UNIVERSIDADE FEDERAL FLUMINENSE

IGOR TRAJANO DA SILVA

SEGURANÇA CIBERNÉTICA NAS ORGANIZAÇÕES: MITIGANDO RISCOS

NITERÓI

2024

IGOR TRAJANO DA SILVA

SEGURANÇA CIBERNÉTICA NAS ORGANIZAÇÕES: MITIGANDO RISCOS

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Orientador(a): Ricardo Nolasco

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

S586s Silva, Igor Trajano da
Segurança Cibernética nas Organziações: Mitigando Riscos / Igor Trajano da Silva. - 2024.
56 f.: il.

Orientador: Ricardo de Oliveira Nolasco.
Trabalho de Conclusão de Curso (graduação)-Universidade Federal Fluminense, Instituto de Computação, Niterói, 2024.

1. Segurança Cibernética. 2. Segurança da Informação. 3. Política Nacional de Cibersegurança (PNCIBER). 4. Lei Geral de Proteção de Dados (LGPD). 5. Produção intelectual. I. Nolasco, Ricardo de Oliveira, orientador. II. Universidade Federal Fluminense. Instituto de Computação. III. Título.

CDD - XXX

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

IGOR TRAJANO DA SILVA

SEGURANÇA CIBERNÉTICA NAS ORGANIZAÇÕES: MITIGANDO RISCOS

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói, 25 de Junho de 2024.

Ricardo de Oliveira Nolasco

Assinado de forma digital por Ricardo de Oliveira Nolasco
Dados: 2024.06.25 20:07:57 -03'00'

Prof. Ricardo de O. Nolasco, Msc - Orientador
UFF - Universidade Federal Fluminense

gov.br

Documento assinado digitalmente
ELY SEVERIANO JUNIOR
Data: 27/06/2024 11:18:30-0300
Verifique em https://validar.iti.gov.br

Prof. Ely Severino Junior, Msc - Avaliador
UFF - Universidade Federal Fluminense

Dedico este trabalho a minha família, meus amigos da faculdade e colegas que contribuíram para meu crescimento pessoal e me incentivaram a nunca desistir dos sonhos.

AGRADECIMENTOS

Agradeço a Deus por me conceder saúde para enfrentar obstáculos em meio a tantas incertezas, aos meus pais e irmã, meus avós, tios, primos e amigos que sempre me deram incentivos para continuar no constante estudo. Ao meu orientador por contribuir para meu aprendizado durante todo este processo.

“Deus quer, o homem sonha, a obra nasce”.
Fernando Pessoa

RESUMO

A crescente interconexão digital traz consigo uma série de desafios, especialmente no que diz respeito à segurança das informações e sistemas. Este trabalho investiga as ameaças emergentes, as vulnerabilidades existentes e as estratégias de proteção que podem ser empregadas para mitigar os riscos associados à cibersegurança.

Sendo assim, a cibersegurança é um desafio contínuo em um mundo cada vez mais digitalizado. Destacar a importância de entender as ameaças emergentes, identificar vulnerabilidades e implementar estratégias eficazes de proteção para salvaguardar os ativos digitais é de suma importância para proteção de dados em organizações de diferentes níveis. A colaboração entre organizações, governos e indivíduos é fundamental para enfrentar os desafios crescentes e garantir a segurança cibernética a longo prazo.

Palavras-chave: cibersegurança, mitigar e dados.

ABSTRACT

Increasing digital interconnection brings with it a series of challenges, especially with regard to information and systems security. This work investigates emerging threats, existing vulnerabilities, and protection strategies that can be employed to mitigate risks associated with cybersecurity.

Therefore, cybersecurity is an ongoing challenge in an increasingly digitalized world. Highlighting the importance of understanding emerging threats, identifying vulnerabilities and implementing effective protection strategies to safeguard digital assets is of paramount importance for data protection in organizations at different levels. Collaboration between organizations, governments and individuals is critical to addressing growing challenges and ensuring long-term cybersecurity.

Keywords: cybersecurity, mitigate and data.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

5G	5° Generation
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
AT&T	American Telephone and Telegraph
BD	Banco de Dados
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro Nacional de Pessoa Física
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
E-Ciber	Estratégia Nacional de Segurança Cibernética
ENSI	Estratégia Nacional de Segurança da Informação
ETIRs	Equipe de Tratamento e Resposta a Incidentes Cibernéticos
IaaS	Infrastructure as a Service
IBM	International Business Machines
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IOCTA	Internet Organised Crime Threat Assessment
IOT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO/IEC	Organization for Standardization e pelo International Electrotechnical Commission
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
M2M	Machine-to-Machine
NBR	Norma Brasileira de Regulamentação
OECD	Organisation for Economic Cooperation and Development
PaaS	Platform-as-a-service
PNCIBER	Política Nacional de Cibersegurança
PNSI	Política Nacional de Segurança da Informação

SaaS	Software as a Service
SIM Card	Subscriber Identity Module Card
SQL	Structured Query Language
SSL	Secure Sockets Layer
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLS	Transport Layer Security
VPN	Virtual Private Network
Web	Word Wide Web

SUMÁRIO

1 INTRODUÇÃO

Na era da informação digital, onde a interconexão entre sistemas, dispositivos e indivíduos é onipresente, a cibersegurança emerge como um pilar fundamental para garantir a integridade, confidencialidade e disponibilidade das informações e dos sistemas. A cibersegurança engloba um vasto espectro de desafios, desde a proteção contra ataques cibernéticos maliciosos até a mitigação de vulnerabilidades inerentes aos sistemas e infraestruturas digitais.

Com a rápida evolução da tecnologia, novas ameaças cibernéticas surgem constantemente, desafiando as organizações e indivíduos a manterem-se um passo à frente dos criminosos digitais. *Malwares* sofisticados, ataques de *phishing* direcionados e explorações de vulnerabilidades de *software* são apenas algumas das ameaças que podem comprometer a segurança dos dados e a operacionalidade dos sistemas.

Além das ameaças externas, a cibersegurança também enfrenta desafios internos, como a falta de conscientização dos usuários, falhas de configuração e erros humanos. A segurança cibernética, portanto, não é apenas uma questão técnica, mas também uma questão cultural e organizacional, exigindo um compromisso coletivo com boas práticas de segurança e uma abordagem holística para proteger os ativos digitais.

Neste trabalho, exploraremos os principais conceitos e desafios da cibersegurança, bem como as estratégias e medidas que podem ser implementadas para mitigar os riscos e fortalecer a postura de segurança cibernética. Ao compreendermos a natureza das ameaças cibernéticas e adotarmos uma abordagem proativa em relação à segurança, estaremos melhor preparados para enfrentar os desafios do mundo digital em constante evolução.

1.1 JUSTIFICATIVA

Em um mundo cada vez mais digitalizado, onde a tecnologia permeia todos os aspectos da vida moderna, a cibersegurança emerge como uma preocupação central e premente. Esta justificativa para falar sobre cibersegurança se baseia em diversos pontos cruciais:

Relevância Global: A cibersegurança é um tema de relevância global, afetando não apenas empresas e organizações, mas também governos, instituições financeiras, infraestruturas críticas e até mesmo indivíduos comuns. Os ataques cibernéticos têm o potencial de causar danos significativos, desde a interrupção de serviços essenciais até o comprometimento de dados pessoais e financeiros.

Aumento das Ameaças: Com o avanço da tecnologia, surgem também novas formas de ameaças cibernéticas, cada vez mais sofisticadas e difíceis de detectar e combater. *Malwares*, *ransomwares*, *phishing* e ataques de engenharia social são apenas algumas das ameaças que representam riscos constantes para a segurança digital.

1.2 OBJETIVO GERAL

Analisar, compreender e implementar métodos e ferramentas que podem colaborar para mitigar os riscos relacionados a cibersegurança em organizações.

1.2.1 Objetivos específicos

- Proteção da privacidade de pessoas e ativos de uma organização;
- Minimizar riscos associados à segurança cibernética tanto no nível pessoal quando organizacional;
- Desenvolver e implementar planos de resposta a incidentes que permitam uma reação rápida e eficaz a ataques cibernéticos, minimizando o tempo de inatividade e os danos causados

2 REVISÃO DE LITERATURA

2.1 O QUE É INFORMAÇÃO

A informação tem desempenho importante na sociedade ao longo da existência humana, como forma de passar ideias, técnicas e conhecimentos para as pessoas em todo o mundo. A palavra informação vem do latim *informatio*, que significa apresentar, representar, criar uma ideia ou noção do que foi transmitido. Para Ducker (2010), o termo informação é “dado investido de relevância e propósito”.

Segundo Mcgee & Prusak (1994, p. 24), a informação são “dados coletados, organizados, ordenados, aos quais são atribuídos significados e contexto".

Para HOUSAISS *et al*. (2001, p.1615), retrata a informação como “a interpretação ou significado de dados”, demonstrando que, existe um elo entre informação e dados, pois sem dados não há informação. Sendo assim, a informação é agrupamento de dados analisados, tratado e coeso, que pode ser utilizado de forma proveitosa e adequada a pessoas e organizações nas tomadas de decisões.

Contudo, dados são diferentes de informações, pois os dados não tem real significado quando não há intervenção humana mediante análise e que pode ser utilizado em um momento oportuno quando transformado em informação.

Para Shedroff (1999, p.272), descreve dado como “produto de pesquisa, criação, coleta e descoberta. É o material bruto que encontramos ou criamos para construir nossas comunicações”. Indo de encontro, e voltado ao vocabulário da área da computação, HOUSAISS et al. (2001, p. 903), destaca que dado é a “informação capaz de ser processada por um computador”. Assim, um dado passa por um processo de entrada (*input*), é analisado, interpretado, tratado e sai transformado (*output*), em dados organizados e rico em valor e significado.

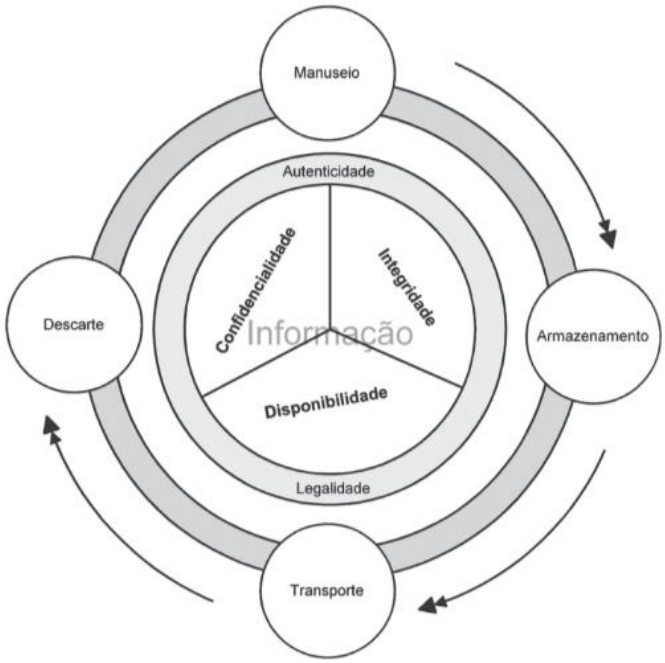
No entanto, podemos perceber através dos conceitos, que os dados ainda não são informações com relevância, significado e assim, não transmitida com completude. Porém podem futuramente, serem transformadas em informações importantes e com sentido, mas que podem conter informações sensíveis caso estejam em posse de agentes maliciosos.

2.2 CICLO DE VIDA DA INFORMAÇÃO

A fim de reforçar e contribuir para melhor entendimento da segurança da informação, é necessário conhecer as etapas do ciclo de vida da informação.

Segundo Sêmola (2013, p.09), diz que “o ciclo de vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco”.

Figura 1 – Ciclo de vida da informação



Fonte: Sêmola, 2013, p.11.

Existem quatro ciclos de vida da informação, são conhecidos como:

I. Manuseio: Momento em que a informação é manipulada;

II. Armazenamento: Momento em que a informação é arquivada;

III. Transporte: Momento em que a informação é encaminhada;

IV. Descarte: Momento em que a informação é eliminada;

Desta maneira, existem pilares para segurança da informação dentro do ciclo de vida da informação, sendo gerado a autenticidade e legalidade do que está sendo tratado e envolto de confidencialidade, integridade e disponibilidade da informação para as partes interessadas e autorizadas.

Qualquer informação manuseada, transportada, armazenada ou descartada de forma inadequada, pode gerar falhas, que acarretem na exposição e risco da integridade dos dados.

2.3 SEGURANÇA DA INFORMAÇÃO

Nos ambientes organizacionais, cada vez mais há uma preocupação em como manter os dados e informações disponíveis de maneira segura, integra e acessível ao público autorizado.

Sendo assim, a segurança da informação tem papel fundamental para contribuir para a diminuição da falta de credibilidade e exposição de informações a terceiros não autorizados.

Segundo Summers (1997, p.21), diz que:

> Percebe a segurança da informação como um componente intrínseco ao uso de computadores e a considera como uma meta a ser atingida para proteger os sistemas computacionais contra ameaças à confidencialidade, à integridade e a disponibilidade.

A norma *ISO/IEC* 17799:2005 (2014, p.410, descreve que “a segurança da informação é uma área de conhecimento voltada à proteção da informação e dos ativos associados contra indisponibilidade, alterações indevidas e acessos não autorizados”.

Embora quando pensamos em segurança da informação, tenhamos tendência de considerar somente recursos computacionais, a segurança da informação também engloba questões relacionadas aos recursos humanos.

Conforme expressado por Marciano, define que:

> A segurança da informação é um fenômeno social no qual os usuários dos recursos informacionais têm razoável conhecimento sobre o uso desses recursos, incluindo os ônus decorrentes, bem como sobre os papéis que devem desempenhar no exercício desse uso (Marciano, 2006, p.114).

Diante disso, a dinâmica das organizações em meio ao aumento explosivo de informações fez com que a visão de negócio seja de maneira ampla e holística, bem como a segurança da informação. A finalidade fundamental da segurança da informação, preza proteger a informação, como prática da gestão de riscos, no que tange ao comprometimento da confidencialidade, integridade e disponibilidade.

Sêmola (2013, p.43), declara como:

> - Confidencialidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apena às pessoas a quem é destinada.
> - Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais
> - Disponibilidade – Toda Informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitem delas para qualquer finalidade.
>
> A violação de qualquer um desses conceitos pode impactar negativamente a organização, e diante da literatura disponível, não há um conceito se sobrepondo ao outro.

2.4 SEGURANÇA CIBERNÉTICA

A segurança cibernética teve início após o surgimento da *internet* em 1960, quando os computadores começaram a se conectar através das redes interligadas, mas em 1980 após tentativas de ataques a *AT&T* e outras instituições de prestígio, foram surgindo a necessidade de buscar maneiras de evitar ataques as redes ao redor do mundo.

Embora segurança da informação tenha termo similar ao da segurança cibernética, ambos possuem diferenças entre si. Conhecer os termos é importante para entender o campo de atuação de cada uma destas áreas.

Enquanto segurança da informação engloba um conjunto de estratégias, ferramentas e processos que tenham como finalidade proteger os dados armazenados de uma organização, a segurança cibernética refere-se à proteção de ativos de informação, através do tratamento de ameaças que coloquem em risco a informação armazenada, processada e transportada nos sistemas de informação. Apesar de serem áreas que possuem finalidades distintas, uma complementa a outra e trabalham em conjunto, pois a segurança cibernética tem ligação com a segurança da informação.

Para Associação Brasileira de Normas Técnicas, expressa que:

> Dessa forma, a segurança cibernética se baseia na segurança da informação, na segurança da Internet e na segurança de *TIC*, como blocos de construção fundamentais, mas sua definição considera que a proteção do ciberespaço deve levar em conta aspectos físicos, sociais, financeiros, políticos, emocionais, profissionais, psicológicos, educacionais ou outros tipos ou consequências de falhas, danos, erros, acidentes, prejuízos ou quaisquer eventos considerados indesejáveis neste ambiente (ABNT, 2015).

Ou seja, a segurança cibernética compreende a proteção e prevenção do ciberespaço (espaço não físico, criado por sistemas interligados) e segurança da informação compreende todo tipo de risco, sejam digitais ou físicos, delimitando acesso de pessoas e sistemas.

Tendo em vista o avanço da tecnologia e sistemas interconectados ao redor do mundo, além da constante evolução e atualização de *software* e equipamentos, surge a preocupação de como serão mitigadas as vulnerabilidades e maximizadas a proteção destes ativos.

Para Agência Nacional de Telecomunicações, diz que segurança cibernética são:

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (ANATEL, 2021).

Segundo a AMAZON, define segurança cibernética como:

> A segurança cibernética é a prática de proteger computadores, redes, aplicações de *software*, sistemas essenciais e dados de possíveis ameaças digitais. As organizações têm a responsabilidade de proteger dados para preservar a confiança do cliente e atender à conformidade regulatória. Elas usam medidas e ferramentas de segurança cibernética para proteger dados sigilosos de acesso não autorizado e evitar interrupções nas operações comerciais causadas por atividades de rede indesejadas. As organizações implementam a segurança cibernética simplificando a defesa digital entre pessoas, processos e tecnologias (Amazon, 2023).

Para Canongia e Júnior (2010, p.19), é:

> Arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. É um conceito abrangente, portanto, e maior que segurança em *TI*, pois envolve pessoas e processos.

Os autores ainda acrescentam que:

> 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 outro (ibidem, 2010).

No chamado “livro verde”, Canongia e Júnior (2010, p.13), destacam que, o espaço cibernético não tem fronteiras ainda claramente definidas, e impacta o dia a dia de todos os dirigentes governamentais, de empreendimentos privados e dos

próprios cidadãos. Portanto, a promoção da cooperação entre as diversas esferas da sociedade, podem permitir o entendimento dos diferentes aspectos da segurança cibernética e quais impactos podem ser produzidos.

O principal agente de violação e obtenção de acesso não autorizado são os chamados *Hackers*, que após um ataque bem sucedido, podem roubar informações, modificar ou excluir dados confidenciais e importantes. Segundo alguns autores, o termo *Hacker*, vem sendo aplicado de forma equivocada, sendo relacionado a pessoas que praticam atividades criminosas na *internet*.

Segundo MANCINI (2011, p. 15), o *hacker* “faz algo para melhorar ou alterar o funcionamento de um sistema com uma solução criativa ou não convencional. *Hackers* são pessoas que buscam excelência em sua profissão através de métodos pouco ortodoxos, inexplorados ou inovadores “.

Em meio a era digital e crescente armazenamento de informação sigilosas e determinantes na última década, faz com que organizações sejam alvos de ataques maliciosos de programadores. Contudo, esses são chamados de *cracker*, que diferente do *hacker*, buscam vantagens para si ou terceiros, e muitas vezes com viés monetário.

SILVEIRA (2004, p. 05), descreve o termo *cracker* como: “pessoa que usa sua destreza para invadir sistemas e praticar crimes eletrônicos”. Diante disso, é perceptível a confusão entre os termos, e com grande ganho de notoriedade do termo nos últimos anos, é atribuído ao uso indevido e a violações criminosas.

Apesar dos termos terem significados diferentes, ainda há bastante referência literária destinada aos *hackers* como praticante de crimes cibernéticos, mas há ressalvas quando se referem aos com boas práticas.

Ainda assim, existem diferentes tipos de *hackers* que possuem habilidades e objetivos diferentes. Segundo Mcafee (2019), menciona os tipos de hacker:

Quadro 1 – Tipos de Hackers

Tipos	Descrição
Hackers White Hat	Conhecidos como *hackers* do “bem”, são especialistas em segurança computacional que se concentram em fazer testes de penetração e outras metodologias de modo a garantir que os sistemas de informação de empresas são realmente seguros.
Hackers Black Hat	Esses por sua vez são conhecidos como *hackers* “malvados”, geralmente chamados simplesmente de *hackes*. O termo usado para criminosos que invadem redes ou computadores, ou ainda que criam vírus de computador. Puristas usam o termo “*crackers*” para se referir aos hackers desse tipo.
Hackers Gray Hat	Usam suas habilidades para benefício próprio, mas não operam de forma totalmente legal. Por exemplo, um *hacker* que invada o sistema de uma empresa para revelar uma vulnerabilidade e poste a descoberta na *internet* pode, em última instância, estar fazendo algo positivo para os clientes daquela empresa, mas, por outro lado, comprometeram um sistema sem permissão.
Script Kiddies	Termo pejorativo indicando *hackers Black Hat*, que usam programas baixados da internet para atacar redes, alterar sites para se tornarem conhecidos, e são conhecidos como “*Green Hat*” ou amadores.
Hacktivists	São *Hackers* que almejam fazer parte de mudanças sociais. A revelação de transgressões, ou ganhos religiosos ou políticos motivam alguns *hacktivists*.
Hackers patrocinados por governos	Governos ao redor do mundo estão conscientes de que é útil a seus objetivos militares estarem bem posicionados no mundo *on-line*. Hoje o controle do ciberespaço é decisivo. *Hackers* patrocinados por governos não têm limite de tempo e contam com orçamento para focar civis, empresas e outros governos.
Hackers espiões	Empresas contratam hackers para que se infiltrem em concorrentes e roubem segredos comerciais. Podem tentar ataques externos ou conseguir empregos para agir como infiltrados. *Hackers* espiões podem usar táticas semelhantes às de *hacktivists*, mas sua única meta é atingir os objetivos do cliente e obter benefícios monetários.
Whistleblowers	Trata-se de uma pessoa inserida em uma organização que usa seu acesso a sistemas para vazar informações. Esses *hackers* podem acessar informações para vender segredos comerciais ou conseguir emprego em outras empresas.
Ciberterroristas	Geralmente motivados por crenças religiosas ou políticas, esses *hackers* tentam criar medo e caos ao interromper o funcionamento de serviços cruciais de infraestrutura. Os ciberterroristas são de longe, os mais perigosos e contam com uma ampla variedade de habilidades e objetivos. Em última instância, a motivação de ciberterroristas é espalhar medo, terror e violência.

Fonte: Adaptado de Mcafee (2019).

2.5 TIPOS DE ATAQUES CIBERNÉTICOS

Constantemente, diversos métodos, técnicas e ferramentas são utilizados como forma de ataque em redes de diversas organizações. Qualquer usuário no seu exercer laboral e rotina pessoal, em meio à conexão a uma rede, pode estar vulnerável a ataques cibernéticos no ambiente digital, por mais seguro que esteja usuário se sinta. Desta maneira, podemos pensar que não existe um sistema isento de algum grau de vulnerabilidade, a não ser que esteja desconectado de alguma rede, o que nos dias atuais, é difícil de acontecer, pois vivemos em uma era conectada a todo momento.

Sabendo que a segurança cibernética está em busca de assegurar a veracidade da informação, quais são os tipos de ataques que podem ser executados e quais são suas motivações?

Segundo a *International Business Machines Corporation* (IBM, 2023), apesar de existir variedades de motivações, há três categorias principais em que possam ser classificadas: criminoso, político e pessoal.

- Criminoso: os ataques tem como foco ganhos financeiros, por meio do roubo monetário, roubo de dados ou interrupções de negócios. Os criminosos cibernéticos podem invadir uma conta bancária para roubar dinheiro diretamente ou usar golpes de engenharia social para enganar as pessoas a enviar dinheiro a estes. Os *hackers* podem roubar dados e usá-los para cometer roubo de identidade ou vendê-los na *dark web* ou mantê-los como resgate.

- Político: frequentemente associados à guerra cibernética, ao terrorismo cibernético ou ao "*hacktivismo*." Na guerra cibernética, os atores dos estados-nação geralmente têm como alvo as agências governamentais ou a infraestrutura crítica de seus inimigos.

- Pessoal: como atuais ou ex-funcionários descontentes, buscam principalmente retribuição por alguma percepção de menosprezo. Eles podem pegar dinheiro, roubar dados confidenciais ou interromper os sistemas de uma empresa.

Sabendo que existem diferentes motivações por trás de ataques cibernéticos em organizações, existem também, diversos tipos de ataques que podem se aproveitar de vulnerabilidades em um ativo, em processos, em recursos humanos e tecnologias.

Para Coelho *et al* (2014, p. 5), afirmam que “o ataque é um ato deliberado de tentar se desviar dos controles de segurança, com o objetivo de explorar as vulnerabilidades”. Podemos definir dois tipos de ataques:

- Passivos: Tem como objetivo, obter informação baseado no monitoramento das transmissões, sendo de difícil detecção, pois não envolvem nenhuma alteração de dados. A partir de uma análise de tráfego de mensagens, é possível obter informações confidenciais. Uma maneira de evitar que isso ocorra, é através da criptografia. Neste tipo de ataque, não há modificações de informações e nem em seu fluxo.
- Ativos: Intervém no fluxo de informações, onde a mensagem é adulterada e com intuito de investir contra um sistema. Existem quatro subtipos de ataques ativos, são: representação (quando determinada entidade finge ser outra), reenvio (executada uma captura passiva dos dados e então, feita uma retransmissão produzindo efeitos danosos), modificação (quando partes da mensagem é alteradas) e negação de serviço (impede o uso normal de um serviço, proporcionado por um sistema).

Ainda assim, existem diversas técnicas, métodos e ferramentas que podem ser usadas para explorar vulnerabilidades, não se atendo apenas a pessoas que tem conhecimento tecnológico, mas também, podendo contar com qualquer usuário mal intencionado em atacar fontes de informações de uma organização.

Os profissionais de segurança cibernética possuem dificuldades diversas para conter de alguma maneira formas de infiltrações em um sistema e mitigar os riscos de ataques cibernéticos, e cada tipo de ataque, possui uma técnica empregada para atingir um objetivo. A seguir, as técnicas de ataques mais comuns:

- *Malware*: Significa “*software* mal intencionado”. Abrange uma série de softwares concebidos com intuito de permitir que terceiros obtenham

acesso não autorizado às informações sigilosas ou interrompam o funcionamento normal de uma infraestrutura essencial. Exemplos: Cavalos de Tróia (*Trojan*), *Spyware, backoors, keyloggers, worms, bots* e vírus.

- *Ransomware*: é um modelo de negócios e uma ampla gama de tecnologias associadas que atores proibidos usam para extorquir dinheiro de entidades.

- *Phishing*: é uma ameaça cibernética que usa técnicas de engenharia social para induzir usuários a divulgar informações de identificação pessoal. Exemplo, são invasores cibernéticos enviando e-mails que levam os usuários a clicar e inserir dados de cartão de crédito em uma página de pagamento falsa. Esses ataques também podem fazer com que sejam baixados anexos mal-intencionados que instalam *malware* em ativos de uma organização.

- *DDoS*: Conhecido como *Denial of Service* ou em tradução em português como “negação de serviços”, é um esforço coordenado para sobrecarregar um servidor enviando um grande volume de solicitações falsas. Esses eventos impedem usuários normais de se conectar ou acessar o servidor de destino.

- Pharming: é uma variante do *Phishing*, que explora as vulnerabilidades dos *browsers* (navegadores), dos sistemas operacionais e dos servidos *DNS* (*Domain Name System*), com o objetivo de redirecionar os usuários a páginas web falsas para obter suas informações sensíveis.

- *IP Spoofing*: tem objetivo de assumir a identidade de outro computador, através do envio de pacotes contendo *IP* (*Internet Protocol*) falsos de origem de outra máquina.

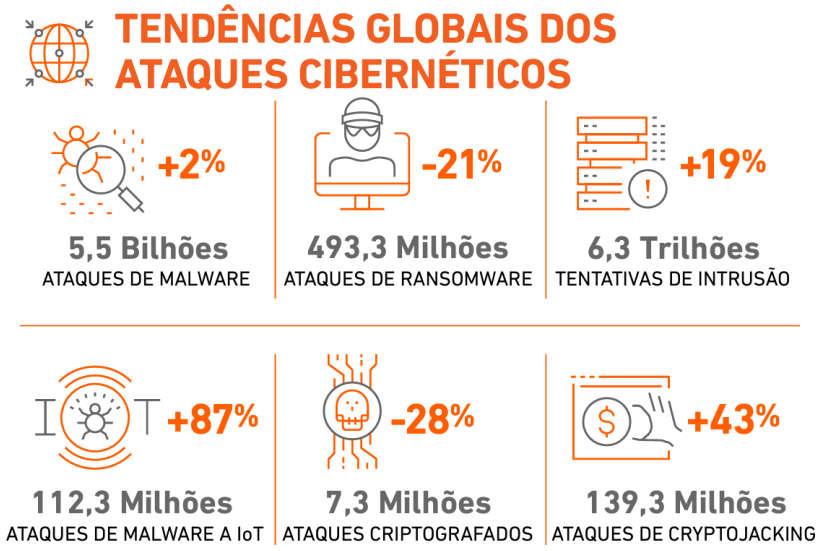
- Ataque *man-in-the-middle*: envolve uma parte externa que tenta obter acesso não autorizado por uma rede durante uma troca de dados. Esses ataques aumentam os riscos de segurança de informações sigilosas, como dados financeiros.

- *Scripting* entre *sites* (*XSS*): Os ataques de *scripts* entre *sites* (*XSS*) inserem códigos maliciosos em uma página da *Web* ou aplicativo da *Web*

legítimo. Quando um usuário visita o *site* ou aplicativo, o código é executado automaticamente no navegador do usuário, geralmente roubando informações confidenciais ou redirecionando o usuário para um *site* malicioso e falsificado. Os invasores frequentemente usam *JavaScript* para ataques *XSS*.

- *Password Cracking*: Significa o processo de quebrar senha criptografada ou com *hash* (forma em que normalmente as senhas são armazenadas no sistema), método mais comum de nome técnico "*Brute-Force Attack*". Busca um dicionário de palavras e caracteres possíveis para uma senha (*passoword*). Estes dicionários e programas costumam já existir em *sites* especiais para *hackers*. Dois dos mais conhecidos programas do gênero é o *Crack* e o *CrackJack*.
- Ameaças internas: é um risco à segurança introduzido por funcionários de uma organização que tenham más intenções. Os funcionários contam com acesso de alto nível aos sistemas de computador e podem desestabilizar a segurança da infraestrutura internamente.

Figura 2 – Tendências globais dos ataques cibernéticos



Fonte: SonicWall, 2023.

2.6 TIPOS DE SEGURANÇAS CIBERNÉTICAS

No meio digital, todos estão suscetíveis aos ataques cibernéticos, e consequentemente a exposição e deturpação de informações. A relevância dos profissionais que lidam com a cibersegurança vem crescendo em diferentes organizações, independente do seu ramo de atuação.

Nos dias atuais, utilizamos diversos tipos de dispositivos que acessam uma rede privada ou pública, e no meio corporativo, uma organização consiste em possuir uma rede em que usuários ou clientes internos e externos acessam constantemente.

AMAZON destaca que um programa de segurança cibernética eficaz envolve:

> “A instrução de funcionários sobre as práticas recomendadas de segurança e o uso de tecnologias automatizadas de defesa cibernética na infraestrutura de *TI* existente. Esses elementos atuam juntos, criando várias camadas de proteção contra ameaças potenciais em todos os pontos de acesso a dados. Identificam riscos, protegem identidades, infraestrutura e dados, detectam anomalias e eventos, respondem e analisam a causa raiz e se recuperam após um evento” (Amazon, 2023).

Apesar de esforços para atenuar os ataques sofridos nas organizações, os criminosos digitais se aperfeiçoam para executar da melhor forma, esses ataques. A CISCO, assevera que:

> “Os criminosos digitais estão continuamente aperfeiçoando suas técnicas, ou buscando novas técnicas a serem alugadas de outros grupos, o que forma outro mercado extremamente rentável. Dessa forma, qualquer criminoso tem acesso fácil a *malware* extremamente sofisticado. As empresas precisam avaliar continuamente se sua segurança está em linha com as tecnologias mais recentes em uso pelos criminosos digitais” (CISCO, 2021, p. 17).

Nakamura (2024, p. 10), diz que “Os ataques cibernéticos podem ocorrer em diferentes camadas, das redes às aplicações, passando pelas infraestruturas e pelas pessoas”. Muitos destes ataques exploram a vulnerabilidade, sejam tecnológicas, de processos ou humanas. Mas é importante conhecer quais são as formas de segurança cibernéticas que podem ser utilizadas em organizações para mitigar potenciais riscos em que seus ativos estão expostos.

2.6.1 Segurança cibernética da infraestrutura essencial ou crítica

Entendem-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade, como Energia, Transporte, Telecomunicações, Águas, Finanças, Informação, dentre outras. (Canongia e Júnior, 2010, p. 19). Neste tipo de abordagem, as organizações precisam de uma estrutura cibernética bem sólida, pois caso ocorra a interrupção destes serviços ou avaria de dados, a sociedade pode sofrer e entrar em colapso.

Para a *OECD (Organization for Economic Co-operation and Development)*, ressalta como indicativos de competências importantes para segurança cibernética de estruturas críticas, os seguintes pontos:

- Definir a política e as normas específicas, com objetivos claros, no âmbito do mais alto nível de governo;
- Atuar como o órgão central de governo com competência (responsabilidade e autoridade) para prover as melhores condições de implantação da política de segurança cibernética e seus objetivos;
- Promover tanto a cultura, quanto a educação em segurança cibernética;
- Promover mútua cooperação entre os *stakeholders* – setor privado, agência(s), terceiro setor, governo – visando à efetiva implantação da política nacional de segurança cibernética;
- Atuar com transparência assegurando delegação de competência, ou seja, governança estabelecida, facilitando e fortalecendo a cooperação, em especial entre governo e setor privado;
- Rever sistematicamente a política, normas e respectivo(s) marco(s) legal(is), com especial atenção às ameaças e vulnerabilidades das infraestruturas críticas da informação de cada país, buscando minimizar riscos e desenvolver novos instrumentos e/ou mecanismos de segurança da informação e comunicações;

- Desenvolver e exercer macrocoordenação da política e estratégia nacional de segurança cibernética, envolvendo cúpula de governo e setor privado;

- Promover e exercer a macrocoordenação do monitoramento e da avaliação de risco, baseados na análise das vulnerabilidades e ameaças das infraestruturas críticas da informação, visando proteger a economia e a sociedade contra altos impactos;

- Promover e exercer a macrocoordenação do processo nacional de gestão de risco, orientando desde aspectos da organização, ferramenta(s), até mecanismos de monitoramento, para a implementação de uma estratégia nacional de gestão de risco que compreenda:

  a) Estrutura organizacional apropriada que promova melhores práticas de segurança, e que incluam prevenção, proteção, resposta e recuperação de ameaças naturais e maliciosas; e,

  b) Sistema de medidas que permita avaliar continuamente o processo, o que inclui itens de controle, níveis de maturidade, exercícios e testes apropriados;

- Promover e exercer a macrocoordenação da capacidade de resposta à incidentes em redes computacionais, como as das equipes que atuam em *CERTs/CSIRTs*, incluindo mecanismos de forte cooperação e comunicação entre tais equipes;

- Estreitar as relações com o setor privado:

  a) Estabelecendo parcerias público-privadas e acordos de cooperação, com foco na gestão de risco, tratamento de incidentes e recuperação de sistemas e redes de informação e comunicações, e na gestão da continuidade de negócios;

  b) Estimulando o intercâmbio regular de informação, por meio do estabelecimento de acordos com cláusulas específicas para o caso de conhecimentos sensíveis ou informações classificadas;

- Estimular e apoiar a aceleração da inovação da segurança cibernética por meio da pesquisa e do desenvolvimento;
- Promover a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento das estratégias de segurança cibernética.

2.6.2 Segurança de rede

Nesta abordagem, a segurança de rede é proteção de segurança cibernética para computadores e dispositivos conectados a uma rede. Equipes de Tecnologia da Informação usam tecnologias de segurança de rede como *firewalls* e controle de acesso à rede para regular o acesso do usuário e gerenciar permissões para ativos digitais específicos, assim, ajudando a proteger informações proprietárias contra ataques cibernéticos.

Figura 3 – Segurança de Rede

Fonte: Fibracem, 2018

Segundo Gimenes (2005), uma rede é considerável vulnerável “quando acessos mal intencionados conseguem invadir, alterar ou excluir informações confidenciais e até mesmo inutilizar o sistema. Pensando nesses acessos, ao longo dos anos foram sendo criadas políticas, tecnologias e protocolos que auxiliam no aumento da segurança de uma rede.” A seguir a quadro 2 informa:

Quadro 2 – Algumas principais segurança de rede

Tipos de segurança	Descrição
Firewall	*Firewalls* colocam uma barreira entre a rede interna confiável e as redes externas não confiáveis, como a *Internet*. Eles usam um conjunto de regras definidas para permitir ou bloquear o tráfego. Um *firewall* pode ser um *hardware*, *software* ou ambos.
Segurança de e-mails	Os *gateways* de *e-mail* são os principais vetores de ameaça de uma violação de segurança. Os invasores usam informações pessoais e táticas de engenharia social para criar campanhas de *phishing* sofisticadas, com o objetivo de enganar destinatários e enviá-los para sites de *malware*. Um aplicativo de segurança de *e-mail* bloqueia a entrada de ataques e controlam mensagens de saída para impedir a perda de dados confidenciais.
Controle de acesso	Nem todo usuário deve ter acesso à rede. Para impedir possíveis invasores, será necessário reconhecer cada usuário e cada dispositivo. Após, será possível aplicar as políticas de segurança. Será possível bloquear dispositivos de *endpoint* não compatíveis ou conceder a eles apenas acesso limitado.
Segurança de aplicações	Qualquer *software* usado para administrar os negócios precisa ser protegido, independentemente de sua equipe de *TI* criar ou comprar de terceiros. Infelizmente, qualquer aplicação pode conter falhas ou vulnerabilidades que os invasores usam para se infiltrar na rede. A segurança da aplicação abrange o *hardware*, *software* e processos para corrigir essas falhas.
Prevenção contra perda de dados	As organizações devem garantir que a equipe não envie informações confidenciais para fora da rede. As tecnologias de prevenção contra perda de dados, ou *DLP*, podem impedir as pessoas de enviar, encaminhar ou, até mesmo, imprimir informações importantes de modo não seguro.
Sistemas de prevenção contra invasão	Um sistema de prevenção contra invasão (*IPS*) analisa o tráfego da rede para bloquear ativamente os ataques.
VPN	Uma rede virtual privada criptografa a conexão de um *endpoint* para uma rede, geralmente pela *Internet*. Normalmente, uma *VPN* de acesso remoto usa *IPsec* ou o protocolo *SSL* (*Secure Sockets Layer*) para autenticar a comunicação entre o dispositivo e a rede.
Segurança da Web	Uma solução de segurança da *Web* controlará o uso da *Web* da equipe, bloqueará ameaças baseadas na Web e negará acesso a sites mal-intencionados. Ela protegerá o *gateway* da *Web* no local ou na nuvem. "Segurança da *Web*" também se refere às etapas que você executa para proteger o próprio *site*.
Criptografia	Prática de proteger informações por meio do uso de algoritmos codificados, *hashes* e assinaturas. As informações podem estar em repouso (como um arquivo em um disco rígido), em trânsito (como comunicação eletrônica trocada entre duas ou mais partes) ou em uso (durante a computação de dados).

Fonte: Adaptado de CISCO e AMAZON.

2.6.3 Segurança de iot

A *Internet of Things* (*IOT*) ou “Internet das Coisas” em tradução para português, tem como referência, os dispositivos que operam remotamente na Internet em diferentes plataformas e se comunicam, através do ambiente *web*.

A grande diversidade de dispositivos e tecnologias, viabilizam a ideia por trás do *IOT*, que são dispositivos diferentes conectados em outros. Esses dispositivos com tecnologia *IOT* podem enviar e receber informações diversas, sendo por intervalos ou mesmo de forma contínua.

SANTOS (2016), define como:

> “A *Internet* das Coisas, em poucas palavras, nada mais é que uma extensão da *Internet* atual. Esta extensão é feita ao proporcionar que objetos do dia-a-dia (quaisquer que sejam) se conectem à Internet. A conexão com a rede mundial de computadores viabiliza, primeiro, controlar remotamente os objetos e, segundo permitir que os próprios objetos sejam acessados como provedores de serviços. Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial. Todavia, estas possibilidades apresentam riscos e acarretam amplos desafios técnicos e sociais” (SANTOS *et. al* 2016).

Segundo a *emnify* (2023), existem formas de mitigar riscos em conexões *IOT*:

- Segurança Física: Devido muitas vezes aplicações em *IOT* serem remotas, é primordial ter uma segurança física para evitar acessos não autorizados. A utilização de *hardware* e componentes especializados que assegurem a integridade dos dados, torna o acesso de terceiros mais difícil.

- Segurança de acesso remoto: Importante se obter um protocolo robusto de segurança de acesso remoto, que permita ações de bloqueio do *SIM Card* para dispositivos que utilizam esse componente e capacidade de desativar remotamente as conexões, caso ocorra violação de segurança física.

- Redes Privadas: O fato de enviar e receber mensagens através de dispositivos implantados por si só já apresentam riscos, mas a criptografia em mensagens pode ser uma alternativa, mas ainda com uso de redes públicas para enviar dados sensíveis pode ser uma porta de entrada de acessos indesejados. Com isso, a criação de redes privadas sobre os

mecanismos de segurança utilizados, podem garantir a segurança dos dados.

- Detecção de Anormalidades: Quando há tentativas de acessos ao dispositivo ou uma atividade fora do normal na rede, podem ser indicativos que há anormalidades.
- Bloqueio de *IMEI*: A possibilidade de bloqueio do *IMEI* – "*International Mobile Station Equipment Identity*", número disponível e exclusivo para cada dispositivo, permite configurar um *SIM* e em casos de atividades suspeitas, realizar o bloqueio do dispositivo por completo.
- Transferência de dados criptografados: Por meio da criptografia, é possível ter transferenciais de dados dentro da rede com segurança. Há diversos protocolos que os desenvolvedores podem usar, para garantir a comunicação de um dispositivo, como o *Transport Layer Security* (*TLS*)
- *Firewall* baseado em rede: Protege os dados assim que dispositivos acessem a rede, mesmo sendo dispositivos do tipo *M2M* (*Machine-to-Machine*) que possuem capacidade limitada de processamento, o que contribui para dificuldade de implantação de *firewall*. O *firewall* na própria rede garante que os processos intensivos de filtragem fiquem fora do dispositivo, e dá a possibilidade de que o tráfego malicioso não será transmitido ao dispositivo. Nesta abordagem, as organizações conseguem monitorar e bloquear tráfegos fora as suas *VPN* e bloqueiam comunicações especificas.
- Perfil de conectividade limitada: Quanto mais for possível limitar e isolar a conectividade de rede para um objetivo específico, mais seguro será a aplicação *IOT*, restringindo a somente funções vitais para o que foi projetado.

2.6.4 Segurança na nuvem

A questão de segurança na nuvem vem sendo fortemente abordada, diante do crescimento de multiplataformas conectadas a uma aplicação rodando em Nuvem, o

que vem preocupando em relação a proteção de dados e a possíveis ataques cibernéticos destas aplicações.

Segundo a AMAZON (2023), a segurança em nuvem tem como finalidade, definir medidas que garantam que a organização possa proteger dados e aplicações em execução, para que assim, seja possível aumentar a confiança do cliente e garantir que sejam cumpridas regulamentações de privacidade de dados em um ambiente escalável e operações tolerantes a falhas, tendo em vista, a cooperação e responsabilidade compartilhada entre o fornecedor do serviço em nuvem e a organização.

Assim como no armazenamento físico em servidores, os dados podem estar expostos a ameaças e ser alvo de potenciais ataques de invasores, podendo comprometer os três pilares da informação: a confidencialidade, a integridade e disponibilidade e como consequência, afetando toda a segurança em nuvem.

Serviços como *SaaS* (*software* como serviço), *IaaS* (Infraestrutura como serviço) e *PaaS* (Plataforma como serviço), estão sendo cada vez mais utilizados por organizações que contratam fornecedores para ofertarem serviços e com essa crescente, é importante a segurança em nuvem está sendo aplicada.

Para Velte A., Velte T. e Elsenpeter (2010), apontam os principais pontos positivos em relação a segurança na nuvem, sendo o:

- Monitoramento: facilidade no controle da segurança, devido a atenção está direcionada para uma nuvem e não para servidores e numerosos clientes.

- Intercâmbio Instantâneo: Em caso de ocorrência de alguma falha no servidor, é possível realizar a transferência de forma instantânea a outro dispositivo, garantindo assim, a integridade das informações armazenadas.

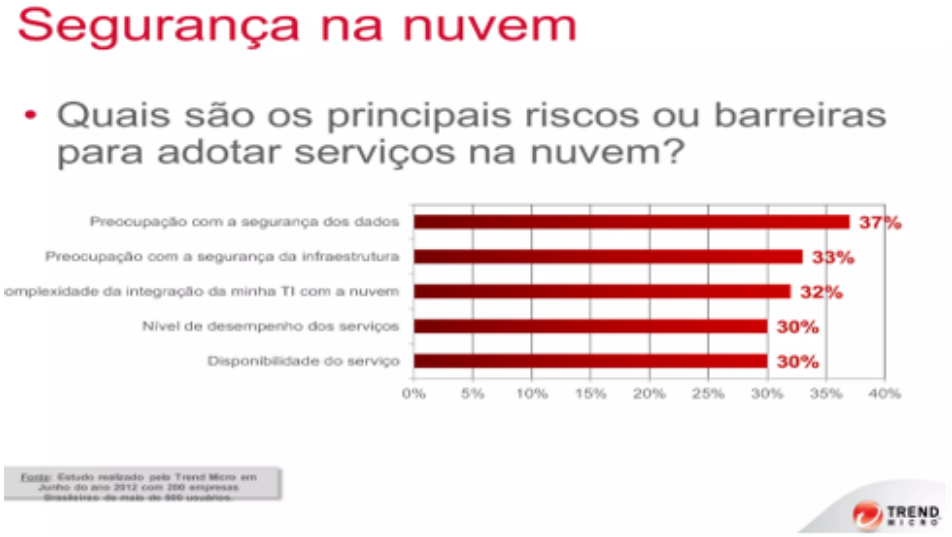
- Construções Seguras: Pode existir a possibilidade de agrupamento da rede da organização com o *software* de segurança, desenvolvendo assim, em um nível de segurança desejado.

- Melhoria da Segurança de *Software*: Com foco em não perder vendas, os fornecedores dos serviços irão aplicar o melhor *software* em segurança.

- Teste de Segurança: Em servidores do tipo *software* como serviço (*SaaS*), não são cobrados aos clientes destes serviços, os testes e segurança.

Mesmo diante de pontos cruciais que explicam os benefícios de segurança em nuvem, existem levantamentos que apontam a preocupação com determinadas áreas, como exemplificado a seguir.

Gráfico 1 – Quais os riscos ou barreiras para adotar serviços em nuvem?



Fonte: Amazon e Trend Micro, 2013

Organizações que investem em segurança na nuvem garantem maior gerenciamento das informações e integridade destes, podendo permitir melhores práticas de tomadas de decisões, sem comprometer as informações relevantes.

2.6.5 Segurança de dados

A proteção de dados é a pratica de assegurar as informações contidas em um servidor para que indivíduos não autorizados acessem os dados, mantendo assim, a informação em plenitude.

Segundo IBM (2023), a segurança de dados é um conceito que engloba todas as questões tratadas pela segurança da informação, levando em consideração a

segurança física até a de controles administrativos e segurança lógica das aplicações de *software*, além de conter procedimentos e políticas organizacionais.

A importância de ter ferramentas e tecnologias que fortaleçam a segurança de dados é crucial para criar mais uma camada de proteção contra ataques cibernéticos aos dados armazenados, diante do crescente volume de dados criados, alterados e armazenados nas organizações.

Existem três formas de proteção de dados que podem ser uteis a serem implantadas nas organizações para prevenção de ataques, segundo Oracle:

1. Proteção de dados: Por meio da criptografia, gerenciamento de chaves, edição e mascaramento de dados, é possível minimizar risco de romper dados sensíveis;

2. Controle de acesso aos dados: Investir em etapas de autenticação para saber quem irá acessar os dados e autorização para quem irá executar inclusões, modificações e deletar, além de delimitar níveis de privilégios do usuário no sistema, ajudam a proteger os dados de invasores.

3. Auditoria e monitoramento: Toda e qualquer atividade no *BD* (Banco de dados), deve ser registrada para fins de auditoria, seja por meio de informação do *login* do usuário, cliente que está fazendo a solicitação de acesso, detalhes de operação e instruções *SQL*.

2.6.6 Segurança de aplicativos

Durante a concepção de uma aplicação, é importante manter o *software* seguro em todas suas etapas de criação, desde o desenvolvimento aos testes realizados, assim reforçando a aplicação contra manipulações indesejadas de cibercriminosos.

Para Nitto et al. (2022), descreve que existem requisitos gerais para segurança no desenvolvimento e manutenção de aplicações *Web*:

i) Gerenciamento de Ambientes: Investimento em novos recursos como patches de segurança para aplicações devem ser lançados regularmente, para várias tecnologias que sustentam as aplicações para correção de vulnerabilidades que são descobertas ao longo do ciclo de vida destas

tecnologias, por meio de uso de técnicas, configurações, ferramentas e melhores práticas, para eliminar potenciais vetores de ataque e tornar as aplicações mais maduras e resistentes (*hardening*), até o momento em que as mesmas se tornem obsoletas e sem suporte. A organização deve adotar para que estes *patches* sejam realizados de forma eficiente, um processo de gerenciamento para identificar as atualizações necessárias, planejar essas atividades e documenta-las, executá-las e mensurar todo o processo.

ii) Proteção de perímetro de aplicação: Resume a fronteira entre a rede interna da organização e a internet ou qualquer fonte externa. Consiste na aplicação de controles de regras para o tráfego que flui entre a fronteira da rede interna e externa. O perímetro inclui: *Firewalls*, roteadores de borda e sistema de prevenção e detecção de intrusões (*IPS* e *IDS*), limitando o acesso às aplicações somente a endereços confiáveis e necessários, registrar informações sobre os pacotes de rede que atravessam a fronteira, de modo a identificar possíveis incidentes de segurança, impedindo-os ou reportando-os ao responsável pela segurança da aplicação.

2.7 POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO (PNSI)

Com aprovação através do Decreto n° 9.637/2018, a *PNSI* – Política Nacional de Segurança da Informação, tem como finalidade o foco na segurança e defesa cibernética, segurança física e também, a proteção dos dados organizacionais, visando através de ações, assegurar a confiabilidade, integridade, disponibilidade e autenticidade das informações.

Por meio da elaboração da *ENSI* – Estratégia Nacional de Segurança da Informação, a *PNSI* pode ser implementada, através de módulos da *ENSI*:

I. Segurança Cibernética;

II. Defesa Cibernética;

III. Segurança das Infraestruturas Críticas;

IV. Segurança da Informação Sigilosa;

V. Proteção Contra Vazamento de Dados

A *ENSI* tem como função fortalecer três setores de importância estratégica: o espacial, o cibernético e nuclear. Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio país não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço. (Brasil, 2008).

Esta política foi um esforço conjunto entre o setor público (Governo), setor privado e meio acadêmico, através de estudos de vários aspectos que abrangem a segurança cibernética. Atualmente, segundo o ranking da *ONU* (Organização das Nações Unidas), o Brasil ocupa 66° lugar em crimes cibernéticos e o 2° em prejuízos com ataques cibernéticos, o que vem levantando e fomentando a importância da uma política de segurança da informação no país.

Segundo o relatório da *Internet Organised Crime Threat Assessment* (*IOCTA*) de 2018, da Agência da União Europeia para Cooperação Policial - *Europol*, destacado no documento do decreto n° 10.222 de 2020, relata que “a falta de legislação adequada sobre crimes cibernéticos fez com que o Brasil fosse o alvo número um e a principal fonte de ataques online na América Latina; 54% dos ataques cibernéticos reportados no Brasil supostamente são originários de dentro do país” e ainda afirma que “de modo semelhante aos EUA, o Brasil é um dos principais hospedeiros de sites de *phishing*, com alguns relatos colocando o Brasil como uma das dez maiores fontes mundiais de ataques cibernéticos.”

Para *NBR* (*ISO/IEC* 17799:2005), a “A segurança da informação é obtida através da implementação de controles, de processos, de políticas e de procedimentos, que juntos fortalecem os objetivos de negócio com a minimização dos seus riscos, e a promoção da segurança da organização.”

A proposta da implementação do *PNSI* é uma tarefa que requer muita análise, devido a multidisciplinaridade do grupo que realizam os estudos deste campo, envolvendo diversos órgãos públicos. É importante que cada órgão do setor público ou privado identifique, planeje e execute ações ao qual são de sua competência, para que o país torne realidade os rumos materializados por cada ação estratégia (Brasil, 2020).

A *PNSI* é algo complexo e que tem colaboração de um time multidisciplinar, para garantir a maior aplicabilidade diante dos critérios apontados. Cada país tem sua política nacional, o que varia os critérios a serem avaliados. No âmbito do estado

brasileiro, existem diversos desafios, desde o que entende no âmbito do senso comum e de estratégias que serão necessárias para mitigar possíveis ataques a nação nos espaços cibernéticos.

Assim, podemos destacar que junto ao desenvolvimento tecnológico, o aumento expressivo de usuários conectados e utilizando e compartilhando conteúdos diversos, podem colaborar para uma desordem na segurança do espaço cibernético, caso não existam ações a serem vigoradas.

Os autores Canongia e Júnior (2010, p.13), expressam que “Diante de tais desafios, as Nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade.”

Ainda complementam:

> “Entender, portanto, tais movimentos e as respectivas oportunidades e desafios são questões estratégicas que o Estado Brasileiro vem se aprimorando e se organizando para melhorar seu posicionamento tanto no nível nacional quanto, consequentemente, no que se refere à sua inserção internacional, no tema.” (ibidem, 2010)

A construção de parcerias internacionais, com o setor privado e acadêmico podem garantir maior conhecimento, análise e ações efetivas dentro do espaço cibernético, e quais os impactos a curto, médio e longo prazo poderão apresentar a sociedade.

2.7.1 Estratégia nacional de segurança cibernética (e-ciber)

A Estratégia Nacional de Segurança cibernética, a *E-Ciber*, criada sob decreto n° 10.222 de Fevereiro de 2020, tem como objetivo manifestar as orientações e estratégias das principais ações definidas pelo governo do Brasil e da sociedade no geral, na área de segurança cibernética, alinhadas as tendências nacionais e internacionais.

Essas ações estratégicas de segurança cibernética para as organizações do país permitem que estas possam se nortear na criação e usufruir de um espaço cibernético resiliente, confiável, inclusivo e seguro (Brasil, 2020). A seguir, a quadro 3 informa de forma resumida e breve algumas das ações.

Quadro 3 – Estratégias de Segurança Cibernética

Ações	Objetivo
Fortalecer as ações de governança cibernética	Realizar fóruns de governança; Criar controles para o tratamento de informações com restrição de acesso; Estabelecer requisitos mínimos de segurança cibernética nas contratações pelos órgãos públicos; Implantar programas e projetos sobre governança cibernética; Intensificar o combate à pirataria de *software*; Designar o gestor de segurança da informação; Recomendar a certificação em segurança cibernética, conforme padrões internacionais e ampliar o uso do certificado digital.
Estabelecer um modelo centralizado de governança no âmbito nacional	Promover a coordenação dos diversos atores relacionados com a segurança cibernética, além da esfera federal; Criar um conselho nacional de segurança cibernética; Criar grupos de debate sobre segurança cibernética, em diferentes setores, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, para fomentar discussões sobre o tema, por meio de mecanismos informais de participação; Estabelecer rotina de verificações de conformidade em segurança cibernética, internamente, nos órgãos públicos e nas entidades privadas.
Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade	Estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas; Estabelecer mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis; Aperfeiçoar a infraestrutura nacional de investigação de crimes cibernéticos; Incentivar a criação e a atuação de equipe de tratamento e resposta aos incidentes cibernéticos - ETIRs, com ênfase no uso de tecnologias emergentes; Estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis.
Elevar o nível de proteção das Infraestruturas Críticas Nacionais	Promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética; Estimular a adoção de ações de segurança cibernética pelas infraestruturas críticas; Incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação, e de revisão periódica.
Aprimorar o arcabouço legal sobre segurança cibernética	Identificar e abordar temas ausentes na legislação vigente; Realizar esforços no sentido de incluir, no Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, novas tipificações de crimes cibernéticos; Criar políticas de incentivo para contratação de mão de obra especializada em segurança cibernética e definir requisitos de segurança cibernética nos programas de trabalho remoto.

Incentivar a concepção de soluções inovadoras em segurança cibernética	Propor a inclusão da segurança cibernética nos programas de fomento à pesquisa; Incentivar a criação de centros de pesquisa e desenvolvimento em segurança cibernética no âmbito do Poder Executivo federal e no setor privado; Viabilizar investimentos em pesquisas, por meio dos fundos públicos e privados; Criar programas de incentivo ao desenvolvimento de soluções de segurança cibernética; Estimular a criação de *startups* na área de segurança cibernética; Estimular o desenvolvimento e a inovação de soluções de segurança cibernética nas tecnologias emergentes; Incentivar a adoção de padrões globais de tecnologia, que permitirá a interoperabilidade em escala internacional; Incentivar o desenvolvimento de competências e de soluções em criptografia; Estimular o prosseguimento das pesquisas sobre o uso de inteligência espectral e Estabelecer requisitos mínimos de segurança cibernética que assegurem o uso pleno, responsável e seguro da tecnologia de quinta geração de conexão móvel - *5G*.
Ampliar a cooperação internacional do Brasil em Segurança cibernética	Estimular a cooperação internacional em segurança cibernética; Incentivar as discussões sobre segurança cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro; Ampliar o relacionamento internacional com os países da América Latina; Ampliar os acordos de cooperação em segurança cibernética e Identificar, estimular e aproveitar novas oportunidades comerciais em segurança cibernética.
Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade	Ampliar a cooperação entre Governo, academia e iniciativa privada para promover a implementação da *E-Ciber*; Manter um ambiente colaborativo que permita o estudo e a ampla utilização das tecnologias emergentes; Estabelecer parcerias para incentivar o setor privado a investir em medidas de segurança cibernética e Incentivar a criação de mecanismos de compartilhamento de informações sobre riscos cibernéticos.
Elevar o nível de maturidade da sociedade em segurança cibernética	Incentivar os órgãos públicos e empresas privadas para que realizem campanhas de conscientização internas; Realizar ações de conscientização da população; Estimular a criação de cursos de nível superior em segurança cibernética; Fomentar a pesquisa e o desenvolvimento em segurança cibernética; Criar programas de capacitação continuada para profissionais do setor público e do setor privado; Incentivar a formação de profissionais para atuar no combate aos crimes cibernéticos.

Fonte: Adaptado de Estratégia Nacional de Segurança Cibernética, Brasil, 2020.

2.8 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Existem leis que buscam proteger direitos da sociedade e sua singularidade, permitindo expressar opiniões e visões diferentes dentre de um espaço virtual. Com esta tendencia, surge a Lei Geral de Proteção de Dados, conhecida como *LGPD*, promulgada sob lei n° 13.709/2018. A *LGPD* estabelece normas para coleta, processamento e armazenamento de dados pessoais.

> “Promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.” (Brasil, 2018).

A legislação tem como fundamento diversos valores e principais objetivos:

- Assegurar o direto à privacidade e à proteção de dados pessoais do titular.
- Estabelecer normas de forma clara e explicita sobre o tratamento de dados do titular.
- Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados.
- Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

A *LGPD* permite o tratamento de dados nos meios digitais para garantia de direitos fundamentais de liberdade e privacidade:

> “Esta Lei 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.” (Brasil, 2018).

O tratamento de dados, na *LGPD* é realizado por meio de dois agentes: o Controlador e Operador. Também há o Encarregado, que funciona como um intermediário na comunicação entre os dois agentes (indicado pelo encarregado), os titulares dos dados e a autoridade nacional de proteção de dados (*ANPD*). A *ANDP* é o órgão responsável por fiscalizar caso ocorra descumprimento da legislação de tratamento de dados.

Qualquer tipo de tratamento de dados, deve ser claramente informado para quais finalidades serão os dados que serão coletados dos titulares, sejam dados que permitam identificação de forma direta ou indireta, como por exemplo: Nome, Sobrenome, *CPF*, Data de nascimento e local, *RG*, fotografia, endereço residencial, renda, endereço *IP*, número de telefone, dados bancários dentre outros.

Existem três classificações de dados que são tratados na *LGPD*, são:

- **Dados Sensíveis:** O sigilo é uma condição em que é mantido de forma privada e limitada a poucas partes interessadas, uma informação. Assim, os dados sensíveis, requer maior atenção, como por exemplo os que são relacionados a crianças e adolescentes, a convicções religiosas, filosóficas, racial, orientação sexual, biométricas, saúde ou genéticas. O tratamento desse tipo de dados, depende do consentimento do titular e com um fim definido para uso. Caso não ocorra o consentimento por parte do titular, somente será possível tratar informações que sejam indispensáveis em situações referente a uma obrigação legal, a políticas públicas, a estudos via órgão de pesquisa, ao exercício regular de direitos, a preservação da vida e da integridade física de um indivíduo, à tutela de procedimentos feitos por profissionais das áreas de saúde ou sanitária, à prevenção de fraudes contra o titular.

- **Dados Públicos:** Os dados em que não estão sujeitos a limitação de privacidade, sem necessidade de solicitar consentimento para tratar dados tornados públicos pelo titular em momento anterior e de forma evidente. Caso uma organização busque compartilhar estas informações com outra, esta deverá solicitar permissão ao titular. Além disso, cabe destacar que a *LGPD* também tem relação com a *LAI* (Lei de Acesso à Informação), sob lei n° 12.527/11, e com os princípios constitucionais, a exemplo do inciso XXXIII do artigo 5°: “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”.

- **Dados Anonimizados:** Consiste em uma técnica de processamento de dados que retira ou até altera informações que remetem e identificam

um indivíduo, assim garantindo seu anonimato. O dado somente será considerado anonimizado se não permitir que por meios técnicos, seja identificado o titular, e neste caso, a *LGPD* não se aplicará aos dados.

Figura 4 – A LGPD em um Giro

Fonte: SERPRO, 2020

A *LGPD* está pautada nos princípios para o tratamento de dados, levando em consideração a boa-fé, bem como:

- **Finalidade**: A motivação da realização do tratamento dos dados, ao qual deve ter proposito legítimo, específicos, explícitos e informados ao titular.
- **Adequação:** Deve acontecer conforme a finalidade informada ao titular, o contexto do tratamento de dados.
- **Necessidade:** Neste caso, o tratamento deve ser limitado a somente as suas finalidades, abrangendo os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
- **Livre Acesso:** É a garantia dada aos titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais.

- **Qualidade dos dados:** É a garantia dada aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
- **Transparência:** É a garantia dada aos titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
- **Segurança:** Por meio de medidas técnicas e administrativas que qualifiquem a proteção dos dados pessoais de acesso não autorizado e de situações de causas acidentais ou ilícitas de destruição, modificação, perda, comunicação e difusão.
- **Prevenção:** Medidas que previnam a ocorrência de danos aos dados, devido ao tratamento de dados.
- **Não descriminalização:** Não deverá ocorrer qualquer tratamento de dados de forma discriminatória, ilícita ou mesmo abusiva.
- **Responsabilização e prestação de contas:** Através do Controlador ou Operador, será demonstrado todas as medidas eficazes e capazes de comprovar o cumprimento da lei e eficácia das medidas aplicadas.

A *LGPD* deve fazer com que as organizações não somente conheçam os dados concedidos pelos usuários, mas também fazer bom proveito e transformar esses dados em informações úteis. Segundo Bioni, retrata que:

> "A *LGPD* parte da premissa de que toda a organização deve não só conhecer os dados que possui, mas, sobretudo, convertê-los em uma informação útil. Todo o sistema gira em torno da lógica em se criar uma trilha auditável do dado, pela qual o cidadão e os demais agentes econômicos enxerguem todo o seu ciclo de vida e principalmente a sua repercussão nas atividades econômicas e relações sociais que fazem parte. A nova lei não veio para travar o fluxo informacional, mas, muito pelo contrário, estimulá-lo dentro de uma lógica de sustentabilidade entre quem produz essa matéria prima e quem a explora." (Bioni, 2021, p. 70)

Além disso, investir em profissionais capacitados voltados a área de proteção de dados, concede as organizações maior entendimento e como modelar sua cultura as leis vigentes para proteção dos dados.

Lugati e Almeida (2020, p. 11), expressam:

> “A criação de um modelo eficiente para ser implementado nas organizações, trouxe a necessidade de conhecê-las a fundo, identificando todo seu cenário, mapeando os dados que são utilizados e coletados, os riscos que a permeiam, o modo como os colaboradores devem ser treinados, entre outros. Entender as empresas e dedicar um time adequado ao assunto é fundamental quando se fala em adequação às legislações de proteção dedados, de fato.”

Buscar formas de proteção dos dados e esclarecer como serão tratadas, colocam o titular como um participante no processamento de dados, pois permite entender o que será feito após o consentimento do uso desses dados as partes interessadas e concebe um sentimento de que seus dados estão em instituições confiáveis. Novas técnicas devem ser planejadas e implementadas nas organizações para permitir que as informações sejam transmitidas de forma clara e transparentes e evitando assim, ruídos e dúvidas aos titulares dos dados.

Contudo, não basta as organizações tratarem a *LGPD* como forma de evitar sansões jurídicas, mas estabelecer a criação de uma cultura em que as ações de todos os membros reflitam na segurança na coleta, armazenamento e processamento e tratamento dos dados, garantindo maior proteção desses dados.

2.9 POLÍTICA NACIONAL DE CIBERSEGURANÇA (PNCIBER)

Medida criada para reforçar e aprimorar combates a cibercrimes no Brasil, a *PNCiber*, entrou em vigor através do decreto 11.856/2023, e leva em consideração as necessidades identificadas e sugeridas por instituições e especialistas na área de cibersegurança, com o intuito de aperfeiçoar a governança nacional no que cabe ao tema considerado.

A *PNCiber* vem em consoante a *PNSI* (Política Nacional de Segurança da Informação), e para preencher lacunas na segurança, pois possuem objetivos alinhados, como confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados coletados, processados, armazenados, transmissão, bem como as soluções para zelo do ciberespaço e desenvolvimento da capacitação técnico-

profissional em segurança na sociedade. Apesar disso, a ênfase da *PNCiber* são a proteção das infraestruturas críticas, como telecomunicações, sistema de energia, transporte, informação entre outros.

A política traz um comitê responsável, chamado de Comitê Nacional de Cibersegurança (*CNCiber*), composto por representantes do governo, sociedade civil, instituições científicas, além de entidades do setor empresarial, para propor atualizações na *PNCiber* e sugestões de aperfeiçoamento nas estratégias de cooperação técnica internacional, de maneira trimestral e fortalecer a cibersegurança no país.

Ainda, a partir da Política Nacional de Cibersegurança, serão formalizadas medidas que poderão elevar mais a segurança no país e nas organizações, como a criação do Plano Nacional de Cibersegurança e também o regime interno do *CNCiber*, já que o Plano Nacional de Cibersegurança idealiza uma série de ações a serem implementadas e executadas a curto, médio e longo prazo para orientação de estratégias estabelecidas, para que ocorram de maneira eficiente e alinhas com a *PNCiber*.

A estatística de vazamento de dados no país é alarmante, cerca de 220 milhões de pessoas tiveram seus dados vazados e expostos (como *CPF* e *CNPJ*), disponibilizados para venda na internet, segundo a *PSafe*. Isso faz com que seja cada vez mais necessárias políticas que busquem minimizar e garantir que as informações não sejam expostas e que ciberataques sejam combatidos de maneira efetiva e eficaz.

Infelizmente, existem indivíduos que tentam espalhar a desinformação, dizendo que a *PNCiber* é um instrumento de censura e vigilância, limitando o acesso à informação e coletando dados para fins distintos, contudo deve se levar em consideração que existem protocolos a serem seguidos para manter a segurança nos ciberespaços utilizados por toda a sociedade.

São princípios da *PNCiber*, descritos no artigo 2°:

I - A soberania nacional e a priorização dos interesses nacionais;

II - A garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

III - A prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade;

IV - A resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos;

V - A educação e o desenvolvimento tecnológico em segurança cibernética;

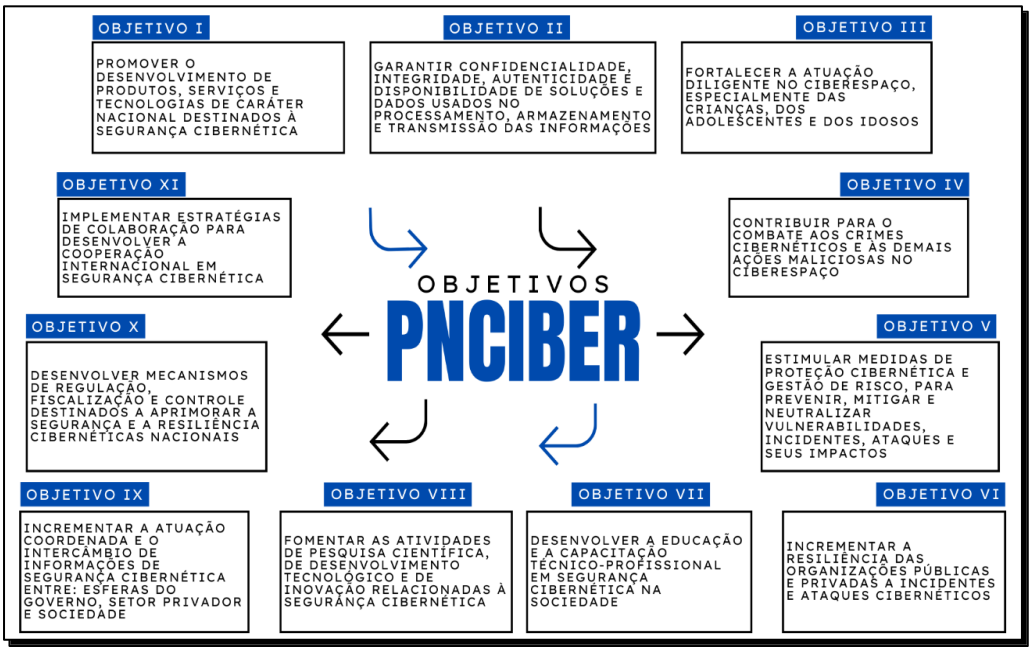
VI - A cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética; e

VII - A cooperação técnica internacional na área de segurança cibernética.

A grande adesão digital ao redor do mundo e em especial no Brasil, pode permitir que cibercriminosos atuem, devido ao pouco conhecimento em relação a medidas de segurança que podem ser colocadas em prática, o que nos vem deixando vulneráveis e expostos diante de agentes que usam de má fé as informações obtidas e que podem ser decisivas em diversos cenários.

Com a *PNCiber*r é esperado que seja reduzido incidentes de ataques e crimes cibernéticos no país em organizações públicas, privadas, além do aumento em segurança nas infraestruturas críticas e na segurança da informação, especialmente com a *LGPD* em vigor, que estabelece diretrizes legais que buscam garantir a proteção de dados e privacidade pelas organizações, um pilar essencial para um ciberespaço seguro, que cada vez mais está mais mutável.

Figura 5 – Objetivos da PNCiber



Fonte: Adaptado de Governo do Brasil, 2023.

Com objetivos postos em ação, cabe ao governo fomentar medidas que contribuam para a constante adesão, fiscalização, atualização e instruções em diferentes esferas da sociedade e organizações, e fortalecer seus instrumentos como Plano Nacional de Cibersegurança e também, a Estratégia Nacional de Cibersegurança (*E-Ciber*), conforme informado no Art. 4° do decreto Nº 11.856 de Dezembro de 2023.

3 CONSIDERAÇÕES FINAIS

Em suma, este trabalho buscou explorar a complexidade e a importância da cibersegurança em um mundo cada vez mais digitalizado. Ao longo deste estudo, analisamos as ameaças emergentes, as vulnerabilidades existentes e as estratégias de proteção que podem ser empregadas para mitigar os riscos associados à segurança cibernética.

Ficou claro que a cibersegurança não é apenas uma preocupação técnica, mas também uma questão cultural, organizacional e social. A segurança cibernética demanda uma abordagem holística, envolvendo a implementação de tecnologias de proteção avançadas, a adoção de políticas e procedimentos de segurança robustos e a promoção da conscientização e educação sobre as ameaças cibernéticas.

Além disso, é destacado a necessidade de colaboração e cooperação entre organizações, governos e indivíduos para enfrentar os desafios crescentes da cibersegurança. A segurança cibernética é uma responsabilidade compartilhada e requer um compromisso coletivo com a proteção dos ativos digitais e da privacidade dos usuários.

À medida que avançamos em direção a um futuro cada vez mais digital, é imperativo que permaneçamos vigilantes e proativos na proteção contra ameaças cibernéticas. Investimentos contínuos em pesquisa, desenvolvimento e implementação de tecnologias de segurança cibernética são essenciais para garantir a segurança e a confiabilidade das redes e sistemas digitais.

Por fim, este trabalho busca contribuir para o avanço do conhecimento e da conscientização sobre a importância da cibersegurança e oferecer insights valiosos para indivíduos, organizações e governos na busca por uma sociedade digital mais segura e resiliente.

REFERÊNCIAS

AMAZON, 2023. **O que é segurança cibernética**? Disponível em: https://aws.amazon.com/pt/what-is/cybersecurity/. Acesso em: 29 Jan. 2024

AMAZON. **O que é criptografia?**, 2023. Disponível em: https://aws.amazon.com/pt/what-is/cryptography/. Acesso em: 11 Mar. 2024.

ANATEL**. Segurança Cibernética**, 2020. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica. Acesso em 28 Jan. 2024.

BIONI, Bruno. **Proteção de Dados: Contexto, Narrativas e Elementos Fundantes**: São Paulo: Câmara Brasileira do Livro, 2021.

CAMPOS, Carlos. **O que é Segurança em IoT? Riscos, Exemplos e Soluções**, 2023. Disponível em: https://www.emnify.com/pt-br/glossario-iot/seguranca-iot. Acesso em: 15 Mar. 2024.

CÂNDIDO, Cristiane Missias; FIDELIS, Joubert Roberto Ferreira. **A administração da informação integrada às estratégias empresariais**, 2006. Disponível em: https://www.scielo.br/j/pci/a/qhxrPnFxf5dYLwMZScyhQQR/?lang=pt. Acesso em: 30 Jan. 2024.

CANONGIA, Claudia; JUNIOR, Raphael Mandarino. **LIVRO VERDE SEGURANÇA CIBERNÉTICA NO BRASIL**, 2010. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf. Acesso em: 01 Fev. 2024.

CISCO. **O que é segurança de rede?** Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html#~tipos. Acesso em: 12 Mar. 2024.

CRISTOVÂO, Andrea Martins; FERNANDES, Guilherme Augusto; GONÇALVES, Guilherme Firmino; PINHO, João Gilberto; DE SIQUEIRA, Talles Rodrigues. **A IMPORTÂNCIA DA SEGURANÇA DE REDES NO CENÁRIO ATUAL: ESTUDO COM O MÉTODO DELPHI.** Disponível em: https://abepro.org.br/biblioteca/TN_STO_213_262_27211.pdf. Acesso em: 08 Fev. 2024.

DA SILVA, Correia; NITTO, Fábio Hitsuki; ANDRADE, Luiz Henrique do Espírito Santo; TÀSSIO, Marcus Paulo Barbosa Vasconselos. **PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)**, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/guia_requisitos_minimos_web.pdf. Acesso em: 05 Abr. 2024.

DE ALMEIDA, Juliana Evangelista; LUGATI, Lys Nunes. **A LGPD E A CONSTRUÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS**, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764/7380. Acesso em: 21 Abr. 2024.

EVANGELIST, José Papo. **Segurança na Nuvem**, 2013. Disponível em: https://pt.slideshare.net/AmazonWebServicesLATAM/seguranca-na-nuvem. Acesso em: 08 Abr. 2024.

FIBRACEM. **6 DICAS PARA ELEVAR A SEGURANÇA DE REDE**, 2018. Disponível em: https://www.fibracem.com/6-dicas-para-elevar-a-seguranca-de-sua-rede/. Acesso em: 28 Fev. 2024.

GOVERNO DO BRASIL. **Classificação dos Dados**, 2021. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acesso em: 16 Abr. 2024.

GOVERNO DO BRASIL. **DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 10 Abr. 2024.

GOVERNO DO BRASIL. **DECRETO Nº 11.856, DE 26 DE DEZEMBRO DE 2023**. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 10 Mai. 2024.

GOVERNO DO BRASIL. **DECRETO Nº 6.703, DE 18 DE DEZEMBRO DE 2008**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 08 Abr. 2024.

GOVERNO DO BRASIL. **ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA – E-CIBER**, 2020. Disponível em: www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf. Acesso em: 10 Mai. 2024.

GOVERNO DO BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 21 Abr. 2024.

GOVERNO DO BRASIL. **O que é a Política Nacional de Cibersegurança, marco no combate aos crimes virtuais**, 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/3/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais#:~:text=A%20PNCiber%20contempla%20um%20conjunto,%C3%A0%20cultura%20institucional%20do%20Pa%C3%ADs. Acesso em: 05 Mai. 2024.

GOVERNO DO BRASIL. **Política Nacional de Segurança da Informação**, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao. Acesso em: 08 Abr. 2024.

GOVERNO DO BRASIL. **Princípios da LGPD**. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd. Acesso em: 21 Abr. 2024.

GRIGUTYTÈ, Monika. **What is password cracking and what techniques do hackers use**, 2024. Disponível em: https://nordvpn.com/blog/password-cracking/. Acesso em: 30 Mar. 2024

IBM. **O que é segurança de dados?** Disponível em: https://www.ibm.com/br-pt/topics/data-security. Acesso em: 15 Mar. 2024.

IBM. **O que é um ataque cibernético?** Disponível em: https://www.ibm.com/br-pt/topics/cyber-attack. Acesso em: 01 Fev. 2024.
INSIDE CYBERTECH REPORT. O avanço dos ataques cibernéticos, 2024. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report4-distrito.pdf. Acesso em: 13 Mar. 2024.

KLUSAITÈ, Laura. **A história da segurança cibernética**. Disponível em: https://nordvpn.com/pt-br/blog/historia-seguranca-cibernetica/. Acesso em: 01 Fev. 2024

LIRA, Waleska Silveira; DE ARAÙJO, Geraldo Maciel; CÂNDIDO, Gesinaldo Ataíde; DE BARROS, Marcelo Alves. **A busca e o uso da informação nas organizações**, 2008. Disponível em: https://www.scielo.br/j/pci/a/dFwYmNVCQw6wXX84kDwFrjs/. Acesso em: 27 jan. 2024.

Lisboa, Cícero Araújo; DE OLIVERIA, Guilherme Ziebell. **O conceito de dissuasão cibernética: relevância e possibilidades**, 2022. Disponível em: https://www.redalyc.org/journal/531/53172100004/html/. Acesso em: 29 Jan. 2024.

McAFEE. **9 Tipos de hackers e suas motivações**, 2019. Disponível em: https://www.mcafee.com/blogs/pt-pt/family-safety/9-tipos-de-hackers-e-suas-motivacoes/. Acesso em: 30 Jan. 2024.

MICROSOFT. **O que é a segurança de IoT?** Disponível em: https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-is-iot/security. Acesso em: 22 Mar. 2024.

NAKAMURA, Emilio Tissato. **O PAPEL DA SEGURANÇA CIBERNÉTICA NO UNIVERSO DIGITAL: A IMPORTÂNCIA DO FATOR HUMANO**, 2024. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/12758/11/Digitalizacao_e_tecnologias_Capitulo_9.pdf. Acesso em: 20 Fev. 2024.

NETO, Pedro Tenório Mascarenhas; ARAÙJO, Wagner Junqueira. **Segurança da Informação: Uma visão sistêmica para implantação em organizações**. João Pessoa: Editora UFPB, 2019.

ORACLE. **O que é Segurança de Dados?** Disponível em: https://www.oracle.com/br/security/database-security/what-is-data-security/#:~:text=A%20seguran%C3%A7a%20de%20dados%20refere,integridade%20e%20disponibilidade%20dos%20dados. cesso em: 02 Abr. 2024.

PUC-Rio. **Dados, Informação e Conhecimento**. Disponível em: https://www2.dbd.puc-rio.br/pergamum/tesesabertas/0710752_09_cap_03.pdf. Acesso em: 27 Jan. 2024.

RICARTE, Ivan Luiz Marques; MAGALHÂES, Léo Pini. **Segurança - Overview.** Disponível em: https://www.dca.fee.unicamp.br/courses/IA368F/1s1998/Monografias/luciana.html#:~:text=Ataques%20passivos%20s%C3%A3o%20aqueles%20que,a%20seguran%C3%A7a%20de%20um%20sistema. Acesso em: 21 Fev. 2024.

SEBRAE. **O que é LGPD?**, 2021. Disponível em: https://sebrae.com.br/sites/PortalSebrae/canais_adicionais/conheca_lgpd. Acesso em: 17 Abr. 2024.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva. 2° ed**. Elsevier: Campus, 2013.

SEPRO. **Brasil lança sua primeira Política Nacional de Cibersegurança**, 2023. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2023/brasil-lanca-pnciber. Acesso em: 06 Mai. 2024.

SILVA, Flávio de Oliveira. **Segurança-Serviço-Mecanismos.** Disponível em: https://www.facom.ufu.br/~flavio/security/files/2013-01/01-Seguranca-servicos-mecanismos.pdf. Acesso em: 20 Fev. 2024.

SOARES, Ana Eliza Trajano. **CULTURA HACKER: OS NOVOS SUJEITOS DO COMUM(S)**, 2014. Disponível em: https://periodicos.ufrn.br/interlegere/article/download/5311/4286/12991. Acesso em: 30 Jan. 2024.

SonicWall. **RELATÓRIO DE AMEAÇAS CIBERNÉTICAS DA SONICWALL**, 2023. Disponível em: https://www.sonicwall.com/medialibrary/pt/infographic/2023-cyber-threat-report-infographic.pdf. Acesso em: 06 Fev. 2024.

SOUZA, Diego. **A ética hacker**, 2013. Disponível em: https://pantheon.ufrj.br/bitstream/11422/4104/1/DSousa.pdf. Acesso em: 30 Jan. 2024.

TEIXEIRA, Clayson Fernando Araújo. **Segurança cibernética em redes modernas: Como proteger e mitigar ataques cibernéticos**, 2021. Disponível em: https://monografias.ufop.br/bitstream/35400000/3567/1/MONOGRAFIA_SegurançaCibernéticaRedes.pdf. Acesso em: 28 Jan. 2024.

USP. **Vazamento de mais de 220 milhões de CPFs demonstra sério problema na segurança de dados**, 2021. Disponível em: https://jornal.usp.br/atualidades/roberto-pfeiffer-comenta-vazamento-de-dados-pessoais-de-milhoes-de-pessoas-no-brasil-2/. Acesso em: 06 Mai. 2024.