PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE EMPRESARIAL

INFORMATION SECURITY POLICIES IN THE BUSINESS ENVIRONMENT

Larissa Aparecida Teixeira[1], Mauro Aparecido Fracarolli Junior[2], Marcia Regina Reggiolli [3]

1- Discente na Faculdade de Tecnologia de Itapira “Ogari de Castro Pacheco”;; 2- Discente na Faculdade de Tecnologia de Itapira “Ogari de Castro Pacheco”;; 3- Doutora em Ciências (Instituto de pesquisa Energéticas e Nucleares – USP), Docente da Faculdade de Tecnologia de Itapira” Ogari de Castro Pacheco.

Contato: marcia.reggiolli@fatec.sp.gov.br

RESUMO

De acordo com pesquisas o número de ataques cibernéticos cresceu muito no primeiro semestre de 2022. Portanto a implementação de políticas de segurança da informação nas empresas tornou-se fundamental para a segurança dos dados. Com o avanço da tecnologia a maioria da população e do meio empresarial, não conhecem os riscos que a *internet* pode causar. Com a falta de conhecimentos das políticas de segurança as pessoas se tornam vulneráveis aos ataques. Este trabalho tem como objetivo geral analisar a gestão e gerenciamento das políticas de segurança em uma empresa. Nesse trabalho foi utilizado pesquisas bibliográficas, a fim de coletar dados teóricos sobre o tema. Também foi realizado pesquisa exploratória, para levantar dados na empresa. Além de um estudo de casos sobre o tema. Ao comparar as políticas seguidas pela empresa com as normas, podemos constatar que ela não se enquadra em vários quesitos, e por falta de treinamentos para seus funcionários e permitir que eles enviem qualquer informação que possa ser confidencial, a empresa está sujeita a uma série de riscos de segurança, como vírus, trojans e *spyware*. O trabalho atingiu seus objetivos, tendo como oportunidade identificar e viabilizar as adequações necessárias na área da segurança da informação para a empresa seguir seu negócio de forma segura e com risco minimizado para os ataques cibernéticos além de sugerir a implantação de uma política de segurança da informação.

Palavras-Chave: Cibersegurança. Políticas. Segurança. Informação.

ABSTRACT

According to research, the number of cyber attacks grew a lot in the first half of 2022. Therefore, the implementation of information security policies in companies has become fundamental for data security. With the advancement of technology, the majority of the population and the business environment are not aware of the risks that the internet can cause. With the lack of knowledge of security policies, people become vulnerable to attacks. The general objective of this work is to analyze the management of security policies in a company. In this work, bibliographic research was

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

used in order to collect theoretical data on the subject. Exploratory research was also carried out to collect data on the company. In addition to a case study on the subject. When comparing the policies followed by the company with the norms, we can see that it does not fit in several aspects, and due to the lack of training for its employees and allowing them to send any information that may be confidential, the company is subject to a series of security risks such as viruses, trojans and spyware. The work reached its objectives, having the opportunity to identify and make viable the adjustments necessary for the company to continue its business safely in addition to suggesting the implementation of an information security policy.

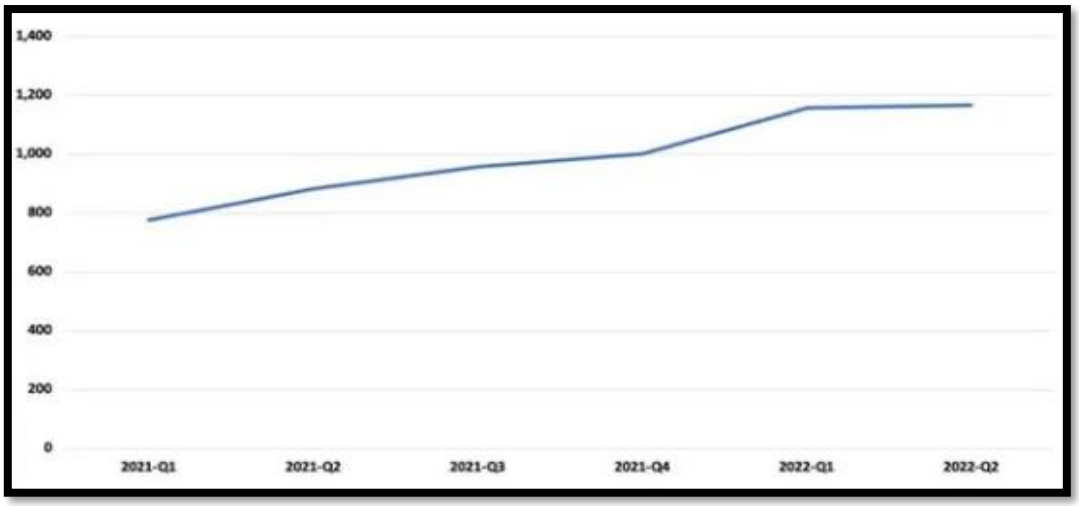
Keywords: Cybersecurity. Policies. Security. Information.

INTRODUÇÃO

Levantamento realizado por Ferreira (2022), membro de empresa multinacional de cibersegurança com sede no Japão, revelou que o Brasil está no *ranking* dos cinco países que mais sofrem ataques *ransomware*, ocupando a quarta posição.

De acordo com pesquisa realizada por Oliveira (2022), o Brasil registrou no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas. O número é 94% superior na comparação com o primeiro semestre do ano passado, quando foram 16,2 bilhões de registros. Sendo possível observar com maior detalhe esse aumento na figura 1.

Figura 1*: Average Weekly Attacks per Organization*



Fonte: *Canaltech* (2022)

Raposo (2019) enfatiza que a implementação de políticas de segurança da informação nas empresas que busquem reduzir as chances de perda de informações ou fraude é imprescindível.

O autor completa que a Política de Segurança da Informação (PSI) é um documento que deve conter um conjunto de métodos, normas e procedimentos relacionados à

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

segurança da informação na organização, a qual deve ser comunicada a todos os colaboradores, bem como analisada e revisada criticamente, em intervalos regulares ou mesmo quando mudanças se fizerem necessárias.

É o Sistema de Gestão de Segurança de Informação (SGSI) que vai garantir a viabilidade e uso dos dados apenas por pessoas autorizadas que realmente deles necessitem para o desempenho de suas funções dentro da empresa (SABINO, 2020).

Segundo Soares, Soares e Alves (2021), o desenvolvimento de um PSI deve ser baseado na NBR ISO/27001:2005, que é um código de prática padrão para gestão de segurança da informação. No qual deve conter as melhores práticas para iniciar, implementar, manter e melhorar o gerenciamento de segurança da informação em uma organização. Tendo-se por base a importância e a relevância do tema o presente trabalho tem como objetivo analisar a gestão e gerenciamento das políticas de segurança em uma empresa.do segmento de varejo localizada no interior do Estado de São Paulo.

Apesar do avanço tecnológico e do crescente uso da *internet*, a maioria da população não sabe dos riscos desse meio, principalmente no meio empresarial.

A abordagem deste tema tem por finalidade trazer ao leitor com detalhes a política de segurança da informação dentro de uma empresa, além das ameaças que permeiam pelo ambiente *Web*, proporcionando a ele a capacidade de verificar se dentro do ambiente empresarial no qual atua, as medidas para a segurança dos dados são efetivamente tomadas.

FUNDAMENTAÇÃO TEÓRICA

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO PARA AS EMPRESAS

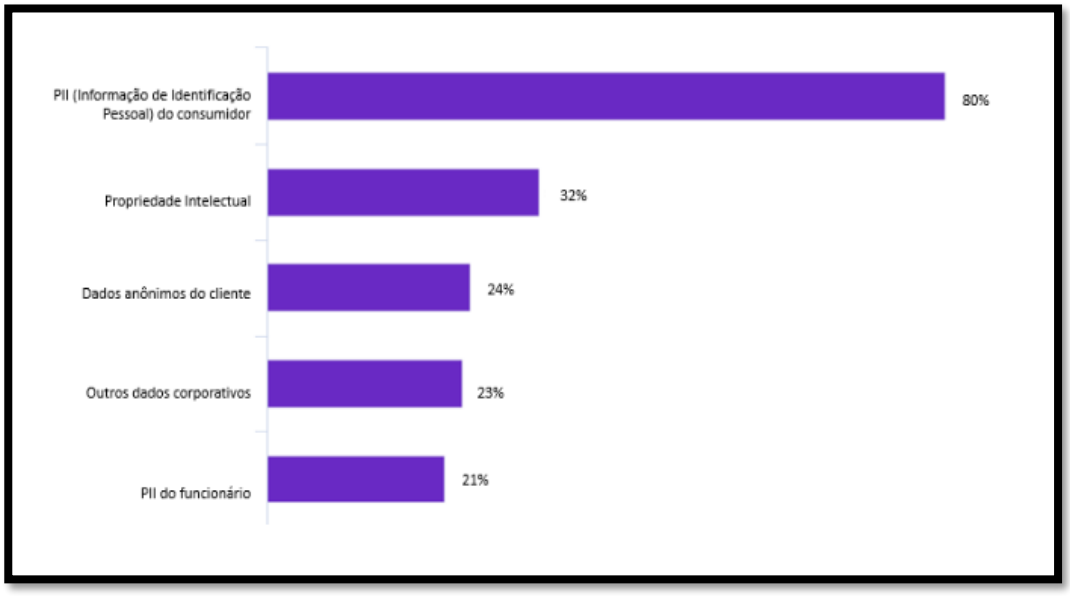
Segundo Ferreira (2022) um ataque cibernético pode causar danos incalculáveis a uma empresa, como prejuízos financeiros, prejuízos ao posicionamento da marca, perda de sigilo da informação e comprometimento do negócio.

Complementando essa ideia, Brown e Stallings (2013) relatam que os riscos envolvendo dados variam de organização para organização, dependendo do tipo de informação e da importância que ela tem para a própria empresa. Embora os números dos cartões de crédito e da previdência social sejam certamente perigosos, os planos da empresa, as finanças e as informações confidenciais dos funcionários também requerem cuidado. Abaixo seguem as figuras 2 e 3, onde se observa, respectivamente, os tipos de registros que são comprometidos após um ataque cibernético e as 4 principais categorias no vazamento de dados e seu respectivo prejuízo para a empresa (medido em milhões de dólares).

PROSPECTUS
ISSN 2674-8576

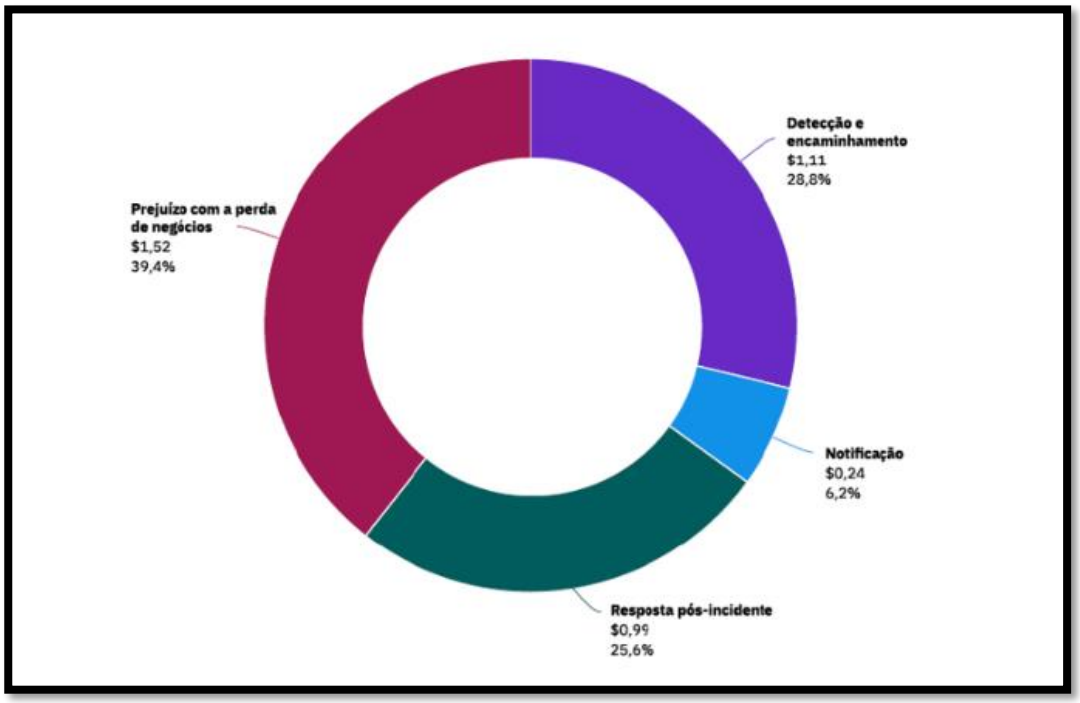
DOI: 10.5281/zenodo.10082438 *Artigo Original*

Figura 2. Tipos de registros comprometidos: porcentagem de vazamentos envolvendo dados em cada categoria.



Fonte: LinkedIn (2021)

Figura 3. Prejuízo total médio de um vazamento de dados dividido em quatro categorias.



Fonte: LinkedIn (2021)

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

CLASSIFICAÇÃO DAS INFORMAÇÕES

De acordo com Raposo (2019), a classificação das informações é essencial nesse processo e deve ocorrer pelo fato de as informações não possuírem o mesmo grau de confidencialidade, caso contrário às pessoas podem ter diferentes interpretações quanto ao nível de confidencialidade das informações.

Seguindo essa ideia, Hintzbergen (2018) exemplifica que para um simples funcionário de uma empresa, um relatório contendo suas demonstrações financeiras anuais pode não significar nada, mas para o pessoal financeiro e a alta administração é uma informação muito importante, que deve ser bem preservada.

Dessa forma, Sabino (2020) diz que para classificar a informação, é importante saber quais as consequências que terá para a sua organização se for divulgada, alterada ou apagada sem autorização. Somente por meio da interação com os responsáveis diretos pelas informações corporativas será possível estabelecer essas consequências e criar graus de classificação adequados.

RISCOS PARA AS EMPRESAS

No que diz respeito à segurança, os riscos são entendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento ocorrer e produzir perdas (HINTZBERGEN, 2018, s/p).

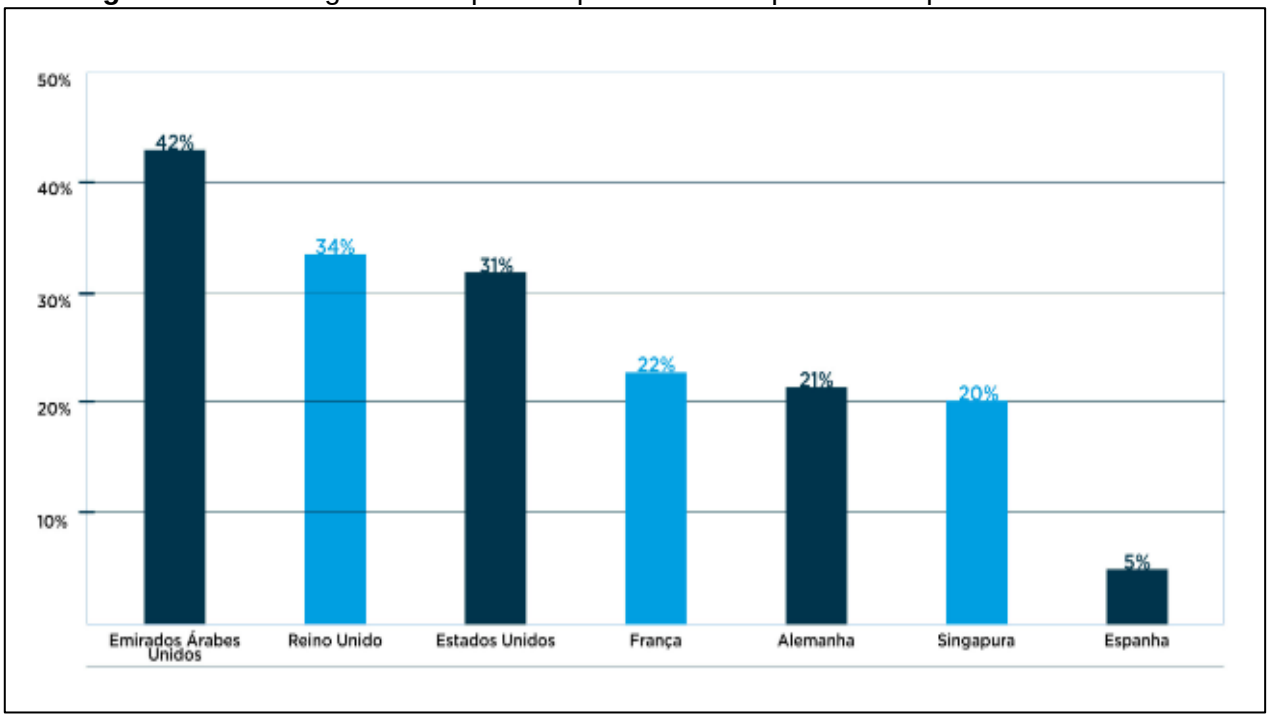
Caruso e Steffen (2013), listam vários riscos associados à segurança da informação. Isso inclui a possibilidade de que os dados possam ser comprometidos por ameaças de segurança, como *hackers*.

Segundo Sabino (2020), para evitar a possível perda de informações, que dependendo do seu grau de sigilo, podem levar a empresa à falência, é necessário desenvolver uma gestão de riscos, na qual os riscos são determinados e classificados, e então um conjunto equilibrado de medidas de segurança reduzirá ou eliminará os riscos aos quais a empresa está sujeita. Abaixo segue a figura 4, no qual demonstra a porcentagem de empresas que faliram por país, após um ataque cibernético.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

Figura 4. Porcentagem de empresas que fecharam após um ataque de *Ransomware*.



Fonte: Forbes (2021).

VULNERABILIDADES

Segundo Raposo (2019), as vulnerabilidades podem advir de vários aspectos, como estruturas físicas não protegidas contra enchentes, incêndios e desastres naturais; uso de material inadequado na construção; ausência de políticas de segurança para a área de Gestão de Pessoas da organização.

Complementando essa ideia, Sabino (2020) relata que as vulnerabilidades podem vir de funcionários não qualificados e locais de trabalho insatisfatórios; falta de procedimentos para controlar acesso e uso de equipamentos por pessoal contratado; equipamentos obsoletos, isentos de manutenção e sem constrangimentos de utilização; *software* sem *patches* de atualização e sem licença de operação, entre outros.

A NBR ISO/IEC 27002:2013 define vulnerabilidade como uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. São fragilidades presentes nos ativos, que podem ser exploradas, intencionalmente ou não, com consequente violação de um ou mais princípios de segurança de TI. Ao identificar vulnerabilidades ou pontos fracos, será possível mensurar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança adequadas para sua correção (SABINO, 2020, s/p).

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

AMEAÇAS

Segundo Soares, Soares e Alves (2021) a ameaça pode ser considerada um agente externo aos ativos de informação, pois explora suas vulnerabilidades para violar os princípios fundamentais da informação, confidencialidade, integridade ou disponibilidade.

Atualmente, o mundo dos negócios é muito competitivo, onde as empresas devem estar sempre atentas às ameaças aos negócios corporativos, que, se implementadas, podem causar grandes prejuízos, e consequentemente pôr fim às suas atividades para sempre (SABINO, 2020, s/p).

Por outro lado, Raposo (2019) diz que as ameaças também podem ser naturais, como aquelas originadas de fenômenos naturais; involuntárias, quando decorrem de ações sem a intenção de causar dano; e intencional, que são deliberados, cuja intenção é causar danos, como os *hackers.* Segue abaixo a figura 5, no qual pode-se observar os principais ataques que ocorreram no Brasil em 2021.

Figura 5. Retrospectiva com os principais ataques em 2021

Fonte: *Verhaw* (2022).

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Política de segurança pode ser definida como um documento que estabelece valores, princípios, requisitos, compromissos, responsabilidades e diretrizes sobre o que

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

precisa ser feito para atingir um padrão desejável de segurança da informação (RAPOSO, 2019, s/p).

Complementando essa ideia Hintzbergen (2018), diz que a política de segurança é essencialmente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados, sendo considerado o pilar de uma segurança da informação eficaz. Sem regras definidas, torna-se inconsistente e podem surgir vulnerabilidades.

Segundo Soares, Soares e Alves (2021), a política tende a estabelecer normas e regras de conduta com o objetivo de reduzir a probabilidade de ocorrência de incidentes que causem a indisponibilidade do serviço, por exemplo, roubo, ou mesmo perda de informações, o que mostra que, em geral, as políticas de segurança são construídas a partir das necessidades da empresa, para depois serem aperfeiçoados pela experiência do gestor.

Com a NBR ISO/IEC27002, recomenda-se que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para garantir a continuidade de sua adequação, relevância e eficácia (SABINO, 2020, s/p).

PRINCIPAIS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Autenticação multifatorial e leitura biométrica

Segundo Nakano (2022), a autenticação multifatorial e a leitura biométrica, fornecem uma camada de proteção para os usuários se protegerem de invasores. Essa abordagem reduz o efeito cascata de credenciais comprometidas, pois o nome de usuário e a senha sozinhos não são suficientes para concluir o acesso.

De acordo com Caruso e Steffen (2013), a autenticação multifatorial usa várias técnicas para verificar a identidade de um usuário. Por outro lado, a autenticação de fator único, usa uma única técnica para provar a autenticidade de um usuário. Com a autenticação multifatorial, os usuários devem combinar tecnologias de autenticação de pelo menos dois grupos ou fatores de autenticação diferentes. Esses fatores devem se enquadrar em três categorias: algo que o usuário conhece, algo que o usuário tem e algo que o usuário é. Portanto, o uso de uma senha (ambos da categoria "algo que o usuário sabe") não seria considerado. Já a autenticação usando um reconhecimento facial (ambos da categoria “algo que o usuário é”) seria considerado como autenticação multifatorial.

Encriptação de dados

Segundo Oliveira (2021), a criptografia de dados é o processo de codificação de mensagens ou arquivos. Esse processo é responsável por gerar um código que permite que apenas pessoas com as chaves corretas acessem essas informações. O objetivo da criptografia é proteger os dados digitais enquanto estão sendo transmitidos.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

Complementando essa ideia, Cabral (2004), enfatiza que o objetivo principal da criptografia de dados é impossibilitar, ou senão, dificultar o acesso não autorizado a estes dados.

Identity and access management (iam)

Segundo Brown e Stallings (2013), o gerenciamento de identidade e acesso (IAM) é a prática de garantir que pessoas e entidades com identidades digitais tenham o acesso correto aos recursos da empresa, como redes e bancos de dados. As funções do usuário e os direitos de acesso são definidos e gerenciados por meio do sistema IAM.

Complementando essa ideia, Kim (2014) diz que uma solução IAM permite que os administradores de TI gerenciem com segurança e eficiência a identidade digital e os direitos de acesso relacionados dos usuários. O IAM permite que os administradores definam e modifiquem as funções do usuário, monitorem e gerem relatórios sobre a atividade do usuário e apliquem políticas corporativas e regulamentares para proteger a segurança e a privacidade dos dados.

Para Hintzbergen (2018), o *Identity Access Management* (IAM) é essencial para a segurança e a conformidade regulamentar. Ele também pode ser um compromisso difícil de lidar quando não se tem as habilidades, a estratégia e o suporte qualificados de especialistas em segurança e identidade que ajudam a arquitetar e gerenciar soluções em todos os ambientes de *cloud* híbrida e produtos e plataformas de IAM.

RESPOSTA A INCIDENTES

De acordo com Caruso e Steffen (2013), a resposta a incidentes é o processo de uma empresa para reagir a ameaças de TI, como ataques cibernéticos, violação de segurança e tempo de inatividade do servidor.

Complementando essa ideia, Kim (2014), relata que existem 7 principais etapas a serem seguidas que tornam a resposta a incidentes mais eficaz. São elas: Identificar o incidente; definir canais de comunicação da equipe; avaliar o impacto e aplicar um nível de gravidade; comunicar-se com os clientes; escalonar para os respondentes certos; delegar funções de resposta a incidentes; resolver o incidente.

ANÁLISE COMPORTAMENTAL

De acordo com Gomes (2020), a análise do comportamento do usuário, é um processo de segurança cibernética sobre a detecção de ameaças internas, ataques direcionados e fraudes financeiras, que se tornou fundamental para os times de segurança das empresas.

Seguindo essa ideia, Hintzbergen (2018) diz que a análise comportamental consiste em combinar inteligência artificial e aprendizado de máquina para analisar minuciosamente todas as atividades do usuário com base em seu comportamento. Com isso, ajuda a

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

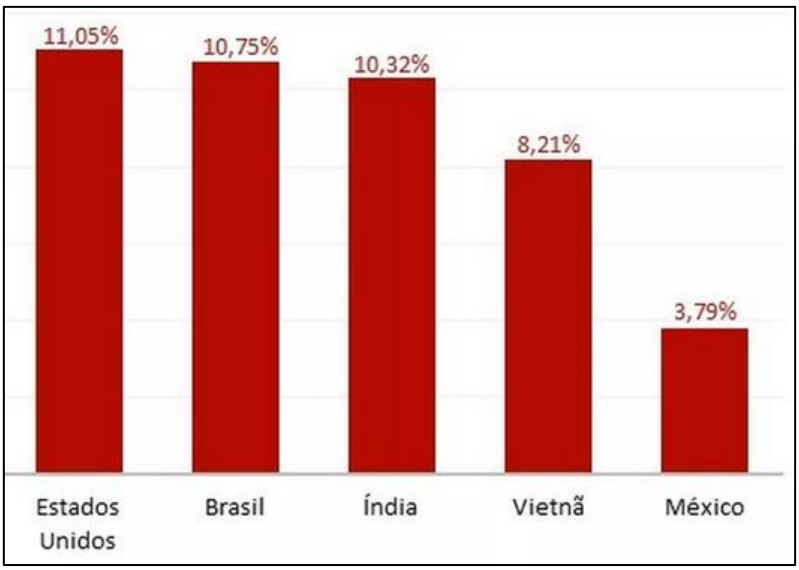
identificar quais situações podem ser consideradas normais e quais são suspeitas para cada empresa. Nesse filtro de milhares de eventos em tempo real, é possível direcionar um número muito menor de ameaças do mundo real, direcionando as equipes de segurança e concentrando seus esforços em ataques do mundo real.

PREVENÇÃO CONTRA O *RANSOMWARE*

De acordo com Kim (2014) as consequências deste tipo de ataque podem ser desafiadoras para a empresa, já que o *Ransomware* impede o acesso a dados pessoais importantes.

Brown e Stallings (2013) definem *Ransomware* como um tipo de *malware* cujas características ameaçam revelar, deletar ou bloquear o acesso a informações pessoais importantes. Em vez disso, o vírus exige um resgate financeiro de suas vítimas. O invasor envia um arquivo para o seu dispositivo que, ao ser aberto, pode criptografar seus próprios arquivos e impedir que você acesse a máquina. Os arquivos são mantidos para resgate até que se pague para descriptografá-los. Segue abaixo a figura 6, no qual demonstra os países que mais tiverem *Ransomware* no mundo em 2019.

Figura 6. Brasil é o 2°país com mais Ransomwares no mundo, revela pesquisa



Fonte: Techtudo (2019).

BACKUP

De acordo com Hintzbergen (2018), a ISO/IEC 27002 recomenda armazenar sistemas de *backup* em outro local o mais longe possível do ambiente atual, como em outro prédio ou em outro meio, como armazenagem *online* (nuvem). Sendo possível observar com maior detalhe o ciclo dos dados de um *backup* e restauração em nuvem, na figura 7.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

Figura 7. Backup e restauração.

Fonte: *Supportexpress* (2015)

Dessa forma, Soares, Soares e Alves (2021) relatam que o procedimento de *backup* é um dos recursos mais eficazes para garantir a continuidade das operações em caso de paralisação em caso de acidente.

SEGURANÇA FÍSICA

Conforme Raposo (2019) relata, o objetivo dessa forma de segurança é impedir o acesso físico não autorizado. Perímetros de segurança devem ser usados para proteger áreas contendo informações e instalações de processamento de informações de acordo com a ISO/IEC 27002:2005.

Sabino (2020) complementa essa ideia relatando que a proteção física pode ser alcançada criando uma ou mais barreiras físicas ao redor das facilidades e recursos de processamento de informações, como portas de acesso com cartões magnéticos, leitores biométricos, posicionamento de vigilantes em locais de acesso limitado, portões elétricos, entre outras medidas.

METODOLOGIA

Para o desenvolvimento deste trabalho, foi utilizada a pesquisa bibliográfica, com o intuito de coletar a maior quantidade possível de materiais teóricos sobre o tema proposto.

A busca, foi realizada nas bases de dados eletrônicas do Google Acadêmico e *Scientific Electronic Library Online* – Scielo utilizando as palavras-chave Gestão, Segurança de Dados, Política de Segurança da Informação, Riscos, Vulnerabilidades nas organizações, e Importância da segurança das informações, sendo selecionados artigos escritos em português ou inglês e publicados entre 2004 e 2022. Foram excluídos artigos em outros idiomas, além daqueles citados anteriormente, artigos anteriores ao período estipulado e que não condiziam com o tema do presente estudo

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

Segundo Sousa, Oliveira e Alves (2021), a pesquisa bibliográfica é o levantamento ou revisão de obras publicadas sobre a teoria que irá direcionar o trabalho científico o que necessita uma dedicação, estudo e análise pelo pesquisador que irá executar o trabalho científico e tem como objetivo reunir e analisar textos publicados, para apoiar o trabalho.

Também foi utilizada a pesquisa exploratória, a fim de obter informações sobre a gestão da segurança da informação aplicada por uma empresa que atua no ramo do varejo, localizada no Interior do Estado de São Paulo. Trata-se de uma empresa de porte médio, com aproximadamente 300 funcionários, faturamento bruto de 20 milhões de reais por mês, atendendo o mercado varejista desde 2002.

Segundo Patah e Abel (2022), a pesquisa exploratória tem como função preencher as lacunas que costumam aparecer em um estudo, levantando informações sobre o assunto abordado. Para a realização da pesquisa exploratória tomou-se como base a Norma ISO/IEC 27002:2013(ABNT, 2013) que é um guia prático para o desenvolvimento e implementação de procedimentos e controles de segurança da informação nas organizações.

Na norma ISO 27002 cada seção define um ou mais objetivos de controle de boas práticas para que a organização adote uma postura preventiva e proativa diante dos requisitos de segurança da informação.

Estas seções foram estudas e comparadas com as práticas de gestão da segurança da informação da empresa objeto do estudo e o compilado da análise foi demostrada através de um quadro comparativo na seção resultados e discussão.

RESULTADOS E DISCUSSÃO

A seguir apresenta-se os resultados e a discussão acerca dos pontos padronizados que são utilizados para a definição das políticas de segurança da informação dentro das organizações. A elaboração dos resultados e discussão foi baseada em uma análise minuciosa das principais recomendações da ISO/IEC 27002:2013 em comparação com a as práticas de gestão da segurança da informação da empresa estudada, após esta análise os pontos em desacordo com as boas práticas de segurança da informação foram classificadas como “Não Conformes” e aquelas que estavam em acordo com as boas práticas de segurança da informação foram classificadas como “Conformes” sempre utilizando-se como guia a ISO/IEC 27002:2013.

O quadro 1 apresenta o resumo desta comparação e em seguida há a discussão dos pontos não conformes e as possíveis consequências e impactos negativos às pessoas, aos negócios e até mesmo à reputação da empresa estudada.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

Quadro 1. Comparação das práticas de gestão da segurança da informação da empresa estudada com a NBR ISO/IEC 27002: 2013

Itens da política de segurança da informação	Conforme	Não conforme	Análise
1) controle de acesso		X	Não está conforme pois a empresa não segue a maioria dos requisitos que a NBR ISO/IEC 27002:2013. Como proteção de acesso para dados e serviços etc
2) classificação e tratamento da informação	X		
3) segurança física e do ambiente		X	Não está conforme pois no ambiente onde se localizam os equipamentos, há matérias inflamáveis, causando risco de incêndio e há o acesso facilitado a qualquer pessoa, sem qualquer cobrança de identificação ou controle de acesso.
4) tópicos orientados aos usuários finais:		x	
5) uso aceitável dos ativos		X	não está conforme pois não há nenhuma documentação associada aos recursos de processamento da informação.
6) mesa limpa e tela limpa	X		
7) transferência de informações	X		
8) dispositivos móveis e trabalho remoto		X	Não está conforme pois tanto o usuário estando na empresa, quanto estando em casa, não há controle de acesso dos usuários.
9) restrições sobre o uso e instalação de software	X		
10) backup	X		
11) transferência da informação	X		
12) proteção contra malware	X		
13) gerenciamento de vulnerabilidades técnicas		X	Não está conforme pois a empresa não possui nenhum monitoramento das vulnerabilidades, avaliação de riscos e correções.
14) Controles criptográficos	X		
15) segurança nas comunicações	X		
16) proteção e privacidade da informação de identificação pessoal	X		
17) relacionamento na cadeia de suprimento	X		

Fonte: Elaborado pelos autores

Ao comparar o levantamento efetuado das práticas de gestão de segurança da informação, na empresa objeto do estudo, com a norma NBR ISO/IEC 27002:2013, e a observação da rotina dos funcionários da organização, pode se verificar que 42%(n=5) itens da política de segurança estão não conformes contra 58%(n=12) itens conformes.

Dos itens não conformes cabe destacar que há a navegação descontrolada em *sites* potencialmente perigosos pelos funcionários, expondo a empresa a uma série de riscos de segurança, como vírus, trojans e *spyware, a*lém de permitir que os funcionários enviem qualquer informação que possa ser confidencial para a empresa, abrindo-se oportunidades para muitos problemas legais e até mesmo acesso a informações confidenciais sobre os produtos, fórmulas e preços e problemas em relação ao acesso a informações, gerenciamento de riscos e vulnerabilidades e até mesmo ao ambiente de armazenamento dos equipamentos de informática.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

Ferreira (2000) ao estudar uma pequena empresa verificou que a mesma não possuía em ambiente confiável, pois todos os funcionários tinham acesso a todo e qualquer dado da empresa, sem qualquer controle e que, portanto, vulnerável a qualquer ataque cibernético. Pondo em risco os negócios da empresa, da mesma forma que a condição atual da empresa deste estudo que não faz a gestão do acesso dos indivíduos às informações sobre o negócio.

De acordo com Fontes (2008) a informação é o elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor.

A informação é um bem valioso para as organizações, mas pode ser alvo de uma série de ameaças, que já foram descritas no referencial teórico do presente estudo e da forma como a empresa estudada faz a gestão das informações, está correndo muitos riscos e vulnerável a vários ataques que podem até mesmo afetar a área produtiva da empresa.

Segundo Freitas & Araújo (2008) toda e qualquer informação, cujo comprometimento possa causar perda de vantagem competitiva, pode gerar um dano ou prejuízo ao negócio ou a imagem da organização.

. Existe, portanto, a necessidade de implementar políticas de segurança da informação, que visem reduzir as chances de fraudes ou mesmo de perda de informações.

Cabe destacar, ainda, que uma política de gestão de informações ou uma política de segurança da informação, deve ser de acesso e conhecimento de todos os funcionários da organização e todos devem estar realmente comprometidos na sua aplicação e cumprimento, inclusive a NBR ISO/IEC 27002:2013 recomenda, fortemente o treinamento dos funcionários visto que são eles os operadores de informações e equipamentos, o conhecimento sobre segurança da informação deve ser socializado e compartilhado com todos, n~so só com os funcionários da área..

Os contratos de confidencialidade para assinatura dos funcionários da empresa, e outro item importante para a ciência dos riscos, em termos de segurança da informação, inclusive no gerenciamento das identidades e acesso.

Estudo de Netto & Siveira(2007) demonstram que o fator humano é a que carece de maior atenção por parte das empresas, os dados confirmaram que as empresas investem muito controles tecnológicos para diminuir o risco de incidentes de segurança da informação, mas esquecem que o indivíduos é uns dos grandes responsáveis por falhas na segurança.

Estes procedimentos podem ajudar a manter os problemas sob controle. Além de conscientização dos usuários a não violação das políticas de navegação segura.

Já o não uso de *software* licenciados pode gerar para a empresa multas com valores altíssimos, além de acarretar processos administrativos e judiciais.

O uso de *software* licenciado traz como garantia para a empresa a integridade de seus dados. Apesar das conformidades superarem as não conformidades na comparação das práticas de segurança da informação da empresa com a NBR ISO/ICE 27002: 2015,

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

os itens não conformes precisam ter um plano de ação para serem solucionados para que a empresa se mantenha em um padrão aceitável de segurança das informações.

CONCLUSÃO

Pode-se verificar no desenvolvimento de presente trabalho que a empresa em estudo, quando compara-se os requisitos mínimos para uma política de segurança e as práticas empresariais que há não conformidades na aplicação das normas de segurança da informação, o mesmo acontece quando há a mesma comparação com as normas NBR ISO/IEC 27002:2013, indicando que há a necessidade se se implantar melhorias na gestão e gerenciamento das políticas de segurança para que os negócios, processos, pessoas e lucratividade sejam preservado.

O trabalho, também, foi capaz de levantar os riscos a que o negócio da empresa está submetido pela não adequação das normas de segurança das informações aos padrões da NBR ISO/IEC 27002:2013 e de sugerir à empresa a adoção de uma política de segurança da informação para o gerenciamento de riscos e para a orientação, treinamento e compartilhamento de informações seguras entre todos os membros da organização, bem como para todas as pessoas, clientes e fornecedores que são seus parceiros.

Portanto, o presente trabalho atingiu os seus objetivos, ficando como oportunidade remanescente, um estudo para viabilizar a adequação da gestão da política de informação às normas visando a manutenção e continuidade dos negócios da empresa de forma segura e um treinamento comportamental para os empregados a fim de apresentar os riscos e consequências de comportamentos inseguros de navegação na *internet*, redes sociais etc.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(ABNT). **NBR ISO/IEC 27002:2013: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2013.

BROWN, L; STALLINGS, W. **Segurança de computadores**. Rio de Janeiro: Campus, 2013.

CABRAL, Carlos Cristiano. **Criptografia de dados**. São Paulo: Novatec, 2004.

CARUSO, C.A.A; STEFFEN, F.D. **Segurança em Informática e de Informações**. 4. ed. São Paulo: SENAC, 2013.

DOI: 10.5281/zenodo.10082438 *Artigo Original*

FERREIRA, Fabiana. **Segurança da Informação**: conceito, importância e sua relação com o RH e a ISO/IEC 27001. Disponível em: https://blog.solides.com.br/seguranca-da-informacao/. Acesso em: 10 nov. 2022.

FERREIRA, Tamires. **Brasil está entre os cinco países que mais sofrem ataques ransomware**. Disponível em: https://olhardigital.com.br/2022/09/11/seguranca/brasil-esta-entre-os-cinco-paises-que-mais-sofrem-ataques-ransomware/. Acesso em: 15 nov. 2022.

FERREIRA, L.H. **implementação de segurança em tecnologia da informação em pequenas empresas**. Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gerencia de Projetos de Tecnologia da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gerente de Projetos de Tecnologia da Informação. Disponível em : https://repositorio.animaeducacao.com.br/handle/ANIMA/3726. Acesso em 23 julho 2023

FREITAS, F; ARAUJO, M. **Políticas de Segurança da Informação**: Guia prático para elaboração e implementação. 2ed. Ciência Moderna Ltda, 2008

FONTES, E. **Praticando a Segurança da Informação**. São Paulo: Brasport Editora,2008

GOMES, Waldo. **O que a análise de comportamento do usuário revela para a segurança.** 2020. Disponível em: https://olhardigital.com.br/2020/08/25/pro/o-que-a-analise-de-comportamento-do-usuario-revela-para-a-seguranca/. Acesso em: 15 nov. 2022.

HINTZBERGEN, Jule; et al. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

KIM, D. **Fundamentos de segurança de Sistemas de Informação**. São Paulo: LTC, 2014.

NAKANO, Alexandre. **Autenticação multifator**: descubra mais sobre este processo. Descubra mais sobre este processo. Disponível em: https://blog.ingrammicro.com.br/seguranca-da-informacao/autenticacao-multifator/. Acesso em: 20 nov. 2022.

NETTO, A. S.; SILVEIRA, M.A.P. gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. Revista de Gestão da Tecnologia e Sistemas de Informação. **Journal of Information Systems and Technology Management.** Vol. 4, No. 3, 2007, p. 375-397.Disponível em: https://www.scielo.br/j/jistm/a/Vx8Ypv6mDjxdYkKKrfYVgqz/?format=pdf&lang=p.Acesso em 23 maio 2023.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10082438 *Artigo Original*

OLIVEIRA, Ingrid. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%**. Disponível em: https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/. Acesso em: 10 nov. 2022.

OLIVEIRA, Silvana de. **Dados encriptados**: vocês sabem o que são?. 2021. Disponível em: https://blog.pmcursos.com.br/dados-encriptados/. Acesso em: 20 nov. 2022.

PATAH, Rodrigo; ABEL, Carol. **O que é pesquisa exploratória?** Disponível em: https://mindminers.com/blog/o-que-e-pesquisa-exploratoria/. Acesso em: 19 nov. 2022.

RAPOSO, Cláudio Filipe Lima; et al. LGPD-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac,** v. 4, p. 58-67, 2019.

SABINO, Richard. Gestão da segurança da informação orientado a LGPD: impactos da implantação das normas LGPD nos processos da ADM Sistemas LTDA. **Tecnologia em Gestão da Tecnologia da Informação.** Unisul Virtual**,** 2020.

SOARES, Sória Pereira Lima; SOARES, Augusto Cezar da Silva; ALVES, Aldo Agustinho. A importância da implementação de uma política de segurança da informação. **Brazilian Journal of Development,** v. 7, n. 4, p. 37162-37171, 2021.

SOUSA, Angélica Silva de; OLIVEIRA, Guilherme Saramago de; ALVES, Laís Hilário. **A pesquisa bibliográfica**: princípios e fundamentos. Campinas: Krauss, 2021.

Os autores declararam não haver qualquer potencial conflito de interesses referente a este artigo.