/A SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE MÉDIO PORTE NA CIDADE DE AMERICANA-SP: OS PROFISSIONAIS E AS POLITICAS ADOTADAS

THE INFORMATION SECURITY IN MIDDLE ENTERPRISES IN THE CITY OF AMERICANA-SP: THE PROFESSIONALS AND THE POLICIES ADOPTED

LA SEGURIDAD DE LA INFORMACIÓN EN EMPRESAS DE MEDIO PORTE EN LA CIUDAD DE AMERICANA-SP: LOS PROFESIONALES Y LAS POLÍTICAS ADOPTADAS

Bárbara de Castro Barbosa

Bruno Celso Pascoti Zuzzi

Pedro Domingos Antoniolli[1]

Maria Cristina Aranda[2]

Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas – Faculdade de Tecnologia de Americana (FATEC Americana)
Americana – SP – Brasil

barbaracastrols2014@gmail.com, djbrunozuzzi@gmail.com, pedroantoniolli@yahoo.com.br, mcrisaranda@gmail.com

Resumo

O objetivo deste artigo é mostrar como a Segurança da Informação tem sido um dos temas mais comentados dos últimos tempos no âmbito empresarial. A certificação e profissionalização dos profissionais nessa área tem colaborado nesse processo de manter as empresas atualizadascom TI, ressaltando que todos os recursos, certificações, treinamentos são de extrema importância para estruturar a empresa e garantir a continuidade dos negócios, automaticamente alinhando-se com a segurança da informação, e política de Segurança da Informação, zelando assim pela integridade, disponibilidade e confidencialidade dos dados, assim tendo um bom desempenho, maior segurança e garantir a continuidade dos negócios.

Palavras-chave: Segurança da Informação, Profissionais, Atualização, Empresas

Abstract

The objective of this article is to show how Information Security has been one of the most commented themes of recent times in the business sphere. The certification and professionalism of the professionals in this area has collaborated in this process of keeping companies up to date with IT, emphasizing that all resources, certifications and training are extremely important to structure the company and ensure business continuity, automatically aligning with the information security, and information security policy, thus ensuring the integrity, availability and confidentiality of data, thus performing well, ensuring greater security and ensuring business continuity.

Keywords: Information Security, Professionals, Update, Companies

[1] DR. **PEDRO DOMINGOS ANTONIOLLI** (Orientador)

Universidade Metodista de Piracicaba
Doutora em Engenharia de Produção

[2] DR. MARIA CRISTINA ARANDA (Orientadora)

FATEC Americana

Doutora em Engenharia Mecânica

1. Introdução

A Segurança da Informação vem se tornando um dos assuntos mais comentados no mundo, pois, a todo tempo, nova tecnologia vem surgindo, diferentes ataques vêm denegrindo a integridade física de dados, ou até algumas vezes, sendo uma forma de chantagem onde quando é efetuada, para a devolução, a vítima deve pagar um valor para que obtenha seus dados de volta. Com isso, a falta de Segurança da Informação se torna um grande potencial de risco para a continuidade de negócios, visto que, quando defasada ou ineficaz pode potencializar grandes danos ou até mesmo a falência de empresas de médio porte, como é o foco de nosso tema.

A busca constante por vantagem competitiva pode resultar em possibilidade de apropriação de informações dos concorrentes, com intenção de usar tais informações privilegiadas em benefício próprio. Não só para proteção de ataques via *internet*, a segurança da informação em empresas também é muito importante para a proteção contra perda de dados antigos como documentos, contratos entre outros. Não somente em caso de extravio, será vista também a importância dos *backups* "(...) a técnica de *backup* está disseminada nas empresas na área de TI, pois garante ao gestor que, em caso de falhas, arquivos corrompidos, excluídos ou alterados indevidamente possam ser facilmente recuperados caso a infraestrutura de *backup* tenha sido bem planejada. (...)" (JESUS; ALENCAR, 2018, p.3). Alguns tipos de *backups* podem ser utilizados dependendo da circunstancias, prioridade ou tamanho de armazenamento. Os mais utilizados atualmente são o de disco (*Hardware)* e em nuvem, porém em todos os casos será mostrado medidas de segurança "(...) A segurança é semelhante a uma corrente: sua resistência será igual a resistência de seu elo mais frágil. (...)" (FONTES, 2006, p. 19).

Também foram discutidas quais medidas as empresas devem adotar para proteger tanto os *backups* quanto os servidores. Além disso, foi considerado o foco de quem pode ter acesso aos dados, e como vão ser guardados / armazenados, levando-se em consideração não só o acesso de pessoas estranhas ao ambiente de TI, como também a possibilidade de incidentes que comprometam a segurança da informação, sejam estes naturais ou intencionais. Um outro ponto é a criptografia, que também foi abordada de forma aplicada ao âmbito empresarial e circunstancias de utilização.

O foco da pesquisa é direcionado às medidas de segurança da informação rotineiras dentro do ambiente empresarial. Dentre tais medidas destacam-se autenticação de usuários, controle de *logins/logouts*, gerenciamento de acessos (meio físico / lógico), prevenção de ataques, atualização dos *softwares* e dispositivos principalmente quando se refere a antivírus, controles de acessos a *e-mails*, utilização à risca da política de segurança por todos os funcionários da empresa e implementação da mesma, caso não exista, análise de riscos e planos de contingencia de negócios, segurança em sistemas operacionais, segurança em banco de dados, dentre outras medidas.

O objetivo geral desta pesquisa compreende: mostrar a importância da segurança da informação no âmbito empresarial e seus benefícios imediatos e em longo prazo.

Com base no objetivo geral, destacam-se os seguintes objetivos específicos:

- Investigar normas e condutas mais efetivas para empresas adotarem de Segurança da Informação;
- Averiguar a importância do profissional de segurança da informação no âmbito empresarial e o crescimento *versus* importância do mesmo em tendências futuras;
- Avaliar a importância dos *backups* como forma de armazenamento seguro dos dados;
- Identificar e relacionar a segurança *versus* criptografia quando necessário, investigar se existem procedimentos de segurança da informação nas mesmas e como funcionam quanto à eficácia, e sobre as políticas de segurança e seu funcionamento.

Com todos estes fatores, pretende-se mostrar a relevância do profissional de segurança da informação nas empresas, para que políticas de segurança na governança de tecnologia da Informação (TI) sejam efetivamente eficientes.

Para o desenvolvimento deste trabalho, realizou – se uma pesquisa quantitativa de campo, de natureza destituída, que foi realizada por meio de entrevistas em forma questionários fechados e de tabulação quantitativa, dos dados coletados. Além disso, a mesma considera a análise e interpretação qualitativa dos dados coletados apresentando-os em forma de percentuais.

Foram entrevistadas pessoas que trabalham nas empresas e tem contato com o sistema de informação/segurança das empresas, que aceitaram participar da pesquisa. Importante ressaltar que foi usado um termo de consentimento, que conta com a autorização para uso das informações das empresas para pesquisa, mantendo-se o anonimato das mesmas.

Os questionários são fechados pois mesmo estes sendo mais rígidos que os abertos, permitem a aplicação direta para tratamentos estatísticos, utilizando computadores para a aplicação dos mesmos, eliminando-se assim a necessidade de classificar respostas que podem induzir conclusões indesejadas.

O universo da pesquisa é de empresas de médio porte localizadas na cidade de Americana-SP. Esta escolha se justifica pelo grande aumento de empresas deste porte na cidade.

Assim, também foi realizado um levantamento bibliográfico relativo aos conceitos associados à segurança da informação. Na sequência foi aplicada a pesquisa de campo, que será feita por meio de entrevistas com pessoas do âmbito empresarial e das respectivas empresas onde trabalham. Para isso, inicialmente foi solicitada a autorização para a realização da pesquisa dentro de cada empresa, apresentando no momento do contato um termo de consentimento. Neste documento consta todas as informações necessárias e explicativas da pesquisa. Da mesma maneira, após a autorização das empresas, foi aplicado um termo de consentimento as pessoas que podem participar deste estudo, explicando os objetivos do estudo, bem como, os procedimentos éticos para que os nomes dos envolvidos sejam mantidos em sigilo.

Quanto a entrevista, esta pode ser considerada "(...) a principal fonte de coleta de dados ou ser parte de outras formas de buscar as informações necessárias, permitindo tratar de temas complexos que dificilmente poderiam ser investigados adequadamente através de (...) outras formas de coleta" (GAIO; CARVALHO; SIMÕES, 2008, p.165).

A análise e interpretação dos dados versarão do cruzamento das informações obtidas pelos métodos de pesquisa adotados.

2. A segurança da informação como elemento para a continuidade dos negócios e para a gestão de riscos na TI.

Partindo-se do princípio básico do papel da Segurança da Informação:

> Assim, a Segurança da Informação visa proteger estes ativos com base na preservação de três princípios básicos: Confidencialidade: Ter confidencialidade é garantir que o que foi dito a alguém ou escrito em algum lugar somente será escutado ou lido por quem tiver direito. Integridade: Uma informação íntegra é uma informação original que não tenha sido alterada indevidamente (sem autorização) ou danificada. Disponibilidade: Para que uma informação possa ser utilizada ela precisa estar disponível. Garantir a disponibilidade é permitir que quem necessite da informação e esteja autorizado a tenha no momento de fazer uso dela (GONÇALVES *et al*., 2005, p.03).

Como pode-se perceber, este é o tripé da Segurança da Informação, que é de extrema importância para manutenção, bom funcionamento e continuidade dos negócios e deve ser respeitado a qualquer custo. Todo e qualquer funcionário dentro da área de Segurança da Informação deve ficar atento a este, lembrando sempre da aplicabilidade, usando quando necessárias nas mais diversas situações rotineiras dentro do âmbito empresarial.

A confidencialidade deve ser respeitada normas que regem a empresa, onde somente poderão ter acesso as informações quem tem autorização para isso, por exemplo, não podendo deixar com que outros funcionários que não tenham estas usem desta informação, evitando que esta informação vaze, em muitos casos correndo o risco de cair em mãos erradas como, por exemplo, na empresa concorrente.

Deve - se zelar pela integridade da informação para que ninguém danifique ou a mude a partir do original, sendo preservada o tempo todo sem que haja alteração. A preservação da

informação é de extrema importância para que a empresa mantenha um controle sobre a administração geral de suas economias, por exemplo, ou até mesmo em sua organização. Pode se supor que um contrato milionário seja alterado, e com o passar dos anos a empresa recebe um processo e necessita deste contrato para a comprovação de sua inocência ou de que não há nenhum documento ilícito, se o mesmo foi salvo, porém, foi alterado, pode a mesma sair no prejuízo podendo ter um ponto agravante contra si.

Quanto a disponibilidade que ela possa ser utilizada e disponível para o uso em todo o momento por autorizados. Neste caso pode-se deixar claro e objetivo os *backups*, sendo um dos métodos para garantir a disponibilidade de dados.

> A abrangência da política de Segurança da Informação será tanto maior quanto mais interconectada estiver a empresa e mais estratégico for o papel que a TI exerce para o negócio, pois qualquer evento de risco estabelecido com a Segurança da Informação poderá originar diversos prejuízos para a empresa. Por outro lado, a Segurança da Informação tem como objetivo a produtividade dos usuários através de um ambiente interativo, onde haja maior controle sobre os recursos da tecnologia da informação, possibilitando o desenvolvimento de aplicações organizadas e confiáveis. Vários tipos de vulnerabilidades podem colocar uma empresa em risco. Eles vão desde as invasões de sistema por *vírus, spams* e *links* maliciosos a funcionários que expõem dados sensíveis. Com a popularização dos *smartphones*, ganham força as ameaças que atingem os dispositivos móveis (ACIAS, 2013)

A política da Segurança da Informação depende muito da integração da empresa e o quanto é estratégico o papel de TI para os negócios, ou seja, somente vai funcionar esta política se tiver esta interligação, com isso, melhorando além da proteção contra qualquer problema indesejado que possa fazer com que a empresa tenha algum tipo de prejuízo, contribuindo também com as melhores práticas e uma maior organização.

As ameaças em uma empresa podem ser de diversas formas, desde vírus, *spams* ou *links* maliciosos ou até mesmo funcionários que expõem dados sensíveis sobre si próprio na internet. Portando é de extrema importância que o profissional de Segurança da Informação ou gestor da empresa aplique normas que restrinjam não só o que cada funcionário pode acessar como também o que poderá ser acessado por ele, contribuindo parcialmente para que o sistema esteja mais protegido destes tipos de ameaças.

Segundo Dawel (2005), o objetivo primário da atividade de segurança é procurar eliminar totalmente o risco e quando não, reduzir ao mínimo aceitável para um determinado processo.

Inicialmente o objetivo da Segurança da Informação é proteger totalmente o sistema da empresa. Mas isso é impossível, pois as pessoas e empresas estão sujeitas o tempo todo a invasões ou coleta de informações, tanto dentro do sistema de rede como fora, pode-se sofrer estes tipos de ameaças. Dentro da empresa, qualquer funcionário pode ter acesso às informações se elas não forem restringidas, desde um funcionário como um faxineiro, por exemplo, que pode ser especializado em ciência da computação ou até mesmo em segurança da informação, como fora da empresa, através de *crakers* ou até mesmo através de um *worm* ou um *trojan* instalado em alguma máquina.

> O administrador de segurança irá consultar empresas especializadas e apresentar a melhor proposta a diretoria, cumprindo assim seu papel inicial de implementar a medida de segurança mais adequada para reduzir o risco mínimo para aquela venerabilidade. Em outras palavras este é o princípio da segurança em camadas conhecido também como barreiras em profundidade. Essas são barreiras em sequência com o objetivo de colocar diversos níveis de proteção para intimidar ou desencorajar um eventual invasor (DAWEL, 2005).

Foi visto que sempre que o gestor de Segurança da Informação for implementar algum sistema de segurança, ele sempre tem que apresentar o mesmo aos diretores das empresas que poderão fazer ou não modificações, como também aprova-los ou não. E também, com um sistema de monitoramento qualquer através de entrada e saída de pessoas em um estabelecimento por câmeras guardas etc, na área de proteção de dados também tem todo este processo, porém com instruções e passos voltados a área computadorizada e estes devem ser respeitadas.

> Lançadas as luzes sobre alguns dos aspectos técnicos, é oportuno discutir um pouco da viabilidade econômica e justificativa financeira desse projeto, já que o retorno sobre estes investimentos e analise custo *versus* benefício são os parâmetros básicos para uma decisão de investimento (DAWEL, 2005).

Depois de decidido como vai ser o sistema de segurança, é importante fazer uma análise de quanto será seu custo e quais benefícios para ela. É muito importante que além de eficaz, este possa garantir a integridade, confidencialidade e disponibilidade de dados de forma segura, pois, em

muitos casos são investidos uma boa quantia neste quesito e a empresa com certeza não quer arcar com prejuízos futuros. A partir daí, é muito importante enxergar o quanto o papel do profissional de Segurança da Informação é alto dentro de uma empresa, onde este, tem uma responsabilidade alta nos negócios e dados que devem ser preservados. Uma vez que a empresa é invadida ou algum funcionário que não tem autorização subtrai informações não autorizadas através de algum tipo de falha, este poderá vender esta informação a terceiros, de forma que possa comprometer o lançamento de algum produto novo com preço mais acessível por exemplo, não só tendo prejuízo por ter sua informação roubada, a empresa também sairá no prejuízo de anos de pesquisa e montagem do produto que deixa de ser vendido em alta escala por ter sido fabricado antes por ser concorrente

Algumas ferramentas podem contribuir para melhores práticas de trabalho relacionada a tecnologia da informação, e duas delas são o ITIL e o COBIT.

Uma boa sugestão para melhorar TI são os serviços do *Information Technology Infrastructure Library (*ITIL) que é o *framework* para gerenciamento de serviços de TI mais adotado mundialmente. O ITIL tem como objetivo reduzir custos, aumentar a disponibilidade e ajustar a capacidade, aumentar a eficiência e eficácia, melhorar escalas e reduzir riscos principalmente à melhoria de práticas.

As ferramentas básicas para qualquer administração em Tecnologia da Informação auxiliam as empresas tanto estruturar as rotinas e procedimentos que serão adotados para cada situação que aparecerá dia após dia, como também, ajudará a guiar os investimentos na área de Tecnologia da Informação que são guiados pelas necessidades do negócio gerando valor à organização.

Todos esses recursos, treinamentos, certificações, além de ajudarem a estruturar a empresa e garantir a continuidade dos negócios, automaticamente, alinham-se com a Segurança da Informação que é extremamente primordial, criando-se assim juntamente com todos esses requisitos, uma política de Segurança da Informação eficaz, garantindo assim e zelando pela integridade, disponibilidade e confiabilidade dos dados, de forma a ter um bom desempenho e funcionamento para a continuidade dos negócios.

3. Segurança da Informação quanto a segurança de Acesso Físico e Lógico nas empresas

Todo ambiente empresarial depende muito da segurança de seus ambientes físicos e lógicos, visto que, tais procedimentos garantem a continuidade dos negócios e segurança integra dos dados e informações privilegiadas pois caso vazem, se tornam uma vulnerabilidade para que concorrentes lancem um produto antecipadamente, ou até, possam ter contato ao catalogo de clientes daquela determinada empresa, causando assim danos que podem ser irreversíveis. Com isto, todas as empresas necessariamente devem ter Políticas de Segurança da Informação, que englobam e restringem procedimentos de acessos físicos e lógicos nestes ambientes.

A política de Segurança da Informação deve ser o princípio de qualquer empresa, visto que, qualquer instituição que não tem regras de segurança, consequentemente, terá mais problemas, divergências e pode-se gastar mais que o previsto A Política de Segurança deve englobar a segurança de acesso físico e lógico:

Segurança Física: Referente ao acesso físico dos funcionários e terceiros dentro dos estabelecimentos, restringindo pessoas não autorizadas, como também, o acesso de locais específicos na empresa, aumenta-se a segurança tanto física e lógica. Da mesma forma que pode acontecer um incidente de característica física. Pode também acontecer um incidente por característica lógica causado por pessoas, por diversos motivos, seja por ser da concorrência, como também, um funcionário ou ex-funcionário mal-intencionado, que possa vir a comprometer a continuidade dos negócios da empresa.

> A Política de Segurança Física nada mais é do que uma declaração formal da diretoria acerca do seu compromisso com a segurança. Ela também está relacionada com as garantias de incolumidades físicas das pessoas, integridade do patrimônio ou do que estiver sob a sua responsabilidade.

> A abrangência da Política de Segurança Física busca englobar a segurança da equipe, das informações empresariais, a segurança física das instalações e também dos eventos externos. A melhor definição e conceito desse termo seria o de: princípios, diretrizes e responsabilidades, contidas em padrões formais, os quais norteiam as atividades de segurança física nos assuntos relacionados à incolumidade física das pessoas e a integridade do patrimônio das empresas. (GLOBALSEG, 2017)

Tendo em vista a importância da segurança física para a empresa, se estabelece um padrão a ser seguido que não basta apenas aplicar a segurança, mas também uma colaboração mútua entre o empregador e o empregado. A segurança tem o papel como citado acima de garantir a integridade do patrimônio e do que está sobre responsabilidade da empresa. Sendo assim, a diretoria deve garantir a implementação da mesma e garantir (através de regras, vigilâncias entre outros) que todos os seus funcionários tenham ciência das regras de segurança e sigam para não ocorrer surpresas.

Dessa forma ressalta a importância de se ter na empresa uma boa segurança física, para melhor desempenho da mesma e garantindo que se acaso ocorra algo não planejado a empresa sofra o menor impacto, assim preservando seu patrimônio, pois as informações sobre os produtos e serviços prestados não colocaram em risco a integridade dos contratantes e de quem faz ou já fez o uso do serviço, fazendo com que futuramente a empresa não corra risco de vir a falir.

> A segurança física corresponde à constituição de barreiras de forma a evitar, ou retardar, intrusões e garantir uma resposta mais eficaz às mesmas. É o ramo da segurança que visa prevenir acessos não autorizados a equipamentos, instalações, materiais ou documentos. Este tipo de segurança pode ser concretizado através de uma simples porta ou envolver complexos sistemas de segurança onde a tecnologia de ponta é uma constante. Ao contrário do que se pode pensar, a preocupação com a segurança física não é um fenómeno do século XX. Deste muito cedo na história da humanidade que garantir a segurança de certos espaços foi uma preocupação. Por esta razão é com relativa facilidade que encontramos no passado vários exemplos de aplicação de medidas para garantir a segurança física de determinados lugares. As muralhas e os fossos construídos nos castelos medievais são apenas dois exemplos arcaicos de segurança física. (APSEI, 2018)

Desde muito tempo atrás o ser humano se preocupa em proteger aquilo que é de seu uso ou que traga algum benefício, com o passar do tempo esse cenário mudou, pois nos tempos atuais ainda mais do que nunca a segurança deve ser colocada em primeiro principalmente se tratando do âmbito empresarial, desde o mais simples impedimento de acesso pode garantir que uma tragédia maior não venha a afetar a empresa e, se acaso ocorra algum problema com a segurança esse impacto seja minimizado ao máximo.

Para poder ter uma ideia de como a preocupação com segurança vem aumentando e se tornando cada vez mais necessária para tudo, é só olharmos para o avanço dos sistemas de proteção.

O mais básico que se pode imaginar é uma simples catraca ou guarita para fazer o controle de acesso de pessoas, mas se for pensar em empresas que investem alto nessa parte temos acesso através de cartões de identificação, documentos que são assinados nas entradas e saídas, portas com trava automática, portas com senha numérica, portas que abrem a partir de comando de voz e ainda mais sofisticadas portas que abrem através da leitura ótica da pessoa em questão.

Segurança Lógica: A segurança de acesso lógica é extremamente importante, visto que, com o vazamento de dados por ordem lógica, pode-se denegrir não somente informações privilegiadas, como também, dados de clientes, novos projetos, roubo de informações de *backups* e demais informações.

Consequentemente, podem abalar a continuidade dos negócios causando danos irreparáveis. Para que não ocorra isso, é de extrema importância não somente uma Política de Segurança da Informação eficaz, como também, profissionais de Segurança da Informação capacitados atuando tanto na parte de segurança (prevenção), na análise, nos testes de vulnerabilidades e tratativa de incidentes, para garantir que as vulnerabilidades tenham o mínimo de impacto possíveis como também, prevenção de incidentes. Também é extrema importância

constantes auditorias nos sistemas para fazer análises de aderência de políticas adotadas pelos funcionários.

> Previne o acesso a aplicações, dados, sistemas operativos, senhas e arquivos de *log*, por meio de *firewalls*, criptografia, antivírus e outras aplicações contra *hackers* e possíveis invasões às fontes internas da empresa. A segurança lógica permite que o acesso seja baseado nas necessidades específicas de cada utilizador, fazendo a identificação através de *login* e *password*. Assim, cada funcionário apenas poderá executar funções que lhe sejam permitidas. Os riscos que a empresa corre por não ter uma boa estrutura de segurança lógica são muitos, como acesso de terceiros a informações sigilosas, perda de dado, falhas na rede causada por fraudes, entre outros. (CRISPIM, 2018)

Não basta apenas investir alto na segurança física e esquecer da segurança lógica que tem o mesmo princípio de proteção física. A empresa por sua vez pode ter o mais alto controle de quem entra e sai da mesma, porém se sua segurança lógica não for boa pode acontecer uma invasão que pode acarretar problemas tão grandes quanto se não tivesse uma segurança física de ponta. Por isso se deve manter a proteção externa (física) e a proteção interna da empresa também (em sua maior parte lógica).

Assim como na segurança física, a segurança lógica pode ser aplicada da mais simples até a mais complexa, só que ao contrário da física, se sua segurança for a mais cara e não tiver os passos mais simples será um desperdício de tempo e dinheiro. Desse modo nunca deve ser esquecido que para uma pessoa ter acesso aos computadores ou informações de uma empresa (sendo ela funcionária ou não) deve ser feito através de um *login* para que, se futuramente necessário possa ser consultado quem fez o acesso naquele dia em questão facilitando o trabalho de solucionar um crime por exemplo.

> Esse tipo de proteção controla o acesso a aplicativos, dados, sistemas operacionais, senhas e arquivos de *log* por meio de *firewalls* de *hardwares* e *softwares*, criptografia, antivírus e outras aplicações contra hackers e possíveis invasões às fontes internas da empresa. Para aprimorar esses mecanismos, é importante sempre manter sistemas e protocolos operacionais atualizados. A proteção da informação vem sendo um grande desafio para as empresas, devido às diversas ameaças existentes que podem trazer grandes prejuízos. Por isso, para se ter uma proteção eficaz dos dados, é importante ter uma equipe de TI bem treinada e atualizada com as novas tecnologias de Segurança da informação que surgem a cada dia e encontram novas soluções de segurança. Os riscos que uma empresa corre por não ter uma boa estrutura de segurança lógica são muitos, como acesso de terceiros a informações sigilosas, perdas de dados, falhas na rede causada por fraudes, entre outros. Os principais riscos à segurança da informação são: a perda de confidencialidade, que acontece quando há quebra de sigilo e informações restritas apenas a determinados funcionários são vazadas; a perda de integridade, que significa que uma pessoa não autorizada consegue ter acesso e modificar algum dado importante e a perda de disponibilidade, quando pessoas autorizadas passam a não conseguir acessar uma aplicação que necessitam. (WESTCON COMSTOR AMERICAS, 2017)

Quando implementada uma boa política de segurança lógica, deve se também não esquecer de controlar quem pode acessar o que, porque se a pessoa trabalha no departamento de *design* por exemplo, ela não terá necessidade e nem deverá acessar a folha de pagamento dos funcionários por não fazer parte da sua área. Também se deve atentar a mudanças simples de uma empresa que já trouxeram no passado grande dor de cabeça para TI, quando houver a demissão de uma pessoa, antes mesmo dela sair do ambiente de trabalho deve-se bloquear seu acesso, pois por vingança ela pode muito bem invadir o sistema e trazer prejuízos de alto valor, fazendo com que a empresa possa ir à falência.

Após garantir que as devidas normas e políticas de segurança sejam aplicadas a empresa, é necessário fazer com que os funcionários tenham o conhecimento delas e também que saibam fazer o uso, pois o que mais acontece é a empresa ter a mais alta segurança do mercado, porém não estar seguro pois os funcionários não sabem como usar a mesma. Também é importante falar para que os funcionários não anotem a senhas em lugares visíveis e que em hipótese alguma façam o

compartilhamento de sua senha pois a mesma é pessoal e intransferível. Se entendido a importância tanto da segurança física quanto da lógica e fazendo o uso das duas uma ao lado da outra será reduzido a chance de a empresa sofrer algum problema quanto a sua segurança.

4. Pesquisa de campo

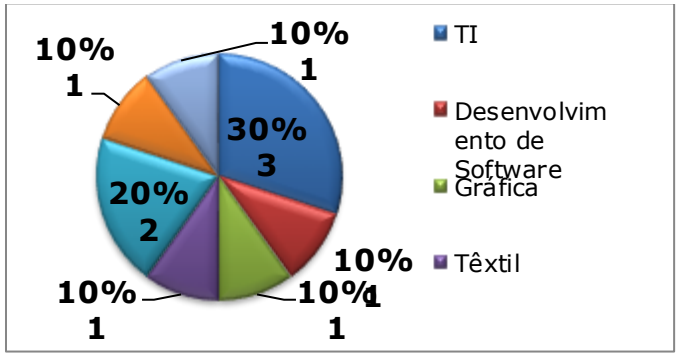
A pesquisa de campo tem como objetivo fortalecer todo o conteúdo estudado na revisão bibliográfica, colaborando assim, de forma eficaz, para posteriormente fazer o afunilamento de todos os dados coletados e atingir possíveis conclusões referentes a eficácia da segurança da informação em empresas de médio porte na cidade de Americana-SP.

Para isso, foi aplicado um questionário objetivo e quantitativo para que possa ser feita a coleta de dados e informações referentes a temática abordada. É importante ressaltar que todas as informações coletadas são mantidas em sigilo, assim, contribuindo com a integridade das pessoas e empresas entrevistadas. Foi anexado no final do trabalho, um termo de consentimento que será entregue para as pessoas entrevistadas e em seguida, será explicado todas as informações e procedimentos pertinentes a pesquisa e ressaltado sobre o sigilo e segurança dos dados coletados de forma quantitativa, apresentados em percentual e numérico.

Será exibido o resultado da coleta de dados, feito com 10 empresas (uma pessoa de cada) primeiro foi perguntado qual a empresa que o entrevistado atua. Sendo a maioria de TI, seguido por logística, depois com igualdade entre gráfica, têxtil, venda de *software*, desenvolvimento de software e qualificação profissional.

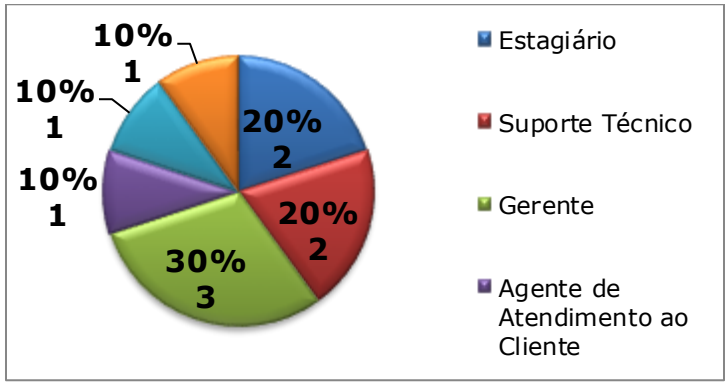
Com 30%, o cargo de gerente predomina, seguido com pouca diferença pelo suporte técnico e estagiário, depois por técnico de TI, consultor de TI e agente de atendimento ao cliente.

Gráfico 1 - A Empresa que você trabalha é de qual área?



Fonte: Autoria Própria

Gráfico 2 - Qual seu cargo na empresa?

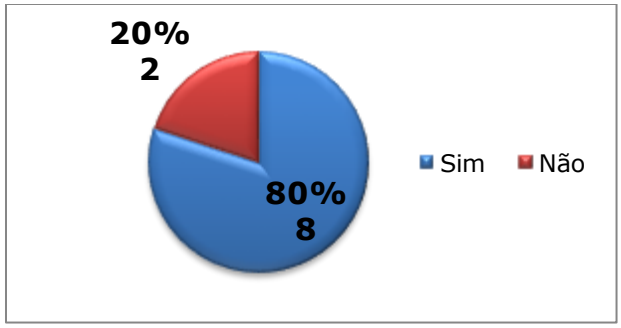


Fonte: Autoria Própria

Na maioria das empresas existe uma política de Segurança da Informação.

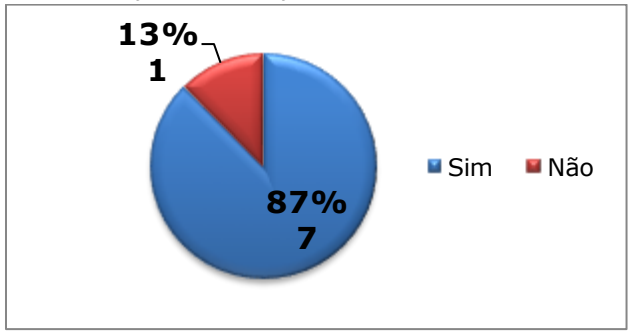
A atualização das políticas de Segurança da Informação, seguindo políticas e padrões da mesma em conformidade com a atualidade é feita em grande parte das empresas pesquisadas.

Gráfico 3 – A empresa tem uma política de segurança da informação?



Fonte: Autoria Própria

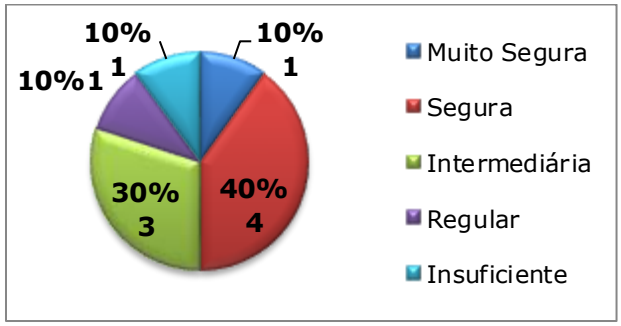
Gráfico 4 – Caso sim, a empresa faz periodicamente a atualização desta política, seguindo políticas e padrões de segurança da informação, em conformidade com a atualidade?



Fonte: Autoria Própria

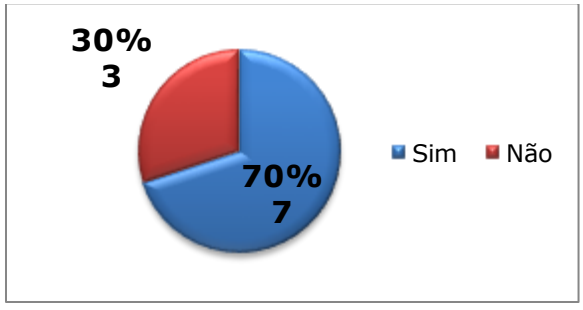
Se tratando de segurança da política da informação a maioria do alvo considera a mesma segura, com pouca diferença para intermediária, por último com muito segura, regular e insuficiente. Em 70% das empresas foi adotado procedimentos de segurança de acesso físico, apenas 30% não adotaram.

Gráfico 5 – O Quanto você considera segura a política de segurança da informação da sua empresa?



Fonte: Autoria Própria

Gráfico 6 – A empresa adota procedimentos de segurança de acesso físico?

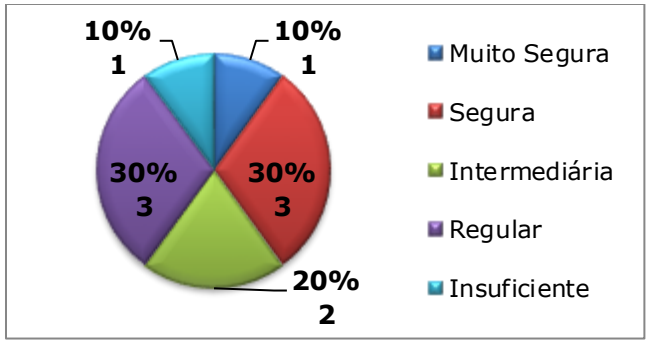


Fonte: Autoria Própria

A maioria dos entrevistados acham a segurança física da empresa segura e regular, vindo depois por intermediária, tendo poucos a classificando como muito segura e insuficiente.

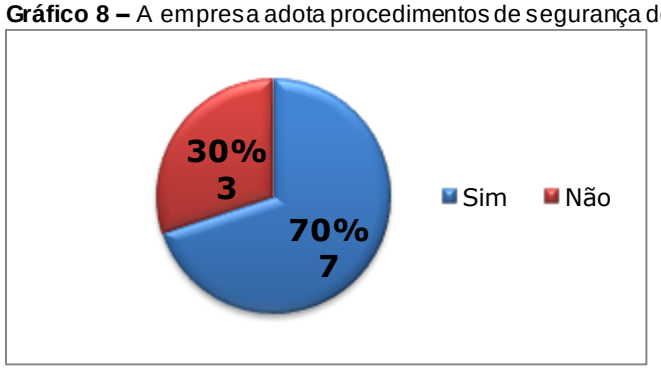
A maioria das empresas fazem a adoção de procedimentos de segurança de acesso lógico.

Gráfico 7 – O Quanto você considera segura a segurança de acesso físico da sua empresa?



Fonte: Autoria Própria

Gráfico 8 – A empresa adota procedimentos de segurança de acesso lógico?

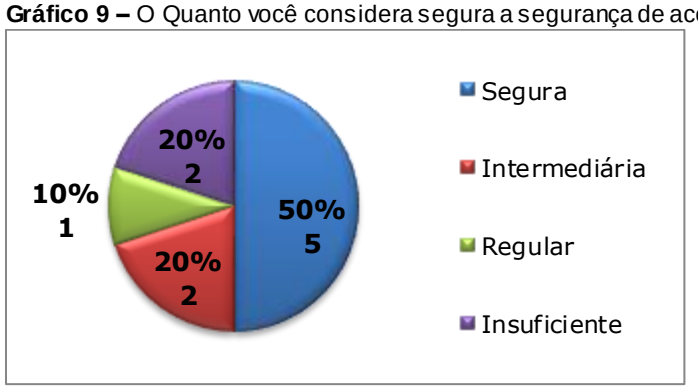


Fonte: Autoria Própria

Metade das empresas tem como segura seu acesso lógico, seguido por intermediária e insuficiente, por último com regular.

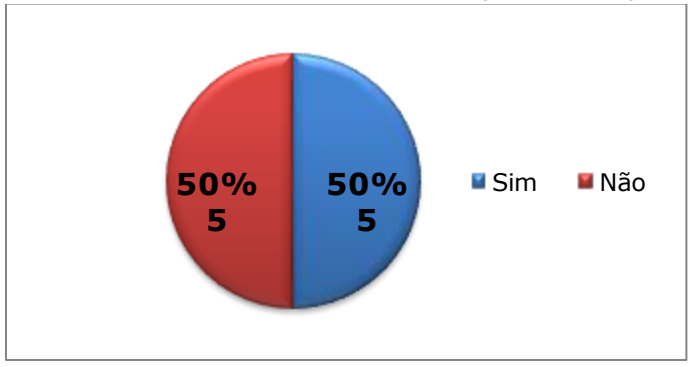
Metade das empresas tem uma equipe de Segurança da Informação especializada e treinada atuando na empresa.

Gráfico 9 – O Quanto você considera segura a segurança de acesso lógico da sua em presa?



Fonte: Autoria Própria

Gráfico 10 – Existe uma equipe de segurança da informação, especializada e treinada, atuando na empresa?

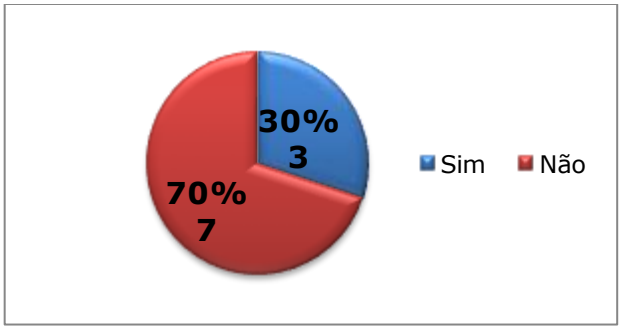


Fonte: Autoria Própria

A maioria das equipes não realiza constante treinamento em todos os setores, mostrando como deve ser seguida a política de Segurança da Informação das empresas.

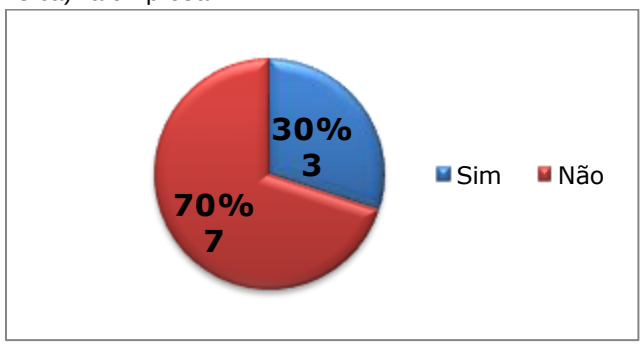
Apenas 30% das empresas pesquisadas fazem regularmente auditorias de segurança geral e Segurança da Informação.

Gráfico 11 – Essa equipe faz constantes treinamentos em todos os setores, implicando como deve ser seguida a política de segurança da informação da empresa?



Fonte: Autoria Própria

Gráfico 12 – Acontecem eventuais auditorias de segurança da informação e segurança em geral (lógica e física) na empresa?

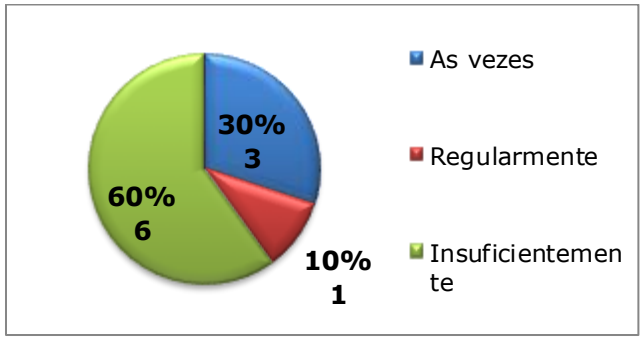


Fonte: Autoria Própria

Mais da metade dos entrevistados considera a auditoria das empresas feita insuficientemente, com metade desse percentual ás vezes e muito pouco regularmente.

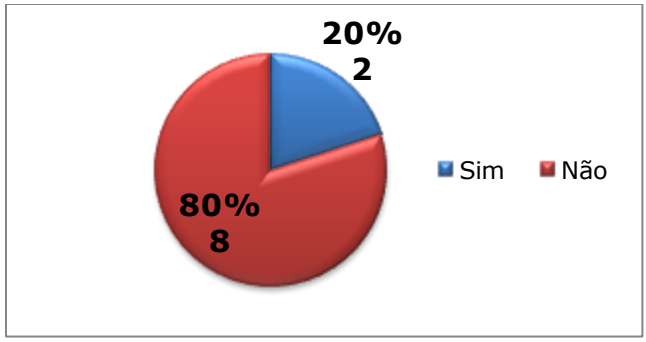
O percentual de profissionais especializados em testes de ataques e vulnerabilidades quanto a segurança lógica atuando nas empresas é de apenas 20%.

Gráfico 13 – O quanto isso é frequente?



Fonte: Autoria Própria

Gráfico 14 – Existem profissionais especializados em testes de ataques x vulnerabilidades na empresa enquanto segurança lógica?

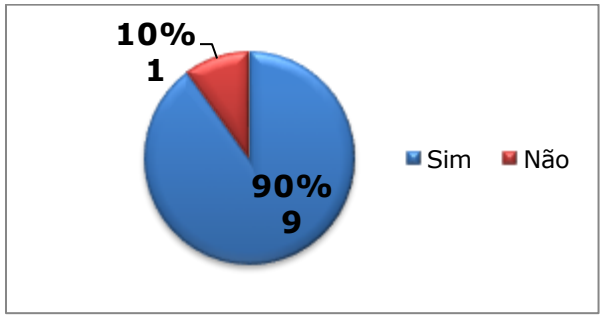


Fonte: Autoria Própria

Quase todas as empreses adotam uma política de *backup.*

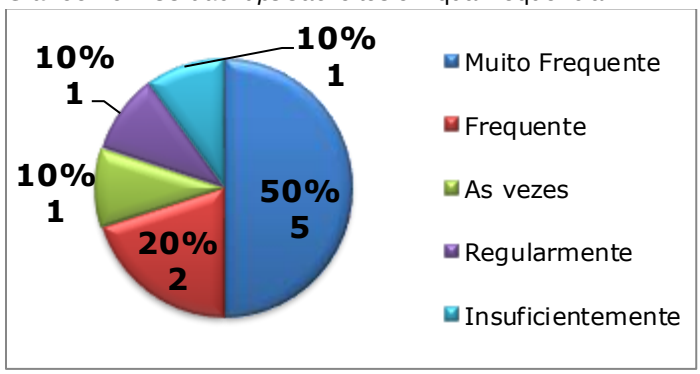
A realização dos backups ocorre com muita frequência em metade das empresas, vindo depois com frequente e com ás vezes, regularmente e insuficiente com percentual iguais.

Gráfico 15 – Existem políticas de backups da empresa?



Fonte: Autoria Própria

Gráfico 16 – Os *backups* são feitos em qual frequência?

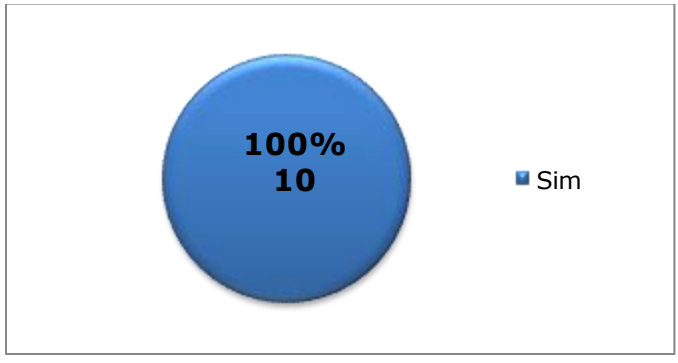


Fonte: Autoria Própria

Em todas as empresas, após o funcionário ser desligado da mesma, tem seu acesso automaticamente barrado.

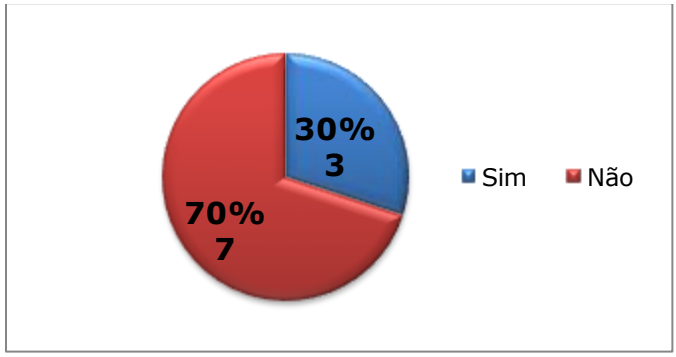
O acesso a redes sociais é proibido na maioria das empresas.

Gráfico 17 – Quando um funcionário é desligado da corporação, é automaticamente barrado o seu acesso físico na empresa, principalmente em locais que se deve manter sigilo de dados e segurança a ativos da empresa?



Fonte: Autoria Própria

Gráfico 18 – Todas as formas de acessos digitais de comunicação como *whatsaap*, *facebook* etc, são liberados para acesso na empresa?

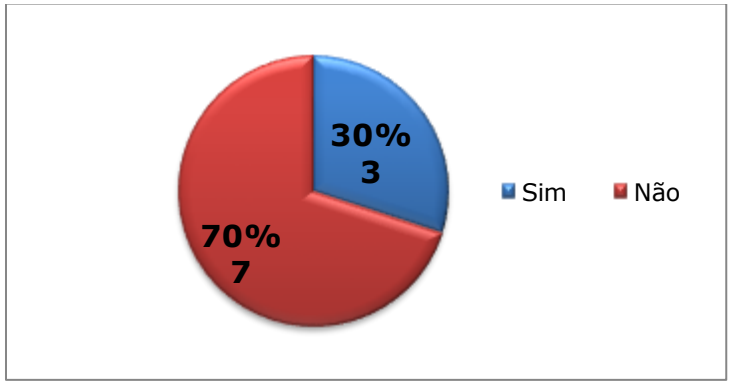


Fonte: Autoria Própria

Não existe normas e diretrizes para acesso de *USBs* na maioria das empresas.

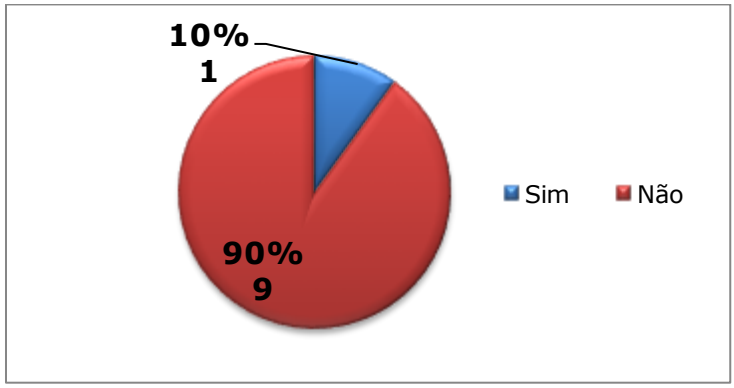
Apenas 10% das empresas entrevistadas sofreram ataques no tempo em que atuam no mercado.

Gráfico 19 – Existem normas ou diretrizes que protegem a empresa, quanto a acesso de *USBs* em maquinas em geral?



Fonte: Autoria Própria

Gráfico 20 – A empresa já sofreu algum ataque em geral, durante o tempo que atua no mercado?



Fonte: Autoria Própria

5. Considerações Finais

Ao realizar esse trabalho foi possível ver como, mesmo com o avanço da tecnologia e sabendo dos prejuízos, que a falta de proteção da mesma pode causar, como as empresas ainda não aplicam totalmente a proteção necessária, que ainda tem muita facilidade para que pessoas possam fazer algo prejudicial as mesmas. Isso ressalta a importância de como é necessário cada vez mais profissionais para cuidarem disso, fazenda a implementação de regras e políticas necessárias para assim poder garantir o máximo de eficiência.

Para a realização deste trabalho, optou-se como objetivo, estudar a importância e eficácia da Segurança da Informação em empresas de médio porte, que abrangem a cidade de Americana SP, proporcionando uma análise geral de aplicação prática em questões de eficiência das vulnerabilidades gerais destas instituições.

Como resultado, os objetivos gerais e específicos foram atingidos, pois foi possível perceber a relevância de problemas propostos quanto a segurança física e lógica nas empresas. A proposta foi aplicar aos funcionários das empresas uma pesquisa quantitativa com questões referentes a Segurança da Informação (acesso físico e lógico), para obter um índice quanto análise de resultados e aplicabilidade da segurança.

A grande maioria das empresas tem a implementação de uma política de Segurança da Informação, mostra-se com isso, que existem normas e diretrizes que conduzem os acessos a toda e qualquer informação da empresa, corroborando assim com uma maior efetividade na segurança. Neste mesmo seguimento, as empresas também fazem constantes atualizações na política da empresa, com isso se tornando mais eficaz, podendo assim se proteger de diversas novas ameaças que podem comprometer a continuidade dos negócios roubo de informações privilegiadas entre outras diversas ameaças eminentes.

Os voluntários em maior parte, consideram seguras a política de Segurança da Informação das suas empresas, visto que, foi proposto a opção muito segurança para as mesma e a opção segura foi a mais escolhida, conclui-se que mesmo com todos os procedimentos de segurança, os sistemas sempre são vulneráveis, sempre tem brechas e precisam ser melhorados constantemente, para acompanhar toda e qualquer precaução para todas as situações atualizadas referentes a roubo de dados e informações privilegiadas.

As grandes totalidades adotam procedimentos de segurança de acesso físico e lógico de pessoas não autorizadas. Enquanto a eficácia, a maior parte considera segura, contudo, desconsiderado a opção muito segura, podendo-se concluir que há o que melhorar enquanto acesso às partes físicas e de acesso lógico das empresas.

Quanto profissionais de Segurança da Informação, metade das empresas tem profissionais especializados na área e a outra metade não, tendo assim maior despreparo dos profissionais que atuam na segurança. Além disso, não há constantes treinamentos e auditorias de segurança dessas equipes e a todos os setores da empresa. Foi possibilitando brechas para espionagens e ataques de *crakers* de diversas partes de mundo, sendo um risco para essas corporações. Os *backups* em grande maioria são feitos com frequência, tendo uma menor taxa de perca de dados.

Em grande maioria, as empresas não sofreram ataques em geral, mostra-se com isso, que a Segurança da Informação foi suficiente até então, porem pode-se considerar insuficientes em quesitos de não ter profissionais especializados de Segurança da Informação, os mesmos não são treinados e não conduzem treinamentos especializados aos demais funcionários da empresa, tornando este tópico um grande risco.

6. Referências

ACIAS. Associação Comercial de Sumaré. O papel da segurança da informação: Como proteger os dados da Empresa? Junho, 2013. Disponível em: <http://www.acias.com.br/index.php/colunistas/prof-edinho/item/o-papel-da-seguranca-da-informacao-como-proteger-os-dados-da-empresa>. Acesso em 7 jun. 2018.

APSEI. Segurança física e proteção perimetral. 2018. Disponível em: https://www.apsei.org.pt/areas-de-atuacao/seguranca-eletronica/seguranca-fisica-e-protecao-perimetral/ Acesso em 15 set. 2018.

COBIT. Disponível em https://www.devmedia.com.br/governanca-de-ti-e-cobit/27577 Acesso em 07 Setembro 2018.

CRISPIM, JOSÉ. Consultoria em TIC a PME: hardware, redes, sistemas, segurança, formação. 2018. Disponível em: https://www.jose-crispim.pt/pt/seguranca/seguranca.html Acesso em 16 set. 2018.

DAWEL, George. A segurança da informação nas empresas. Rio de Janeiro: Editora Ciência Moderna, 2005 Acesso em 12 jul. 2018.

FONTES, EDISON LUIZ GONCALVES, Segurança da Informação, Editora Saraiva, 2006.

GAIO, Roberta; CARVALHO, Roberto Brito de, SIMÕES, Regina. Métodos e técnicas de pesquisa: a metodologia em questão. In: GAIO, Roberta. (Org.) Metodologia de Pesquisa e Produção do Conhecimento. Rio de Janeiro: Vozes, 2008. Acesso em 18 jun. 2018.

GLOBALSEG. Política de segurança física: saiba o que é e como aplicá-la. 27 de Julho de 2017. Disponível em: http://www.globalsegmg.com.br/politica-de-seguranca-fisica/ Acesso em 15 set. 2018.

GONÇALVES, Marcelo; PECIN, João Lucas; ANTÔNIO, Marcos; NOGUEIRA, Guilherme. Segurança da informação. SENAC, 2015. Disponível em: http//http://gti.projetointegrador.com.br/~101M154200090/discmod5/docs/SegurancadaInformacao.pdf. Acesso em 18 ago. 2018.

GUIMARÃES DO LAGO, D.; GUIMARÃES, E. B. Segurança da informação e sua história., 2009. Disponível em: http:://www.viajus.com.br/viajus.php?pagina=artigos&id=2202&idAreaSel=20&seeArt=yes. Acesso em 05 set. 2018.

JESUS, GUILHERME BINDI ALENCAR; JULIANO SCHIMIGUEL, “Implementação de backup como processo de segurança da informação.”, Revista Atlante: Cuadernos de Educación y Desarrollo Fevereiro de 2018. Disponível em: http://www.eumed.net/2/rev/atlante/2018/02/backup-seguranca-informacao.html Acesso em: 31 de Outubro 2018

MUNDO ITIL. (Information Technology Infrastructure Library) ITIL. Disponível em http://www.mundoitil.com.br/. Acesso em 07 set. 2018.
MUNDO ITIL, O Que é ITIL? Disponível em: https://www.mundoitil.com.br/ Acesso em: 20 de out. 2018

PROJECT BUILDER, O que é COBIT e como ele vai melhorar sua gestão de TI. Disponível em: https://www.projectbuilder.com.br/blog/o-que-e-cobit-e-como-ele-vai-melhorar-sua-gestao-de-ti/ Acesso em: 20 de out. 2018

SORTICA, E. A.; CLEMENTI, S.; CARVALHO, T.C.M.B. Governança de TI: comparativo entre cobit e itil. anais do congresso anual de tecnologia da informação – CATI. FGV: EAESP, 2004. Disponível em: http://www3.fsa.br/LocalUser/gestaoti/Ativ09%20CLEMENTI%202004%20%20Governan%C3%A7a%20de%20TI%20-20Comparativo%20entre%20Cobit%20e%20Itil.pdf. Acesso em 10 set. 2018.

WESTCON COMSTOR AMERICAS, Qual a diferença entre segurança física e segurança lógica? 30 de Outubro de 2017. Disponível em: https://blogbrasil.westcon.com/qual-a-diferenca-entre-seguranca-fisica-e-seguranca-logica Acesso em: 16 set. 2018.

7. APÊNDICES

Apêndice 1 – Termo de consentimento para os Dirigentes e Funcionários

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO
DIRIGENTES E FUNCIONÁRIOS DAS EMPRESAS

PROJETO DE PESQUISA - A SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE PEQUENO E MÉDIO PORTE NA CIDADE DE AMERICANA SP: OS PROFISSIONAIS E AS POLITICAS ADOTADAS

Bárbara de Castro Barbosa
Bruno Celso Pascoti Zuzzi
Curso de Tecnologia de Segurança da Informação
Fatec Americana

Estamos desenvolvendo uma pesquisa científica que tem o interesse de investigar as políticas de segurança da informação que as empresas de pequeno e médio porte da cidade de Americana-SP adotam, bem como, a relevância do profissional de Tecnologia de Segurança da Informação neste contexto.

Para isso, estamos pedindo autorização para realizar esta pesquisa nesta empresa, que consistirá em realizar uma entrevista com os funcionários que trabalham diretamente com os sistemas de segurança de informação. Estes funcionários serão convidados a conceder a entrevista sem que seja feito qualquer tipo de pressão.

Os dados da empresa e dos funcionários serão mantidos em sigilo e poderão ser utilizados em publicações futuras. Mas para isso, garantimos manter o anonimato da empresa, de seu nome e dos funcionários entrevistados.

Esta pesquisa é de grande valia para o setor empresarial, bem como para o conhecimento científico, principalmente aquele voltado para a segurança da informação.

Colocamo-nos a disposição para possíveis dúvidas e/ou maiores esclarecimentos.

Eu_____,RG_____
declaro estar devidamente esclarecido e autorizo que o pesquisador realize a pesquisa junto aos funcionários desta empresa.

.

Data____/____/____. Assinatura_____
Assinatura do/da dirigente

---

8. *Questionário da Pesquisa de Campo*

1) A Empresa que você trabalha é de qual área? _____?
2) Qual seu cargo na empresa_____?
3) A empresa tem uma política de segurança da informação?
   ( ) SIM ( ) NÃO
4) Caso sim, a empresa faz periodicamente a atualização desta política, seguindo políticas e padrões de segurança da informação, em conformidade com a atualidade?
   ( ) SIM ( ) NÃO

5) O Quanto você considera segura a política de segurança da informação da sua empresa?
( ) Muito segura ( ) Segura ( ) Intermediária ( ) Regular ( ) Insuficiente

6) A empresa adota procedimentos de segurança de acesso físico?
( ) SIM ( ) NÃO

7) O Quanto você considera segura a segurança de acesso físico da sua empresa?
( ) Muito segura ( ) Segura ( ) Intermediária ( ) Regular ( ) Insuficiente

8) A empresa adota procedimentos de segurança de acesso lógico?
( ) SIM ( ) NÃO

9) O Quanto você considera segura a segurança de acesso lógico da sua empresa?
( ) Muito segura ( ) Segura ( ) Intermediária ( ) Regular ( ) Insuficiente

10) Existe uma equipe de segurança da informação, especializada e treinada, atuando na empresa?
( ) SIM ( ) NÃO

11) Essa equipe faz constantes treinamentos em todos os setores, implicando como deve ser seguida a política de segurança da informação da empresa?
( ) SIM ( ) NÃO

12) Acontecem eventuais auditorias de segurança da informação e segurança em geral (lógica e física) na empresa?
( ) SIM ( ) NÃO

13) O quanto isso é frequente?
( ) Muito Frequente ( ) Frequente ( ) Às vezes ( ) Regularmente ( ) Insuficientemente

14) Existem profissionais especializados em testes de ataques x vulnerabilidades na empresa enquanto segurança lógica?
( ) SIM ( ) NÃO

15) Existem políticas de backups da empresa?
( ) SIM ( ) NÃO

16) Os backups são feitos em qual frequência?
( ) Muito Frequentes ( ) Frequentes ( ) Às vezes ( ) Regularmente ( ) Insuficientemente

17) Quando um funcionário é desligado da corporação, é automaticamente barrado o seu acesso físico na empresa, principalmente em locais que se deve manter sigilo de dados e segurança a ativos da empresa? ( ) SIM ( ) NÃO

18) Todas as formas de acessos digitais de comunicação como whatsaap, facebook etc, são liberados para acesso na empresa? ( ) SIM ( ) NÃO

19) Existem normas ou diretrizes que protegem a empresa, quanto a acesso de USB´S em maquinas em geral? ( ) SIM ( ) NÃO

20) A empresa já sofreu algum ataque em geral, durante o tempo que atua no mercado?
( ) SIM ( ) NÃO

Bárbara de Castro Barbosa
Bruno Celso Pascoti Zuzzi

A SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE MEDIO PORTE NA CIDADE DE AMERICANA-SP: OS PROFISSIONAIS E AS POLITICAS ADOTADAS

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

Americana, 03 de dezembro de 2018.

Banca Examinadora:

Pedro Domingos Antoniolli (Presidente)
Doutor em Engenharia de Produção
Fatec Americana

Edson Roberto Gaseta (Membro)
Especialista em Redes de Computação
Fatec Americana

Benedito Apatecido Cruz (Membro)
Mestre em Multimeios
Fatec Americana