SEMANA ACADÊMICA
REVISTA CIENTÍFICA
ISSN 2236-6717

ANÁLISE DA SEGURANÇA NA TRANSMISSÃO DE DADOS/SEGURANÇA DA INFORMAÇÃO

FABIO HENRIQUE PIZZAIA[1]
RENATA MIRELLA FARINA[2]
FABIANA FLORIAN[3]

RESUMO: Este artigo tem por objetivo realizar uma análise da segurança da informação com algumas empresas do setor. O tema segurança da informação é uma área que trata especificamente da proteção de um ou mais conjuntos de dados, no sentido de preservar as informações e seus respectivos valores dentro de uma empresa, ou para um indivíduo em particular. Garantir a segurança da informação em uma empresa é necessário dentro de um mercado de ampla concorrência. Vale enfatizar que está fundamentada em três pilares: confidencialidade (onde os acessos aos dados são limitados por permissões); integridade (a garantia da veracidade das informações); disponibilidade (acesso as informações com facilidade). Foi realizada pesquisa bibliográfica e um estudo com 14 empresas do setor de tecnologia no Município de Araraquara – SP. Verificou-se que as empresas utilizam um ou mais métodos de segurança da informação e por questões de sigilo, de acordo com a Lei Geral de Proteção de Dados, esses métodos foram divulgados, mas não foi identificado o nome da empresa.
Palavras-chave: segurança; informação; dados.

ANALYSIS OF SECURITY IN DATA TRANSMISSION/INFORMATION SECURITY

ABSTRACT: This article aims to carry out an analysis about information security, areas that specifically deal with the protection of one or more sets of data, in the sense of preserving information and its respective values within a company, or for an individual in particular. Within this context, it is important to remember that the concept of data security or information security is inserted within a larger context, which is computer security, that is, the security of the systems themselves. Ensuring information security in a company, for example, is extremely necessary within a highly competitive market. It is worth emphasizing that information security works based on three tangents, which are confidentiality (where access to data is limited by permissions); integrity (the guarantee of the veracity of information); availability (access to information easily).
Keywords: Security; information; data;

Submetido em: 18/10/2023 – **Aprovado em**: 13/11/2023 – **Publicado em**: 16/11/2023

[1] Aluno cursando Sistema de Informação, fhpizzaia@uniara.edu.br
[2] Professora, mestre em Engenharia de Produção, Uniara, São Paulo, rmfarina@uniara.edu.br
[3] Docente, Doutorado em Alimentos e Nutrição pela Universidade Júlio de Mesquita Filho (UNESP) - FCFAr Araraquara-SP; Mestrado em Desenvolvimento Regional e Meio Ambiente pela Universidade de Araraquara-SP- UNIARA, Araraquara-SP; Graduação em Ciências Econômicas e Bacharel em Direito pela UNIARA; UNIARA- Araraquara-SP; fflorian@uniara.edu.br

http://dx.doi.org/10.35265/2236-6717-240-12850

1 INTRODUÇÃO

Segundo a Fundação Bradesco (2017), antigamente as informações importantes eram armazenadas de maneiras diferente em pastas e gavetas, na grande maioria das vezes com acesso restritos e demorados. Atualmente a realidade está bem diferente, e estas informações ficam na internet, que possui inúmeros recursos, onde inúmeros usuários fazem uso de milhares de informações.

Com a evolução da tecnologia as empresas conseguiram automatizar os seus serviços, ficando cada vez mais eficientes. Contudo, com o aumento da conectividade as ameaças as quais as mesmas estão expostas também aumentaram, principalmente quando os computadores estão conectados as redes mundiais (UNIVERSIDADE DE BRASÍLIA, 2010).

Portanto, a Segurança da Informação passa ocupar um lugar de destaque, pois a "sua importância não está mais conectada somente a detecção de invasão e proteção das informações, mas também engloba medidas para a prevenção, detecção, resposta, recuperação e continuidade do negócio" (DANTAS, 2011, p. 6).

Pode se considerar uma invasão sempre quando as informações são divulgadas ou acessadas sem um consentimento prévio, e para a proteção das mesmas se faz necessário aplicar os princípios básicos da segurança da informação, que são: autenticidade, confidencialidade, disponibilidade e integridade (OLIVEIRA, 2017).

Quando é citado "dados", busca-se nos referir a um conjunto de informações organizadas, podendo ser números, imagens, palavras, textos, dentre outros. Já quando falamos de informação é todo e qualquer processamento de dados que resulte em uma modificação no conhecimento do sistema que recebe tal informação. Um dado isolado, por si só, pode não fazer sentido em determinado contexto. Deste modo, informação é um conjunto de dados organizado e estruturado para trazer sentido a quem o acessa ou interpreta.

Ou seja, quando nos referimos a segurança da informação, estamos mencionando a proteção do conjunto de informações que podem pertencer a uma pessoa, um grupo ou uma empresa, por exemplo. Quando há um conjunto de informações, refere-se a todo e qualquer conjunto de dados que possa ter ou representar algum valor para uma ou mais pessoas ou organização.

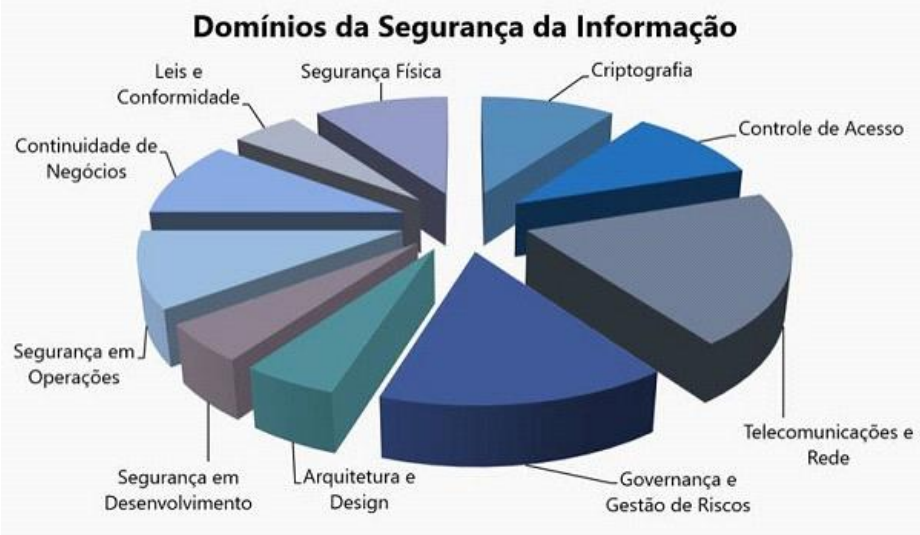
O nível de segurança das informações pode ser medido através do uso de algumas ferramentas, porém é importante lembrar que a segurança das informações está diretamente ligada a forma com a qual elas são utilizadas, bem como pelo ambiente onde está inserida, no que toca a infraestrutura, por exemplo.

Os principais aspectos relacionados à segurança da informação são chamados de Tríade CIA (*Confidentiality, Intregity and Availability*), e estão diretamente relacionados ao planejamento e implementação de um plano de segurança para um grupo de informações ao qual se deseja proteger.

Um dos aspectos mais preocupantes nos dias de hoje, em relação a segurança da informação, é a privacidade. Uma vez estabelecido um plano de segurança, é preciso que ele seja seguido por todos que tenham acesso ou façam uso das informações, para que o nível de segurança seja mantido continuamente.

A figura 1 demonstra os domínios da segurança da informação:

Figura 1: Domínios da Segurança da Informação



Fonte: GO2WEB,2023.

A Política de Segurança da Informação (PSI) é um documento onde abranger um conjunto de normas, métodos e procedimentos, que devem ser comunicados a todos os funcionários, assim como deve ser revisado periodicamente. O Sistema de Gestão de Segurança da Informação (SGSI) garante a viabilidade e o uso correto somente por pessoas autorizadas (FONTES, 2006).

Dentro de toda e qualquer política de segurança, existem dois grupos, sendo eles o proibitivo, que engloba tudo aquilo que não se pode e não se deve, de maneira alguma, ser feito, e o permissivo, que engloba tudo aquilo que deve ser realizado.

Falhas em sistemas computacionais, seja em componentes de software, seja em componentes de hardware, têm provocado desde *blackouts* de grandes proporções a falhas em robôs utilizados nos programas de exploração espacial (NEUMANN, 2004).

A realização da pesquisa se dará em duas etapas distintas.

Na primeira etapa, foi realizada pesquisa bibliográfica dos métodos e políticas de segurança existentes e que podem ser utilizados por empresas no intuito de gerar segurança aos seus dados, bem como os prós e contras de cada método apresentado.

Foi aplicado questionário via google forms para funcionários de 14 empresas do setor de tecnologia da cidade de Araraquara - SP, com o intuito de buscar saber quais os métodos mais usados pelas empresas, bem como o nível de satisfação de cada uma com os mesmos. As empresas utilizam um ou mais métodos de segurança da informação. Neste sentido por

questões de sigilo, de acordo com a Lei Geral de Proteção de Dados, esses métodos foram divulgados, mas não foi identificado qual empresa usa tal método.

2 REVISÃO BIBLIOGRAFICA

Quando não existe uma cultura de segurança das informações cria- se um ambiente propício para ataques, invasões e golpes. Os vazamentos de informações e exposições ocorrem em momentos simples do dia a dia da empresa (DANTAS, 2011).

Segundo Davis, a importância da informação só é reconhecida quando ela é perdida. "O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir". (DAVIS, 1997 APUD BLUEPHOENIX, 2008).

"Tenho observado que a maioria dos problemas de segurança da informação ocorridos em organizações está relacionada a um conjunto básico de falhas na implantação e desenvolvimento do processo de segurança da informação" (SILVA, 2008).

Ainda, segundo Silva, 2008, os principais erros em relação a segurança da informação são:

- A falta de políticas;
- A falta de uma gestão de controle de acesso;
- A falta de um gestor da informação;
- Não cumprir os planos de continuidade;
- Falta de registros das ações realizadas;
- Cópias de segurança;
- A falta de um gestor de processo de segurança;
- A falta de uma gestão de risco;
- A não existência de um paralelo entre a segurança e o negócio;
- Funcionário pouco treinado e não conscientizado.

Atualmente, e cada vez mais, o uso de sistemas informatizados por meio de redes (redes sociais, por exemplo), faz com que a segurança da informação seja cada vez mais imprescindível.

O ambiente digital é um universo de conteúdo, dentre os quais podem existir ameaças que comprometam a segurança da relação usuário-sistema-informação.

Para Moraes (2011, p. 139):

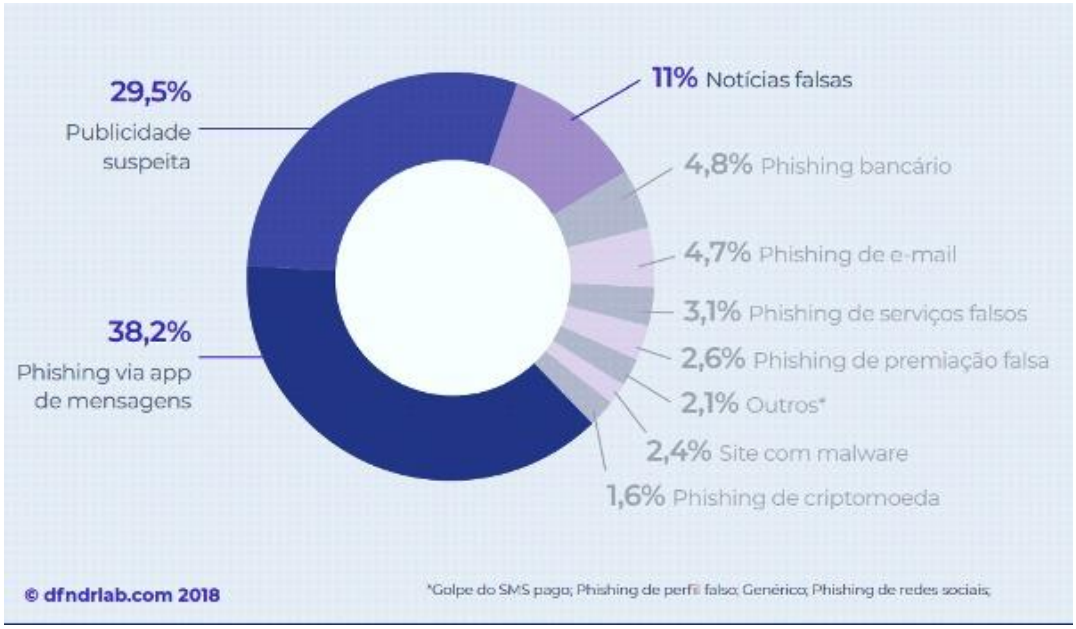
> da mesma forma que as redes sociais podem ser usadas para divulgação de conteúdo útil, ela também tem sido usada por criminosos, que induzem os usuários a clicarem em links e efetuar download de malware.

Quando isso ocorre, vários arquivos do computador podem ser prejudicados e até mesmo roubados, colocando em risco o usuário que pode ter informações bancárias e pessoas compartilhadas sem autorização com pessoas mal-intencionadas.

Contudo da mesma forma que as redes sociais são usadas para divulgação de conteúdo útil, as mesmas podem ser usadas para a divulgação de conteúdos criminoso e aplicarem golpes. E quando isso acontece vários arquivos dos computadores são prejudicados, colocando em riscos informações primordiais para os usuários (MORAES, 2011).

A empresa PSafe, empresa de segurança digital líder de mercado na América Latina que desenvolve produtos de cibersegurança para pessoas e empresas, publicou as principais categorias de link maliciosos (Figura 2).

Figura 2: Principais categorias de links maliciosos



Fonte: PSafe, 2023.

Já não se trata mais da possibilidade de existirem ataques virtuais que comprometam nossos dados e informações, mas sim de quando esses ataques vão ocorrer.

Em empresas e organizações, o prejuízo pode ser ainda maior.

Segundo especialistas, a maior parte dos problemas de segurança são causados por ausência de políticas de segurança que possibilitem uma boa gestão de riscos e ameaças.

Outro aspecto que merece atenção especial é a urgente necessidade de uma discussão aprofundada dos preceitos subjacentes as políticas de segurança da informação adotadas no Brasil – em sua maioria, do lado estatal (MARCIANO, 2006).

É preciso, então, que as práticas de segurança da informação existam e sejam eficientes, além de serem centradas no usuário, seja ele uma pessoa física, usuária de rede social, ou uma empresa ou corporação usuária de um sistema, ou uma rede de sistemas.

Então se faz necessário a implementação de uma política de segurança da informação, onde existira diversos processos e rotina que visem resguardar ao máximo os arquivos da empresa, através de processos como: backup, uso antivírus, IDS, firewall, monitoramento de pacotes, entre outros. Outra implementação que se faz necessário são os testes invasão, onde o intuito é achar falhas e vulnerabilidades (OLIVEIRA, 2017).

A segurança na transmissão de dados se classifica em quatro tópicos, sendo eles: **pública**: é a mais comum, trada de informações que, caso vazem, não causarão danos; **interna**: o acesso dessa informação deve ser evitado, sua integridade é importante, porém não é vital; **confidencial**: quando a informação é de extrema importância, desestabilizando a empresa caso ela seja exposta; **secreta**: é a informação mais crítica, sendo de extrema valia e podendo pôr em risco a empresa (FUNDAÇÃO BRADESCO, 2017).

3 DESENVOLVIMENTO

A finalidade deste trabalho é de estabelecer uma análise sobre as diferentes políticas de segurança existentes, no que toca a segurança de transmissão e armazenamento de dados, com o intuito de buscar definir qual a melhor política de segurança a ser adotada dentro de contextos diferentes.

Foi realizada uma pesquisa envolvendo 14 empresas do setor de tecnologia da cidade de Araraquara - SP, com o intuito de buscar saber quais os métodos mais usados pelas empresas, bem como o nível de satisfação de cada uma com eles, se as empresas utilizam um ou mais métodos de segurança da informação. Neste sentido por questões de sigilo, de acordo com a Lei Geral de Proteção de Dados, esses métodos foram divulgados, mas não foi identificado qual empresa usa tal método.

Foi enviado questionário via *google forms* para 1 funcionário da área de desenvolvimento de software de cada empresa pesquisada.

Foram aplicadas 4 perguntas fechadas (Figura 3, 4, 5, 6).

Na primeira pergunta o funcionário da empresa foi questionado se a empresa em que atua investe em segurança da informação (Figura 3).

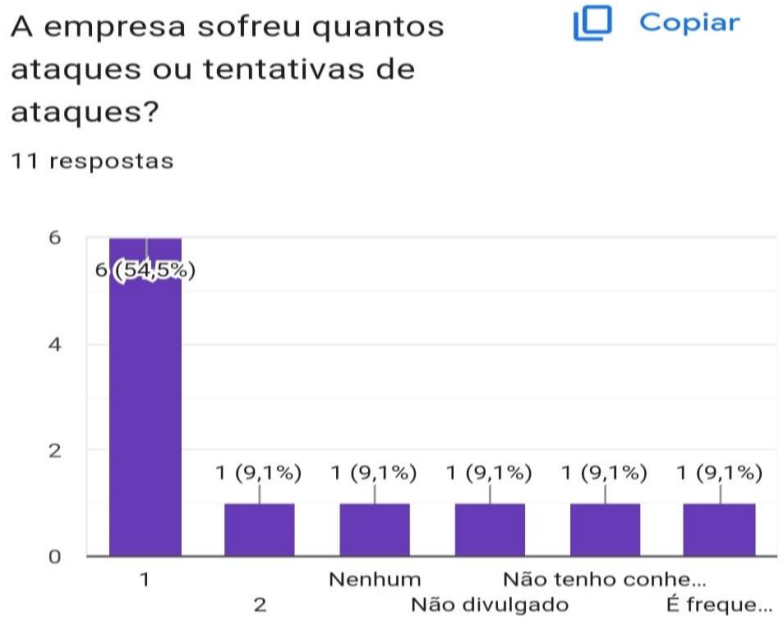
Figura 3: A empresa investe em segurança

Fonte: própria, 2023.

Pode-se constatar que 78,6% das 14 empresas (total das empresas pesquisadas) investem na segurança, pois a maior parte dessas tem medo que suas informações acabem sendo vazadas.

Na segunda pergunta o funcionário da empresa foi questionado se a empresa em que atua sofreu ataque(s) ou tentativa(s) de ataque (s) e a frequência desse(s) ataque (s): um, dois ataques, nenhum, não divulgado pela empresa, não tenho conhecimento e, é frequente, quase semanal. (Figura 4).

Figura 4: A empresa sofreu ataques ou tentativas de ataque



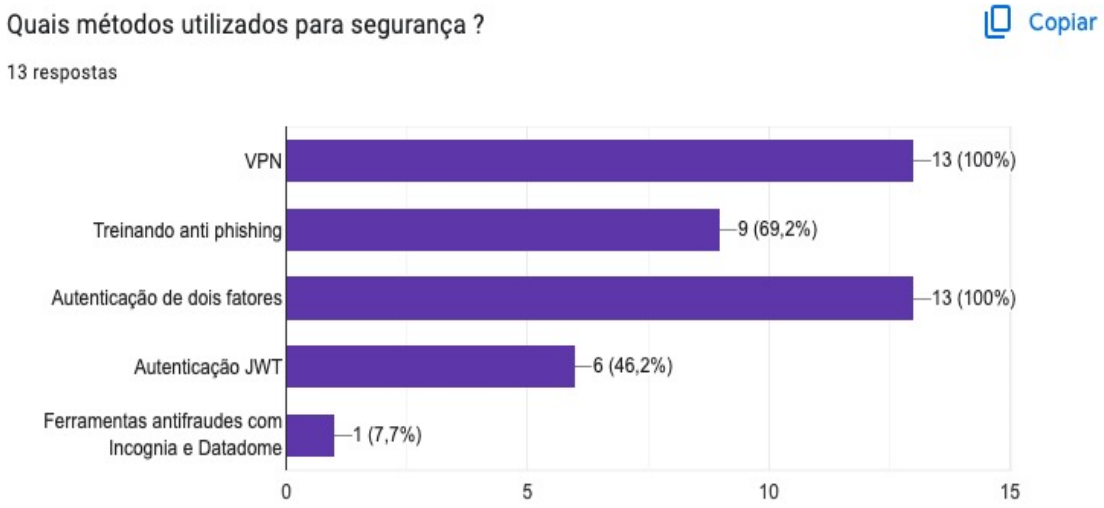
Fonte: própria, 2023.

Observa-se que 11 empresas (do total de 14) responderam o questionário e dessas 11, seis delas já sofreram algum tipo de ataque ou invasão, mostrando que qualquer tipo de empresa independente do seu porte está sujeito a sofrer um tipo de ataque; há poucas empresas que nunca foram alvo de algum tipo de invasão.

Ressalta-se que de todas as perguntas do questionário os funcionários tem a opção de não querer responder.

A terceira pergunta ao funcionário da empresa se refere aos métodos de segurança da informação utilizados pelas empresas (Figura 5). Do total de 14 empresas pesquisadas, 13 delas utilizam o VPN e o método de autenticação de dois fatores.

Figura 5: Métodos utilizados para segurança da informação nas empresas

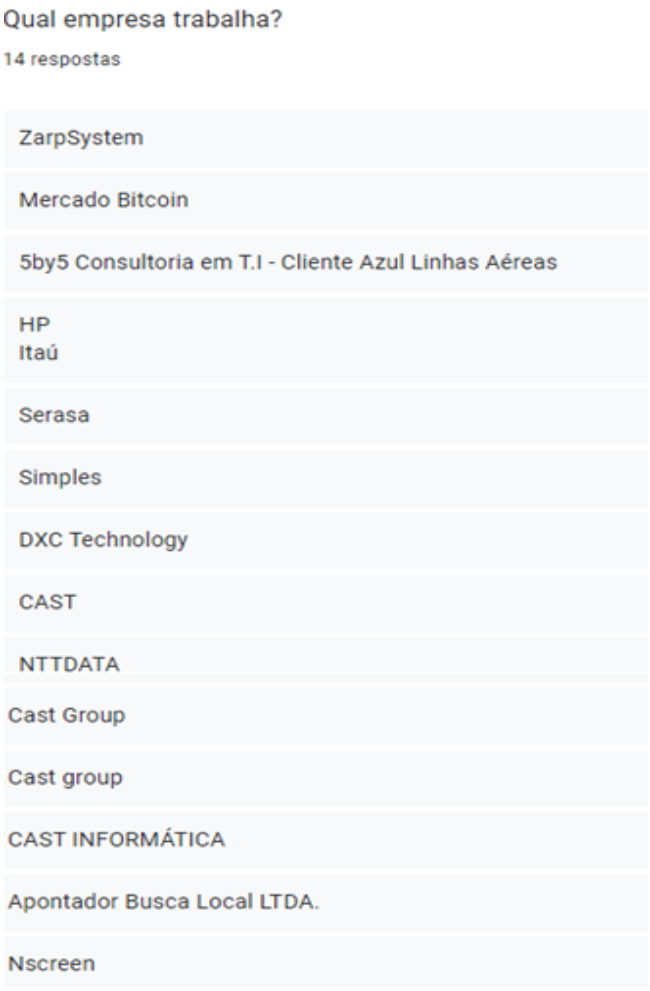


Fonte: própria, 2023.

Ressalta-se que as empresas podem utilizar um ou mais métodos de segurança.

A quarta pergunta busca identificar o nome das empresas pesquisadas (Figura 6). Ressalta-se que os nomes de algumas empresas estão duplicados porque envolvem projetos/métodos diferentes e consequentemente medidas de segurança diferentes.

Figura 6: Relação das empresas pesquisadas



Fonte: própria, 2023.

4 CONCLUSÃO

Pode-se constatar que as empresas de modo geral já sofreram algum tipo de ameaça e, portanto, vem cada vez mais se importando e adequando suas políticas às diretrizes de segurança. Com base no estudo realizados podemos notar que atualmente e as informações de uma empresa é o que mantém a mesma de pé, portanto a segurança da mesma se torna vital, sendo assim ignorar as ameaças que vem constantemente crescendo, pode sim comprometer a empresa.

E com o aumento do acesso à internet e as informações cada minuto que passa as tendências que só aumente os riscos que as empresas correm. A segurança é um tema que tem amplitude em todos os aspectos na administração de uma empresa, e com a facilidade que a internet nos proporciona somente a estendeu.

Não importando o tamanho da empresa, a mesma não está isenta da ameaça, portanto se faz de extrema importância que a empresa invista em segurança da informação, não importando a tecnologia ou o recurso utilizado o mais importante e chega em um nível aceitável de segurança conseguindo assim minimizar os impactos gerados.

Com o estudo realizado podemos constatar que todas as empresas em questão sofreram pelo menos uma vez algum tipo de ataque, ressaltando assim que nenhuma empresa está livre do perigo dos ataques virtuais, e a grande maioria já investiam em pelo menos uma forma de segurança, porém vale a ressalta que não importa se investir na segurança e não ir atualizando e incrementando, porque a tecnologia é rápida e cresce diariamente, ou seja temos que estar sempre acompanhando essas atualizações, para não ficar obsoleta a segurança investida.

REFERÊNCIAS BIBLIOGRÁFICAS

BLUE PHOENIX. **Boas práticas de segurança.** 2008. Disponível em: http://www.bluephoenix.pt. Acesso em: 16 jun.2020.

DANTAS, Marcus Leal. S**egurança da Informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 150 p. ISBN 978-85-406-0047-8.

FONTES, Edison. **Vivendo a segurança da informação**: orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2006.

FUNDAÇÃO BRADESCO - Escola Virtual. **Segurança em Tecnologia da Informação.** 2017. Disponível em: (gabrielle texeira monteiro) MicroPower Learning - Segurança em Tecnologia da Informação (ev.org.br). Acesso em: 31 mai. 2023.

GO2WEB. **Domínios da Segurança da Informação**. Disponível em: http://www.go2web.com.br/. Acesso em: 30 ago.2023.

MARCIANO, João Luiz Pereira. Seg**urança da informação:** uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2006.

MORAES, Paulo. **Mente Anti-hacker :** Proteja-se! Rio de Janeiro: Brasport, 2011.

NEUMANN, Peter G. **Risks to the public in computers and related systems.** ACM SIGSOFT Software Engineering Notes, v. 25, n. 3, p. 15-23, 2004.

OLIVEIRA, Waldes. **Riscos, vulnerabilidade e ameaça em Segurança da Informação**. 2017. Disponível em: https://www.techtem.com.br/seguranca-da-informacao-riscosvulnerabilidade-e-ameaca Acesso em: 31 mai. 2023.

PEREIRA, Eduardo Martins et al. **Segurança da informação**. 2003.

PSAFE. **Principais categorias de links maliciosos.** Disponível em: https://www.psafe.com/blog/links-maliciosos/. Acesso em: 30 ago.2023

SILVA, Alexandro. **Dez falhas em segurança da informação.** 2008. Disponível em: http://softwarelivre.org/alexos/blog/dez-falhas-em-seguranca-da-informacao. Acesso em: 16 jun.2020.

UNIVERSIDADE DE BRASÍLIA. Faculdade de Ciência da Informação (Ed.). **Gestão da segurança da informação e comunicações**. Brasília, DF: Faculdade de Ciência da Informação, 2010. 121 p.