Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Segurança da informação em Internet Banking

Marcos Roberto Cardoso Junior

Ricardo Bueno Pavan

Alberto Martins Junior (Orientador)

RESUMO. Com o aumento de pessoas utilizando serviços bancários devido ao grande avanço tecnológico, este artigo apresenta métodos que são utilizados para manter a segurança de dados, em aplicativos bancários via *Internet Banking*. A metodologia que foi usado nesse artigo, foram os métodos de pesquisa e análise qualitativa. Foi definido como a segurança da informação é importante para as pessoas e para as empresas no dia a dia e com isso apresenta-se os princípios básicos da segurança da informação. O *Internet Banking* é um dispositivo bancário utilizado através da *internet*, cada instituição bancária possui o seu, podendo ser acessado através de computadores ou celular. Os principais problemas da segurança no *Internet Banking* apresentado nesse artigo, são o spam que é uma mensagem de e-mail com ato malicioso, o scam que é uma versão aprimorada do spam onde é enviado e-mail em massa, phishing scam onde a vítima é direcionada para uma página falsa na *internet* e o *pharming* que é parecido com o *phishing scam*, mas tem o objetivo de direcionar para as instituições financeiras falsas. Os métodos apresentados neste artigo apontam para utilizar computador ou celular confiável, ter um bom antivírus em seus dispositivos, acessar sites seguros, sempre utilizar o endereço oficial do banco, não se conectar em redes públicas, utilizar senhas fortes, não acessar *e-mails* desconhecidos e ter cuidado com o uso do *token* que o banco disponibiliza.

Palavras-chave: Segurança de dados; *Internet Banking*; Aplicativos bancários

ABSTRACT. Through increasing people's using banking services due to the great technological advancement, this article presents methods that are used to maintain data security, in banking applications via Internet Banking. The methodology that was used in this article, were the methods of research and qualitative analysis. It was defined how information security is important for people and companies on a day-to-day basis and thus introduces the basic principles of information security. Internet Banking is a banking device used over the internet, each bank has its own, and can be accessed through computers or cell phones. The main Internet Banking security problems presented in this article are spam, which is an e-mail message with

a malicious act, scam which is an enhanced version of spam where mass email is sent, phishing scam where the victim is it is directed to a fake internet page and pharming which is similar to phishing scam but aims to target fake financial institutions. The methods presented in this article aim to use a reliable computer or cell phone, have a good antivirus on your devices, access secure websites, always use the bank's official address, do not connect to public networks, use strong passwords, do not access unknown e-mails and be careful about using the token that the bank makes available.

Keywords: Database security; Internet Banking; Banking applications

1. Introdução

Que a informação é um bem valioso para as pessoas e empresas isso já é consenso há um bom tempo. Assim, dispositivos de Segurança da Informação são essenciais para neutralizar as ameaças e vulnerabilidades que os usuários de sistemas estão sujeitos, principalmente quando se fala em uso de aplicativos de bancos, comércio eletrônico entre outros.

Dessa forma, verifica-se o grande avanço da tecnologia e o aumento do uso da *internet*, com isso as organizações de todas as áreas foram forçadas a se adequar a esse novo momento tecnológico. Com esse aumento, as instituições financeiras foram incentivadas a fornecer seus serviços via *internet*, e seus clientes se utilizam cada vez mais essa plataforma, visando economia de tempo e a comodidade.

A Febraban afirma que:

> A comodidade de efetuar transações por meio do celular ajuda a explicar a adesão dos consumidores a esse canal. No entanto, quando falamos de operações com movimentação financeira, a segurança se torna especialmente relevante. Compreendendo isso, os bancos têm acompanhado a evolução contínua e veloz das ferramentas de segurança para oferecerem ao mercado os mais avançados recursos (FEBRABAN, 2019)

Além disso devemos destacar que o momento é de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), sendo necessário observar os princípios da lei por parte das instituições bancárias, sendo que as mesmas devem adotar práticas que visam manter tanto a segurança dos dados, quanto à conformidade.

O objetivo desse artigo é divulgar aos usuários de bancos e ao público geral, os principais métodos que são utilizados para manter a segurança dos dados em serviços bancários via internet (*Internet banking*). Apresentando a finalidade e a importância de cada um deles.

Justifica-se a escolha do tema abordado devido ao aumento de pessoas que utilizam os serviços de bancos via internet e não tem conhecimento de quais são os métodos de segurança que são utilizados.

Segundo Bertão (2020):

> Cerca de 74% das transações bancárias feitas pelos clientes pessoas físicas foram realizadas pelos canais digitais no mês de abril, um mês após o início da quarentena e das medidas de isolamento social para o combate da covid-19 em grande parte do país.
> O resultado representou um aumento de 10 pontos percentuais em relação a janeiro e foi impulsionado pelo uso intenso dos smartphones. Os celulares, sozinhos, representaram 67% das transações analisadas neste mês. Somente no *mobile banking*, a alta foi de 22%.

A metodologia utilizada para o desenvolvimento do artigo foram os métodos de pesquisa e de análise qualitativa.

Além dessa seção introdutória, o presente artigo apresenta, em sua segunda seção, a Revisão de Literatura sobre Sistemas de informação, Segurança da Informação, *Internet Banking*, Problemas de segurança em *Internet Banking* e os principais métodos de segurança em *Internet Banking*. A terceira seção é dedicada a apresentar considerações finais sobre o artigo.

2. Sistemas de informação

Nas últimas décadas, as organizações passaram por um grande desenvolvimento em todo o mundo. Com a globalização e a competitividade crescente, as empresas passaram a ter como meta a maximização de seus resultados e a redução de seus custos, sendo dessa forma necessário organizar de maneira mais eficiente suas informações.

Nesse novo contexto econômico-empresarial, um Sistema de Informação tem um papel importante nos processos anteriormente, pois permite à empresa monitorar e controlar os mesmos, de modo a assegurar eficácia e eficiência, possibilitando o controle de todas as alterações que ocorrem na empresa, como observado por Albertão (2001, p.75), ou seja, a importância de um Sistema de Informação nas empresas está relacionada aos tomadores de decisão, sendo de fundamental importância para as organizações e seus gestores. Francini (2002, p.3) afirma que:

> A área de Sistemas de Informação tem tido a responsabilidade de viabilizar tecnicamente projetos orientados para as mais diversas demandas – tanto aquelas com intuito de dar apoio à melhoria de desempenho, em especial aos tomadores de decisão.

Existem várias definições sobre sistemas. Dentre essas destaca-se a de Balarine (2002, p.3), que afirma "Sistemas de Informação (SI): são os resultados da implementação da TI, através da utilização de computadores e telecomunicações" e a de Laudon & Laudon (1999, p. 4), para os quais "Um sistema de informação consiste em três atividades básicas – entrada, processamento e saída que transformam dados originais em informação útil".

Os Sistemas de Informação têm como finalidade beneficiar seus usuários, procurando auxiliar na melhoria do conhecimento do mercado, aumentando sua capacidade de resposta, aperfeiçoando as comunicações e aprimorando as suas estratégias.

O Sistema de Informação adotado por uma organização deve ser entendido como uma tecnologia que irá auxiliar na sua operacionalização e estratégia, sendo necessário que se tenha clareza da sua importância. Gates (2000, p.32), entende que "O trabalho de informação é trabalho de pensamento. E quando o pensamento e a colaboração são auxiliados significativamente pela tecnologia da computação, tem-se um sistema nervoso digital". O citado autor aponta para a necessidade e importância do Sistema de Informação estar alinhado com a estratégia da organização para a utilização da Tecnologia da Informação, devendo esse estar compatível com sua estratégia de negócios, de tal forma que:

> O Sucesso de um Sistema de Informação não deve ser medido apenas por sua eficiência em termos de minimização de custos, tempo e uso de recursos de informação. O sucesso também deve ser medido pela eficácia da tecnologia da informação no apoio às estratégias de uma organização, na capacitação de seus processos empresariais, no reforço de suas estruturas e culturas organizacionais (O' BRIEN, 2002, p.8).

Finalizando esse componente do resgate teórico sobre Sistemas de Informação registra-se que esses não podem ser ignorados pelas organizações e gestores, pois auxiliam as organizações a se tornarem mais eficientes no seu gerenciamento e em muitos casos obterem vantagem competitiva.

2.1 Segurança da Informação

Com o passar dos anos e com o avanço tecnológico as organizações tiveram que migrar a maioria seus processos e atividades que eram desenvolvidos em meios físicos para meios digitais, após isso a informação ficou cada vez mais valiosa para as organizações, pois juntamente com essa migração surgiram as vulnerabilidades, que as fazem um alvo interessante para pessoas mal-intencionadas. Segundo Abreu:

> Entende-se por informação qualquer conteúdo ou conjunto de dados com valor para determinada organização ou pessoa, sendo esta, um recurso de extremo valor na sociedade atual. Com a utilização de sistemas informatizados

> conectados e integrados através das redes, as informações armazenadas e trafegadas dentre estes estão, de uma forma ou de outra, vulneráveis e sujeitas a ameaças diversas que possam comprometer a integridade destes sistemas, também como a segurança das entidades e outras informações a elas concernentes. A segurança da informação nesse contexto se mostra essencial, e até mesmo crítica em alguns casos, para que a consistência dos sistemas não seja afetada, garantindo a redução de riscos de fraudes, erros, vazamento, roubo e uso indevido e uso indevido de informações (ABREU, 2011, p. 11).

A segurança da informação preza por alguns princípios básicos que são: Confidencialidade, integridade e disponibilidade, que de acordo com Abreu (2011) "Estes principais atributos do conceito de segurança de informação orientam a análise, o planejamento e a implementação da segurança para um determinado conjunto de informações que se deseja proteger".

Diante dos riscos que rodeiam a informação, Benz menciona que:

> A questão do alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI se torna relevante em função dos grandes investimentos que as organizações fazem nesta área, dos muitos riscos relacionados à segurança e da falta de sincronia entre administração das organizações e segurança da informação (BENZ, 2008, p.17)

Nessa questão de adequação ao alinhamento estratégico e políticas de segurança da informação corporativa, Beal descreve que no setor de instituições financeiras:

> As instituições financeiras vêm desenvolvendo suas políticas internas de segurança, visto que a informação é tratada como ativo. Assim, qualquer perda ou dano à informação pressupõe perdas e risco de imagem das instituições envolvidas. A segurança é fator decisivo para um banco a ponto de comprometer todos os outros pertinentes ao negócio bancário (BEAL, 2005, apud FERRARI, 2011, p.11).

Além do alinhamento estratégico e das políticas da informação, serão abordadas algumas das principais técnicas de segurança da informação que são utilizadas em serviços bancários oferecidos via *Internet Banking* e alguns dos problemas enfrentados na segurança.

2.2 *Internet Banking*

O *Internet Banking* é um serviço bancário que usamos através da internet, no qual todos os bancos disponibilizam um site ou uma plataforma onde o cliente consegue realizar diversas transações bancárias sem precisar sair de casa.

O *Internet Banking* permite que utilizarmos a tecnologia ao nosso favor, podendo fazer tudo o que faríamos em uma em uma agência, fazendo da nossa casa ou onde estivermos, devendo considerar que a cada dia mais clientes estão adotando essa tecnologia.

Com a digitalização de alguns serviços que usamos durante o nosso dia a dia, os bancos e as empresas financeiras tiveram que se atualizar, para não ficarem ultrapassadas. O *Internet Banking*, é usado pela web e são acessados através de sites e aplicativos, podendo realizar funções de transações financeiras com maior rapidez e praticidade que a forma tradicional, considerando que através dessa modalidade trata-se de uma forma mais segura de realizar transações bancárias.

Com o aumento desse serviço, em 2018, o Banco Central realizou um levantamento que resultou o seguinte apontamento,

> Duas em cada três transações financeiras eram feitas por meio de aplicativos de celular, *internet banking* ou *call center*, o que resultava em uma quantidade de 66% do total de operações feitas no país. E o celular era o dispositivo mais usado, somando 35% do total — ou quase 25 milhões de transações registradas. (DIALOGANDO VIVO, 2020)

O termo utilizado "*Internet Banking*" refere-se, para serviços que usamos, para ter acesso a nossa conta bancária, através de computadores e celulares, e os serviços bancários que usamos através dos celulares é conhecido como *mobile banking*.

Por isso é de extrema importância que se tenha algumas medidas de segurança, para proteger essas informações, que usamos ao ter acesso para usarmos o *Internet Banking*.

2.3 Problemas de Segurança no Internet Banking

Como citado nas seções anteriores, a grande valorização da informação e o crescimento do uso dos serviços da *Internet Banking*, fizeram com que surgissem também as vulnerabilidades e os ataques nesses serviços financeiros. Nesse item serão abordados alguns problemas de segurança e os principais métodos que pessoas mal-intencionadas utilizam para roubar/invadir e coletar dados no ambiente de *Internet Banking*.

De acordo com Lau (2006, p.60), "No Brasil as tentativas de fraude realizadas sobre clientes do sistema financeiro, usuários do ambiente *Internet* se basearam ou estão baseadas em ataques conhecidos como *SCAM, PHISHING SCAM* e *PHARMING*". Onde, ainda segundo o autor, o *SCAM* e o *PHISHING SCAM* utilizam como principal meio de propagação o envio de mensagens eletrônicas fraudulentas para as vítimas, o famoso *SPAM*. Já o *PHARMING*, podem ser utilizados outros tipos de ambiente para o sucesso da fraude (LAU,2006, p.60).

Para melhor entendimento dos itens citados acima, segue uma breve descrição:

***Spam*:**

Entre as definições de *spam*, podemos destacar a de Almeida:

> Na sua forma mais popular, um spam consiste numa mensagem de *e-mail* com fins publicitários. O termo *spam*, no entanto, pode ser aplicado a mensagens enviadas por outros meios e com outras finalidades. Geralmente, os *spams* têm caráter apelativo e, na grande maioria das vezes, são incômodos e inconvenientes (ALMEIDA, 2010, p.10).

Além de causar incomodo com as diversas mensagens que a maioria das vezes é de sem interesse para o destinatário, o spam também pode ser mensagens de caráter fraudulento.

***Scam*:**

Segundo Silva, o scam é uma versão aprimorada do spam onde:

> Existe o envio de mensagens em massa, porém com um diferencial, esse tipo de mensagem carrega *link* de condução a *download* de arquivo. Ao efetuar o *download*, o usuário proporciona a instalação de arquivo de vírus em seu computador (SILVA, 2018, p.21).

No caso de Instituições financeiras, Silva (2018, p.21), entende que "As mensagens que carregam o *scam* instigam as vítimas, tornando-se curiosas, pois tem aparência da instituição financeira, onde informam notícias de destaque, download de programas, promoções, entre outros ".

Após o *download* do arquivo anexado junto a mensagem e ter seu dispositivo infectado por vírus, a vítima tem seus dados coletados, principalmente dados bancários, onde esses criminosos os utilizam para se beneficiar financeiramente, deixando o prejuízo para a vítima

***Phishing Scam*:**

Este tipo de ataque é parecido ao scam, nesse caso a vítima é direcionada a uma página idêntica a original, mas falsa, que são criadas especificamente para o crime. Assim, qualquer tipo de dado que a vítima informar ao site, automaticamente será enviado via HTML ao fraudador. Em comparação com os métodos citados anteriormente, a quantidade de casos do phishing scam é bem menor, por ser um método mais trabalhoso e mais caro (SILVA, 2018).

***Pharming*:**

"O *Pharming*, tal como o *phishing*, consiste no redirecionamento da vítima à páginas falsas de instituições financeiras. Entretanto no *pharming* não há a utilização de mensagens eletrônicas como vetor de propagação" (PACHECO,2008, P.80).

Para entender o funcionamento desse ataque, destaca-se a definição de Lau (2004):

> O mecanismo utilizado por este ataque é realizar um redirecionamento da vítima para páginas falsas de instituições financeiras. O atacante utiliza falhas de segurança dos serviços de resolução de nomes na *Internet*, o DNS, que resultam em acesso errado do usuário às páginas das instituições financeiras, mesmo se o usuário digitar o endereço da página do banco na URL do *browser* este redirecionamento vai ser feito (LAU, 2004, apud GALLAO,2014, p.24).

Acima foram conceituados os principais problemas com segurança enfrentados no *Internet Banking*. Na próxima seção serão abordados os principais métodos de segurança utilizados nesse ambiente.

2.4 Principais métodos de segurança em *Internet Banking*

Existem vários métodos para se ter segurança enquanto usamos o *Internet Banking*, pois é muito importante que não seja roubado nenhuma informação, caso isso ocorra os prejuízos poderão ser grandes quando pensamos que a informação é um bem valioso.

É necessário sempre utilizar um computador ou notebook confiável, evitando usar computadores públicos, como em *lan houses*, bibliotecas, cafeterias e etc. É de extrema importância ter um bom antivírus no computador que esteja usando para acessar o *Internet Banking,* para que qualquer vulnerabilidade ou ameaça seja detectada e resolvida a tempo, antes que criminosos se aproveitem disso para roubar dados pessoas e bancários e se beneficiar financeiramente.

É sempre importante fazer uma verificação de segurança do site que deseja acessar, sites de bancos são sempre acessados através de uma conexão segura. Para fazer o acesso ao site do banco que é cliente, é relevante utilizar o endereço oficial do mesmo, e não acessar pelo campo de busca, pois na maioria das vezes os sites que são retornados pelo navegador são de origem maliciosa, criados por criminosos para fisgar os usuários e subtrair seus dados, o famoso *PHISHING* citado no capitulo acima.

Não se conectar a redes públicas, como de *shoppings* e restaurantes, pois os dados podem ficar expostos para os crackers, que são indivíduos que praticam a quebra de um sistema de segurança de forma ilegal ou sem ética, procure sempre se conectar a uma rede segura e que conheça, redes públicas não são seguras para o acesso, pois são mais vulneráveis.

Sempre utilizar senhas fortes para acessar suas contas no *Internet Banking*, pois dificulta para o *cracker* decifrar e ter acesso a sua conta.

Não acessar *links* de e-mails desconhecidos e que não contenham o endereço de mensagem eletrônica correto da instituição bancaria, pois pode se tratar de um ataque *phishing scam*.

Ter cuidado com o uso do seu *token*, a grande maioria dos bancos usam *token* para gerar senhas, para colocar no momento de alguma transação bancária, esse método do *token* foi implementado para ter uma maior segurança, nas transações bancárias, então como dica, sempre tomar cuidado com o que você faz com o seu *token*, pois ele é usado como segurança do *Internet Banking*.

3. CONSIDERAÇÕES FINAIS

Com base na pesquisa realizada do artigo desenvolvido, foi possível perceber que além das inúmeras facilidades nas atividades realizadas no cotidiano que o avanço tecnológico proporcionou, também surgiram alguns elementos que afrontam nossa segurança no âmbito da informação, seja ela pessoal ou organizacional.

Constatou-se também que a informação se tornou um ativo valioso para as pessoas e organizações, já que tudo que fazemos hoje em dia gera algum tipo de informação e que com o uso dos sistemas informatizados interligados através das redes torna-as vulneráveis e rodeadas de ameaças diversas.

Com o aumento de uso de aplicativos bancários, por clientes e empresas, tanto pela comodidade e pela segurança pessoal, sendo facilitado por que a maioria das pessoas tem acesso ao telefone móvel e a internet estarem presente em todos os lugares, facilitou as transações bancarias pois elas podem ser feitas, em qualquer lugar.

Dessa forma com esse aumento do uso do serviço de *Internet Banking*, os bancos foram obrigados a investir em segurança da informação, para que os usuários, possam ter confiança em usar o aplicativo daquele determinado banco, tendo em mente que a segurança das suas informações pessoais, não caiam na *internet*, pois elas são muito valiosas.

Com intuito de contribuir ao leitor as ameaças que perseguem a informação no ambiente de *Internet Banking*, foram abordados os diferentes tipos de problemas de segurança existentes neste meio, que servem também como dicas do que não se fazer para não ter suas informações violadas.

Com isso é apresentado alguns dos principais métodos, que são usados pelas instituições financeiras, para manter a segurança de dados e apresentar ao público que não convivem com a tecnologia, saber a finalidade e a importância de cada método apresentado nesse artigo.

É possível concluir que, com o avanço tecnológico constante, evoluíram não só as facilidades no dia a dia, mas também elementos que podem acabar com as informações de uma organização ou até mesmo fazer fechar suas portas quando falamos em um roubo de informações, elementos estes são as vulnerabilidade e ameaças. Contudo, em especifico as instituições financeiras, deverão manter suas ferramentas de segurança em constante evolução e aprimoramento, visando a segurança de suas informações e de seus clientes, deverão também conscientizar seus usuários quanto ao uso seguro de seus serviços no *Internet Banking*.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Leandro Farias dos Santos. **Segurança da informação em redes sociais**. São Paulo .2011. Disponível em http://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em: 21 set. 2020.

ALBERTÃO, Sebastião Edmar. **Erp sistemas de gestão empresarial** – metodologia para avaliação, seleção e implantação. São Paulo: Iglu, 2001.

ALMEIDA, Tiago. **Spam: do surgimento à extinção**.2010. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/260586/1/Almeida_TiagoAgostinhode_D.pdf. Acesso em: 05 out. 2020.

BALARINE, Oscar Fernando Osório. **Tecnologia da informação como vantagem competitiva**. São Paulo: Revista Eletrônica RAE, v.1, n.1, jan-jun/2002, www.rae.com.br/eletronica.

BENZ, Karl Heinz. **Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI:** estudos de caso em instituições financeiras**.** 2008. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/12905/000636569.pdf?sequence=1&isAllowed=y. Acesso em: 22 set. 2020.

FEBRABAN disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf. Acesso em: 02 set. 2020.

FERRARI, Luís Rafael. **A contribuição do bancário na segurança da informação do cliente usuário do internet banking**. Porto Alegre. 2011. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/77519/000895877.pdf?sequence=1&isAllowed=y. Acesso em: 23 set. 2020.

FRANCINI, William Sampaio. **A gestão do conhecimento: conectando estratégia e valor para a empresa. São Paulo**: Revista Eletrônica RAE, v.1, n.2, jul-dez/2002, www.rae.com.br/eletronica.

GATES, Bill. **A empresa na velocidade do pensamento:** com um sistema nervoso digital. São Paulo: Companhia das Letras, 1999.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente internet banking.** São Paulo. 2006. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3142/tde-19092006-164238/publico/Dissertacao.pdf. Acesso em: 02 out. 2020

LAUDON, Kenneth C., LAUDON, Jane Price. **Sistemas de informação**. Rio de Janeiro: LTC, 1999, Quarta Edição.

O' BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da internet.** São Paulo: Saraiva, 2002.

SILVA, Michele. **Principais fraudes de engenharia social envolvendo pessoas físicas no setor bancário brasileiro.** 2018. Disponível em: https://core.ac.uk/download/pdf/225574144.pdf. Acesso em :06 out. 2020.

BERTÃO, Naiara. **74% das transações bancárias em abril foram feitas pelos canais digitais.** São Paulo. Jun./2020. disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/06/23/74percent-das-transacoes-bancarias-em-abril-foram-feitas-pelos-canais-digitais.ghtml. Acesso em: 29 set. 2020.

DIALOGANDO VIVO disponível em: https://www.dialogando.com.br/seguranca/como-usar-o-internet-banking-com-seguranca. Acesso: 19 out. 2020.

ESALES disponível em: https://esales.com.br/blog/7-cuidados-para-ter-seguranca-no-uso-de-internet-banking/. Acesso em: 19 out. 2020.

Faculdade de Tecnologia de Americana

Marcos Roberto Cardoso Junior

Ricardo Bueno Pavan

Segurança da informação em Internet Banking

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: SI

Americana, 07 de dezembro de 2020.
Banca Examinadora:

_____

Alberto Martins Junior (Presidente)

Prof. Ms.

Fatec Americana - Ministro Ralph Biasi

_____

Eduardo Antônio Vicentini (Membro)

Prof. Ms.

Fatec Americana - Ministro Ralph Biasi

_____

José Luiz Zem (Membro)

Prof. Dr.

Fatec Americana - Ministro Ralph Biasi