ISSN 2358-8829
Conedu VII Congresso Nacional de Educação
Educação como (re)Existência: mudanças, conscientização e conhecimentos.
15, 16 e 17 de outubro de 2020
Centro Cultural de Exposições Ruth Cardoso - Maceió-AL

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NA EDUCAÇÃO PROFISSIONAL DO BRASIL

Mastroianni Rufino de Oliveira [1]
Thomas Victor Rodrigues de Oliveira [2]

RESUMO

A segurança da informação é uma área da ciência da computação, que disponibiliza em seu pilar: a confidencialidade, disponibilidade e integridade, com isso colaborando para uma maior proteção no âmbito da educação digital, pois dados, que trafegam na rede mundial de computadores, tendem a serem monitorados por criminosos e com isto gerando grandes lucros ilicitos e riscos eminente no roubo de dados, atraves do uso da internet. Tendo em vista as crescentes evoluções tecnológicas, que caminham lado a lado, sobre os diversos ataques de malwares em sistemas finais(smartphones, servidores e computadores), tudo o que for dispositivos conectados, torna-se vulnerável. O objetivo da pesquisa é baseado em um estudo de caso, identificando as debilidades dos docentes, discentes e profissionais de ti, sobre a temática da importância da segurança da informação na educação profissional, através de um questionário compostos por sete perguntas, das quais as quatro primeiras, serão abordadas no artigo, e que abrangem alguns assuntos tais quais: o que é a informação, sistemas de informação, segurança da informação, acesso a internet e tipos de ataques, e sendo assim, abrindo a possibilidade no futuro próximo da segurança da informação, ser inserida como disciplina obrigatória na grade curricular do ensino profissional no Brasil. Os resultados foram alcançados, dentro da pesquisa realizada com três grupos de profissionais: docentes(46), discentes(6) e profissionais de ti(5), totalizando(56) pessoas, entrevistadas via formulário online, na plataforma do google docs, no período de 08 de Janeiro a 28 de Fevereiro de 2019, disponibilizado no link https://docs.google.com/forms/d/1DGpJiJRXjqEvjcRh6dl30CHgjDi29QgW_EPl7uWvBHo/closedform.

Palavras-chave: Segurança da informação, Malwares, Internet, Sistemas finais, Educação.

1. INTRODUÇÃO

A rede mundial de computadores conhecida como internet, é um núcleo bastante complexos nos requisitos de sistemas finais, conexões, malwares, dados, equipamentos e demais conexões ocultas aos olhos dos usuários leigos, porém o grande desafio para com a internet dentro do processo de ensino-aprendizado, tornando-os desafiador para

1 **Universidade Estadual do Ceará, Programa de Pós-Graduação em Ciência da Computação (PPGCC), Fortaleza-Ceará, mastroiannioliveira@gmail.com**
2 **Universidade Estadual do Ceará, Programa de Mestrado Profissional em Computação Aplicada (MPCOMP), Fortaleza-Ceará, tthomasvictor@gmail.com**

segurança da informação, assim como existe o processo evolutivo da internet, os perigos reais ficam mais próximos, por usuários não terem o conhecimento necessário para evitar um possível ataque na rede da instituição, em sua residência pela simples abertura de um link ou a execução de um programa malicioso.

A aprendizagem deve ser um direito garantido a todos, não bastam a frequência ou a integração, entendida como a participação efetiva de todos os educandos na dinâmica escolar (CARVALHO, 2016, p.70), o desafio é a garantia da aprendizagem para todos.

De acordo com informações coletadas da pesquisa TIC Domicílios 2019 – mais relevante levantamento sobre acesso a tecnologias da informação e comunicação, realizado pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), vinculado ao Comitê Gestor da Internet no Brasil –, três a cada quatro brasileiros acessam a internet, o que corresponde a 134 milhões de pessoas, que, em regra, utilizam smartphones e outros dispositivos móveis (99%), computadores (42%), TVs (37%) e videogames (9%) (VALENTE, 2020).

A evolução do acesso às tecnologias digitais no cenário atual, existe uma maior facilidade e com isto apresenta-se uma enorme lacuna na educação, pois com esta brecha é propício a abertura de uma vulnerabilidade, que pode ser explorada por cibercriminosos no âmbito dos sistemas informáticos. A artigo foi baseado em um estudo de caso, acerca do problema que temos com a devida carência e ausência da segurança da informação, no processo de ensino aprendizado, tornando-se necessária ter a disciplina de segurança da informação na grade curricular de ensino em nosso País.

Pesquisa disponibilizada na plataforma virtual da google.inc, sobre o uso da ferramenta google forms, gerado um formulário online, abordando algumas perguntas no contexto aplicado da obrigatoriedade da segurança da informação no ensino-aprendizado, a identificação de um possível ataque, o conhecimento sobre a temática em questão.

2. TECNOLOGIA

Já a tecnologia da informação se traduz nas ferramentas tecnológicas utilizadas em um determinado meio (sistema), representada a partir da existência dos *softwares*, vídeo e teleconferências, bem como o uso da *internet*, Walton (1994).

O uso da tecnologia tornou-se cada vez mais frequente na sociedade, inclusive no âmbito escolar. Segundo os Parâmetros Curriculares Nacionais do Ensino Médio (PCNEM) "as tecnologias da comunicação e da informação e seu estudo devem permear o currículo e suas disciplinas" (BRASIL, 1999). E, segundo os Parâmetros Curriculares Nacionais (PCN) é muito importante que os alunos façam uso de computadores como instrumento de aprendizagem escolar, para que possam estar atualizados em relação às novas tecnologias da informação e se instrumentalizam para as demandas sociais presentes e futuras (BRASIL, 1998).

3. A INFORMAÇÃO

A informação é um ativo como qualquer outro ativo importante para o negócio, tem um valor para a organização e consequentemente necessita ser adequadamente protegida (ABNT, 2013).

Segundo Marciano e Lima-Marques (2006), existe uma via de mão dupla entre o contexto social no qual se inserem os sistemas de informação e a sua segurança: a partir do contexto social chega-se à definição dos requisitos necessários à Segurança da Informação. A definição de Segurança da Informação que nos apresentam visa abranger todos os componentes de sua estrutura:

1) os atores do processo (os usuários);

2) o ambiente original de sua atuação (os sistemas computacionais de informação, potencializados pelos recursos tecnológicos);

3) o alcance final dessa mesma atuação (a própria sociedade, mediante o impacto causado pelas modificações introduzidas pela utilização dos sistemas de informação). Além dos três conceitos importantes que foram vistos, existem outros que o padrão internacional ISO 27001 preconiza e que auxilia no entendimento da dinâmica da Segurança da Informação:

a) Risco – combinação da probabilidade de um evento e de suas consequências;

b) Ativos – qualquer coisa que tenha valor para a organização;

c) Ameaças – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

d) Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

e) Agentes ameaçadores – atores responsáveis pelas ameaças.

Conforme Costa e Silva (2009), embora os três pilares sejam importantes para que a SI seja sustentável, é necessária a inclusão do fator humano como um novo princípio, de igual tamanho e responsabilidade. Tais ameaças são:

> *(...) agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização, (SÊMOLA, 2003:47).*

Assim, em contrapartida dentro do processo de ensino educacional, tem grandes possibilidades de no contexto mais informativo, podendo assim abrir a permissão permitindo a todos os envolvidos em inúmeras questões de educação profissional, segurança da informação, ensino, tecnologia digital em tempos da nova era digital, que estamos vivenciando em todos os setores da tecnologia da informação, atribuindo assim uma grande quantidade de perigos oriundos da navegação na internet.

4. SISTEMA DE INFORMAÇÃO

Na sua execução, os sistemas de informação trabalham com três elementos de grande valor, que devem ser diferenciados, para melhor atenderem as necessidades dos componentes de entrada, processamento e saída (TURBAN, 2003), que são (Figura 0):

1) Dados – são fatos, ou descrições básicas de eventos, atividades e transações que são capturados, registrados, armazenados e classificados, porém, não são organizados.

2) Informação – conjunto de fatos, ou seja, dados organizados com significado para o usuário final.

3) Conhecimento – conjunto de informações organizadas e processadas prontas para transmitir discernimento, experiências e habilidades que podem ser aplicadas a um problema ou decisão gerencial.

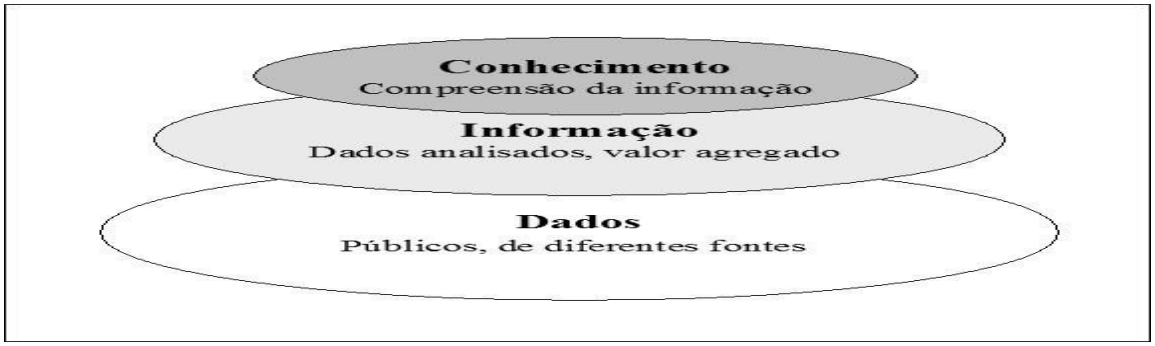

Figura 0 – Conhecimento, informação e dados.

https://www.google.com.br/search?q=-+Dado+,+Informa%C3%A7%C3%A3o+e+Conhecimento&rlz=1C1HLDY_pt-BRBR796BR796&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiZp6Ph2c3eAhWIvZAKHSKJBD8Q_AUIDigB&biw=1360&bih=667#imgrc=Jcy-3FJlg7dLwM /> Acessado em 19 de Agosto de 2020.

5. A SEGURANÇA DA INFORMAÇÃO.

A segurança da informação é uma forma de garantir que a informação seja disponibilizada aos demais mediante autorização de acesso, para seus verdadeiros fins, evitando o roubo de dados. Para Schneier (2001);

> *Para Schneier (2001), as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados." O crime no ciberespaço inclui tudo o que se pode esperar do mundo físico: roubo, extorsão, vandalismo, voyeurismo, exploração, jogos de trapaças, fraude etc.*

A segurança da informação em sua amplitude de conhecimento, ela é gerida por três grandes pilares importantes: confidencialidade, integridade e disponibilidade.

A confidencialidade é Segundo Diógenes Yuri e Mauser Daniel (2013, p03), trata se da prevenção do vazamento de informação para usuários ou sistemas que não estão autorizados a ter acesso a tal informação. Um exemplo disto é quando seu número de cartão de crédito vaza para outras fontes que não tinha autorização de ter aquele número. Neste momento a confidencialidade da sua informação foi comprometida.

A integridade é Segundo Diógenes Yuri e Mauser Daniel (2013, p03), trata se da preservação manutenção do dado de uma forma íntegra, ou seja, sem sofrer modificações através de fontes não autorizadas. Um exemplo de integridade é quando você transmite uma mensagem para alguma pessoa e no meio do caminho essa

mensagem é adulterada e o conteúdo, modificado. Neste momento houve um comprometimento da integridade da mensagem por uma fonte não autorizada.

A disponibilidade é Segundo Diógenes Yuri e Mauser Daniel (2013, p03), trata-se da manutenção da disponibilização da informação, ou seja, a informação precisa estar disponível quando se necessita. Um exemplo de disponibilidade seria quando você tenta fazer uma transação bancária e ao tentar efetuar a mesma o sistema encontra se indisponível. Neste momento de disponibilidade do serviço que fornece acesso a informação desejada.

6. ACESSO DA INTERNET

Segundo (Cert.br, 2018), temos alguns riscos quanto ao acesso à internet:

Acesso a conteúdos impróprios ou ofensivos: ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.

Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.

Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação.

Invasão de privacidade: a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serão repassadas. Além disto, os *sites* costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.

7. TIPO DE ATAQUES

Na internet diariamente é inserido malwares em computadores e na rede de sistemas, através de códigos maliciosos, pondo em risco os dados e a própria vida de usuários desprovidos de conhecimento básico de segurança da informação. Sera citado pela (Cert.br, 2018), alguns eventos, porém existem outras formas ilícitas.

Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Dos: (DoS --*Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

8. A EDUCAÇÃO PROFISSIONAL

A inovação tecnológica causou de certa forma positivamente, grandes mudanças irreversíveis dentro do processo educativo, e sendo assim as escolas necessitam se adequar aos novos tipos de saberes adivinhos da cultura digital, pois são frequentadas por jovens que nasceram em era de transformações e evoluções tecnológicas. Segundo Marinho (2008), com o progresso tecnológico a escola passa a ter a finalidade de formar cidadãos para uma sociedade tecnologicamente desenvolvida.

Assim, de acordo com Queiroz, Braga e Leick (2008, p5):

> "*Os educadores estão sendo desafiados a mudar e a inovar com o intuito de atender as expectativas da atual sociedade. Mudar para adquirir novas técnicas metodológicas capazes de transformarem o espaço-escola do aprendiz em algo dinâmico, significativo e participativo, aproximando a teoria da prática com uma postura interdisciplinar, permitindo assim a criação de destrezas para com a vida.).* Queiroz, Braga e Leick (2008, p5).

Em nosso país tivemos um grande avanço no início da década de 1990, com a aprovação da lei de diretrizes e bases, que outorgada abriu caminho para um melhor forma de educação do nosso povo e com uma possível qualidade no ensino, e abrangendo todas os grupos de pessoas para com a educação nacional.

Segundo a LDB 9394/96, a educação brasileira é dividida em dois níveis: a educação básica e o ensino superior. Porém é citado neste artigos referentes dois pontos importantes, tais quais:

1) Educação Profissional e Tecnológica – Visa preparar os estudantes a exercerem atividades produtivas, atualizar e aperfeiçoar conhecimentos tecnológicos e científicos.

2) LDB 9394/96 aborda temas como os recursos financeiros e a formação dos profissionais da educação.

Segundo(LDB,1996) é a mais importante lei brasileira que se refere à educação. Esta lei foi aprovada em dezembro de 1996 com o número 9394/96, foi criada para garantir o direito a toda população de ter acesso à educação gratuita e de qualidade, para valorizar os profissionais da educação, estabelecer o dever da União, do Estado e dos Municípios com a educação pública.

9. METODOLOGIA

Baseado no estudo de caso, foi possível realizar a coleta de informações, pertinentes as cincos perguntas realizadas, nos seguintes aspectos da importância da segurança da informação no cenário educacional profissional para esta nova era digital, o saber solucionar um ataque cibernético na instituição de ensino, o interesse em aprender sobre a SI (Segurança da Informação), o Mec ajuda a difundir a segurança da informação na educação e a preparação dos docentes, para este cenário.

Bruyne, Herman e Schoutheete (1977, 251p) afirmam que o estudo de caso justifica sua importância por reunir informações numerosas e detalhadas que possibilitem apreender a totalidade de uma situação.

10. RESULTADOS E DISCUSSÃO

No requisito da primeira pergunta aos grupos entrevistados, sobre a importância da segurança da informação, como disciplina no ensino profissional, e sobre a obrigatoriedade no cenário educacional. Segundo a visão da norma NBR ISO/IEC 2700:2019, a ação convém que a atividade ou condição que dá origem a um determinado risco seja evitada (ABNT,2019, p24).

Figura 01 – A segurança da informação como disciplina no ensino profissional

Fonte: Elaborada pelo Autor

A necessidade de termos a segurança da informação, como disciplina obrigatória, faz-se jus devido ao grande avanço da rede mundial de computadores, pois na medida do avanço tecnológico, surge os ataques cibernéticos orquestrados, por hackers do mal. Os entrevistados têm a consciência da necessidade desta disciplina, no cenário educacional é de(100%)(Figura 01), enquanto que(71%)(Figura 02), sabem a real importância da segurança da informação, para o ensino profissional.

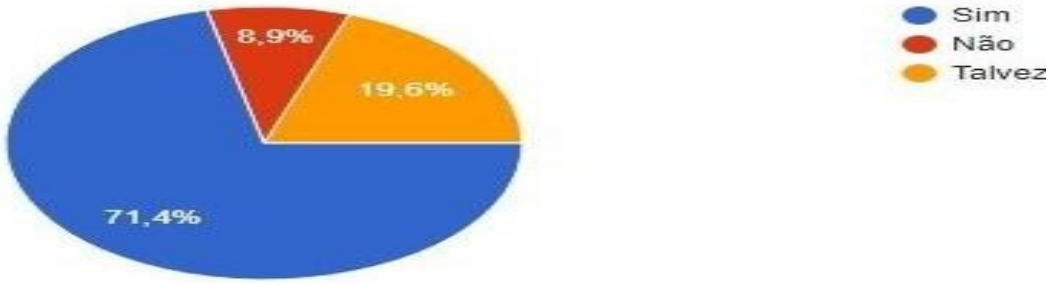

Figura 02 - Você sabe a importância da segurança da informação para o ensino profissional
Fonte: Elaborada pelo Autor

O cenário da desinformação sobre a importância da segurança da informação, ainda é um grande lacuna(8,9%)(Figura 02), e tabu em sua propagação nos meios de comunicação acadêmicos, devido a esta debilidade, que gera ainda dúvidas que são em torno de(19,6%)(Figura 02), entre os entrevistados. Segundo (Fortinet, 2019), temos uma grande quantidade de (9 Bilhões), de tentativas de ataques cibernéticos, e um aumento contínuo de malware, explorações e atividades de botnet na América Latina e no Caribe .

Devido a esta debilidade que é de(19,6%)(Figura 02), que talvez saibam a real importância da segurança da informação, para o ensino profissional, porém numero pequeno e preocupante, em comparativos a fatia de 09 Bilhões de tentativas em 2019, encontra-se o Brasil, ranking negativo.

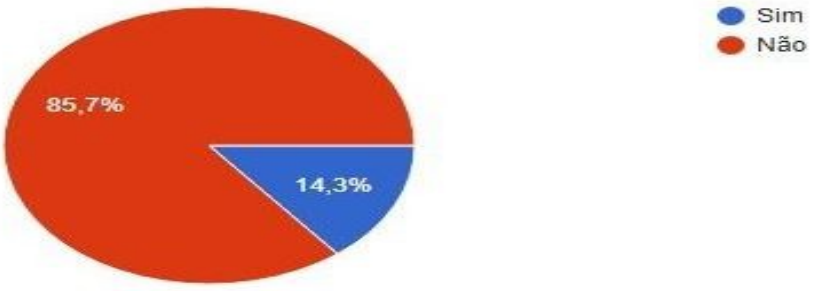

Figura 03 - Caso sua instituição de ensino, sofresse um ataque de hackers em sua rede

Fonte: Elaborada pelo Autor

Nos dados obtidos do relatório(Fortinet, 2019), como estamos sitiados na América Latina, ocorrer que(85,7%)(Figura 03), dos entrevistados relatam este problema de propagação da SI, na educação profissional no Brasil.

Figura 04 - Tem interesse em aprender sobre a segurança da informação no ensino profissional

Fonte: Elaborada pelo Autor

Mesmo assim ainda é mínima, a atuação do governo, para mudar a realidade no cenário educacional no Brasil. Conforme os relatos dos entrevistados, ensino profissional(8,9%)(Figura 01), ainda não o sentido real de conhecer este conhecimento protetor, que é a segurança da informação e em contrapartida, tornar-se mais agravante é saber que temos(1,8%)(Figura 04), o tem o desinteresse é saber esta pratica educacional de proteção aplicada em todo o cenário mundial, e é a partir deste dado, que pode surgir uma possibilidade no futuro de inserir a segurança da informação, como disciplina obrigatório no ensino profissional, pelo Mec.

Isto significa que o interesse dos grupos entrevistadas, ocasionou na seguinte pergunta aos grupos sobre se “Suas informações estão expostas na internet, e aprender

como aplicar a segurança da informação, retornaria algum benefício, para proteção destes dados(98,2%)(Figura 04), gerando um grande benefício, frente a mitigação dos dados negativos(Fortinet, 2019).

11. CONSIDERAÇÕES FINAIS

Os resultados foram alcançados na contribuição da pesquisa para os envolvidos, referentes ao ensinamento sobre segurança da informação, e na abertura deste processo para conscientização na nossa educação profissional, para que todos tenham o benefício deste aprendizado que impacta na vida pessoal, profissional e academica.

A ausência da disciplina de segurança da informação, geram danos e riscos irreparáveis, principalmente na vida das pessoas. A maioria dos entrevistados, tem a necessidade e querem aprender, sobre segurança da informação, para assim poder discerminar e a usar para sua própria proteção, e reduzindo os ataques cibernéticos, oriundo de algum tipo de arquivo malware, que em sua maioria vindo da internet. As políticas publicas voltada para o educação profissional, adotada pelo do MEC, ainda precisa melhorar muito, para alavancar e sermos referência em educação profissional.

12. REFERÊNCIAS

ABNT. **Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança:** ABNT NBR ISO/IEC 27002:2013. 1. Ed. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS. **NBR ISO/IEC 2005:2019. Tecnologia da informação – Técnicas de segurança - gestão da segurança da Informação.** Rio de Janeiro: ABNT, 2019.

BRASIL. Ministério da Educação, Secretaria de Educação Média e tecnológica. **Parâmetros Curriculares Nacionais**: Ensino Médio. Brasília: Ministério da Educação, 1999.

BRASIL. Ministério da Educação. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais: Ciências Naturais. (3º e 4º ciclos do ensino fundamental).** Brasília: MEC, 1998.

BRASIL, **Lei de Diretrizes e B. Lei nº 9.394/96**, de 20 de dezembro de 1996.

BRUYNE, P.; HERMAN, J.; SCHOUTHEETE, M. **Dinâmica da pesquisa em ciências sociais: os pólos da prática metodológica**. Rio de Janeiro: F. Alves, 1977. 251p.

CARVALHO, Rosita Edler. **Educação Inclusiva: com os pingos nos "is". 11.** ed. Porto Alegre: Mediação, 2016.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança para a Internet.** Disponível em: <https://cartilha.cert.br/seguranca/>. Acesso em: 20 de Agosto de 2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança para a Internet.** Disponível em: <https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html /> Acessado em 25 de Agosto de 2020.

COSTA, Veridiana Alves de Sousa Ferreira.; SILVA, Maicon Herverton Lino Ferreira da. **O fator humano como pilar da Segurança da Informação: uma proposta alternativa. 2009. IX Jornada de Ensino Pesquisa e Extensão (JEPEX) da UFRPE**. Disponível em: <http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf>. Acesso em: 19/08/2020.

DIÓGENES, Yuri; MAUSER, Daniel. **Certificação security +, da pratica para o exame syo-301.** 2. Ed. Rio de Janeiro: Novaterra, 2013.

MARCIANO, João Luiz.;LIMA-MARQUES, Mamede.**O enfoque social da segurança da informação**. Ciência da Informação, v. 35, p. 89 – 98, 2006. ISSN 0100-1965.

QUEIROZ, Tânia D.; BRAGA, Márcia M. V.; LEICK, Elaine Penha. **Pedagogia de Projetos Interdisciplinares.** São Paulo: Rideel, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva da segurança da informação.** Rio de Janeiro: Elsevier, 2003.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001.

WALTON, Richard E. *O **uso de TI pelas empresas que obtêm vantagem competitiva, tecnologia de informação***. São Paulo, Atlas, 1994.

TURBAN, Efraim; RAINER, K. R.; POTTER, JUNIOR., R. E. **Administração de Tecnologia da informação.** Tradução de Tereza Cristina Felix de Souza. Rio de Janeiro: Elsevier, 2003.

VALENTE, Jonas. **Brasil tem 134 milhões de usuários de internet, aponta pesquisa**. Agência Brasil, Brasília, 26 de maio de 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/**brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa**/>. Acesso em: 20 de Agosto de 2020.

https://www.fortinetthreatinsiderlat.com/pt/**Q4-2019/BR/html/trends/**>.Acessado em 23 de Agosto de 2020.