



ISSN: 1696-8352 - BRASIL – MARZO 2017

SEGURANÇA EM AMBIENTE DE TI:
SEGURANÇA FÍSICA DA INFORMAÇÃO EM PEQUENAS EMPRESAS E ESTUDO
DE CASO EM JUNDIAÍ/SP

SILVA, Gilson Ferreira.

SCHIMIGUEL, Juliano.

Para citar este artículo puede utilizar el siguiente formato:

SILVA, Gilson Ferreira y SCHIMIGUEL, Juliano (2017): "Segurança em ambiente de TI: Segurança física da informação em pequenas empresas e estudo de caso em Jundiaí/SP", Revista Observatorio de la Economía Latinoamericana, Brasil, (marzo 2017). En línea:

<http://www.eumed.net/cursecon/ecolat/br/17/jundiai.html>

RESUMO

Este trabalho pretende demonstrar o risco que a falta de segurança física da informação pode trazer às pequenas empresas. O objetivo geral é estudar os principais benefícios que a segurança física da informação vem a oferecer às pequenas organizações, sob o ponto de vista técnico. É um trabalho de abordagem qualitativa, baseado em pesquisa bibliográfica e o estudo de caso de uma empresa que atua com vendas online, situada em Jundiaí-SP. Esse estudo nos permite concluir que a segurança física da informação é tão importante quanto o uso de senhas e restrições de acesso aos dados, justificando assim, o investimento necessário para a implantação da mesma.

Palavras-Chave: Segurança, Informação, Tecnologia, Infraestrutura, Dados.

* Sistemas de Informação (Unianchieta). Analista de Suporte Infraestrutura, Rua José Valter Pacheco, 330, São José I, Campo Limpo Paulista-SP. gilsonfsilva@gmail.com

** Doutor e Mestre em Ciência da Computação pelo Instituto de Computação da Unicamp. Professor dos cursos de Sistemas de informação, Análise e Desenvolvimento de Sistemas e Engenharia de Produção no Centro Universitário Padre Anchieta. Campus Prof. Pedro C. Fornari. jschimiguel@anchieta.br

ABSTRACT

This paper intends to demonstrate the risk that the lack of physical security of the information can bring to the small companies. The overall objective is to study the key benefits that physical security of information has to offer to small organizations from a technical point of view. It is a qualitative study, based on literature review and case study of a company engaged in online sales, located at Jundiaí-SP. This study allows us to conclude that the physical security of information is as important as the use of passwords and data access restrictions, thus justifying the necessary investment for the implementation of the same.

Keywords: Security, Information, Technology, Infrastructure, Data.

1. Introdução

As empresas se encontram em um contexto regido pela informação, isto é, em um mercado onde quem possui a informação correta e sabe aplicá-la em seu ambiente certamente estará se diferenciando de seus concorrentes.

A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa (PEIXOTO, 2006).

Hoje em dia, a maioria das empresas é, se não for totalmente, ao menos parcialmente dependente de sistemas de informação computadorizados para a realização de suas atividades. As que optam por não se utilizar desses sistemas perdem muito tempo executando atividades que poderiam ser automatizadas sem muito esforço e, com isso, acabam por perder um tempo precioso que poderia estar sendo despendido em outras tarefas que ainda necessitam da intervenção humana direta.

Vive-se em uma sociedade que se baseia em informações e que exibe uma crescente propensão para coletar e armazenar informações (KATZAM, 1977).

Os sistemas de informação computadorizados e o acesso às dependências onde eles se encontram são em muitos casos negligenciados. Muito se ouve falar de criptografia, bloqueio, restrição de acesso, e tantas outras técnicas criadas para dificultar o acesso de pessoas não autorizadas à dados sigilosos, no entanto muito pouco sobre técnicas de segurança para proteger o hardware sobre o qual esses sistemas estão funcionando e, quando o assunto é colocado em pauta, as informações não são divulgadas como deveriam.

O cenário atual, principalmente das pequenas e médias empresas revela que é possível acessar fisicamente a maioria das estruturas de rede sem maiores dificuldades. Em muitos casos, o controle de acesso a determinadas características da rede é feito pelos próprios usuários, não existindo um responsável direto por esse controle ou sequer pela manutenção desses dispositivos, sendo essa manutenção feita em sua maioria por empresas terceirizadas ou até mesmo por profissionais freelancer objetivando uma redução nos custos, os quais são contratados para realizar serviços esporádicos sem responsabilidade contratual pelas informações ou dados que estão sendo manipulados.

Conforme observado por GIL (1998), os profissionais usuários com pouco conhecimento de segurança em informática, acabam por desacreditar da possibilidade de ocorrência de graves prejuízos para a empresa.

Do ponto de vista de uma empresa, os sistemas a partir dos quais ela é operada são de suma importância para a sua sobrevivência, sendo por consequência, necessário assegurar que esses sistemas operem de forma contínua e satisfatória. Para isso é necessária uma abordagem das características físicas com relação à segurança.

O objetivo geral deste trabalho é, sob do ponto de vista técnico, estudar os benefícios que a segurança física da informação tem a oferecer às organizações.

Este trabalho apresenta uma abordagem qualitativa, composto por pesquisa bibliográfica e do estudo de caso de uma empresa que atua com vendas online situada em Jundiaí-SP.

Pretende-se, com este estudo, contribuir para uma melhor conscientização tanto dos administradores de empresas quanto dos profissionais da área de tecnologia da informação sobre a necessidade e a importância da segurança física da informação nas pequenas empresas.

2.REVISÃO BIBLIOGRÁFICA

A preocupação com a segurança física da informação, embora infelizmente não seja uma das primícias ao se pensar na instalação de um ambiente informatizado, tem se mostrado um tópico interessante olhando-se o crescimento da quantidade de empresas de segurança da informação que visam este campo nos últimos tempos. Empreendedores com um olhar crítico acerca dos serviços de tecnologia da informação, tem observado que esse importantíssimo tópico, ao ser deixado de lado pelas pequenas empresas, tem permitido que uma lacuna interessante fique aberta, onde eles podem atuar em consultoria com suas empresas. O foco dessas empresas é cobrir ou eliminar a inabilidade em tratar de segurança da informação dos empresários e administradores de empresas que contam com sistemas informatizados.

Para elucidar esta questão é que foi elaborada a revisão bibliográfica presente neste estudo, apresentando alguns pontos relevantes para a elucidação das questões referentes às lacunas deixadas ao se projetar a estrutura de uma empresa de pequeno porte, lacuna essa que pode se tornar um empecilho quando se trata de guardar o bem mais precioso de uma empresa, que é a informação.

2.1.A Segurança Física da Informação

A segurança física surgiu da necessidade do ser humano em proteger o acesso aos seus bens. Esse tipo de segurança evoluiu ao ponto de ser aplicado na área de

tecnologia da informação devido a necessidade em se guardar os dados contidos nos equipamentos de hardware com o objetivo de proteger as informações salvas nesses equipamentos.

Além de proteger os equipamentos e as informações contra acesso não autorizado, limitando o acesso a esses recursos de forma que somente pessoal treinado, capacitado e autorizado possa manuseá-los, a segurança física também tem como propósito evitar danos materiais, pois com a limitação de acesso, a confiabilidade da guarda da informação se torna bem maior.

A norma da ABNT, NBR ISO/IEC 17799, (ABNT, 2005), substituída pela norma NBR ISO/IEC 27002 em 2013, da seção 5 a 9, descreve exatamente como deve ser tratada a gestão da segurança da informação.

- **Seção 5 - Política de Segurança da Informação.**

Descreve o procedimento para garantir que a informação seja tratada da melhor maneira possível com a criação de documentos com os conceitos, análise e avaliação de riscos e outros princípios específicos.

- **Seção 6 - Organizando a Segurança da Informação**

Trata sobre como deve ser implementada a SI em uma organização, descrevendo como as atividades que devem ser gerenciadas, define também como devem ser tratadas as informações de caráter sigiloso, aquelas acessadas por terceiros e clientes.

- **Seção 7 - Gestão de Ativos**

Demonstra como deverão ser tratados os ativos, como devem ser protegidos e mantidos de acordo com o nível de confidencialidade recomendado a cada um.

- **Seção 8 - Segurança em Recursos Humanos**

Informa como deve ser tratada a questão da contratação de pessoas, as responsabilidades com a segurança da informação e como lidar com cada tipo de funcionário de acordo com o nível de acesso que terá às informações.

- **Seção 9 - Segurança Física do Ambiente**

Especifica como deve ser a segurança física do ambiente onde informações críticas são processadas, o nível de acesso que deve ter o funcionário que irá trabalhar nesse ambiente, suas responsabilidades, conforme citadas anteriormente, complementam a segurança.

Como podemos constatar, o uso da norma NBR ISO/IEC 27002 é de vital importância para administradores de empresas e profissionais de tecnologia da informação que desejam manter um ambiente minimamente seguro para que seja possível trabalhar com informações sigilosas sem comprometer a integridade da empresa.

É importante salientar também a importância de haver análises periódicas neste sistema afim de garantir que a documentação exigida esteja em ordem, que os responsáveis pelas informações estejam cumprindo com as exigências acerca da segurança da informação, bem como também garantir que os equipamentos que processam essas informações estejam sempre disponíveis para uso quando for necessário.

3.METODOLOGIA

Este trabalho é de pesquisa de natureza aplicada que, de acordo com VILAÇA (2010), possibilita coletar dados que possibilitarão atingir o seu objetivo e “identificar” respostas para as perguntas de pesquisa.

É uma abordagem qualitativa, de objetivos exploratórios que segundo Gil (2008), esse tipo de pesquisa tem o intuito de estudar os pontos mais relevantes do assunto abordado.

Foi utilizado o procedimento de pesquisa bibliográfica e de estudo de caso de uma empresa que mantém 12 funcionários localizada em Jundiaí-SP.

Esse estudo foi realizado através de 8 reuniões na empresa entre os horários das 08:00hs às 17:00hs, em diferentes datas, todas devidamente agendadas com o responsável e administrador da empresa, onde foram destacados os pontos principais do seu sistema de segurança da informação, as ferramentas necessárias para melhorar o gerenciamento e as ferramentas atualmente em uso e, de posse dessas observações, foi possível realizar algumas sugestões de melhoria ao final desse estudo.

4.SEGURANÇA FÍSICA DA INFORMAÇÃO

De acordo com FURTADO (2002), a segurança física dos equipamentos de informática se refere aos danos que podem ser causados a estes por negligência ou propositadamente, assim como por fatores naturais, acidentais ou criminais.

Tendo-se em conta que a segurança física não depende apenas de fatores internos como a restrição de acesso aos equipamentos criada através de procedimentos e investimento em equipamentos que garantam essa restrição, deve-se também levar em conta fatores ambientais externos, como intempéries.

No caso de fatores externos concernentes ao clima deve-se adotar medidas de forma a garantir que o sistema esteja protegido como um todo não só internamente, mas também externamente, como descargas elétricas, exposição direta à luz solar, entre outros fatores que podem agir diretamente sobre os equipamentos diminuindo a sua vida útil ou até mesmo tornando-os inutilizáveis a curto ou a longo prazo.

4.1. Controle de segurança

O controle da segurança é de vital importância para a segurança física da informação. Para evitar o acesso não autorizado, mecanismos físicos e lógicos são extremamente necessários na gestão da segurança. Podem ser mencionados nesta

categoria diversos mecanismos utilizados para executar a limitação de acesso a determinadas área da empresa, como portas equipadas com painéis com teclado, onde é obrigatória a digitação de senha, catracas, câmeras, segurança biométrica, entre outros.

A autorização é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acessos (Access Control Lists - ACL), definindo quais atividades poderão ser realizadas, desta forma gerando os chamados perfis de acesso (LAUREANO, 2005).

Sobre a detecção de acesso não autorizado, existe a tecnologia *Intrusion Detection System (IDS)*. Esses sistemas são criados de forma a analisar julgar se determinado comportamento é intrusivo ou não. Os dados são enviados para uma central que, quando a tentativa é detectada, apresenta uma notificação ao responsável pela área informando sobre o ocorrido.

Atualmente os processos de autenticação estão baseados em três métodos distintos sendo eles:

- **Identificação positiva (O que você sabe):** É necessário informar no processo de autenticação alguma informação de posse somente daquele que tem acesso àquela área restrita, como por exemplo, uma senha.
- **Identificação proprietária (O que você tem):** Quando o requerente exhibe ou usa alguma informação com uma característica própria, como por exemplo, um crachá ou cartão.
- **Identificação biométrica (O que você é):** Onde o requerente utiliza alguma característica própria a ser utilizada no processo de autenticação, como por exemplo, um cartão magnético. (LAUREANO, 2005)

5.A EMPRESA E A SEGURANÇA DA INFORMAÇÃO

5.1.Dados Gerais da Empresa

A empresa objeto deste estudo será tratada pelo nome Maverin Shop, fundada em 2007, deu início às suas atividades de venda de artigos de departamentos.

A empresa é regida pelos seguintes princípios:

- **Missão:** “Comercializar artigos que atendam às necessidades dos nossos clientes proporcionando a melhor experiência possível”.
- **Visão:** “Ser referência no mercado de vendas online tanto quanto a qualidade dos produtos quanto no atendimento prestado”.
- **Valores:** “Responsabilidade social, excelência no atendimento, aperfeiçoamento constante.

A empresa trabalha com a venda de diversos itens, desde papelaria até brinquedos, sendo:

- Brinquedos;
- Equipamentos de informática;
- Telefones celulares;
- Armarinhos;
- Eletrodomésticos.

O processo de venda se inicia com a compra e o recebimento de materiais e equipamentos, onde funcionários separam os itens a serem vendidos de acordo com cada categoria para facilitar a logística.

Os materiais são catalogados e inseridos no sistema de ERP com os dados de compra, valor inicial e valor final de venda, após esse processo o material fica disponível para ser vendido.

A empresa conta atualmente com 30 fornecedores, com uma infraestrutura que já não está atendendo mais a demanda e, devido a isso, está atualizando seus terminais de venda e adquirindo novos para suprir a necessidade do mercado.

6.CONTROLE DE ACESSO ÀS DEPENDÊNCIAS DA EMPRESA

Foi possível observar, durante as visitas à empresa Maverin Shop que, pelo fato de se tratar de uma empresa de pequeno porte, não investiu em sistema de segurança.

A segurança no acesso aos dados não era item crítico quando desde o início da criação da empresa, muitos dos softwares utilizados para a dinâmica de aquisição e venda não tinham custo e alguns eram livres, objetivando exatamente a diminuição do capital despendido em algo que não era prioridade na época.

Essa situação motivou a necessidade de se formular estratégias de mudança nos planos de futura expansão nos negócios.

Atualmente a estrutura funciona assim:

Há um servidor para todas as funções (backup, banco de dados, controle de acesso e arquivos e ERP). Esse servidor fornece todos os dados necessários ao funcionamento da empresa, porém a restauração de dados fica prejudicada em caso de falha crítica no servidor, pois não há um equipamento específico para backup, mas somente um HD externo que fica disponível caso seja necessário realizar a recuperação de dados.

Esse ambiente não se mostrou satisfatório para a empresa, pois o trabalho de recuperação de dados e outras informações fica a cargo de um analista de suporte freelancer que é chamado sempre que há algum problema no ambiente de informática. Esse analista não tem qualquer vínculo com a empresa, gerando assim preocupação quanto a segurança dos dados manipulados.

A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem os

seus objetivos, pois seus sistemas de informação serão mais confiáveis (LAUREANO, 2005).

Tendo sistemas confiáveis, é possível que a empresa se destaque no mercado, pois assim nenhuma de suas informações será divulgada sem prévio conhecimento e consentimento. Cabe ao departamento de TI, que no caso dessa empresa, deverá ser criado, a criação de ações e normas para gerenciar o sistema e a criação de políticas que resguardem as informações que circulam entre os computadores.

Foram sugeridas algumas práticas a serem seguidas pela empresa para eliminar os riscos com relação a segurança da informação.

Seguem abaixo as questões:

- Elaborar um relatório de atividades executadas por terceiros;
- Elucidar questões sobre ocorrências do sistema de ERP;
- Analisar as atividades executadas e o acesso aos dados.

A empresa deverá analisar seu planejamento de modo a incluir os itens citados anteriormente para ter a garantia de que seu sistema esteja mais seguro, além de garantir que sejam não gerados custos com itens desnecessários para o atual ambiente.

A seguir, seguindo padrões de segurança da informação, foram incluídas análises dos recursos para garantir o melhor desempenho da infraestrutura e de acesso aos dados.

7.SUGESTÕES DE MELHORIA

A segurança da informação tem sido vista cada vez mais necessária e tem se tornado um assunto cada vez mais relevante quanto a necessidade de se tratar as informações, uma vez que atua diretamente com os riscos de adulteração, roubo ou eliminação de dados e como podemos evitar que isso aconteça.

Com as crescentes mudanças no ambiente computacional, o modo como as empresas lidam com o seu negócio também teve que ser reformulado, isso exige que sejam contratados serviços especializados para lidar com essa informação. Dessa maneira a Tecnologia da Informação se destaca, pois trata-se do setor que lida com a informação e visa garantir que ela seja tratada da maneira mais simples e segura possível.

Sendo assim, sugere-se à empresa Maverin Shop que construa um plano de negócios que tenha por objetivo aumentar a segurança da sua informação.

Abaixo são apresentadas uma série de sugestões para diminuir as consequências em questão de forma que a rotina de trabalho ou a maneira como ele é realizado não sejam afetados.

- Identificar a fonte do problema;
- Confirmar onde o problema ocorre ou se propaga;
- Se possível, fazer testes para replicá-lo;
- Consultar a maneira como ele geralmente é resolvido;
- Verificar se a solução atende a necessidade da empresa;

Pode-se garantir que a segurança da informação aplicada atenda às suas necessidades se as soluções descritas acima forem implementadas corretamente, assim, a empresa deverá analisar seu plano de negócios e investir somente nos equipamentos necessários para eliminar os riscos à sua segurança, evitando dessa maneira, gastos desnecessários ou adquirindo equipamentos com desempenho inferior ao necessário.

Em seguida foram sugeridas, com base na pesquisa realizada, análises com padrões de segurança que deverão ser seguidos com detalhes do que deve ser realizado para garantir a correta implementação dos procedimentos.

8.APLICAÇÃO DAS DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

8.1.Execução do projeto

Objetivando a melhoria da empresa como um todo, assim como também o seu sistema de informação, foi aplicado o projeto abaixo com foco na segurança física do ambiente, tendo-se em conta que essa é a maior dificuldade enfrentada por ela.

8.1.1.Análise do ambiente de TI

Foi possível identificar as diferentes visões dos membros da administração acerca do modo de administração dos sistemas de segurança. Alguns preferem um sistema com acesso mais livre, já outros preferem a restrição como a melhor forma de segurança, mas pecam quanto ao excesso de restrição aplicada ao uso dos sistemas, travando o processo e prejudicando o desempenho da empresa.

Dessa forma chegou-se a conclusão de que o melhor método é liberar o acesso às dependências de forma a monitorar todos os procedimentos, pois assim é possível verificar qual a real necessidade de acesso a determinados ambientes e ferramentas, possibilitando, dessa forma, definir a quais recursos determinado funcionário deverá ter acesso.

Esses relatórios fazem que seja possível visualizar informações como tempo de acesso, informações colhidas, tempo de execução, locais e áreas acessados.

8.1.2.Treinamento

As ações a seguir englobam o conjunto de normas e diretrizes que compõem a política de segurança da informação e tem por objetivo apresentar os procedimentos para melhorar e disciplinar no uso dos recursos computacionais.

A política foi originada após várias discussões com os membros da diretoria da empresa e pode ser alterada para melhor se adequar a futuras melhorias que forem implantadas na empresa.

8.1.3.Sugestões e melhorias propostas

Objetivando minimizar o risco de perda de informações e também a proteção de acesso aos dados, foi proposta a construção de:

- Uma sala específica para os equipamentos de TI que armazenam os dados dos usuários e os servidores com equipamento específico para backup das informações;
- Uma porta contra incêndio;
- Uma porta de entrada para a sala propriamente dita, com acesso via senha, onde somente os responsáveis diretos poderão ter acesso;
- A instalação de um sistema de câmeras de segurança, já que esse também faz parte da segurança física do ambiente por ser capaz de manter os dados do monitoramento do ambiente onde estão instaladas;
- Um sistema de backup online que irá guardar as imagens do local em caso de acesso não autorizado.
- Criptografia do disco rígido utilizado para backup, afim de resguardar as informações contidas.

Os responsáveis pela implantação da política de segurança da informação são os administradores da empresa e os funcionários do departamento de TI que deverão ser contratados.

9.SEGURANÇA FÍSICA - APLICAÇÃO PRÁTICA

Estabelecido sobre qual seria a melhor opção para se aplicar ao atual ambiente da empresa, o plano de segurança foi aplicado focando a segurança física da informação e o bloqueio do acesso indevido aos ambientes.

O projeto foi motivado focando na ausência de um departamento de TI, que nesse caso, seria o responsável pela implantação dessa política. Assim, com os pontos abordados, procura-se eliminar a necessidade imediata de um funcionário responsável

pela aplicação da política, podendo assim ser aplicada pelo responsável direto do local onde ela deverá ser seguida.

9.1. Aplicação da Política de Segurança Física da Informação

Sobre a segurança física da informação, fica estabelecido o que segue.

- Todos os funcionários deverão ter as suas funções revistas, de forma que sejam obrigados de se movimentar pelas dependências da empresa o mínimo possível, aumentando com isso, sua produtividade;
- Cada funcionário será o responsável pela manutenção e o zelo do equipamento que utilizar, devendo reportar ao seu superior imediato qualquer problema que ocorra com o equipamento no ato do evento;
- Só deverão ter acesso ao gerenciamento de informações, seja ele planilha ou sistema ERP, aqueles funcionários que realmente necessitarem dessa informação, devendo assim, os responsáveis pelos departamentos limitar a quantidade de funcionários que poderão se utilizar desses equipamentos;
- Informações confidenciais não poderão ser guardadas em computadores compartilhados ou em pastas públicas na rede, para isso deverão ser disponibilizados a quem se utilizar desse tipo de informação, pendrives ou HD's externos com a opção de criptografia de dados, bem como os notebooks deverão ser protegidos por senha para a maior segurança tanto dos dados, quanto dos portadores;
- Deverá haver reuniões mensais com os funcionários com o objetivo de permitir uma maior integração entre os departamentos, facilitando assim a colaboração e a discussão de temas relevantes e inclusive a solução de problemas que eventualmente estiverem sendo enfrentados;

10.RESULTADOS OBTIDOS PÓS IMPLANTAÇÃO

Após a aplicação das diretrizes estabelecidas pelo conselho formado com a administração da empresa, pode-se discutir as melhorias que foram alcançadas.

Neste projeto buscou-se desenvolver uma política de segurança aplicável não somente à empresa que foi estudada, como também às pequenas empresas, de forma a melhorar sua segurança e, por consequência o seu desempenho. Com a implantação da política, conseguiu-se que os funcionários ficassem mais cientes de suas funções, uma vez que as funções não estavam bem distribuídas antes da aplicação, os equipamentos ficaram mais disponíveis, pois agora com um responsável direto, o tempo de máquina parada diminuiu devido ao pedido de manutenção se tornou mais rápido. Foi observado também que a informação guardada disponível para todos se tornou mais sucinta, pois somente dados relevantes são armazenados no servidor e somente para os usuários autorizados a manipular tal informação.

O departamento de logística, um dos mais afetados pelas novas regras de acesso teve o seu desempenho consideravelmente aumentado, pois como se trata de um departamento onde a movimentação dos funcionários, objetos e sua perfeita localização é de extrema importância, assegurar que os dados dos produtos estocados estavam corretos foi de suma importância, tendo sido este objetivo alcançado através da diminuição de usuários que se utilizam de computadores, diminuindo drasticamente assim, possíveis erros no sistema.

Tendo, os responsáveis pela empresa posse de dados como a função de cada funcionário, foi possível prever o que cada um estaria fazendo em determinado período, melhorando assim a visibilidade por parte dos supervisores e diretores, de forma que estes, com a posse de tais informações poderão traçar planos de metas com maior facilidade e também acompanhar o desempenho individual de seus funcionários.

11. CONSIDERAÇÕES FINAIS

Há algum tempo o investimento em segurança da informação era visto como algo desnecessário, um gasto para o qual não havia necessidade pois muitos olhavam o setor de tecnologia da informação como custo somente. Atualmente a situação se reverteu e os investimentos em segurança física tem se mostrado cada vez mais interessantes do ponto de vista financeiro, pois é um setor que, quando há o investimento correto, traz vários benefícios, entre eles, a proteção dos dados, tão vitais para a sobrevivência de uma empresa.

Infelizmente, paralelamente a esse investimento, tem crescido também o aumento no acesso não autorizado aos dados, como podemos ver em empresas de grande porte, daí a necessidade de se investir cada vez mais na segurança dos dados.

Portanto, deve-se ter em conta que a segurança física da informação deve ser encarada como essencial para as pequenas empresas hoje em dia, mesmo porque, caso os dados venham a ser destruídos ou mesmo copiados, concorrentes poderão ter acesso à essas informações, o que significaria uma queda nas vendas ou até mesmo o fechamento da empresa.

Esse trabalho tomou para estudo uma empresa de vendas online, cuja pesquisa possibilitou a criação de um plano de negócios e ajudou efetivamente a resolver a problemática dessa pesquisa, ou seja, a segurança física da informação pode trazer tantos benefícios para empresas de pequeno porte, que o investimento feito na infraestrutura para garantir a integridade dos dados facilmente se confirma como algo de extrema importância quando comparado ao risco de fechamento da empresa ou a perda de seus segredos.

Assim este trabalho alcançou o seu objetivo que foi estudar os principais benefícios que a segurança física da informação pode trazer às pequenas empresas do ponto de vista técnico e até mesmo empresarial. Dentro desses benefícios pode-se

citar a melhoria na infraestrutura, na organização e no gerenciamento dos recursos da empresa, como também melhor visão no sistema de tomada de decisão.

12. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. ABNT, 2005.

AHMAD, David R. M., RUSSEL, Ryan. Rede segura Network. Alta Books, 2002.

DAVIS, Willian S. Análise e Projeto de sistemas - Uma abordagem Estruturada: Editora LTC 1994.

DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books, 2000.

FONTES, Edison. Políticas e normas para segurança da informação - Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

FURTADO, Vasco. Tecnologia e Gestão da Informação na Segurança Pública. Rio de Janeiro, Editora Garamond, 2002.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2008.

GIL, Antonio de Loureiro. Segurança em Informática. 2ª Edição. São Paulo: Atlas 1998.

GORDON, Steven R., GORDON, Judith R. Sistemas de Informação - Uma abordagem gerencial. 3ª Edição. Editora LTC 2006.

LAUREANO, Marcos A. Pchek. Gestão de Segurança da Informação. 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 01 jun. 2015.

LISBOA, Gilvânia dos Santos. Segurança de sistemas de informação: o contexto da segurança dos sistemas de informação. 2011. Disponível em: <http://www.atenas.edu.br/faculdade/arquivos/NucleoIniciacaoCiencia/REVISTAS/>

REVIST2011/6.pdf, recuperado em 10/03/2016.

OLIVEIRA, D.P.R. Planejamento estratégico: conceitos, metodologia e práticas. São Paulo: Editora Atlas, 1988.

PORTER, Michael E. Estratégia Competitiva: Técnicas para análise de indústrias e da concorrência. Rio de Janeiro: Elsevier Editora, 2004.

REZENDE, Denis Alcides, ABREU, Aline França. Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas. 5ª Edição. Editora Atlas 2008.

SANTOS, Antonio R. dos et al. Gestão do Conhecimento como Modelo Empresarial. Disponível em: http://www1.serpro.gov.br/publicacoes/gco_site/m_capitulo01.htm, recuperado em 05/10/2016.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. 2ª Edição. Rio de Janeiro: Elsevier 2014.

SEVERINO, Antonio. J. Metodologia do trabalho científico. 21. ed. São Paulo: Cortez, 2000.

SOMMERVILLE, Ian. Engenharia de software: Edição editora Person 2005. 6ª Edição.

VILAÇA, M. L. C. Pesquisa e Ensino; Considerações e Reflexões E-scrita. Volume 1. Número 2. Maio-Agosto de 2010.