SEGURANÇA DA INFORMAÇÃO: sua importância dentro das organizações.

Fernando Cristaldo dos Santos[1]
Matheus De Araujo De Sampaio[2]
Patrick Lucio Silverio[3]
Orientador: Luiz Fernando Corcini[4]

RESUMO: Esta investigação tem como finalidade apresentar a necessidade de cuidados dentro da segurança da informação, um fator essencial para a proteção da informação, estando presente não apenas em ambientes organizacionais, mas também em ambientes pessoais. Os temas abaixo são divididos em tópicos importantes para entender o que é segurança da informação e porque a sociedade é obrigada a compreender sua relevância e seus métodos. Sendo de extrema importância para a sociedade atual por conta que a tecnologia está evoluindo cada vez mais, tanto para o bem quanto para o mal, com isso é necessário manter seus arquivos e sistemas protegidos, sem se preocupar com invasões, ataques e até mesmo falhas.

Palavras-chaves: Informação; cibercrimes; segurança da informação; vulnerabilidades.

ABSTRACT: This investigation aims to present the need for care within information security, an essential factor for the protection of information, being present not only in organizational environments, but also in personal environments. The topics below are divided into important topics to understand what information security is and why society is obliged to understand its relevance and methods. Being extremely important for today's society because technology is evolving more and more, both for good and for bad, with this it is necessary to keep your files and systems protected, without worrying about invasions, attacks and even failures.

Keywords: Information; cybercrimes; security information; vulnerabilities.

1.INTRODUÇÃO

A segurança da informação passou a ser um tema relevante nas organizações e na rotina diária de seus respectivos usuários, deixando de ser apenas uma questão de tecnologia para se tornar essencial para os negócios.

As informações são bens importantes, que outrora eram guardadas em ambientes físicos e hoje estão em ambientes virtuais espalhados pelo mundo.

---

[1] Acadêmico do Curso de Tecnólogo em Gestão da Tecnologia da Informação da UniSantaCruz.
[2] Acadêmico do Curso de Tecnólogo em Gestão da Tecnologia da Informação da UniSantaCruz.
[3] Acadêmico do Curso de Tecnólogo em Gestão da Tecnologia da Informação da UniSantaCruz.
[4] Orientador: Professor Luiz Fernando Corcini - Graduado em Engenharia Eletrônica, Especialização em Gestão da Tecnologia da Informação e da Comunicação, Mestrado em Novas Mídias aplicada à Educação.

Falhas em sua proteção podem gerar muitas consequências como perdas financeiras e até mesmo processos judiciais.

O intuito dos investigadores que empreenderam este estudo foi entender se a segurança da informação é relevante para as organizações, demonstrando a importância das informações geradas através do grande volume de dados e como elas podem ser gerenciadas. Constatar como a segurança da informação apoia as empresas através de métodos e boas práticas para evitar ataques ou reduzir os prejuízos e, bem como, as ameaças e vulnerabilidades que possam existir dentro dos sistemas de informação de uma empresa.

2. DESENVOLVIMENTO

2.1. INFORMAÇÃO

O conceito de informação é abordado por autores como Machlup e Mansfield (1983), citado por Costa e Cruz (2019, p. 2) como um meio necessário para a extração e construção do conhecimento, bem como Rodrigues et al. (2021) afirma que informação consiste em qualquer conteúdo que serve a algum propósito e que é de utilidade do ser humano. Agregando a essas ideias Miranda (1999) citado por Calazans e Toffano (2006) reitera que a informação é composta de dados relevantes organizados de forma significativa para subsidiar a tomada de decisão.

Autores pesquisados salientam que a informação é obtida por meio da coleta e do entendimento dos dados, entretanto, é de se referir que os dados são apenas registros de um acontecimento ou transação que por si só não tem valor. Deste modo, para que os mesmos gerem informação precisam ser classificados e relacionados entre si. Chiavenato (2008), citado por Cunha e Fenato (2013) corrobora essa ideia e destaca que os dados exigem processamento (classificação, armazenamento e relacionamento), para que possam ganhar significado[5] e consequentemente informar.

Neste sentido, a gestão da informação (GI) é um recurso vital para que as informações sejam confiáveis e que possam ser acessadas facilmente por quem

[5] Significado: no contexto de Segurança da Informação o significado da informação refere-se a sua relevância para a organização e pode ser empregada nas estratégias para alcançar seus objetivos.

precisa, reduzindo os riscos, melhorando a comunicação e fornecendo um resultado ideal nas decisões de negócio. Dias e Belluzzo (2003) citado por Baptista (2017) caracteriza a GI como um conjunto de princípios, métodos e técnicas utilizados na prática administrativa colocada em execução pela liderança para atingir a missão e os objetivos.

Segundo Davenport e Prusak (1998) citado por Dutra (2020, p. 33) considera-se a gestão estratégica da informação como sendo um conjunto estruturado de atividades que incluem o modo como as empresas obtêm, distribuem e usam a informação. Para este propósito, os autores propõem o seguinte modelo apresentado na tabela 1, abaixo:

Tabela 1 - Passos para o gerenciamento da informação

Passo 1	Determinação das exigências	Identificar como os gerentes percebem os ambientes informacionais e como compreendem qual tipo de informação um administrador realmente necessita.
Passo 2	Obtenção	Atividade que deve incorporar um sistema de aquisição contínua, que de forma geral, consiste em duas atividades:(1) Classificação e formatação; (2) estruturação das informações.
Passo 3	Distribuição	Refere-se às formas de comunicação e divulgação utilizadas.
Passo 4	Uso da informação	Diz respeito a utilização da informação disponibilizada. Está ligada à maneira como se procura, absorve e dirige a informação antes da tomada de decisão.

Fonte: Davenport & Prusak apud Dutra - Adaptado pelos autores.

Como pode-se perceber pela tabela acima, os autores consideram quatro passos para o gerenciamento das informações, quais sejam: (1) determinar as exigências da informação, a qual constitui-se em definir quais são as informações realmente necessárias; (2) a obtenção da informação precisa ser contínua e consiste

em algumas atividades dentro do processo; (3) a distribuição da informação, a qual consiste em identificar quais serão os canais de divulgação adequados para cada tipo de informação e (4) o uso da informação, o qual diz respeito a boas práticas para a sua utilização. Pode verificar-se que o objetivo final é permitir ao gestor agregar valor à informação com o intuito de auxiliar na tomada de decisão.

Corroborando a ideia, Beuren (1998), citado por Fernandes e Torrens (2020, p.6), destacam que “para assegurar o valor da informação, na fase de execução dos planos organizacionais, precisa haver um processo coordenado de todas as etapas do gerenciamento da informação.” O autor apresenta as seguintes etapas para o processo:

Tabela 2 - Etapas para gerir informações

Etapa 1	Identificação	Levantamento de fontes que permitirão gerar informação estratégica.
Etapa 2	Coleta/entrada de informação	Identificação e compreensão das informações necessárias para posterior extração/coleta da informação.
Etapa 3	Classificação e armazenamento	Tem como alvo o usuário e objetiva a seleção da informação útil a ele.
Etapa 4	Tratamento e apresentação	Trata da disponibilização da informação em um único sistema.
Etapa 5	Desenvolvimento de produtos e serviços	É uma tarefa essencialmente humana que objetiva produzir serviços e produtos de informação.
Etapa 6	Distribuição/disse-minação	Desenvolvimento de interface para estabelecer a ligação entre os usuários e os responsáveis pela distribuição e disseminação da informação.

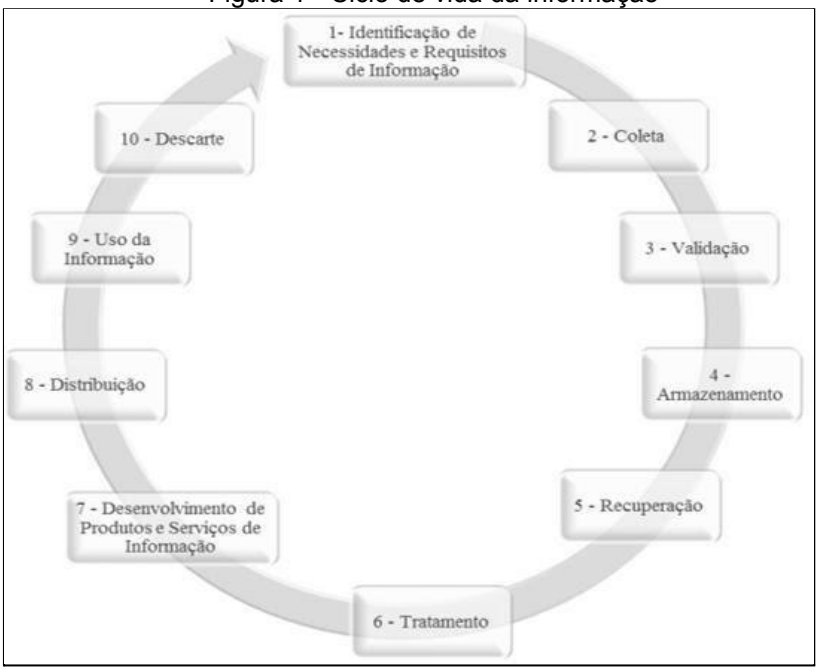
Fonte: Bauren (1998) apud Fernandos e Torrens (2020) - Adaptado pelos autores

Na tabela acima, os autores acrescentam duas etapas no processo de gerenciamento da informação criado por Davenport e Prusak (tabela 1): a identificação (etapa 1) onde torna-se necessário fazer um levantamento das fontes

para gerar informações estratégicas[6] que serão usadas e o desenvolvimento de produtos e serviços (etapa 5) que está inerente à atividade humana.

Moreira (2016) amplia a visão e apresenta uma proposta de gestão da informação orientada ao ciclo de vida da informação conforme apresentado abaixo, na figura 1:

Figura 1 - Ciclo de vida da informação



Fonte: Moreira (2016, p.121)

Como pode ser verificado na figura acima, além das etapas já abordadas pelos autores Davenport & Prusak (tabela 1) e Beuren (tabela 2), a autora apresenta mais três etapas para o processo de gerenciamento da informação.

- A VALIDAÇÃO (etapa 3): responsável por autenticar se as informações coletadas são válidas para a organização.
- A RECUPERAÇÃO (etapa 5): cujo objetivo é garantir que as informações, após serem armazenadas, possam ser resgatadas a qualquer momento.
- O DESCARTE (etapa 10): que deve ser realizada de maneira correta, principalmente com as chamadas informações digitais, pois existem diversas técnicas para recuperação de dados apagados.

No contexto da etapa 10 (descarte) relativamente ao ciclo de vida da informação, destaca-se o aspecto “segurança” e suas respectivas normas ou boas práticas. Neste sentido, para que as informações dentro de uma empresa não sejam

[6]Estratégicas: Informação estratégica é toda a informação que permite às organizações ter uma melhor performance e que contribui para o comprimento dos objetivos da organização.

acessadas por pessoas não autorizadas, a NBR ISO/IEC 27002:2013[7] adverte que “para impedir modificações ou exposição não autorizada é necessário classificar as informações considerando o seu valor, requisitos legais, sensibilidade e criticidade”. Para um maior detalhamento e entendimento a ABNT, com base na NBR indicada acima, indica um esquema de classificação em quatro níveis, como apresentado na tabela 3, abaixo:

Tabela 3 - Níveis da classificação da informação

Nível 1	Pública	Quando sua divulgação não causa nenhum dano.
Nível 2	Interna	Quando a divulgação causa constrangimento menor ou inconveniência operacional menor.
Nível 3	Restrita	Quando a divulgação tem um impacto significativo nas operações ou objetivos táticos.
Nível 4	Confidencial	Quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

Fonte: NBR ISO/IEC 27002:2013 - Adaptado pelos autores

Como visto na tabela acima, o primeiro nível de classificação é a informação pública, que, apesar de não precisar de nenhum tipo de segurança quanto ao seu sigilo, é aconselhável que o usuário não tenha acesso a ela, a menos que seja necessário para a rotina de seu trabalho. No segundo nível, a informação interna mesmo que seja vazada [8]não causa grande prejuízo à organização. A informação restrita está no terceiro nível e deve estar à disposição apenas para um grupo de pessoas selecionadas. No último nível, destaca-se a informação confidencial, as quais precisam de maior proteção, pois podem causar danos financeiros e a imagem da empresa.

[7] NBR ISO/IEC 27002:2013: Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização. Disponível em: ABNT Catálogo

[8] Vazada: No contexto de Segurança da informação, informações vazadas são informações restritas ou confidenciais que são acessadas por uma pessoa não autorizada e disponibilizadas para outras. Disponível em: www.blog.idwall.com

É importante destacar, ainda, que a classificação da informação deve ocorrer antes que seja acessada e manipulada por terceiros e que compete ao proprietário da informação classificá-la adequadamente.

Nesse sentido, autores como Santos e Soares (2019) apontam que “cabe ao proprietário da informação realizar a liberação do tipo de acesso que cada funcionário poderá ter, sendo necessária uma autorização direta ou designada”. Os mesmos autores destacam ainda a importância de que essa classificação seja sempre atualizada de modo a evitar gastos com controles desnecessários ou mesmo expor informações que podem colocar em risco o objetivo do negócio.

Neste contexto, é importante destacar que depois de certo período de tempo algumas informações, outrora classificadas como críticas, podem se tornar públicas, pois já não terão valor e caso sejam divulgadas e não causarão danos.

2.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um conjunto de ações que juntas asseguram a conservação[9], a integridade[10] e a confidencialidade[11] da informação. Segundo Dhillon (2004) citado por Pimenta & Quaresma (2016) foi constatado que a definição da segurança dentro da informação organizacional tem relevância para a empresa e engloba algumas características, quais sejam: responsabilidade, honestidade das pessoas, confiança e ética.

A corroborar a ideia, Dantas (2011), citado por Coutinho et al. (2017, p. 6), salienta que além das características apresentadas acima, a informação também deve possuir disponibilidade[12] como um de seus principais requisitos. Os autores ainda apontam que tais requisitos compõem os princípios da segurança da informação.

Conforme Galegale et al (2017) empresas que possuem uma área específica em segurança da informação (SI) demonstram uma melhor compreensão da importância da proteção de seus dados e informações. As mesmas apontam que

---

[9] Conservação: No contexto de SI, a conservação é a preservação de algo contra um dano ou uma perda.

[10] Integridade: No contexto de SI, a Integridade da Informação pode ser entendida como a informação que se mantém de forma original, não sofrendo alterações..

[11] Confidencialidade: Informação que não pode ser divulgada para indivíduos que não façam parte da organização ou contrato.

[12] Disponibilidade: Garantir acessibilidade à informação sempre que for necessário.

existem fatores internos que podem comprometer esta segurança, como por exemplo o comportamento inadequado de seus colaboradores, que podem divulgar informações, características sobre o ambiente e a infraestrutura em que está armazenada de forma intencional ou não. Para Klug (2019, p. 7) os melhores recursos de segurança não garantem total proteção pois um usuário que, com ou sem intenção, use um dispositivo infectado pode comprometer toda a infraestrutura da organização.

Conforme também apresentado pelos autores estudados existem inúmeras formas de uma organização ser prejudicada em níveis estratégicos ou financeiros. Isto se dá geralmente em decorrência de vulnerabilidades e ameaças.

É relatado por Posthumus e Von Solms (2004) e citado por Costa & Cruz (2016, p. 3) que tais vulnerabilidades e ameaças podem prejudicar as organizações, fato que deve ser evitado ao máximo.

Nesse contexto, as pequenas e médias empresas (PMEs) podem ter maior controle sobre seus dados, verificando e adotando metodologias (e/ou melhores práticas) tais como o Data Loss Prevention (DLP[13]). Estas soluções são utilizadas no processo de monitoramento de ocorrências que podem ocasionar a divulgação indevida das informações. De forma geral, são produtos focados na prevenção e correção de vulnerabilidades quando diagnosticadas. Soluções de segurança, como UTM, soluções endpoint (antivírus) e anti-spams, podem contar com recurso do DLP – justamente para prevenir o vazamento de dados. Para Roebuck (2011) citado por Augusto & Silva (2015) o termo refere-se a sistemas que identificam, monitoram e protegem os dados para evitar transmissão não autorizada.

Outra ferramenta importante, para evitar os ataques, é o *firewall* que usa regras de segurança para evitar que pacotes de dados que não estejam em conformidade com as regras causem dano ao sistema interno da organização. A Cisco[14] define o firewall da seguinte forma:

> Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança

[13] Data Loss Prevention (DLP) - Em sua tradução para português significa prevenção a perda de dados. Fonte:www.flowti.com.br/

[14] Disponivel em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html

Essa ferramenta é muito utilizada para a verificação simultânea de alguma invasão ou perda acidental de informações, fazendo o monitoramento e gerando relatórios para gestores[15] analisarem como está o nível de segurança dentro da organização.

Segundo Da Cruz (2020, p. 6) o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) implementou uma infraestrutura de segurança cibernética, para combater a proliferação de códigos maliciosos[16] e ajudar na detecção antecipada. Esta iniciativa constatou que o monitoramento permanente dos sistemas eletrônicos é eficaz para prevenir possíveis ataques.

Como já citado, os gestores utilizam as informações para a tomada das decisões. Isso significa que ela possui uma importância estratégica para as organizações, porém essa informação às vezes é alvo de cibercriminosos[17], fazendo com que a empresa tenha prejuízos.

Considerando todas as vulnerabilidades identificadas, instituições governamentais e não governamentais passaram a prescrever normas de melhores práticas no intuito de evitar ou minimizar os danos causados pelos ataques cibernéticos. Atualmente existem inúmeras normativas conhecidas como "ISO" (Organização Internacional de Normalização) a qual têm como função principal garantir e auxiliar na organização e otimização dos processos da empresa e sua respectiva qualidade ao cliente interno e/ou externo. Como exemplo, pode-se citar a ABNT NBR ISO/IEC:27002 (2013) a qual destaca:

> A segurança da informação é obtida pela instalação de grupo de controles, contendo políticas, processos, procedimentos, uma cultura organizacional e de algumas funções de softwares e hardwares.

A política de segurança da informação deve conter declarações sobre o comprometimento da direção da organização, responsabilidades gerais e específicas, conscientização, gerenciamento de riscos, objetivos de controle e controles e consequências da violação da política (ABNT, 2005).

---

[15] Gestor é a pessoa que está responsável por planejar o trabalho da empresa através de um grupo de indivíduos , monitorando e tomando decisões para o sucesso da mesma.

[16] Código malicioso: código malicioso em SI é um conjunto de palavras e símbolos que formam um código, o mesmo tem como objetivo deixar o sistema vulnerável a ataques.
Disponível em: www.kaspersky.com.br

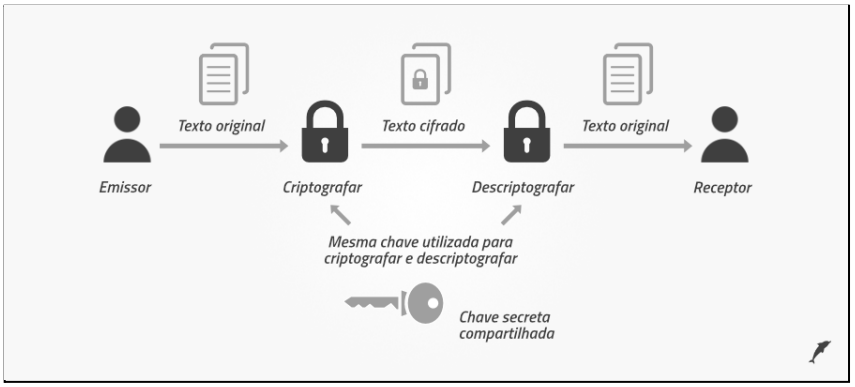
[17] Cibercriminoso: Pessoa que recorre a sistemas eletrônicos e/ou tecnologias da informação para cometer crimes.

Como se pode identificar pelos estudos realizados para este trabalho, a espionagem das informações pode se dar através de um simples clique em um link. A prática cotidiana inadequada realizada na utilização de sistemas de informação e/ou aplicativos próprios ou de terceiros, relatada pelos autores estudados, demonstra que o ato de clicar e ser redirecionado a um site pode causar danos sérios ao indivíduo ou à empresa em que trabalha. Estes danos incluem: senhas de cartões de créditos, documentos pessoais, endereço de e-mail/residencial, número de telefone, saldo bancário, entre outros.

Para evitar este tipo de ataque existe a “criptografia”, uma ferramenta voltada à segurança de um determinado conjunto de dados (como um cadeado que só se abre com uma chave específica). Ela serve para impedir a exposição do arquivo que está sendo enviado. Dentre os tipos de criptografia, as mais utilizadas de acordo com o site Cryptoid[18] são:

- Simétrica: na qual é utilizada uma única chave, esta é compartilhada somente entre o emissor e receptor do conteúdo, caso ela seja comprometida pode se trocar por uma nova, mantendo assim o algoritmo inicial da criação da mesma (Figura 2).
- Assimétrica: é baseada em dois tipos de chave: uma privada que é usada para decifrar mensagens e a outra é a pública que se utiliza para cifrar um conteúdo (Figura 3).

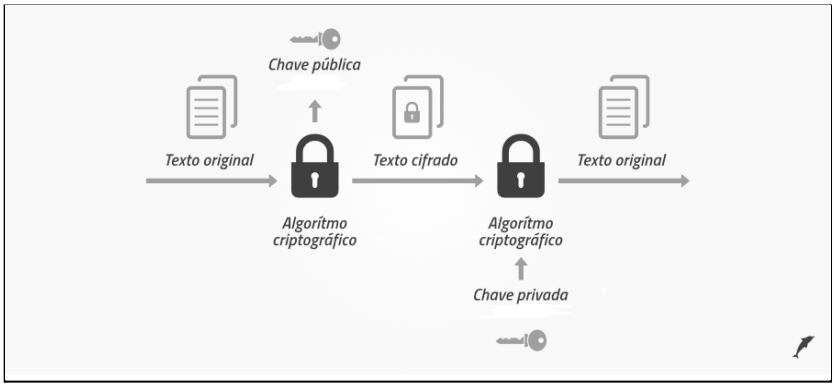
Figura 2 - Algoritmo de chave simétrica



Fonte: Cryptoid (2019).

[18] Disponível em: https://cryptoid.com.br/banco-de-noticias/29196criptografia-simetrica-e-assimetrica/

Figura 3 - Algoritmo de chaves assimétricas



Fonte: Cryptoid (2019).

Araújo (2014) citado por Bitencourt (2018, p. 36) explica que, em ambos os casos, para ocorrer a autenticação é necessário uma verificação do que se é apresentado, com isso irá definir sua autenticidade ou a falta dela. A validação da identidade é baseada nos endereços de IPs, senhas e certificados digitais.

Do que foi apresentado, pode-se identificar que é necessário ter cuidado com o local onde serão salvos os seus dados. É de se referir que não existe solução perfeita, pois mesmo com um treinamento adequado e recursos destinados especificamente a sistemas de proteção, podem ocorrer problemas como: perdas de arquivos, interrupções de suas atividades, bugs[19], uso indevido e invasão por hackers.

2.3 VULNERABILIDADES

Além dos temas já abordados nesta pesquisa, destaca-se aqui outro tópico de grande importância considerado pelos autores pesquisados, a saber: as vulnerabilidades em SI.

Este termo pode ser definido, segundo autores consultados, como não apenas as ameaças já existentes, causadas por brechas[20] de sistemas ou falhas operacionais de usuários, mas também as que ainda não foram descobertas e podem, futuramente, ocasionar risco.

[19]Bugs: São erros imprevisíveis que acarretam no mal funcionamento de alguma tecnologia específica.Disponivel em: https://canaltech.com.br/

[20] Brechas: em SI, pode ser definido como espaços e/ou lacunas, que dão oportunidades para algo/alguém adentrar no sistema. Disponível em: https://www.interop.com.br/blog/principais-brechas-de-seguranca-da-informacao/

Segundo Computer World[21](2021) os ataques cibernéticos aumentaram exponencialmente em 2020, tendo números maiores do que todos os últimos 15 anos juntos, esses ataques visam roubar, expor e/ou alterar informações. Da Silva (2018) afirma “tratar-se de tentativas maliciosas[22] premeditadas de ataques para quebrar a confidencialidade, integridade ou disponibilidade de informações existentes em computadores ou redes computacionais”.

Os atacantes cibernéticos usam malwares[23] para atingir seus propósitos. De acordo com os sites Lumiun Blog[24](2020) e Canaltech[25] esses são alguns exemplos desses softwares e tipos de ataques:

Tabela 4 - Malwares e modos de ataques

Nome	Descrição
Trojan	Também conhecido como Cavalo de Troia, é o termo usado para malwares que fingem ser autênticos ou vêm incorporados a um, deixando a entrada livre para outros malwares.
Adwares	Enviam uma quantidade significativa de anúncios para as suas vítimas , os quais proporcionam brechas na segurança para outros malwares invadirem.
Worms	Propagam por redes inteiras, passando de um dispositivo para outro através de e-mails, compartilhamento de arquivos, serviços de internet entre outros.
Spywares	Softwares que espionam os usuários para coletar dados pessoais e padrões de comportamento.

[21]Disponível em: https://computerworld.com.br/seguranca/ataques-ciberneticos-em-2020-sao-maiores-do-que-nos-ultimos-15-anos-combinados

[22]Tentativas Maliciosas: termo utilizado para demonstrar uma ação feita por um cibercriminoso que busca acessar suas informações.

[23] Malwares: programas desenvolvidos para infectar computadores e sistemas. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

[24] Disponível em: https://www.lumiun.com/blog/8-tipos-de-ataques-ciberneticos-e-como-se-proteger/

[25] Disponível em: https://canaltech.com.br/seguranca/O-que-e-virus-cavalo-de-troia-spyware-etc/

DDos Attack	Denial-of-service attack (Ataque de negação de serviço): estimula o servidor a lotar suas atividades, induzindo-o para uma lentidão em seu sistema e assim, travando boa parte dos acessos.
Port Scan	Busca “portas destrancadas[26]”, enviando mensagens para cada porta de acesso para identificar brechas, e então, rouba os dados e obtém informações da rede e dos usuários que a utilizam. Por mais que seja um método de ataque, também é utilizado para testar a rede quanto a possíveis ataques.
Phishing	Na tradução literária “pescando”, o ataque é feito da seguinte forma: o usuário acessa uma página semelhante a real, e tenta adentrar em sua conta, informando seu login que possivelmente possa ser um e-mail, conta bancária, cpf, entre outros, e então o atacante “fisga” (captura) essas informações e a utiliza
Ataque de força Bruta	Software que realiza a criação de diversas combinações de possíveis senhas, utilizando, por exemplo, todas as palavras do dicionário. Após conseguir o acesso e as informações necessárias. Depois de obter o acesso do usuário, ele envia mensagens e/ou e-mails para outros remetentes inserindo links de páginas Phishing, conseguindo novas capturas, e também solicitando dinheiro a eles.
Crypto Jacking	Esse crime virtual acessa algum dispositivo e utiliza para fazer mineração de criptomoedas, vale ressaltar que é necessário que esse dispositivo esteja com uma conexão ativa com à internet.

[26] Portas Destrancadas: pontos de acessos por onde a informação transita entre dispositivos e redes. Podem ter brechas para a entrada de vírus.

ZeroDay	Esse ataque é realizado normalmente quando se tem atualizações ou lançamento de softwares.Busca métodos de aberturas do sistema, ou até mesmo bugs.

Fontes: Lumiun(2020) e Canaltech - Adaptado pelos autores.

Além das ameaças apresentadas na tabela acima, a referência pesquisada destaca também o malware conhecido como “ransomware”. Esse malware invade o sistema bloqueando o usuário de utilizar e acessar sua máquina ou arquivos do servidor, e então, a vítima só consegue retomar suas atividades quando pagar pelo resgate, por isso o nome de “ransom” (resgate).

Segundo Manky (2018) citado por Santos & Soares (2019, p. 48) há uma padrão nesses ataques de Ransomware, onde sistemas cuja vulnerabilidade já havia sido identificada, mas não corrigida, são infectados, facilitando essa invasão.

Acrescenta-se ao rol de vulnerabilidades, a chamada “Engenharia Social”. Cruz (2017, p. 34) define este termo da seguinte maneira: quando o criminoso faz contato com um usuário da empresa e o persuade, sem ele perceber, e consegue informações secretas que não poderiam ser vazadas ou repassadas para terceiros. Além disso, Costa e Cruz (2016, p.10) apontam que esse termo (Engenharia) não deriva de qualquer curso de graduação, mas sim das especialidades deste indivíduo, que demonstram a sua inteligência em diversos aspectos, e a utiliza para obter esses dados. Entretanto, os mesmos autores mostram que esta não é a única forma de se utilizar este método. Existe também outra técnica, a qual é conhecida como “Engenharia Social Inversa”, onde o hacker cria identidade falsa, outra personalidade e até mesmo começa a trabalhar em determinada empresa, de maneira a passar confiança para os demais colegas (vítimas) e assim conseguir informações cruciais. Verificou-se que, antes de ele criar essa identidade, há todo um estudo, onde características sobre a vida de usuários são levantadas, para não ocorrer falhas de abordagem e não levantar desconfianças.

Segundo o site IT Fácil[27] essas diversas vulnerabilidades prejudicam a empresa como um todo. Os dados vazados de uma determinada empresa ou dados pessoais de funcionários/clientes, com as principais informações (endereço de e-mail, CPF, endereço residencial, número de cartão) podem ser vendidas ou

[27] Disponível em: https://www.itfacil.com.br/5-problemas-graves-gerados-ataques-ciberneticos.

publicadas gratuitamente. Além da empresa ter o nome exposto em diversos lugares pelo ocorrido, perdendo sua credibilidade, ela pode sofrer processos judiciais e multas por tais acontecimentos de liberação de informação.

3. METODOLOGIA

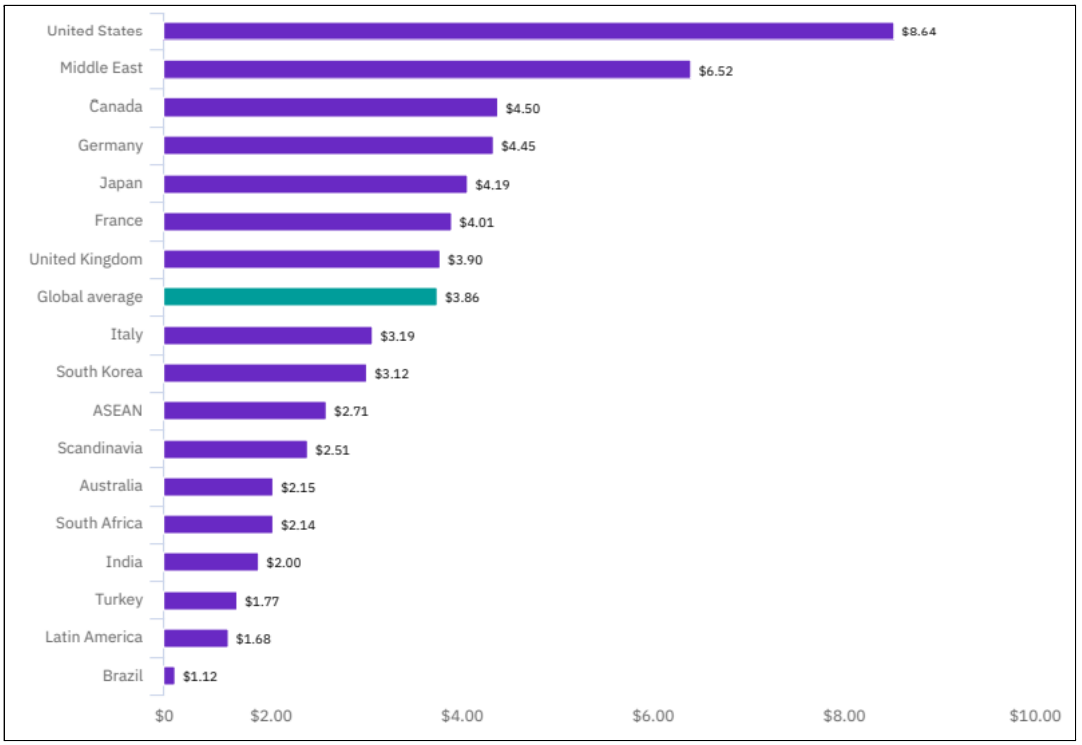
Com base no método da pesquisa pode-se ter um conhecimento amplo sobre o tema relatado. Foram utilizados meios confiáveis na pesquisa, artigos, livros, teses e sites empresariais que contam com as informações detalhadas sobre produtos e serviços que estão presentes dentro da segurança da informação. Com base na questão qualitativa a abordagem focou no embasamento teórico sobre os dados apresentados. Este estudo caracteriza-se como uma pesquisa bibliográfica com abordagem qualitativa, onde a pesquisa para o embasamento teórico contou com dados necessários para todos os fatos apresentados.

4. RESULTADOS

A IBM[28] realizou um estudo com mais de 500 empresas pelo mundo sobre as violações de dados. Foi constatado que as credenciais de funcionários e nuvens mal configuradas são o principal meio de ataque. O relatório (Cost of a Data Breach Report 2020) mostra uma redução de 1,5% nos custos em relação a 2019, mas ainda um aumento de 10% nos últimos cinco anos. Embora o custo médio de uma violação seja relativamente inalterado, a IBM diz que os custos estão ficando menores para empresas preparadas e muito maiores para aquelas que não tomam quaisquer precauções.

Gráfico 1 - Custo médio de uma violação de dados por país

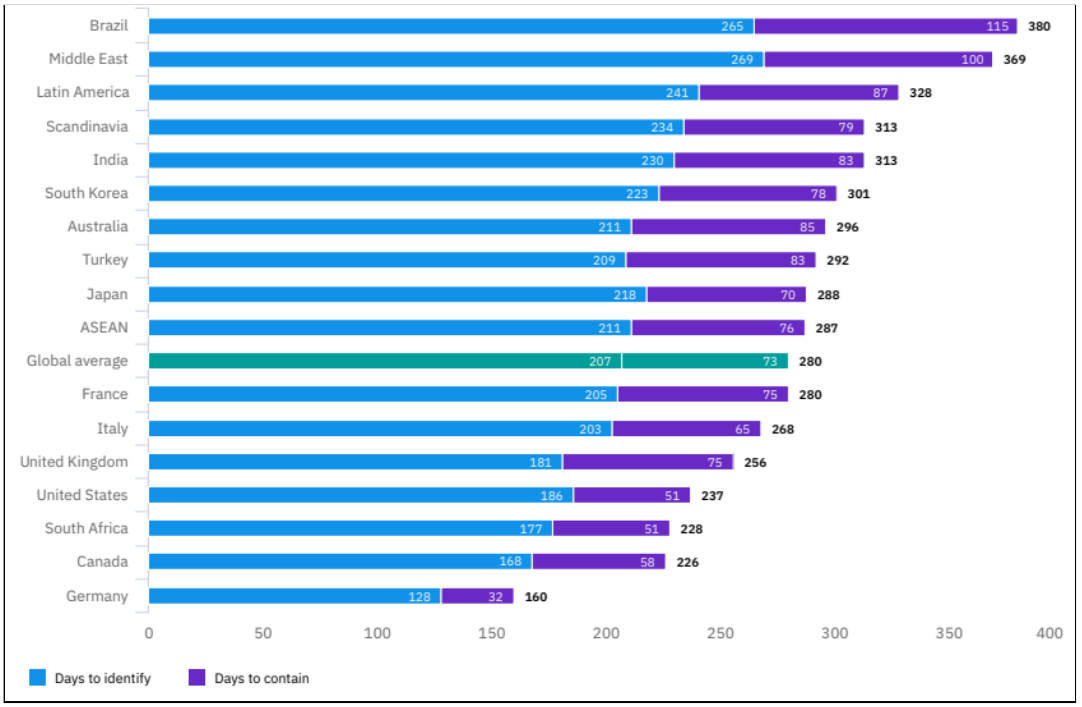
[28] IBM: A International Business Machines Corporation é uma empresa dos Estados Unidos voltada para a área de informática.



Fonte: Cost of a Data Breach Report 2020. IBM Security

O gráfico acima demonstra o custo médio de uma violação de dados por país. Os Estados Unidos, apesar de ter grande influência sobre as tecnologias de segurança digital, lidera o ranking dos países que têm o maior impacto financeiro decorrente das violações de dados, US$ 8,64 milhões (Gráfico 1).

Gráfico 2 - Tempo médio para identificar e conter uma violação por país



Fonte: Cost of a Data Breach Report 2020. IBM Security

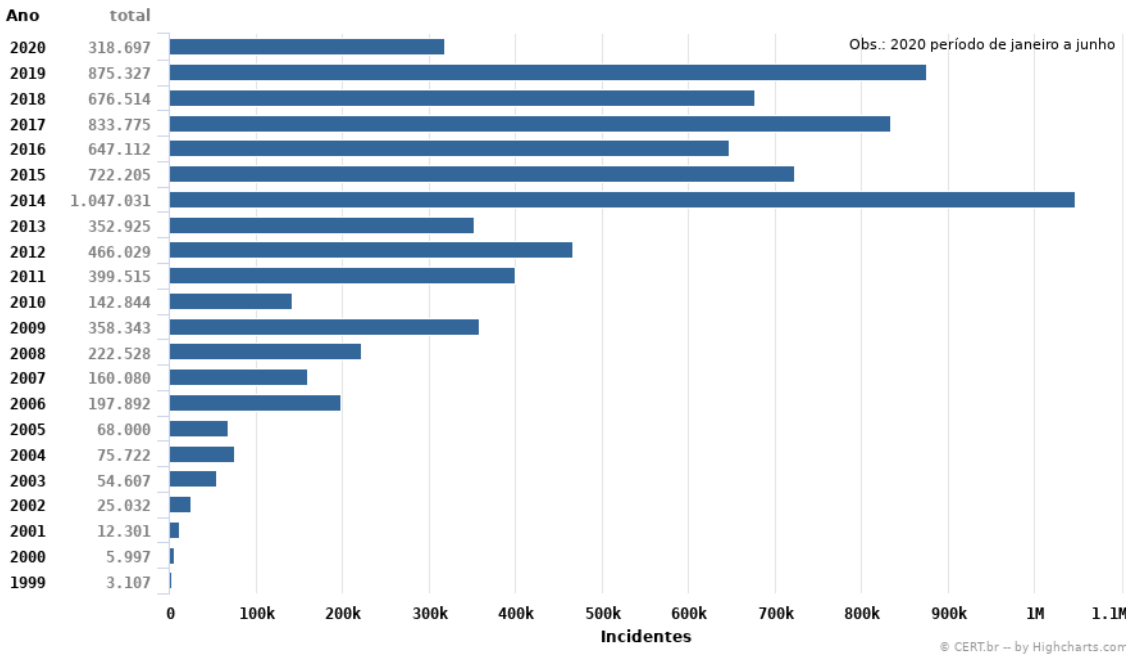
Embora o Brasil tenha o custo médio de US$ 1,2 milhões, o menor da lista, em danos com ataques, leva em média 265 dias para identificar uma violação e 115 dias, após a identificação, para retê-la (Gráfico 2). Foi identificado também que países com sistemas de automação da segurança implantados, tais como, inteligência artificial, machine learning e análise de dados conseguiram tempo de resposta significativamente mais curto.

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br[29]), os incidentes reportados em 2019 tiveram um aumento de 29,39% com relação ao ano anterior, só no primeiro semestre de 2020 foram reportados 318.697 incidentes (Gráfico 3).

Com base em uma análise dos incidentes reportados ao CERT.br, nota-se que a evolução da tecnologia no decorrer dos anos trouxe consigo um crescimento nos incidentes relacionados à segurança da informação.

[29] Disponivel em: https://www.cert.br/

Gráfico 3 - Incidentes reportados



Fonte: CERT.br

5. CONSIDERAÇÕES FINAIS

A segurança da informação é sim relevante pois as ameaças e vulnerabilidades apresentadas oferecem grande risco para as organizações. Em virtude dos fatos mencionados, é perceptível que a segurança da informação seja necessária em ambientes domésticos, mas principalmente em organizações, pois elas têm um potencial para serem afetadas pelo roubo e o sequestro de informações.

O tema está ligado com a evolução da tecnologia e da sociedade atual, nela estão presentes dispositivos eletrônicos que estão conectados a vários servidores e redes wireless que emitem informações a todo momento. Com os dados levantados pode-se verificar que os riscos estão presentes em todos os lugares, nas organizações deve ser feito uma varredura no sistema periodicamente para encontrar inconsistências gerais, evitando possíveis riscos. É necessário ressaltar que as organizações criem uma política de segurança da informação, onde se tem diversas regras e métodos que são utilizadas para manter suas informações seguras, diminuindo riscos e também falhas.

Segurança da Informação é muito mais que ter um software antivírus instalado ou utilizar um firewall que impeça o ataque de agentes indevidos a sua rede corporativa. Segurança da Informação está relacionada a proteção de dados, a segurança física, a segurança ambiental, o alinhamento da Tecnologia da Informação com os objetivos e a missão da empresa, dentre outras funções essenciais para a continuidade dos negócios.

REFERÊNCIAS

AUGUSTO, G.; SILVA, M. A proteção contra o vazamento de dados e sua importância para as empresas privadas. **Revista Eletrônica e-F@tec**, Garças-SP, v. 6 n. 1, 2016. Disponível em: https://fatecgarca.edu.br/ojs/index.php/efatec/article/view/105. Acesso em: 22 fev. 21

BELLUZZO, R. **Bases teóricas de gestão da informação: das origens aos desafios na sociedade contemporânea**. Dossier: Gestión de la Información: Dilema Y Perspectiva. Provincia de Buenos Aires, Argentina, v. 7 n. 1, 2017 Disponível em: https://brapci.inf.br/index.php/res/v/65520. Acesso em: 07 mai.2021

CALAZANS, A. **Conceitos e uso da informação organizacional e informação estratégica Transinformação**, Pontifícia Universidade Católica de Campinas, vol. 18, n. 1,pp. 63-70 abril.2006 Disponível em: https://www.redalyc.org/articulo.oa?id=384334741006 Acesso em: 11 abr.2020

COSTA, L.;CRUZ, S. **A Engenharia Social e os desafios da Segurança da Informação nas Empresas**, Fundação de Ensino e Pesquisa do Sul de Minas, Varginha-MG, mai.2017. Disponivel em: http://repositorio.unis.edu.br/handle/prefix/431 Acesso em: 04 mar.2021

COUTINHO, M.; SANTOS, R.. Estudo de caso: Principais pilares da segurança da informação nas organizações. **Revista Gestão em Foco,** Registro-SP, Revista p.189-500, 2017. Disponível em: https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052 Acesso em: 16 mar.2021

CUNHA, D.; FENATO, A. **A segurança da informação e a sua importância para a auditoria de sistemas**. Revista Científica Semana Acadêmica, Fortaleza-CE, jul.2013. Disponivel em: https://semanaacademica.com.br/artigo/seguranca-da-informacao-e-sua-importancia-para-a uditoria-de-sistemas Acesso em: 08 abr.2021

DA CRUZ, J. **O futuro da segurança cibernética no Brasil: papéis e responsabilidades**, Brazilian Journal of Information Science: research trends, Registro-SP, 1ª Edição, 2020. Disponivel em: https://cdn.discordapp.com/attachments/757591361196130345/809774015426199632/CAM_QCO_2020_Cap_Jorge_da_Cruz.pdf Acesso em:18 fev.2021

SILVA, W. **Análise dos impactos de ataques cibernéticos.** Universidade de Brasília. Brasília-DF, nov.2018 Disponivel em: https://repositorio.unb.br/handle/10482/34838 Acesso em: 20 fev.2021

FERNANDES, C.; TORRENS, E. **O processo de gerenciamento da informação em uma Instituição de Ensino**. Associaçã Brasileira de Custos,São Leopoldo Do Sul-RS, 2020 Disponivem em: https://anaiscbc.emnuvens.com.br/anais/article/view/816 Acesso em: 29 abr.2021

GIFFONI, F. **Monitoramento e uso de informações sobre clientes e marcas em mídias e redes sociais digitais: Um estudo em empresas públicas.** Universidade Ferderal de Minas Gerais, 2020 Disponivel em: https://repositorio.ufmg.br/handle/1843/34091 Acesso em: 29 abr.2021

KLUG, M. **Segurança da Informação nas Empresas: Proteção da rede, dos Sistemas e Educação dos Usuários**. Universidade do Sul de Santa Catarina, Palhoça-SC, 2017. Disponivel em: https://www.riuni.unisul.br/handle/12345/9659 Aceso em: 18 fev.2021

PIMENTA, A., QUARESMA, R. A Segurança dos Sistemas de Informação e o Comportamento dos Usuários. **Revista de Gestão da Tecnologia e Sistemas de Informação**, Vol. 13, No. 3, pp. 533-552 Set/Dez., 2016 Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752016000300533 Acesso em: 18 mar.2021

RIZZOTO, F. **Governança de Segurança da Iinformação: Frameworks.de Gestão de Segurança da Informação em Empresas de Pequeno**
e Médio Porte, Universidade do Sul de Santa Catarina, Santa Catarina, 2018. Disponivel em: https://www.riuni.unisul.br/handle/12345/5691 Acesso em: 11 mar.2021

RODRIGUES, F.; TORRES, M.; FLORIAN, F. Segurança dos Sistemas de Informação, **Semana Acadêmica Revista Científica**, 123ª Ed. Universidade de Araraquara, Araraquara-SP, 2018 Disponivel em: https://semanaacademica.org.br/artigo/seguranca-dos-sistemas-de-informacao Acesso em: 26 mar.2021

SANTOS, E.; SOARES, T. Riscos, Ameaças e Vulnerabilidades: O impacto da segurança da informação nas organizações. **Revista tecnológica da FATEC Americana**, Vol 07, n 02, p. 43-51, abr/set.2019 Disponivel em: https://fatecbr.websiteseguro.com/revista/index.php/RTecFatecAM/article/view/188 Acesso em: 16 mar.2021