UNIVERSIDADE FEDERAL DE ALFENAS - UNIFAL-MG
CAMPUS VARGINHA
INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS - ICSA
BACHARELADO INTERDISCIPLINAR EM CIÊNCIA E ECONOMIA

GIOVANNI MENDES LIMA

RISCO CIBERNÉTICO: UMA IDEIA GERAL COM ÊNFASE NO BRASIL

VARGINHA/MG
2022

GIOVANNI MENDES LIMA

RISCO CIBERNÉTICO: UM CONCEITO GERAL COM ÊNFASE NO BRASIL

Trabalho de conclusão do Programa Integrado de Ensino Pesquisa e Extensão (PIEPEX) apresentado como parte dos requisitos para obtenção do título de Bacharelado em Ciência e Economia pela Universidade Federal de Alfenas.

Orientador(a): Dra. Patrícia de Siqueira Ramos

VARGINHA/MG

2022

GIOVANNI MENDES LIMA

RISCO CIBERNÉTICO: UMA IDEIA GERAL COM ÊNFASE NO BRASIL

A banca examinadora abaixo-assinada aprova o Trabalho de Conclusão de PIEPEX apresentado como parte dos requisitos para obtenção do título de Bacharel em Ciência e Economia da Universidade Federal de Alfenas.

Aprovado em: 17 de Agosto de 2022

Prof. Dr. Manoel Vitor de Souza Veloso Assinatura:

Instituição: Universidade Federal de Alfenas

Profa. Dra. Patrícia de Siqueira Ramos Assinatura:

Instituição: Universidade Federal de Alfenas

Prof. Dr. Pablo Javier Grunmann Assinatura:

Instituição: Universidade Federal de Alfenas

RESUMO

Com o crescimento exponencial da internet na sociedade desde o início do século 21, as empresas viram a necessidade de se adaptar para ofertar os mais diversos tipos de serviços virtuais, entretanto, além da criação destes serviços, outro fator ganhou protagonismo para a tomada de decisão das empresas, os dados obtidos através da navegação dos usuário via rede, contudo, a importância não deve recair somente em usufruir da inteligência contida nos dados, mas também, na segurança e privacidade dos mesmos. Dessa forma, é necessário que as empresas brasileiras reconheçam os riscos cibernéticos e tomem medidas de precaução para combater suas possíveis consequências. A partir disso, o presente trabalho analisou o risco cibernético no Brasil, apontando quais ciberataques são mais presentes em território nacional, o custo médio de uma violação de dados e, por fim, apresentou medidas de segurança para a prevenção de possíveis ataques cibernéticos, como também, expôs o seguro cibernético como a principal ferramenta para o controle de custos elevados para empresa na ocorrência de alguma ação criminosa. O presente trabalho sugere que o ambiente brasileiro apresenta um risco cibernético relevante, como também, custos médios de violação de dados elevados, quando comparados com a américa latina, sendo assim, é necessário que a gerência de qualquer organização determine planos, tanto de prevenção com medidas de cibersegurança, quanto de resposta com a apólice de seguro cibernético.

Palavras-chave: riscos cibernéticos, cibersegurança, seguro cibernético, dados, ciberataques.

1. INTRODUÇÃO **4**

2. A INTERNET **5**

2.1 A INTERNET E SUA DESTRUIÇÃO CRIADORA **5**

2.2 A INTERNET NO BRASIL **6**

3. OS CIBERATAQUES E O RISCO CIBERNÉTICO **9**

3.1 RISCO CIBERNÉTICO **9**

3.2 OS CUSTOS DE UM CIBERATAQUE **12**

3.3 CIBERSEGURANÇA **15**

4. SEGURO CIBERNÉTICO **16**

5. CONSIDERAÇÕES FINAIS **19**

REFERÊNCIAS BIBLIOGRÁFICAS **21**

1. INTRODUÇÃO

O crescimento e a popularização da internet, a partir dos anos 2000, se mostrou uma inovação altamente modificadora do dia a dia da sociedade, seja criando mercados completamente novos ou modificando as formas de produzir e fazer diversas ações. Contudo, um aspecto que merece ênfase nesse ambiente de conexão é a questão dos dados. Muitos executivos já acreditam que os dados são tão valiosos quanto o petróleo, não por consequência da existência deles em si, mas sim por causa das diversas possibilidades que eles trazem para agregar à organização dependendo dos níveis de inteligência que estão carregados em sua composição (RIPARI, 2019).

Porém, apenas obter e analisar os dados não devem ser a única preocupação, as organizações também precisam aprender a proteger essas informações importantes, seja organizacionais ou de terceiros, já que milhares de ataques relacionados à cibersegurança ocorrem todos os dias, no Brasil e no mundo, buscando acessar tais dados. De acordo com o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), foram notificados, em média, 1.800 incidentes por dia no país, em diversas modalidades de ataques cibernéticos, nos computadores brasileiros durante o ano de 2020 (CERT, 2021). Em relação à América Latina, de acordo com o Kaspersky Daily (2021), no Brasil foram detectadas mais da metade das ocorrências de sequestro de dados. Ademais, em 2020, toda a região sofreu quase 515 tentativas por hora desse mesmo tipo de ataque cibernético, acentuando a importância de enfatizar a segurança cibernética para as organizações públicas e privadas.

Desse modo, o presente trabalho tem como objetivo apresentar as principais ameaças cibernéticas que ameaçam as organizações brasileiras, assim como apresentar o custo médio de uma violação de dados e salientar a importância da cibersegurança e do seguro cibernético como uma das principais soluções para resguardar a empresa dos custos de um possível ataque. A metodologia usada é a revisão de literatura não sistemática utilizando o google acadêmico, notícias ou relatórios disponibilizados por organizações privadas ou públicas.

O texto está organizado em cinco seções. Após esta introdução, a segunda seção contextualiza a inovação da internet e sua popularização no Brasil, a digitalização das empresas e o crescimento da importância dos dados. Em seguida, a terceira seção irá definir o que são ciberataques, definir quais são os principais deles no Brasil, apresentar os custos

médios de uma invasão, globalmente e nacionalmente, e tratar de algumas medidas de segurança. Na quarta seção é apresentado o que é o seguro cibernético, sua importância e seu crescimento pós 2020 no Brasil. Por fim, são feitas as considerações finais.

2. A INTERNET

2.1 A INTERNET E SUA DESTRUIÇÃO CRIADORA

A internet é um processo que modificou a maneira como os agentes na economia se relacionam de forma significativa, os televisores saíram da sala e se transportaram para os mais diversos tipos de *smartphones* e computadores, as locadoras de filmes em grande parte sumiram, agora existem, em seu lugar, serviços de *streaming* de filmes e séries, como a Netflix ou a Amazon Prime. Até mesmo um encontro entre familiares pode ocorrer rapidamente por um aplicativo de mensagens instantâneas independente da distância (QMC, 2020).

Dessa forma, a internet transformou o antigo modo de viver dos indivíduos nos últimos anos. Isso pode ser explicado por um processo chamado por Schumpeter (1984) de destruição criadora, ou seja, a revolução tecnológica ocasionada como consequência da internet. Com o passar do tempo, a internet fez com que diversos setores da sociedade fossem forçados a se readaptar às mudanças ou fossem destruídos pela impossibilidade de transformação do setor, como no caso das locadoras já apresentado anteriormente. Entretanto, uma modificação desse nível na sociedade não apenas destrói ou faz as empresas existentes se adaptarem, cria também novos mercados, especializações, produtos e serviços, por exemplo, os já citados serviços de *streaming*, aplicativos de comunicação instantânea, redes sociais, serviços de tráfego de dados para publicidade direcionada etc.

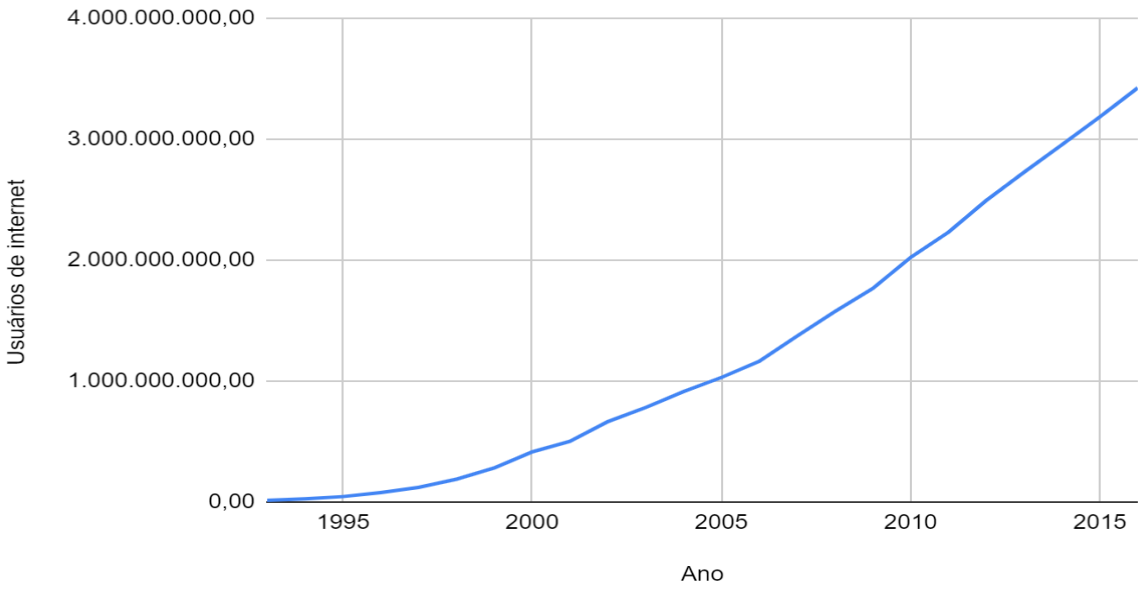
Rapini *et al.* (2021, p. 78) descreve esse processo de criação como:

> Há assim, um movimento em diversas dimensões, iniciado pela criação de novos produtos e/ou novos métodos de produção, que criam novas ocupações e novos postos de trabalho, movimento seguido pelo impacto desses novos produtos e/ou processos em setores estabelecidos, com sua transformação subsequente, a qual libera mão de obra que pode ser deslocada para esses novos setores ou para novas ocupações, possivelmente dependendo de esforços de educação e retreinamento – tarefas para o sistema educacional em geral e da educação técnica em especial.

Portanto, o movimento descrito por Rapini *et al.* (2021) sobre a mobilização dos setores do mercado de trabalho, assim como a popularização da internet no âmbito pessoal dos indivíduos, gerou um crescimento exponencial no número de usuários no mundo todo

desde a década de 90 após a criação do *World Wide Web* (www), como pode ser visualizado no Gráfico 1.

Gráfico 1 - Número de usuários da internet por ano até 2015



Fonte: Elaboração própria. Fonte dos dados: Internet Live Stats, 2016

Dessa forma, é importante entender como esse processo de crescimento se manifestou no Brasil nos últimos anos para entrarmos na discussão sobre risco cibernético.

2.2 A INTERNET NO BRASIL

O primeiro acesso à internet no país aconteceu em 1988 com o Laboratório Nacional de Computação Científica (LNCC) no Rio de Janeiro, porém só em 1994 se inicia o vislumbre da internet comercial no país com o serviço experimental de internet comercial no Brasil da Embratel, serviço que entrou a operar de forma definitiva em 1995 (KLEINA, 2018).

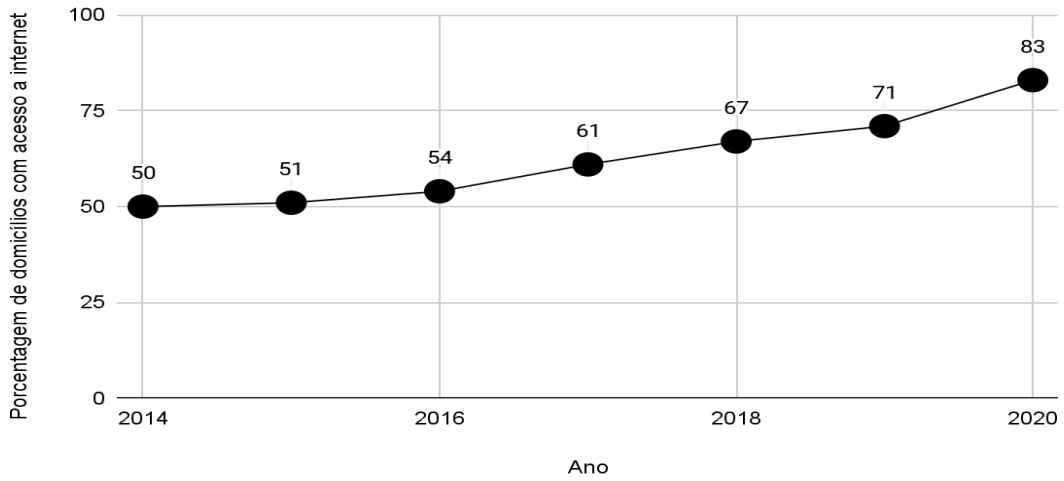
A partir disso, a internet começa a explodir no país. Em 1997, o TSE já consegue divulgar em tempo real o resultado das eleições e um ano depois já são somados o total de 2,1 milhões de usuários conectados à rede brasileira (KLEINA, 2018).

Outro marco importante para o crescimento da internet foi a aprovação da neutralidade da rede, uma das regulamentações e direitos aprovados em 2014 com o Marco

Civil da Internet, que garante o acesso sem limitação e de forma integral ao cliente (KLEINA, 2018).

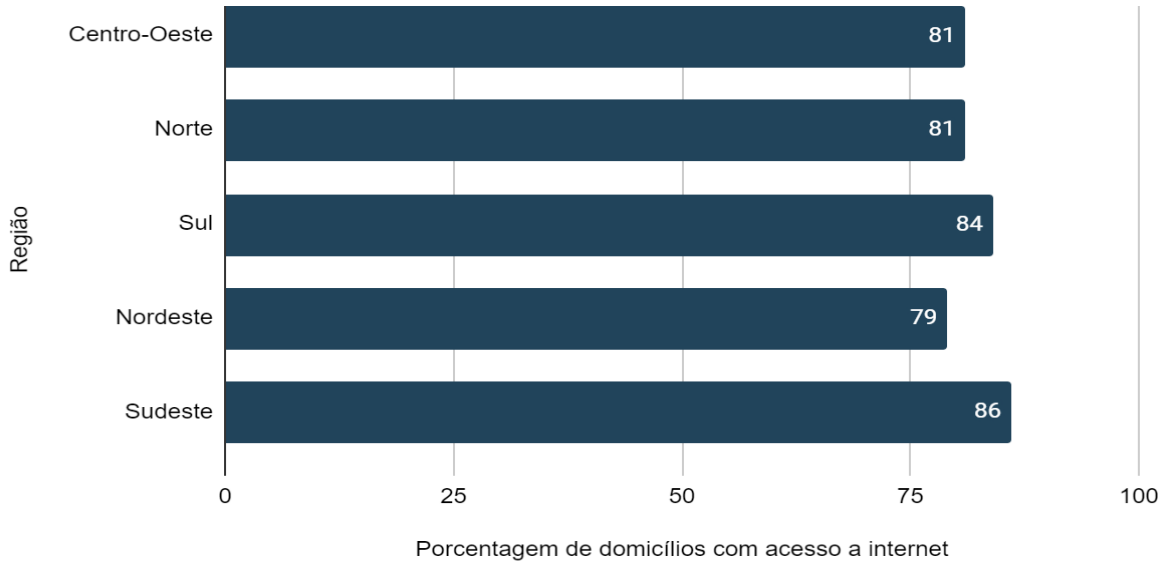
Contudo, depois de tanto tempo da chegada da internet ao país, é importante entender até que ponto ela conseguiu se inserir na sociedade brasileira e se ainda está em crescimento no contexto atual. Segundo o Centro Regional de Estudos para o Desenvolvimento da Informação (CETIC.br), de 2019 para 2020, a porcentagem de domicílios com acesso a internet passou de 71% para 83%, ocorrendo um aumento do acesso em todas as regiões do país (CETIC.br, 2021).

Gráfico 2 - Porcentagem de domicílios com acesso a internet no Brasil



Fonte: Elaboração própria. Fonte dos dados: CETIC.br, 2021

Gráfico 3 - Porcentagem de domicílios com acesso a internet por Região



Fonte: Elaboração própria. Fonte dos dados: CETIC.BR, 2021

Com isso, o crescimento percentual da conectividade nos domicílios brasileiros, proporcionou um ambiente atrativo para diversas empresas, nacionais ou estrangeiras, ofertarem serviços digitais para os usuários, como aplicativos de mensagens instantâneas ou redes sociais. Segundo o Cetic.br (2021), no ano de 2020, a utilização de aplicativos relacionados a comunicação demonstraram a maior popularidade entre os usuários de internet brasileiros, porém, outras atividades não ficaram para trás, conforme apresentado na Tabela 1.

Tabela 1 - Principais ações dos usuários por meio de serviços digitais em 2020

Ações	Usuários de Internet (%)
Mandou mensagens instantâneas	93%
Conversou por chamada de voz ou vídeo	82%
Usou redes sociais	81%
Assistiu a vídeos, programas, filmes ou séries	73%
Ouviu músicas	73%
Leu jornais, revistas ou notícias	54%
Acompanhou transmissões de áudio ou vídeo em tempo real	50%
Buscou informações sobre saúde	50%
Fez transações financeiras	46%

Fonte: Elaboração própria. Fonte dos dados: CETIC.br, 2021

Desse modo, os serviços digitais estão cada vez mais presentes na vida cotidiana dos brasileiros, possibilitando a demanda dos mais diversos tipos de informações e produtos, gerando um mercado propício para que até mesmo organizações tenham suas operações unicamente virtuais.

Contudo, ao mesmo tempo em que é ofertado um número imensurável de produtos e serviços para os usuários na internet, é gerado um novo insumo valioso para muitas organizações, que são os dados dos usuários obtidos pela navegação na rede. Esses dados são capazes de carregar diversas informações importantes, por exemplo, fornecer os conhecimentos necessários para que a organização compreenda os perfis de consumidores para os mais diversos produtos.

3. OS CIBERATAQUES E O RISCO CIBERNÉTICO

3.1 RISCO CIBERNÉTICO

A importância do uso dos dados eletrônicos para a tomada de decisão se tornou prática comum entre as empresas, entretanto, ao obter e guardar informações de clientes, é responsabilidade da organização estruturar um planejamento estratégico voltado para a proteção dos dados, principalmente após a aprovação da Lei Geral de Proteção de Dados (LGPD). De acordo com o Art. 46° da Lei n° 13.709, de 14 de agosto de 2018:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018, p.1)

Dessa forma, é necessário que as empresas estejam atentas aos riscos cibernéticos aos quais estão expostas. De acordo com Fraga (2021), a expressão risco cibernético se refere a todo ataque criminoso ocorrido em ambiente virtual, por exemplo, acesso indevido a dados e informações pessoais/sigilosas, realização de ataques bancários e até mesmo extorsão.

Assim sendo, independentemente do porte da empresa, todo seu escopo precisa estar envolvido com a segurança de dados operacionais e de clientes, posicionando esses elementos como os seus ativos mais importantes. Saber evitar e enfrentar riscos cibernéticos de maneira rápida e efetiva são fundamentais (PINHEIRO; FRERES FILHO; HOEFLICH, 2020).

Portanto, a questão da cibersegurança, deve evoluir conjuntamente com as técnicas de obtenção e análise de dados. A empresa precisa se resguardar das possíveis ameaças, porém, cada região tem suas peculiaridades, ou seja, as organizações brasileiras precisam se conscientizar aos incidentes cibernéticos mais comuns no Brasil e, dessa forma, construírem estratégias de segurança adequadas ao risco cibernético do cenário brasileiro.

Para analisar o contexto brasileiro, o Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil (CERT.br), desde 1999, coleta dados de notificações voluntárias de incidentes de segurança virtual no Brasil. Todavia, os incidentes não são todos iguais e necessitam de uma classificação. O Quadro 1 apresenta todas as categorias de incidentes registrados pelo CERT.br.

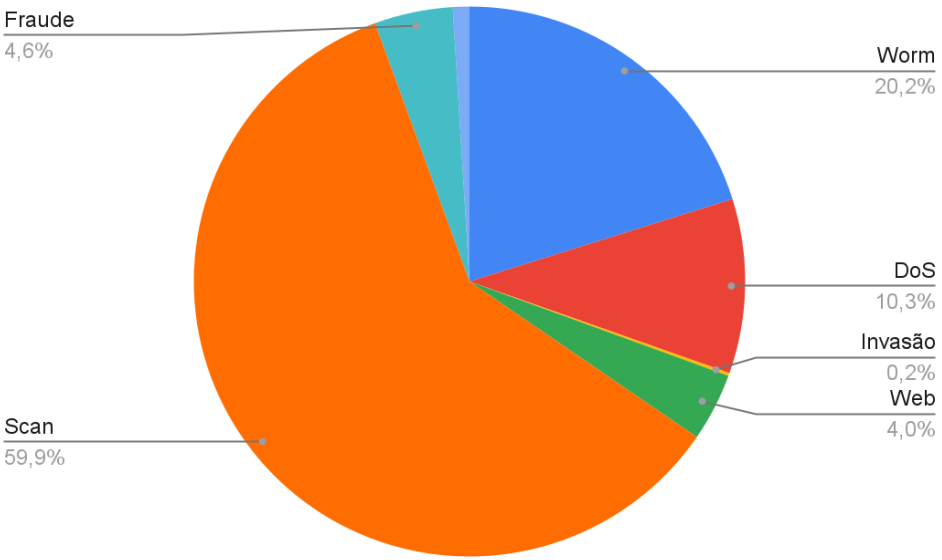
Quadro 1 - Categorias do CERT.br para incidentes cibernéticos

Worm	Notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
DoS	(DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
Invasão	Um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
Web	Um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
Fraude (*Phishing*)	Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
Scan	Notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.
Outros	Notificações de incidentes que não se enquadram nas categorias anteriores.

Fonte: Elaboração própria. Fonte dos dados: CERT.br, 2021

De acordo com o CERT.br (2021) foram notificados cerca de 665.709 incidentes no ano de 2020. O Gráfico 4 mostra a representatividade de cada uma das categorias do Quadro 1 no total de incidentes neste ano.

Gráfico 4 - Representatividade das categorias sobre o total de incidentes de 2020



Fonte: Elaboração própria. Fonte dos dados: CERT.br, 2021

Embora o *scan* auxilie a identificar vulnerabilidades para a construção de sistemas de cibersegurança, ele foi o mais usado usado pelos criminosos cibernéticos, chegando ao valor de 59,9% dos casos, ou seja, identificando vulnerabilidades das redes, em cerca de 398.760 computadores brasileiros, para outras formas de ataques cibernéticos..

Contudo, ataques cibernéticos não são apenas notificados em empresas privadas, o setor público também guarda informações vitais e um vazamento em larga escala pode expor milhares de informações de seus habitantes e organizações, prejudicando, não só a segurança cibernética, mas também, a segurança de todo o Brasil. Um exemplo disso foi o gigantesco vazamento de um banco de dados nacional, noticiado em 2021 que, segundo a Syhunt (2021), expôs cerca de 223 milhões de brasileiros, 40 milhões de empresas e 104 milhões de veículos. A Tabela 2 exibe o vazamento estimado de informações das empresas em algumas categorias.

Tabela 2 - Vazamento estimado de informações de empresas (continua)

Nome do Conjunto de Dados	Descrição	Tamanho Estimado
Classe de Operação	Horário de funcionamento (24h, comercial 9h às 18h, almoço, noite etc.), tipo de distribuição (varejo físico, varejo online, atacado físico)	0,2 GB
Sintegra	Número de registro do estado, data de início da atividade, status do registro	1,4 GB
Mosaic	Grupo de segmentação e subgrupo	1,7 GB
Capital Social	Valor do capital social	1,7 GB
Representante Legal	CPF e nome do representante, situação cadastral (ativa / baixada / imprópria)	2,0 GB
Score de Crédito	Pontuação de risco, nível de risco (baixo / médio / alto)	2,2 GB
Natureza Jurídica	Empresa, empresário individual, cooperativa, agência pública, etc.	2,6 GB
E-mail	..	2,9 GB
CNAE	..	3,8 GB
Simples Nacional	Situação (optante / Não-optante)	4,3 GB
Receita Federal	Data de fundação, status do registro (ativa / baixada / inapta)	5,5 GB

Tabela 2 - Vazamento estimado de informações de empresas (conclusão)

Nome do Conjunto de Dados	Descrição	Tamanho Estimado
Básico	Número do CNPJ, razão social, nome fantasia, cadastro (matriz / filial, situação), data de fundação, número de empregados, tamanho, natureza legal	8,3 GB
Endereço	Endereço, número, bairro, cidade, estado, código postal, tipo (Residencial / Comercial), latitude e longitude	8,5 GB
Devedores	Modalidade (principal, corresponsável), unidade responsável, cadastro, modalidade de crédito (multa, IRPJ, COFINS, CSLL etc.), valor	9,5 - 20 GB
Empresarial	Nome e CPF dos sócios da empresa, participação (ações e percentual), data de entrada na empresa	45,9 GB
Telefone	Código de área, número, operadora, plano, tipo de linha (fixa, pré-paga, pós-paga), data de instalação	48,2 GB

Fonte: Elaboração própria. Fonte dos dados: SYHUNT, 2021

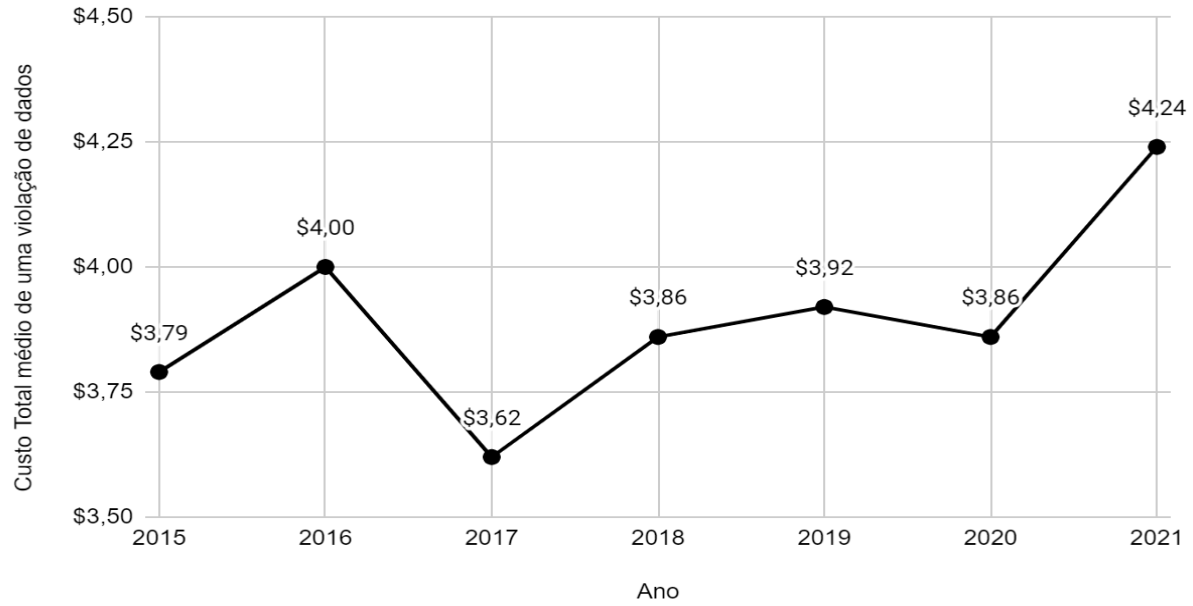
Portanto, a avaliação do risco cibernético deve compor a estratégia da governança, seja na dimensão pública ou privada, pois, com isso, é possível se preparar para criar estruturas de segurança e resposta eficientemente. Garantir a conscientização sobre o tema, previne que o desenvolvimento socioeconômico brasileiro não seja colocado em perigo por conta das ameaças virtuais (MICROSOFT, 2022).

3.2 OS CUSTOS DE UM CIBERATAQUE

A análise do risco cibernético vai além do reconhecimento dos tipos de ataques pelas organizações, um ataque também envolve custos que devem ser compreendidos pela alta administração de qualquer entidade, para isso, analisar a tendência global de custos é importante para identificarmos em qual posição está o cenário brasileiro.

De acordo com a IBM (2021), no ano de 2021, o custo médio global de uma violação de dados foi de 4,24 milhões de dólares. O Gráfico 5 apresenta os custos médios obtidos nos últimos anos desde 2015 pela IBM.

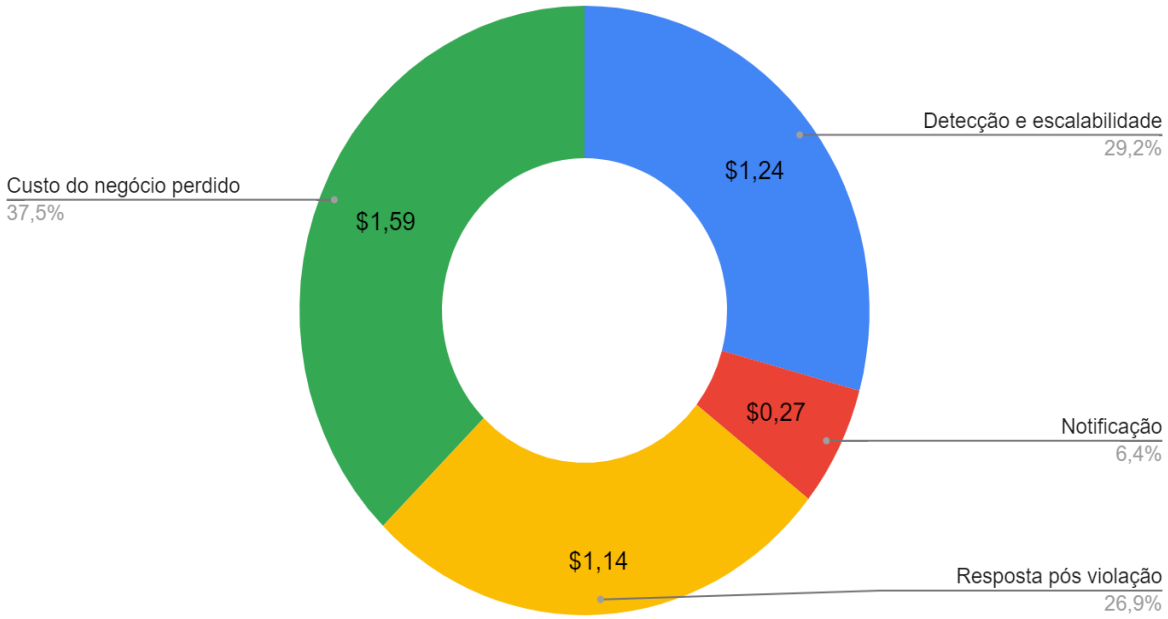
Gráfico 5 - Custo médio de uma violação de dados desde 2015 (em milhões de dólares)



Fonte: Elaboração Própria. Fonte dos Dados: IBM, 2021

Contudo, segundo a IBM (2021), é possível distribuir esses 4,24 milhões em quatro centros de categorias de custos: detecção e escalabilidade, notificação, respostas pós-violação e custo de negócio perdido. O Gráfico 6 demonstra essa divisão para o ano de 2021.

Gráfico 6 - Distribuição do custo médio de 2021 em quatro categorias



Fonte: Elaboração Própria. Fonte dos Dados: IBM, 2021

De acordo com o Gráfico 6, o custo do negócio perdido foi a categoria com maior importância, contribuindo cerca de 37,5%, ou 1,59 milhões de dólares, para o custo total médio de uma violação de dados no ano de 2021. Nessa categoria são considerados todos os custos relacionados com a interrupção de negócios e perdas de receita por tempo de inatividade do sistema, custo de perda de clientes e de aquisição de novos clientes, perdas de reputação e deterioração de imagem comercial (IBM, 2021).

Dessa forma, o fato da categoria de custo de negócio perdido estar em destaque, demonstra os efeitos negativos para a imagem da organização caso ocorra um vazamento de dados. Segundo Diniz (2021), o grau de confiança de um consumidor pode ser impactado negativamente caso a empresa seja atacada no âmbito cibernético, pois um vazamento de dados pode vir em seguida.

As outras categorias envolvem a detecção do ciberataque e a mensuração da profundidade do vazamento, sua notificação para todos os agentes necessários, como os titulares dos dados, reguladores de proteção de dados e outros terceiros e, por fim, a resposta da empresa ao ataque, aqui entram as despesas legais e multas de regulamentações (IBM, 2021).

Retornando para o contexto brasileiro, segundo a IBM (2021), o Brasil está abaixo da média mundial de custos por violação de dados em 2021, cerca de 1,08 milhões de dólares, porém, este valor ao ser comparado com o custo médio da América Latina, que é de 2,56 milhões de dólares, demonstra alta presença do país nos custo médio da região, aproximadamente 42,19%.

Portanto, mesmo estando abaixo da média mundial de custos por violação, o Brasil tem um alto índice de custos ao ser comparado com sua região, além disso, dependendo do nível da empresa, um ciberataque pode definir o encerramento das atividades, caso a organização não tenha um plano de contingência.

Dessa forma, o risco cibernético é uma ameaça cotidiana para as organizações de todo o mundo, ele apresenta diversos custos, dentre os principais deles, como já mencionado por Diniz (2021), a confiança na empresa pode ser afetada bruscamente e, embora, segundo a IBM (2021), os custos do Brasil estarem abaixo da média mundial em 2021, não é algo que deve ser subestimado pelas empresas brasileiras.

3.3 CIBERSEGURANÇA

Usando o conhecimento do risco cibernético, a organização precisa tomar medidas de cibersegurança para diminuir as chances de um possível ciberataque atingir profundamente a organização. As principais ações que podem ser tomadas são adquirir *softwares* de proteção a arquivos maliciosos ou a contratação de profissionais da tecnologia da informação (TI) para construir redes seguras (GAMA, 2022).

Porém, é esperado que além da contratação ou criação de diversas barreiras de segurança aos sistemas da empresa, que também seja difundida a ideia de que não se pode tratar a segurança de dados apenas no âmbito tecnológico, mas também, considerar a conscientização dos funcionários sobre o tema (GAMA, 2022).

Segundo Pinheiro, Freres Filho e Hoeflich (2020), muitas iniciativas de transformação que têm como objetivo melhorar a segurança cibernética são subdimensionadas pela liderança e tratados apenas como problemas de TI. Porém, a mudança deveria ser direcionada não apenas para um setor, mas também para a organização, com o fim de promover uma gestão de riscos mais efetiva e, dessa forma, inserir um novo modo de enxergar a segurança cibernética.

A engenharia social, ou variações, como o *phishing,* é o nome dado para a prática criminosa que tem a intenção de enganar o funcionário para que ele revele dados, credenciais ou brechas importantes ao criminoso de forma consciente ou inconsciente. Muitas vezes essa prática apresenta sucesso por causa do próprio desconhecimento do usuário sobre os perigos do ambiente virtual (PINHEIRO; FRERES FILHO; HOEFLICH, 2020).

Desta maneira, definir, como um objetivo, rotinas que levam a questão dos perigos virtuais de maneira mais enfática, pode proteger as brechas que as tecnologias não conseguem prevenir e, desse modo, criar uma rede forte contra criminosos por meio do treinamento de seus funcionários. O Quadro 2 contém 7 práticas de segurança que merecem atenção das empresas segundo o HSC BRASIL (2018) .

Quadro 2 - Boas práticas de segurança (continua)

Práticas	Descrição
Manter softwares atualizados	Desenvolvedores de softwares originais sempre estão atualizando seus programas em busca de maior proteção contra ciberataques.
Fazer cópias de segurança	Fazer backup facilita e agiliza o processo de recuperação dos dados da empresa caso ocorra roubo ou furto ocasionado por hackers.

(conclusão)

Investir em serviços e equipamentos voltados para a segurança	Investir em melhores fontes de defesa, como os antivírus e sistemas computacionais atualizados, irá ajudar na segurança da empresa
Focar na educação dos funcionários	Todos os funcionários precisam ser conscientizados dos riscos cibernéticos, principalmente aqueles relacionados com a engenharia social.
Implementar uma política de segurança	Uma política de segurança contribuiria para a adoção das medidas de cibersegurança mais rapidamente.

Fonte: Elaboração própria. Fonte dos dados: HSC BRASIL, 2018

Portanto, para que uma estratégia de cibersegurança tenha seu efetivo sucesso, a tecnologia e a conscientização andam de mãos dadas, esses dois vetores se complementam para que a empresa se torne uma muralha para a grande maioria dos ataques (GAMA, 2022).

Entretanto, mesmo que a empresa adote todas as práticas de segurança possíveis, ainda assim, é necessário se resguardar dos altos custos de um possível ataque, dado que, como apresentado pela IBM (2021), estão na faixa dos milhões de dólares, desse modo, a principal ferramenta para isso é o seguro cibernético (PEIXOTO, 2022).

4 SEGURO CIBERNÉTICO

Após a pandemia iniciada pela covid-19 em 2020, muitas organizações em todo o mundo sentiram a necessidade de modificarem suas ações presenciais para o formato *home office*, ou seja, os indivíduos faziam suas ações laborais diretamente de suas casas, no Brasil não seria diferente. Contudo, dado ao problema da falta de conscientização sobre os perigos da internet, já apontado neste trabalho, quanto ao próprio ambiente suscetível para cibercriminosos durante a pandemia, resultaram na intensificação do risco cibernético (ARDITTI, 2021).

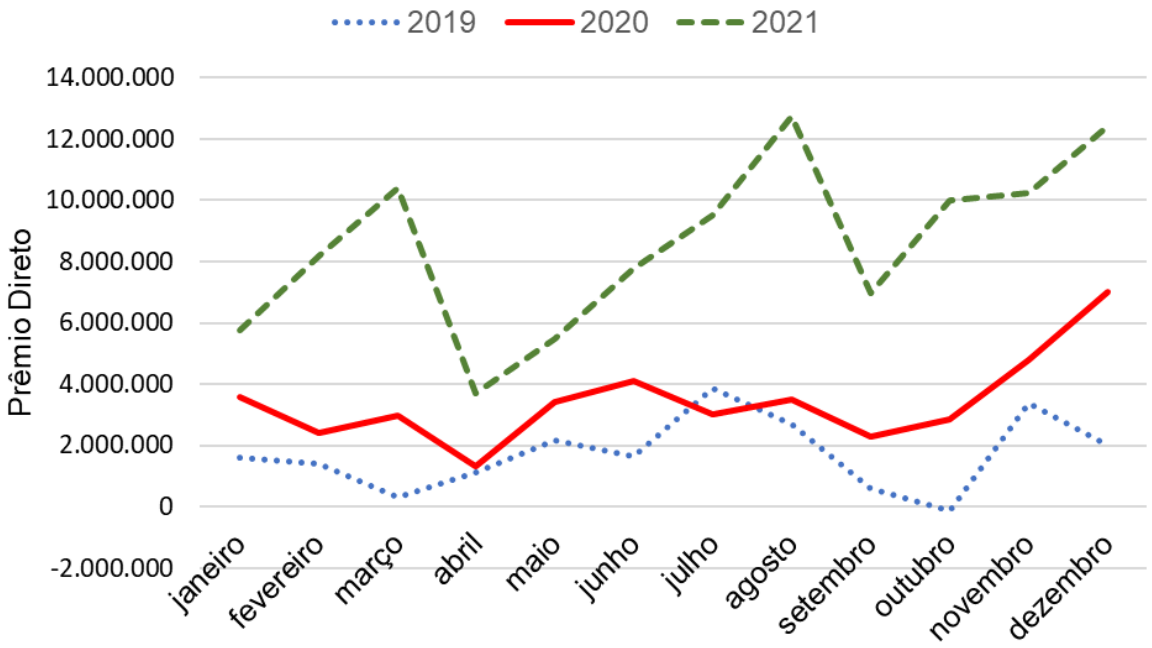
Os altos custos de sofrer um cibercrime, juntamente com a pressão da LGPD, impulsionaram, no Brasil, o crescimento de um produto securitário para controlar possíveis grandes perdas financeiras como consequência de um crime cibernético, o seguro cibernético. Segundo Negócio Seguro (2021, p. 2), o seguro cibernético pode ser descrito como:

> O Seguro Cibernético é um protecional adicional às empresas, uma apólice que visa amparar perdas financeiras decorrentes de ataques virtuais maliciosos, ou mesmo de incidentes decorrentes de erros ou negligências causados internamente na companhia, que resultem em vazamento de dados e outros danos ligados ao sigilo da informação.

Desse modo, o seguro cibernético é um meio para que a empresa responda mais rapidamente ao ataque, ou seja, dependendo da apólice, ela pode reduzir os impactos de todos os pilares de custos apresentados pela IBM (2021) e já discutidas neste trabalho, se tornando essencial para que a empresa complemente sua estratégia de segurança de dados.

A superintendência de seguros de seguros privados (SUSEP) é o órgão responsável pelo controle e fiscalização do mercado do seguro no Brasil, desse modo, ela coleta os dados do mercado segurador e divulga suas estatísticas. O Gráfico 7 demonstra o crescimento, no Brasil, de acordo com a SUSEP (2022), do prêmio direto deste seguro, que é composto pelo valor total do prêmio emitido, deduzindo-se as despesas com cancelamento, restituição e desconto, desde setembro de 2020, em que é possível observar um um marco de crescimento para essa modalidade.

Gráfico 7 - Prêmio direto do seguro cibernético nos anos de 2019, 2020 e 2021



Fonte: Elaboração própria. Fonte dos dados: SUSEP (2022)

Todavia, o seguro cibernético ainda é um produto de complexa mensuração de custo, dado que o risco cibernético varia de organização para organização, muito disso é por causa

das características intrínsecas de cada empresa, como o porte, suas conexões, sistemas de proteção, o interesse dos *hackers* no mercado da organização, volume de informações em risco e extensões de possíveis danos que necessitam da cobertura (PEIXOTO, 2022).

Assim sendo, a apólice de seguro cibernético é um produto multivariado, oferecendo diversas coberturas para auxiliar na proteção organizacional. Elas devem ser discutidas e analisadas pela alta administração da empresa na qual planeja adquirir essa apólice, pois, o conhecimento das necessidades, vulnerabilidades e a comunicação aberta com a seguradora, irão definir o sucesso do seguro caso um sinistro aconteça. O Quadro 3 apresenta algumas das principais coberturas da apólice de seguro cibernético oferecidas pelas seguradoras e suas descrições.

Quadro 3 - Principais coberturas do seguro cibernético

Coberturas	Descrição de sinistros cobertos
Responsabilidade por Dados Pessoais ou Corporativos	A divulgação pública de quaisquer dados privados ou de terceiros que estejam sob custódia da sociedade.
Responsabilidade pela Segurança de Dados	Quaisquer contaminações nos sistemas da sociedade por software não autorizado ou até mesmo furto físico de hardware da empresa por um terceiro, possibilitando possível furto de dados sigilosos.
Dados eletrônicos	Custo para a possível recriação ou recuperação de dados perdida em ocorrência a uma contaminação ou invasão de terceiros nos bancos de dados da empresa.
Custo de Defesa	Honorários e outros custos decorrentes de recurso de um procedimento civil, regulatório, administrativo ou criminal.
Restituição de Imagem da Sociedade e Pessoal	Custos e despesas para mitigar os danos à reputação em consequência de uma reclamação coberta pelo seguro.

Fonte: Elaboração própria. Fonte dos dados: NEGÓCIO SEGURO, 2021

Contudo, o seguro cibernético não é apenas mais uma ferramenta para gerir o risco cibernético, é uma atividade importante para garantir um diferencial competitivo e uma medida de sobrevivência, pois, a cada dia, a segurança de dados se torna uma demanda maior por parte dos clientes. Ao adquirir tal produto, aliado às medidas de cibersegurança, a organização consegue transmitir a importância organizacional depositada sobre o tema, amplificando a segurança do mercado sobre a empresa (SANTOS, 2021).

5. CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo apresentar as principais ameaças cibernéticas que afetam as companhias brasileiras, assim como evidenciar o custo médio de uma violação de para a região, discutir a importância da implementação de uma política segurança voltada não apenas para o setor de TI, mas também para todos os indivíduos da organização como uma política de segurança e, por fim, mostrar o crescimento do seguro cibernético em âmbito nacional e sua importância na gestão de custos elevados em decorrência de um ataque.

Dentre os resultados do trabalho, foi evidenciado dentre todos os incidentes de cibersegurança no Brasil, o principal deles foi o *scan*, contabilizando quase 60% dos casos, este incidente consiste em uma forma de identificar vulnerabilidades dentro de uma rede de computadores e, desse modo, captar dados importantes para o cibercriminosos.

Além disso, foi apresentado os custos médios de uma violação de dados, no âmbito mundial e nacional. Tratando do contexto mundial, foi observado que a média de custos causados por uma violação de dados foi de cerca de 4,25 milhões de dólares. Contudo, este valor pode ser repartido em algumas categorias de custos, entretanto, uma apresentou grande expressividade, a categoria de custos de negócio perdido, contribuindo para aproximadamente 37,5% da média mundial de custos. Já a média de uma violação de dados, no Brasil, apresentou o valor de 1,08 milhões de dólares, abaixo da média mundial, porém tal custo não é baixo, ao comparar com sua região, ele corresponde a aproximadamente 42,19% do custo médio por violação de dados da américa latina.

Com base nisso, foram apresentadas medidas de cibersegurança que influenciam na prevenção de ciberataques, como obtenção de softwares e funcionários da área da tecnologia da informação, entretanto, além destes aspectos relacionados à tecnologia de redes, a conscientização dos funcionários se mostrou de suma importância para complementar a segurança cibernética da organização, devido a práticas conhecidas como engenharia social, em que criminosos enganam funcionários para obter informações sigilosas de maneira conscientemente ou inconscientemente. Dessa forma, é necessário a implementação de uma cultura de segurança que alie as dimensões tecnológicas e humanas para que a estratégia de cibersegurança tenha seu devido sucesso.

Por fim, foi discutido o seguro cibernético como a principal ferramenta na proteção de custos elevados para as empresas, dado que as melhores práticas de segurança cibernética não

previnem totalmente o risco cibernético de ocorrer e, dessa forma, não suprem a necessidade de uma resposta rápida aos custos organizacionais em uma possível violação de dados. Assim sendo, a apólice de seguros cibernéticos, além de resguardar a empresa dos possíveis custos, é também, um diferencial que potencializa a confiança do mercado na organização.

O presente trabalho sugere que o ambiente brasileiro apresenta riscos cibernéticos consideráveis em relação a sua região, dado os seus custos altos por violação de dados e sua alta representatividade na américa latina, desse modo, as organizações devem se resguardar, aliando as práticas de cibersegurança com a apólice de seguro cibernético, para que assim, elas possam gerir o risco de modo eficiente, além disso, tal ação estabelece a confiança do mercado sobre a organização em relação às questões de informações sigilosas, obtendo vantagem competitiva no ambiente digitalizado, impulsionado pela ascensão da internet.

REFERÊNCIAS BIBLIOGRÁFICAS

ARDITTI, F. Cibersegurança: o pós-pandemia é para ontem**. Convergência Digital**, 2021. Disponível em: https://www.convergenciadigital.com.br/Opiniao/Ciberseguranca%3A-o-pos-pandemia-e-para-ontem-57616.html? Acesso em: 24 de julho de 2022.

BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 25 de Julho de 2022.

CERT.BR. Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2020. **CERT.BR**, 2021. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/total.html/ Acesso em: 25 de julho de 2022.

CETIC.BR. **TIC Domicílios 2021 – Apresentação dos principais resultados para a imprensa**. Disponível em: https://cetic.br/pt/pesquisa/domicilios/analises/ Acesso em: 17 de Julho de 2022.

DINIZ, D. 3 a cada 5 brasileiros têm medo de terem seus dados vazados ao comprarem on-line. **dfndr blog**, 2021. Disponível em: https://www.psafe.com/blog/3-a-cada-5-brasileiros-tem-medo-de-ter-seus-dados-vazados-ao-comprarem-on-line/ Acesso em: 25 de Julho de 2022.

FRAGA, C. Riscos cibernéticos: o que são, como avaliar e como prevenir. MUTUUS, 2022. Disponível em: https://www.mutuus.net/blog/riscos-ciberneticos/ Acesso em: 25 de Julho de 2022

GAMA, M. Jornada de Segurança da Informação: como a cibersegurança vem se tornando prioritária no plano de negócios das empresas. **segs**, 2022. Disponível em: https://www.segs.com.br/info-ti/352330-jornada-de-seguranca-da-informacao-como-a-ciberseguranca-vem-se-tornando-prioritaria-no-plano-de-negocios-das-empresas Acesso em: 24 de julho de 2022.

HSC BRASIL. Conheça 7 boas práticas de segurança da informação para empresas. **HSC Brasil**, 2018. Disponível em: https://www.hscbrasil.com.br/boas-praticas-de-seguranca-da-informacao/ Acesso em: 25 de Julho 2022.

IBM. **Relatório de Custo de uma Violação de Dados 2021**. Disponível em: https://www.ibm.com/br-pt/security/data-breach Acesso em: 25 de Julho de 2022.

INTERNET LIVE STATS. Internet Users. **INTERNET LIVE STATS**, 2016. Disponível em: https://www.internetlivestats.com/internet-users/ Acesso em: 17 de julho de 2022

KASPERSKY DAILY. Ransomware cai, mas ainda é maior desafio para empresas. **Kaspersky daily**, 2021. Disponível em: https://www.kaspersky.com.br/blog/ransomware-prejuizo-empresas-pesquisa/18141/ Acesso em: 27 de Julho de 2022.

KLEINA, N. Como tudo começou: a história da internet no Brasil. **Tecmundo**, 2018. Disponível em: https://www.tecmundo.com.br/mercado/129792-tudo-comecou-historia-internet-brasil-video.htm Acesso em: 17 de julho de 2022.

MICROSOFT. Conscientização sobre cibersegurança impulsiona o desenvolvimento no país. **Valor econômico**, 2022. Disponível em: https://valor.globo.com/patrocinado/microsoft/ciber-seguranca/noticia/2022/06/28/conscientizacao-sobre-ciberseguranca-impulsiona-desenvolvimento-do-pais.ghtml Acesso em: 24 de Julho de 2022.

NEGÓCIO SEGURO. Seguro cibernético: O que é e como se proteger desses riscos?. **Negócio Seguro**, 2021. Disponível em: https://www.negocioseguroaig.com.br/industria/de-olho/seguro-cibernetico/ Acesso em: 25 de Julho de 2022.

PEIXOTO, H. Risco cibernético: Quanto deste risco real já está no seu valuation?. **MONEY TIMES**, 2022. Disponível em: https://www.moneytimes.com.br/risco-cibernetico-quanto-deste-risco-real-ja-esta-no-seu-valuation/ Acesso em: 24 de julho de 2022.

PINHEIRO, J.; FRERES FILHO, H.; HOEFLICH, S. Inovação, Riscos Cibernéticos e os Recursos Securitários. **Seguros em Artigos de Acadêmicos Acervo de Cátedras da ANSP**, n. 3, 2020.

QMC TELECOM. A tecnologia mudou muito nosso modo de vida – e a forma de fazer negócio também. **QMC telecom**, 2020. Disponível em: https://blog.qmctelecom.com.br/a-tecnologia-mudou-muito-nosso-modo-de-vida-e-a-forma-de-fazer-negocio-tambem/ Acesso em: 17 de julho de 2022.

RAPINI, *et al.* **Economia da ciência, tecnologia e inovação**: fundamentos teóricos e a economia global. Belo Horizonte: Editora FACE-UFMG, 2021.

RIPARI, C. Dados são ainda mais valiosos que o petróleo. **CIO**, 2019. Disponível em: https://cio.com.br/gestao/dados-sao-ainda-mais-valiosos-que-o-petroleo/ Acesso em: 25 de Julho de 2022

SCHUMPETER, J. **Capitalismo, socialismo e democracia**. Rio de Janeiro: Editora Fundo de Cultura, 1961.

SUSEP. SES – SISTEMA DE ESTATÍSTICA DA SUSEP. **SUPEP**, 2022. Disponível em: http://www2.susep.gov.br/menuestatistica/SES/premiosesinistros.aspx?id=54 Acesso em: 25 de julho de 2022

SYHUNT. O MEGAVAZAMENTO DO BRASIL. **Syhunt**, 2021. Disponível em: https://www.syhunt.com/pt/index.php?n=Articles.BrazilDataLeak2021 Acesso em: 17 de Julho de 2022.