SEGURANÇA DA INFORMAÇÃO NO CONTEXTO ESCOLAR

Douglas da Silva Santos [1]; Luís Henrique de A. Gomes [1]; Victor Hugo de Carvalho Santana[1]
Damon Ferreira Farias [2]

RESUMO

O uso das tecnologias está cada vez mais crescente em nossa sociedade, desde uso pessoal até as aulas remotas ela se faz presente, porém os riscos ao utilizá-la são desconhecidos. Dessa forma, este trabalho teve como objetivo analisar e informar aos alunos sobre o gerenciamento dos dados pessoais, alertando sobre o perigo do mau uso de ferramentas de armazenamento e controle de dados no meio tecnológico. O estudo é do tipo exploratório e utilizou formulário eletrônico para coletar as informações, devido ao distanciamento imposto pela pandemia da Covid-19. Os resultados apontam que são necessárias maiores reflexões dos pibidianos, sobre segurança da informação, especialmente na criação e proteção de senhas. Ainda, é importante salientar que grande parte dos discentes conhecem sobre as formas existentes de proteção. Contudo, verifica-se que é essencial que os discentes entendam mais sobre a segurança da informação, para assim poder disseminar e a usar para sua própria proteção, e reduzir os ataques cibernéticos, oriundo de algum tipo de arquivo *malware*, que em sua maioria vindo da internet.

Palavras-chave: Dados pessoais. Educação. Riscos. Segurança da Informação. Tecnologia.

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 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 (GONÇALVES, 2021).

[1] Graduando do Curso de Licenciatura em Ciências da Computação do Instituto Federal de Educação, Ciência e Tecnologia Baiano, Campus Senhor do Bonfim, (douglasifbaianosb@email.com; lubizinho-2001@hotmail.com; victorhugofny@gmail.com)
[2] Professor orientador: Doutor em Ciencia e Engenharia dos Materiais, Universidade Federal de Sergipe - UFS, damon.farias@enova.educacao.ba.gov.br.

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, é possível perceber que, embora 98% das escolas tenham acesso à Internet, a quantidade de equipamentos conectados é pequena. O estudo indica que apenas 57% das escolas públicas possuíam acesso à Internet na sala de aula. Devido à baixa qualidade não permitir o acesso simultâneo para as equipes administrativas, pedagógicas e para os alunos, a conexão de Internet estava, em grande parte dos casos, direcionada para as áreas administrativas. A pesquisa também relata que na maior parte das vezes, os professores também utilizam sua própria conexão 3G ou 4G para a realização dessas atividades (frequência online, notas, entre outras): 27% dos professores usaram o WiFi da escola e 49% usaram o 3G ou 4G do próprio celular. Ainda de acordo com a pesquisa, 10% dos alunos utilizaram o *WiFi* da escola e 27% utilizaram o 3G ou 4G do próprio celular para realizar atividades em sala. No entanto, os aspectos ligados à infraestrutura ainda são apontados como os principais desafios para a efetivação do uso das tecnologias nas escolas, especialmente nas instituições da rede pública de ensino. O aumento do número de computadores por aluno (28%) e da velocidade da Internet (17%) permanecem como as ações prioritárias para integrar o uso das tecnologias nas práticas pedagógicas, segundo os diretores de escolas públicas (CGI.br, 2019). Mesmo com a evolução dos meios de comunicação e a popularização do computador e da internet, os recursos didáticos mais utilizados nas escolas públicas para o ensino são aulas teóricas, lousa e pincel (CGI.br, 2019).

Além disso, as escolas lidam com informações e dados sigilosos em grande parte de sua rotina. Os dados de alunos e suas famílias, funcionários, colaboradores e fornecedores estão registrados nos arquivos do sistema e precisam ter a sua segurança e privacidade garantidas. Assim, a segurança da informação nas escolas é uma questão importante de ser planejada, pois o uso da tecnologia tornou-se cada vez mais frequente no cenário atual, inclusive no âmbito escolar, uma vez que o acesso à internet, o compartilhamento em rede, o uso de redes sociais e acesso à informação são realidades que trouxeram inúmeros benefícios à sociedade (MASCARENHAS E ARAÚJO, 2019; PEIXOTO, 2006).

Nesse sentido, a Base Nacional Comum Curricular (BNCC) do ensino médio aborda temas de tecnologia e computação de forma transversal em todas as áreas do conhecimento, considerando uma perspectiva interdisciplinar. Além disso, a competência geral número 1 fala na valorização de conhecimentos construídos nos mundos físico, social, cultural e digital, enquanto a número 2 ressalta a importância de fomentar nos/nas estudantes a resolução de problemas e a criação de soluções (inclusive tecnológicas). Notadamente, a competência geral número 5 explicita a necessidade de trabalhar com o tema de tecnologias digitais de informação e comunicação (TDIC), colocando os/as estudantes como aprendizes ativos e criativos – e não apenas consumidores passivos de tecnologias:

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva BRASIL (2018, p.9).

Portanto, neste trabalho, o objetivo foi analisar e informar aos alunos sobre o gerenciamento dos dados pessoais, alertando sobre o perigo do mau uso de ferramentas de armazenamento e controle de dados no meio tecnológico.

METODOLOGIA

A pesquisa é do tipo exploratória, assumindo uma abordagem qualitativa no tratamento dos dados coletados. Para Gil (2002) e Vieira (2002), a pesquisa exploratória tem por objetivo favorecer uma maior proximidade com o tema, tornando-o mais claro, além de propiciar ao pesquisador maior intimidade com o assunto, possibilitando a compreensão do problema. A abordagem qualitativa deste estudo se mostra pertinente aos objetivos deste trabalho.

Para a coleta de dados, utilizou-se um formulário com questões desenvolvido na plataforma *Google Forms*. A opção pelo uso do meio eletrônico para a construção e divulgação do formulário teve como principal motivador o cenário de necessário distanciamento social trazido pela pandemia do Covid-19. O formulário obteve um conjunto amostral de 20 respondentes. É importante destacar que o formulário foi liberado aos estudantes ao final da oficina e somente àqueles que manifestaram interesse responderam. Participaram da pesquisa estudantes voluntários do terceiro ano do Ensino Médio, regularmente matriculados no ano 2021.

O formulário foi organizado com perguntas objetivas e teve o intuito de analisar os seguintes pontos: *(i)* critérios do usuário ao criar senhas; *(ii)* vazamento de dados; e *(iii)* ataques e problemas envolvendo dados pessoais.

REFERENCIAL TEÓRICO

As tecnologias da informação estão acessíveis a todos os usuários que delas precisam, sob alguma circunstância. Por isso, é essencial que todas as pessoas envolvidas com tecnologias, tenha plenos conhecimentos sobre o assunto e estejam aptos a lidarem com os mais variados meios tecnológicos, pois, hoje, a sociedade está cada vez mais se adequando ao uso de tecnologias que potencializam a administração dos dados pessoais, mas o importante não é apenas o acesso a essas tecnologias, mas a otimização do uso dessas tecnologias. Com isso, verifica-se que é fundamental ter uma segurança da informação sólida, pois ter eficiência nos seus três pilares que são a integridade, disponibilidade e confidencialidade, tornou-se indispensável para continuidade de negócio da organização, pois a mesma depende consideradamente das informações armazenadas ao longo de seu funcionamento para realização dos seus processos corriqueiros (SÊMOLA, 2014; RIBEIRO, 2016).

Entretanto, a segurança da informação é um tema muito abrangente, pois trata da proteção física, tecnológica, conscientização organizacional, e cada uma dessas áreas tem suas ameaças, vulnerabilidades e riscos, gerando assim desafios constantes (HINTZBERGEN, 2018; MASCARENHAS E ARAÚJO, 2019). Proteger a informação contra esses desafios é de suma importância na organização, sendo assim, o desenvolvimento de uma boa política de segurança da informação torna-se vital no ambiente corporativo, pois com ela você consegue criar normas e diretrizes para assegurar que as informações estejam seguras (RIBEIRO, 2016; MASCARENHAS E ARAÚJO, 2019).

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.

> Segurança da informação é definida como “[...] uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizado, alterações indevidas ou sua indisponibilidade.” (SÊMOLA, 2014, p. 41).

Hintzbergen *et al.* (2018) a Segurança da Informação (SI) é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Lyra (2008) enfatiza que a segurança da informação é obtida com a implementação de um conjunto de controles adequados que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles, além de implementados, precisam ser estabelecidos, monitorados, analisados criticamente e melhorados onde for necessário, para garantir que os objetivos do negócio e da segurança da organização sejam atendidos.

RESULTADOS E DISCUSSÃO

Este estudo apresentar, os aspectos sobre o gerenciamento dos dados pessoais, alertando sobre o perigo do mau uso de ferramentas de armazenamento e controle de dados no meio tecnológico. Embora tenha a identificação de “Escola do Campo”, é importante destacar que o colégio baiano não trabalha com a Pedagogia da Alternância. Assim, a organização curricular, a distribuição das séries e o calendário escolar são organizados conforme a maioria das escolas brasileiras: currículo estruturado em disciplinas específicas, calendário com aulas de março a dezembro, com recesso escolar em junho. De maneira a tornar a leitura mais fluida, trataremos a instituição de ensino como rural.

A escola rural, atende estudantes da comunidade de Tuiutiba, distrito pertencente ao Município de Campo Formoso, interior da Bahia, além de estudantes de povoados circunvizinhos. O município se localiza na região norte do estado baiano e dista 401 km da capital. Os estudantes da unidade Tuiutiba possuem perfil socioeconômico diversificado; porém, boa parte de suas famílias se encontra cadastrada no programa Bolsa Família do governo federal, o que aponta para o fato de ser uma comunidade predominantemente formada por famílias de baixa renda *per capita*.

Nas turmas ofertadas no turno vespertino, os estudantes possuíam média de idade entre 15 e 17 anos. A unidade contava com cinco salas de aula, cantina, secretaria e sala dos professores. De acordo com Censo Escolar 2019, a escola rural, contava com aproximadamente 200 estudantes na etapa do Ensino Médio.

As senhas permitem a autenticação do usuário quando do acesso às suas contas nas mais diversas plataformas e dispositivos eletrônicos no meio corporativo, garantindo que apenas pessoas autorizadas tenham acesso a determinados equipamentos e informações, validando a identidade e autenticando o usuário para assegurar sua legitimidade de acesso.

Diante da relevância da utilização adequada das senhas para a proteção de informações, é fundamental a escolha e utilização de senhas seguras em suas contas e dispositivos eletrônicos, sendo recomendável a atuação das empresas no sentido de exigi-las em todas as ferramentas corporativas.

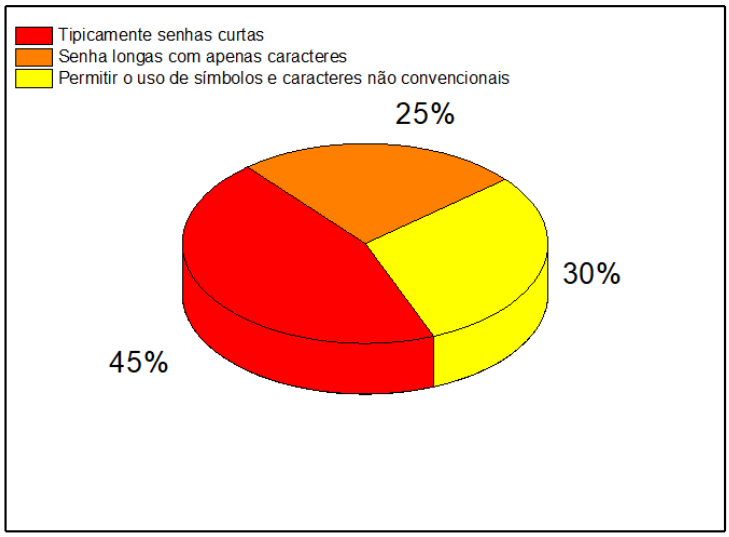
Então, como pode-se observar na Figura 1, os respondentes foram questionados sobre critérios para definir uma senha e verifica-se que apenas 30% utilizam senhas fortes (com caracteres e símbolos) 45% usam senhas curtas que podem ser definidas como fracas, dessa forma os dados do usuário ficam mais desprotegidos e 25% utilizam senhas longas com apenas caracteres, isso pode ser definido como uma senha básica mas que ainda pode ser quebrada, basta o cibercriminoso fazer uma pesquisa sobre o alvo e ele pode encontrar sua senha facilmente. Com relação à elaboração de senhas:

> Muitos usam como senha, palavras que existem em todos os dicionários, seus apelidos, ou até mesmo o próprio nome que, com um software gerenciador de senhas, é possível decifrá-las em segundos. (VIRINFO, 2002 apud POPPER; BRIGNOLI, 2003, p. 4).

Por outro lado, uma senha forte será aquela composta por uma sequência aleatória de caracteres (ALVES, 2010). Com isso, conclui-se que 30% dos respondentes estão mais protegidos por usarem senhas fortes e 70% estão mais expostos a ataques uma vez que utilizam senhas fracas e básicas, pois o uso de senhas fracas, incluindo o uso da mesma senha para acessar várias contas, enfraquece nossa segurança e pode representar sérios riscos à nossa privacidade.

Figura 1. Critérios do usuário para criação de senhas.

Para definir uma senha, qual desses critérios você segue?

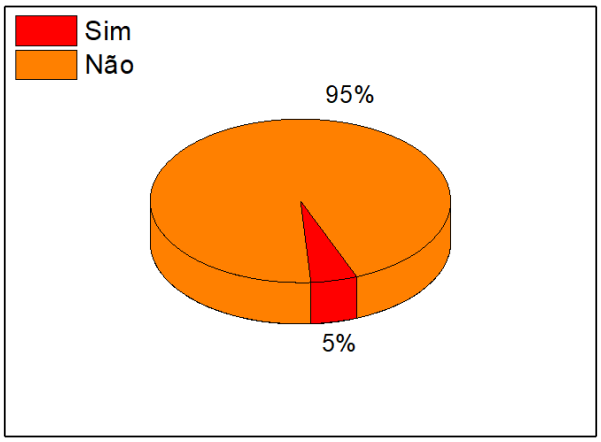


Fonte: Elaborada pelos autores

A Figura 2 mostra como os usuários lidam com seus dados. Pode-se observar que 95% dos respondentes afirmaram que nunca forneceram informações sigilosas por telefone. Esses dados revelam que grande parte dos discentes conhecem sobre as formas existentes de proteção usuário pode tomar atitudes mais seguras para navegar na internet e proteger seus dados. Mas, por outro lado, entende-se que 5% dos respondentes forneceu algum tipo de dado sigiloso por telefone indicando não possui boas práticas de segurança de dados. Essa falta de conhecimento sobre segurança da informação pode ser prejudicial ao usuário devido ao vazamento de informações, fraudes e roubos.

Figura 2. Vazamento de dados.

Já forneceu informações sigilosas por telefone?



Fonte: Elaborada pelos autores

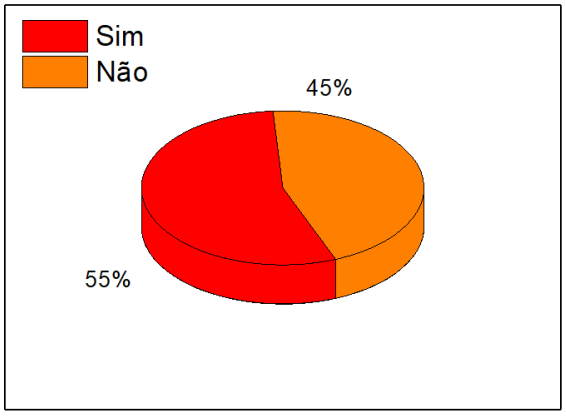
Alguns dos maiores erros cometidos dentro do ambiente corporativo que aumentam potencialmente o risco de se tornar uma vítima da engenharia social: (PEIXOTO, 2006)

> Mencionar senha por telefone é um erro gravíssimo, pois antes de disponibilizar qualquer tipo de informação, deve-se saber com quem se fala e de onde fala, além de conferir através de aparelhos identificadores de chamada se o telefone de origem da ligação está realmente batendo com o mencionado. Também é importante conferir o motivo pelo qual solicitaram determinada informação.

Por outro lado, na Figura 3, observa-se que 55% dos respondentes costumam deixar senhas pessoais gravadas nos dispositivos eletrônicos. Esses dados apresentam um risco a privacidade dos respondentes caso o celular seja furtado ou perdido.

Figura 3. Vazamento de dados.

Você costuma deixar senhas pessoais gravadas nos dispositivos eletrônicos?



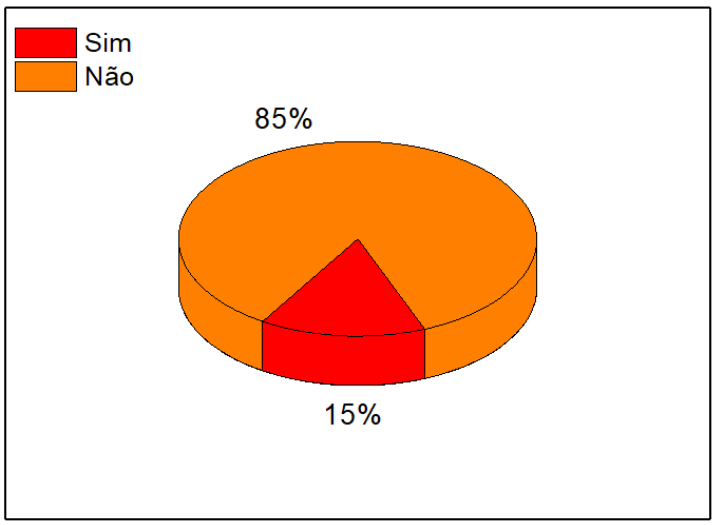
Fonte: Elaborada pelos autores

Por fim, na Figura 4, observa-se os dados sobre o envolvimento dos entrevistados com problemas de perda de dados e ataques cibernéticos. Verifica-se que 85% dos respondentes não caíram em nenhum tipo de ataque cibernético, porém, 15% dos entrevistados responderam que já foram vítimas de fraudes, por esse motivo é essencial que os discentes entendam mais sobre a segurança da informação, para assim poder disseminar e a usar para sua própria proteção, e reduzir os ataques cibernéticos, oriundo de algum tipo de arquivo *malware*, que em sua maioria vindo da internet.

Santos *et al* (2010), em seu trabalho verificou o conhecimento dos colaboradores quanto à segurança da informação no ambiente corporativo da Faculdade Santo Agostinho, cujos resultados apontaram para a necessidade dos colaboradores priorizarem a segurança dos dados e a falta de conhecimento da importância das

informações. Ainda, segundo o estudo 89% dos respondentes sentem necessidade de receber informações sobre a segurança da informação.

Figura 4. Ataques e problemas envolvendo dados pessoais.



Fonte: Elaborada pelos autores

Ao final da oficina, utilizou-se a metodologia do *Design Thinking* [Vianna et al. 2012] apoiada pela ferramenta digital *Mentimeter* na qual, utilizando seus dispositivos móveis, os docentes compartilharam suas visões sobre a oficina ministrada.

Figura 5. Nuvem de palavras

CONSIDERAÇÕES FINAIS

Durante a oficina, foi possível observar o grau de conhecimento dos respondentes em relação à segurança da informação, principalmente sobre os riscos ao usar de forma despreparada os recursos tecnológicos.

O estudo também concluiu que para proteger a informação, é necessário aumentar o conhecimento sobre segurança da informação e mostrar sua importância para os discentes. Além disso, a oficina foi relevante e contribuiu para que eles estejam sempre alertas a ataques cibernéticos.

Ainda, é possível reconhecer que a oficina permitiu ao futuro professor o contato com o ambiente escolar, na perspectiva de desenvolver um olhar atento sobre o processo didático, o planejamento docente, sendo possível vivenciar situações concretas de ensino e aprendizagem mesmo que remotamente, pois este possibilitou dar mais protagonismo, já que observou-se, o crescimento pessoal por meio do amadurecimento, aumento da autoconfiança e profissional, através da apresentação.

Por fim, está oficina contribui para a capacitação dos discentes desenvolvendo competências necessárias para que possam tomar decisões e saberem agirem diante dos riscos, ou até mesmo após um incidente, pois estarão aprendendo a usar a *web* com segurança e confiabilidade.

AGRADECIMENTOS

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pelo financiamento do projeto e pela concessão das bolsas.

Ao Colégio Estadual do Campo de Campo Formoso e seus gestores, por serem parceiros das atividades do PIBID.

REFERÊNCIAS

ALVES, CÁSSIO BASTOS. **Segurança da Informação vs. Engenharia Social: Como se proteger para não ser mais uma vítima**. Brasília, 2010.

BRASIL. Comitê Gestor da Internet no Brasil – **CGI.br.** (2018). Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2017. São Paulo: CGI.br.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Disponível em http://basenacionalcomum.mec.gov.br/images/historico/

BNCC_EnsinoMedio_embaixa_site_110518.pdf. Versão final homologada do Ensino Médio em 20/12/2018. Acesso em: jun. de 2021.

COSTA, JORGE ADELINO; ROQUE, ALBERTO. **A GESTÃO DA INFORMAÇÃO NO CONTEXTO DA GESTÃO ESCOLAR**. Porto, 2005.

GIL, ANTÔNIO CARLOS. **Métodos e Técnicas de Pesquisa Social**. 6 ed. São Paulo: Editora Atlas, 2002.

GONÇALVES, MARIA CÉLIA DA SILVA; JESUS, BRUNA GUZMAN DE. **Educação Contemporânea** - Volume 20. Belo Horizonte – MG: Poisson, 2021.

HINTZBERGEN, JULE et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**, 2018. Brasil: Brasport.

LYRA, MAURÍCIO R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

MASCARENHAS NETO, PEDRO TENÓRIO; ARAUJO, WAGNER JUNQUEIRA. **SEGURANÇA DA INFORMAÇÃO: Uma visão sistêmica para implantação em organizações**. João Pessoa: Editora da UFPB, 2019.

PEIXOTO, MÁRIO C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

POPPER, MARCOS ANTONIO; BRIGNOLI, JULIANO TONIZETTI. **ENGENHARIA SOCIAL: Um Perigo Eminente.** [2003]. 11 f. Monografia (Especialização)– Gestão Empresarial e Estratégias de Informática, Instituto Catarinense de Pós-Graduação – ICPG, [S.l.], [2003]. Disponível em: https://www.academia.edu/38720641/ENGENHARIA_SOCIAL_Um_Perigo_Eminente . Acesso em: 30 jun. 2021.

RIBEIRO, CRISTIANO DA SILVA. **Segurança da Informação: o desenvolvimento de uma política de segurança da informação em conformidade com a norma ABNT ISO/IEC 27002.** Ano 2016. Trabalho de Conclusão de Curso de Sistema de Informação – FAIR Faculdades Integradas de Rondonópolis, 2016.

SANTOS, EDENILZA PEREIRA; MOURA, EULENE CRUZ; SILVA, JANDIRA DE MORAIS. Segurança da Informação: como garantir a integridade, a confidencialidade e a disponibilidade das informações em uma organização educacional privada de Teresina. **Revista Científica da FSA** - Teresina - Ano VII - n° 7 / 2010

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva** - 2 ed. São Paulo: Elsevier, 2014.

VIANNA, M.; VIANNA, Y.; ADLER, I.K; LUCENA, B; RUSSO, B. (2012). "**Design Thinking: Inovação em Negócios**". Rio de Janeiro: MJV Press.

VIEIRA, VALTER AFONSO. As tipologias, variações e características da pesquisa de marketing. Curitiba, **Revista da FAE**, v.5, p.65-70, jan./abr. 2002.