segurança e sugerindo melhorias;
- Proteção Antivírus: Protege contra vírus, Worms, Cavalos de Tróias e outras pragas virtuais.

• 5 CONSIDERAÇÕES FINAIS

O repentino aumento de demanda para uso de dispositivos digitais devido a pandemia ocasionou na facilidade de realizações de trabalhos das organizações, porém, também trouxe perigos novos e tornou os velhos ainda piores do que foram antes. Crimes como furtos, extorsão e fraudes podem ocorrer através da rede e causar inúmeros prejuízos as pessoas e suas organizações. Desta forma, o tema de segurança da informação acabou ganhando destaque dentro da mídia e das empresas e assim evidenciando a relevância em se tornar mais alerta com tipos de ataques e como precavê-los.

Transformar sua rede de computadores menos vulnerável contra ameaças e ataques com o uso de sistemas de detecção e prevenções de ataques é uma tarefa de eterna evolução, mutação e transformação, na qual exige uma dedicação constante para o seu sucesso e uma forte competência para ser capaz de criar mudanças e mudar hábitos de dentro das empresas e suas infraestruturas. Existe uma necessidade de desenvolver com uma perspectiva e de forma mais ampla nos quesitos apresentados, considerando tanto o ponto de vista pessoal de um cidadão comum quanto o técnico com as necessidades da organização.

Falhas nas disponibilidades das informações não devem ser toleradas, pois, as consequências delas podem ser catastróficas para a imagem e reputação institucional e assim, causar problemas dentro e fora das organizações. Sendo assim, para que se

consiga uma total confiabilidade das informações não deveria ocorrer interrupção no fluxo do serviço e nem perda de dados, o que tornaria os sistemas totalmente confiáveis e disponíveis. Mas infelizmente, no mundo real, confiabilidade e disponibilidade absolutas estão muito longe de serem alcançadas. (WEBER, 2003)

REFERÊNCIAS

ABNT NBR, ISO/IEC 27002. Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação. 2005. Disponível em: <nbr_iso_27002-para-impressc3a3o.pdf (wordpress.com)> Acesso em: 04/06/2023

Apenas 16% das empresas brasileiras aumentaram seu orçamento em segurança da informação e cibersegurança desde o início da pandemia – Microsoft News Center Brasil. Disponível em: <https://news.microsoft.com/pt-br/features/apenas-16-das-empresas-brasileiras-aumentaram-seu-orcamento-em-seguranca-da-informacao-e-ciberseguranca-desde-o-inicio-da-pandemia/>. Acesso em: 13 jun. 2023.

BAPTISTA JUNIOR, J. H.; DIAN, M. DE O. CRESCENTE IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, SOBRETUDO DURANTE A PANDEMIA. **Revista Interface Tecnológica**, v. 18, n. 1, p. 56–67, 3 nov. 2021. Acesso em: 03/06/2023

BARBOSA, J. S. et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, p. e40510212557–e40510212557, 20 fev. 2021.

BRANCO, Dácio. História da segurança virtual: a origem da cibersegurança. **CanalTech**, 2021 <História da segurança virtual: a origem da cibersegurança - Canaltech> Acesso em 27/03/2023.

BRANCO, Dácio. **História da segurança virtual: a origem do vírus de computador**. Disponível em: <https://canaltech.com.br/seguranca/origem-do-virus-de-computador-197667/>. Acesso em: 29 jun. 2023.

BREWER, R. Ransomware attacks: detection, prevention and cure. **Network Security**, v. 2016, n. 9, p. 5–9, set. 2016. Acesso em 29/04/2023

CANDIDA, M. et al. **Ética em Pesquisa Científica: conceitos e finalidades**. [s.l: s.n.]. Disponível em: <https://acervodigital.unesp.br/bitstream/unesp/155306/1/unesp-nead_reei1_ei_d04_texto2.pdf>. Acesso em: 22/05/2023

CARREIRAS, H. et al. CIBERSEGURANÇA E CIBERDEFESA EM TEMPOS DE PANDEMIA. **JSTOR.** Portugal. v.1 n.1 jun ./jul. 2020. Acesso em: 20/04/2023

COUTINHO. M. M, SANTOS. R. N. D, CUSTODIO. V. H. S, AMARAL. E. C, SABINO. E, ABE. N. ESTUDO DE CASO: PRINCIPAIS PILARES DA SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES. **Revista Gestão em Foco,** v. 9, p. 489-500. 2017.

DANTAS, L.M. **Segurança da Informação - Uma Abordagem Focada em gestão de Riscos.** Olinda. Livro Rápido, 2011.

Deficit de profissionais de segurança da informação? Ou falta de oportunidades? Como contornar tal situação? Disponível em: <https://pt.linkedin.com/pulse/deficit-de-profissionais-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-ou-falta-dos-santos>. Acesso em: 27 jun. 2023.

DERMATINI, Felipe. 2022 bate recorde com mais de 146 bilhões de ataques cibernéticos. **CanalTech**, 2023 <https://canaltech.com.br/seguranca/2022-bate-recorde-com-mais-de-146-bilhoes-de-ataques-ciberneticos-243560/> Acesso em 27/03/2023.

DOMINGUES, E. J. **Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo**. 2015. Disponível em: <Repositório Comum: Os Ciberataques como um Novo Desafio para a Segurança: O Hacktivismo (rcaap.pt) > Acesso em: 21/04/2023

Federal Bureau of Investigation: Internet Crime Report 2021.

Disponível em: <https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf> 2021. Acesso em: 27/06/23.

FORNASIER, M. D. O.; SPINATO, T. P.; RIBEIRO, F. L. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista **Thesis Juris**, São Paulo, v. 9, n. 1, p. 208–236, 23 jun. 2020. Acesso em: 10/06/2023

GARCIA, L. R. et al. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação.** [s.l.] Editora Blucher, 2020.

How COVID-19-related crime infected Europe during 2020. Disponível em: <https://www.europol.europa.eu/publications-events/publications/how-covid-19-related-crime-infected-europe-during-2020>. Acesso em: 13 jun. 2023.

JÚNIOR, S. **A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual**. Disponível em: <https://econpapers.repec.org/paper/ipeipetds/1850.htm>. Acesso em: 30/04/2023

KAROLCZAK, L. L.; POSSAMAI, V. Roubo de Dados Ransomware: **SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO**, v. 2, n. 1, 17 maio 2020. Acesso em: 22/04/2023

MAJ, O. et al. **Cap QCO Infor JORGE VAGNER VIEIRA DA CRUZ O FUTURO DA SEGURANÇA CIBERNÉTICA NO BRASIL: PAPÉIS E RESPONSABILIDADES**. [s.l: s.n.].Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/7991/1/CAM_QCO_2020_Cap%20Jorge%20da%20Cruz.pdf>. Acesso em: 12 jun. 2023.

MENDES, A. F. DA S. Desafios da cibersegurança no Brasil entre os anos 2000 e 2017. **repositorio.uninter.com**, 2018. Acesso em: 20/04/2023

MILITÃO, Octávio. Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional. 2014. Disponível em <RUN: Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional (unl.pt) > Acesso em: 20/04/2023

MONTEIRO, L. F. Desafios para a transformação digital no setor público brasileiro. **Revista do TCU**, n. 145, p. 4–8, 2020. Acesso em: 25/05/23

NAKAMURA, E. T.; GEUS, P. L. DE. **Segurança de Redes em Ambientes Cooperativos.** [s.l.] Novatec Editora, 2007

NEVES, R. A. C. Vitimação por phishing: um estudo empírico. **repositorio-aberto.up.pt**, 14 nov. 2022. Acesso em 25/05/23

NOBRE, J. et al. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, v. 17, n. 4, 26 nov. 2019.

OLIVEIRA, Beatriz. (IN)SEGURANÇA DIGITAL: O SISTEMA DE CIBERDEFESA BRASILEIRO. 2020. Disponível em: <https://periodicos.uff.br/ocosmopolitico/article/download/53880/31712 > Acesso em: 21/04/2023

PINTO, W. D. G.; MOREIRA, J. P.; SILVA, A. DOS S. **CIBERSEGURANÇA. SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO**, v. 2, n. 2, 28 out. 2020.

PINHEIRO, J. M. DOS S. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. **Cadernos UniFOA**, v. 3, n. 5, p. 11–21, 2007. Acesso em: 08/06/2023

Pesquisa Nacional de Privacidade e Proteção de Dados. Disponível em: <https://materiais.idesp.com.br/pesquisa-protecao-e-privacidade-de-dados>.

SOUZA, L. C. DE; TANAKA, S. S. Estudo sobre ataques de phishing e suas técnicas de defesa. **Revista Terra & Cultura: Cadernos de Ensino e Pesquisa**, v. 39, n. especial, p. 90–95, 16 fev. 2023. Acesso em: 06/05/2023

SANTOS, E. E. DOS; SOARES, T. M. M. K. Riscos, ameaças e vulnerabilidades: o impacto da segurança da informação nas organizações. **ric.cps.sp.gov.br**, 3 dez. 2018.

Security Response Overview. [s.l: s.n.]. Disponível em: <https://www.01net.it/whitepaper_library/Symantec_Ransomware_Growing_Menace.pdf>.

SOBERS, R. **110 Must-Know Cybersecurity Statistics for 2020**. Disponível em: <https://www.varonis.com/blog/cybersecurity-statistics>. Acesso em: 03/06/2023

SILVA, T. **Tolerância a falhas: conceitos e exemplos**. [s.l: s.n.]. Disponível em: <https://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF>. Acesso em: 12 jun. 2023. Acesso em: 08/06/2023.

STEFANELLO, S. A. **Ataques hacker: como surgiram e como proteger sua empresa?** Disponível em: <https://incuca.net/ataques-hacker-como-surgiram-e-como-proteger-sua-empresa/#:~:text=Quem%20foi%20o%20primeiro%20hacker>. Acesso em: 12/04/2023.

SKOUDIS, Ed; LISTON, Tom; HALL, Prenticel. **Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses** (2005).

TELLES, Caio. **2ª Pesquisa Nacional BugHunt de Segurança da Informação.** Disponível em: <2ª Pesquisa Nacional de Segurança da Informação | BugHunt> 2023. Acesso em: 27/06/2023.