COSTA, Tássio Fernandes. COSTA, Rarysson Guilherme da. BARROS, Adriano David Monteiro de. **Gestão de segurança da informação: Um estudo de caso em uma microempresa de Uiraúna – PB.** Revista Interdisciplinar Científica Aplicada, Blumenau, v.11, n.3, p.69-87, TRI III 2017. ISSN 1980-7031

GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UMA MICROEMPRESA DE UIRAÚNA – PB

Tássio Fernandes Costa[1]

Rarysson Guilherme da Costa[2]

Adriano David Monteiro de Barros[3]

RESUMO

Este artigo tem como objetivo verificar como ocorre a Gestão da Segurança da Informação em uma microempresa a fim de que fosse constatado quais são as ações de segurança praticadas e se a mesma segue algumas das recomendações dadas pela norma ABNT NBR ISO/IEC 27002. Para isto aplicou-se um estudo de caso fundamentado em alguns dos Controles de Segurança expostos nesta norma. Além disso, foram feitas revisões bibliográficas em livros, teses e artigos, com vistas a buscar os conceitos usados no decorrer da abordagem. Com base no estudo de caso percebeu-se que existe a necessidade de fazer uso da segurança da informação, pois a microempresa guarda tanto informações pessoais como também de clientes. Das ações de segurança desenvolvidas destacam-se a utilização de antivírus e a adoção de uma política de backup. Por fim, notou-se que há uma baixa conformidade das ações de segurança em relação a referida norma.

Palavras-chave: Gestão. Sistema de Informação. Segurança da Informação. Norma ABNT.

INFORMATION SECURITY MANAGEMENT: A CASE STUDY IN A MICROENTERPRISE OF UIRAÚNA – PB

ABSTRACT

This article aims to verify how Information Security Management occurs in a microenterprise in order to verify which are the security actions practiced and if it follows some of the recommendations given by the standard ABNT NBR ISO/IEC 27002. For this a case study based on some of the Safety Controls set out in this standard was applied. In addition, bibliographical reviews were made in books, theses and articles, in order to search for the concepts used in the course of the approach. Based on the case study it was realized that there is a need to make use of information security, since the micro-enterprise keeps both personal and customer information. The security actions developed include the use of antivirus and the adoption of a backup policy. Finally, it was noticed that there is a low compliance of the security actions with respect to this norm.

Keywords: Management. Information System. Information Security. Standard ABNT.

[1] Graduando do curso de Bacharelado em Tecnologia da Informação – UFERSA. E-mail: tassiokp206@gmail.com

2 Graduando do curso de Bacharelado em Tecnologia da Informação – UFERSA. E-mail: r_guilherme12@hotmail.com

[3] Mestre em Engenharia de Produção pela Universidade Federal da Paraíba, na linha de pesquisa em Tecnologia, Trabalho e Organizações – UFERSA. E-mail: a_david86@hotmail.com

1 INTRODUÇÃO

Uma das marcas da era da informação é o avanço da tecnologia a qual possibilita que haja um aumento expressivo na quantidade de produtos e/ou serviços que são produzidos diariamente no mundo pelas organizações. Esse aumento se dá pelo fato de que os processos produtivos se tornaram cada vez mais rápido, isso graças ao desenvolvimento de máquinas, sistemas, técnicas, métodos, ferramentas e entre outros recursos que juntos automatizam os mais diversos tipos de tarefas as quais em tempos remotos eram executadas diretamente pela força humana.

Dentre estes recursos mencionadas, os sistemas, sejam eles do mais simples até o mais complexo, são essenciais para que uma organização tenha maior eficiência, eficácia, efetividade, controle e celeridade dos processos e atividades que realiza. Percebemos a existência real dessas vantagens ao analisarmos, por exemplo, um sistema de automação comercial o qual permite que seja feito todo o controle de entrada e saída de mercadorias de forma rápida e eficiente, acarretando em melhores resultados para a empresa, isto é, gerando maior eficácia e efetividade.

Um dos conceitos de sistema, que é encontrado na literatura é dado pelos autores Rezende e Abreu (2003, p. 61), para os quais sistema é um "conjunto de parte que interagem entre si, integrando-se para atingir um objetivo ou resultado". Por esse conceito se deduz que existem vários tipos de sistemas. Por exemplo, uma engrenagem de uma moenda de cana de açúcar é um sistema, pois é composta de partes que interagem entre si, de maneira tal que essa interação produz como resultado um produto final. Contudo, é interessante tratar a respeito de um sistema em especial denominado de Sistema de Informação, o qual pode ser definido como, "todo sistema, usando ou não recursos de tecnologia da informação que guarda dados e gera informação[...]" (REZENDE, 2005, p. 26).

Segundo exposto na norma brasileira ABNT NBR ISO/IEC 27002:2005, "a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida". Ativo é "qualquer coisa que tenha valor para a organização" (ABNT NBR ISO/IEC 27001:2006).

De acordo com a norma ABNT NBR ISO/IEC 27002:2005, essa proteção que deve ser dada a esses sistemas que estão tornando o ambiente dos negócios cada vez mais interconectado, deve-se ao fato de que há um crescente número e uma grande variedade de ameaças e vulnerabilidades que

os atingem. Para Rodriguez e Silva (2014, p. 2) "a necessidade de manter as informações seguras surgiu com o crescimento da tecnologia, o que ocasionou vazamentos de dados e informações".

Em razão dessa necessidade inevitável de proteção haja vista a relevância de ter a informação sempre protegida surgiu a Segurança da Informação. De acordo com a norma ABNT NBR ISO/IEC 27002:2005, "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio"

Apesar de ainda existir organizações que resistem ao uso da informática, especialmente as pequenas empresas, o cenário atual demonstra que elas estão cada vez mais aderindo ao uso de sistemas informatizados, seja por força de dispositivos legais ou, por perceber os consequentes benefícios que eles podem proporcionar.

Tendo em vista que um sistema de informação seguro é extremamente relevante para uma empresa por proporcionar a continuidade do negócio, aumento dos lucros e das oportunidades de negócio, foi realizado um estudo de caso numa microempresa da cidade de Uiraúna-PB a fim de analisar a veracidade destas assertivas. Além disto, um outro objetivo deste trabalho é de verificar se algumas das recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão da Segurança da Informação - são seguidas pela microempresa estudada. Feito esse diagnóstico e embasado nos resultados, são apresentadas algumas justificativas que permitirão promover um parecer sobre a relevância de adotar medidas e práticas que tragam segurança para o sistema de informação de uma organização.

2 SISTEMA DE INFORMAÇÃO E A SEGURANÇA DA INFORMAÇÃO

A segurança da informação foi criada com o intuito de possibilitar que as informações estejam sempre seguras, podendo ser aplicada em quaisquer cenários nos quais as informações estejam sendo de alguma forma manipuladas. Atualmente ela está muito voltada a proteger os Sistemas de Informação os quais são utilizados pelas organizações em todo o mundo. Sendo assim, antes de adentrar especificamente sobre a Segurança da Informação em si, será demonstrado alguns aspectos destes sistemas.

2.1 SISTEMA DE INFORMAÇÃO

Como foi demonstrado o conceito de Sistema de Informação (SI) dado pelos autores Rezende e Abreu (2003), agora, será discutido alguns aspectos relacionados a esses sistemas tais como objetivo, foco, benefícios, tipos de sistemas de informação e seus componentes. Após isto será abordado sobre a segurança que os mesmos devem receber a fim de manter as suas informações sempre protegidas.

De acordo com Rezende (2005, p. 27) "os sistemas de informações, independentemente de seu nível ou classificação, têm como maior objetivo auxiliar os processos de tomada de decisões nas organizações". Chiavenato (2003, p. 348) ao tratar sobre o processo decisório nas organizações menciona que o processo de tomada de decisão "é complexo e depende das características pessoais do tomador de decisões, da situação em que está envolvido e da maneira como percebe a situação". Porto e Bandeira (2006, p. 2) associa a complexidade existente no ambiente organizacional com a "globalização, o avanço tecnológico, o desenvolvimento das telecomunicações e a diminuição do tempo de processamento das informações", colocando que estes fatores levam "os administradores a reavaliarem constantemente o processo decisório".

Diante desse cenário complexo no qual as organizações estão inseridas, os Sistemas de Informações é uma ferramenta fundamental uma vez que orienta o tomador de decisão qual o melhor curso de ação a ser seguido.

Quanto ao foco dos sistemas de informações Rezende e Abreu (2003, p. 63) colocam que o mesmo está voltado para o principal negócio da empresa. Os mesmos autores mencionam vários benefícios que estes sistemas proporcionam para as organizações dentre os quais estão: "mais segurança nas informações, menos erros, mais precisão; redução de custos e desperdícios; controle das operações; oportunidade de negócio e aumento das rentabilidades" (REZENDE e ABREU, 2003, p. 64).

No que refere aos tipos de Sistemas de Informações, Falsarella e Chaves (2004, p. 1-5) os categorizam em cinco tipos diferentes, porém, mencionam que existem várias formas de classificá-los. No Quadro 1, será organizado a classificação dada pelos autores, colocando os cinco tipos de sistemas de informações e algumas das principais funções e características de cada um deles.

Quadro 1: Classificação, funções e características dos sistemas de informações.

Classificação	Principais funções e características
Sistemas Transacionais	Coletar, via digitação, os dados existentes nos documentos operacionais das organizações, validando-os; Armazenar esses dados em meio magnético; Ordenar ou indexar esses dados, de modo a facilitar o acesso a eles; Permitir consultas, on-line ou em batch, aos dados, detalhados ou agregados, que permitam retratar diferentes aspectos das operações.
Sistemas Gerenciais	Integrar dados de diversas aplicações e transformá-los em informação; Fornecer informações para o planejamento operacional, tático e até mesmo estratégico da organização; Suprir gerentes com informações para que estes possam comparar o desempenho atual da organização com o que foi planejado; Produzir relatórios que auxiliem os gerentes a tomar decisões.
Sistemas Executivos	Gerar mapas, gráficos e dados que possam ser submetidos a análise estatística para suprir os executivos com informações comparativas, fáceis de entender; Fornecer dados detalhados sobre passado, presente e tendências futuras das unidades de negócios em relação ao mercado para auxiliar o processo de planejamento e de controle da organização; Possibilitar a análise das informações obtidas.
Sistemas Especialistas	Armazenar o conhecimento e as experiências de especialistas em bases de conhecimento; Utilizar mecanismos de inferência integrados às bases de conhecimento para resolver - ou auxiliar a resolver - problemas; Possibilitar a inclusão de novos conhecimentos nas bases de conhecimentos sem eliminar os conhecimentos já armazenados.
Sistemas de Apoio a Decisão	Possibilidade de desenvolvimento rápido, com a participação ativa do usuário em todo o processo; Facilidade para incorporar novas ferramentas de apoio à decisão, novos aplicativos e novas informações;

	Flexibilidade na busca e manipulação das informações; Individualização e orientação para a pessoa que toma as decisões, com flexibilidade de adaptação ao estilo pessoal de tomada de decisão do usuário.

Fonte: Adaptado de Falsarella e Chaves (2004, p. 1-5).

No que tange aos componentes de um Sistema de Informação, O'Brien (2004, p. 9) coloca que o mesmo depende dos recursos humanos, de hardware, software, dados e redes "para executar atividades de entrada, processamento, produção, armazenamento e controle que convertem recursos em produtos de informação".

2.2 SEGURANÇA DA INFORMAÇÃO

Na introdução deste trabalho ao apresentar o conceito de Segurança da Informação dado pela norma ABNT NBR ISO/IEC 27002:2005, é observado que a segurança da informação tem como objetivo garantir a continuidade do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio. Uma outra abordagem sobre os objetivos da segurança da informação é trazida pelo Manual de Boas Práticas em Segurança da Informação do TCU (2012, p. 9) no qual está exposto que "a segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição".

Conforme Nobre, Ramos e Nascimento (2011) a integridade, a confidencialidade e a disponibilidade são os princípios que norteiam todas as ações da Segurança da Informação. Estes três princípios básicos são definidos por estes autores da seguinte forma:

- Integridade: é a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas;
- Confidencialidade: a informação somente pode ser acessada por pessoas autorizadas;
- Disponibilidade: a informação ou sistema de computador deve estar disponível a quem possa acessá-la no momento em que a mesma for necessária (NOBRE, RAMOS e NASCIMENTO, 2011, p. 98).

Para Silva (2011, p. 35) "a partir do momento que um destes princípios é quebrado, comunicando informações fraudadas, isto pode acarretar sérios danos as organizações e consequentemente perdas financeiras".

Com base nestes princípios apresentados e no conceito de Segurança da Informação dado pela norma ABNT NBR ISO/IEC 27002:2005, Neto e Silveira (2007, p. 3) definem Segurança da Informação como a "área do conhecimento que visa à proteção da informação das ameaças a sua integralidade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos".

Pode-se perceber que ambos os conceitos de Segurança da Informação mencionados neste trabalho trazem o termo ameaça, o qual é definido por Coelho, Araújo e Bezerra (2014, p. 3) como "qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização". Os mesmos autores colocam que vulnerabilidade é:

> [...] qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidades são falhas que permitem o surgimento de deficiências na segurança geral do computador ou da rede. Configurações incorretas no computador ou na segurança também permitem a criação de vulnerabilidades. A partir dessa falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais. (COELHO; ARAÚJO; BEZERRA, 2014, p. 3)

Andrade (2011, p. 17) considera que estas ameaças que envolvem a informação são causadas em grande parte pela interconexão das informações possibilitada pela evolução das redes de computadores.

São vários os tipos de ameaças de segurança que existem e com relação isso Corrêa (2014, p. 8) as classificam em dois tipos: ameaças humanas que podem ser intencionais e não intencionais; e as ameaças naturais. As ameaças humanas intencionais são aquelas provocadas de propósito por crackers, vândalos e criminosos, enquanto que as ameaças humanas não intencionais são provocados por treinamento falho. As ameaças naturais podem ser enchentes, incêndios, terremotos e vendavais.

Como as organizações lidam diariamente com informações e geralmente estão fazendo uso de algum tipo de rede de computador que permite a troca de informação é inevitável que elas

estejam sujeitas aos mais diversos tipos de ameaças, logo, é de extrema relevância que as mesmas adotem medidas de Segurança a fim de manter seus ativos de informações sempre íntegros, confidenciais e disponíveis.

Quando citado anteriormente em adotar medidas que tragam segurança para as informações que são manipuladas por uma organização, diversos autores orientam que não se trata apenas de investir no aspecto tecnológico, mas também nos aspectos físicos, comportamentais e culturais haja vista que, apesar da segurança da informação utilizar instrumentos tecnológicos, quem os manipulam são pessoas e estas precisam estar preparadas para usá-los de forma que tragam resultados positivos à organização. Confirmando o exposto Netto e Silveira (2007, p. 379) colocam, "as organizações preocupam-se principalmente com os aspectos tecnológicos (redes, computadores, vírus, *hackers*, Internet) e se esquecem dos outros – físicos e humanos – tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos".

Reforçando esta afirmação de que na Gestão da Segurança da Informação devem ser levados em conta outros aspectos além da tecnologia. Rezende (2005, p. 295) afirma que "a segurança é responsabilidade de todos os envolvidos, como parte integrante de toda a organização, considerando cultura, treinamento, políticas e práticas diárias". Já Pessoa (2012) coloca que:

> A proteção da informação não é apenas um assunto de tecnologia, soluções técnicas, programas antivírus, são fundamentais, mas não o suficiente para que o sistema esteja protegido, é indispensável conta com uma equipe especializa em segurança para tratar de outros aspectos tais como, humanos, organizacionais e estratégicos. (PESSOA, 2012, p. 18).

Para uma boa Gestão de Segurança da Informação é imprescindível, portanto, considerar não somente a parte que envolve os recursos técnicos, mas também todas as outras variáveis envolvidas.

A fim de contribuir com uma Gestão de Segurança da Informação eficaz os países, impulsionados pela popularização da Internet e o aumento dos crimes no ambiente tecnológico, criaram normas e padrões internacionais que servissem como referência para que as organizações pudessem organizar a sua segurança (OLIVEIRA et al., 2015).

No caso do Brasil, uma das normas que contribuem para isto é a ABNT NBR ISO/IEC 27002:2005 a qual serve como "um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança" (ABNT NBR

ISO/IEC 27002:2005). Além dela existe outra que também já foi mencionada neste trabalho que é a norma ABNT NBR ISO/IEC 27001:2006, "[...]preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)" (ABNT NBR ISO/IEC 27001:2006).

Ambas as normas fazem parte da família ISO 27000 que se trata de um padrão internacional sobre as boas práticas na Gestão da Segurança da Informação, que direcionam as organizações a atingir o nível máximo de excelência internacional em SI. Como este trabalho visa fazer um estudo sobre a Gestão da Segurança da Informação cabe aqui aplicar uma abordagem melhor sobre a norma ABNT NBR ISO/IEC 27002:2005, a fim de detalhar um pouco quais são as suas recomendações para uma boa Gestão da Segurança da Informação.

A norma ABNT NBR ISO/IEC 27002:2005 é composta por 15 capítulos organizados de forma a abordar a maioria das questões ligadas a Gestão da Segurança da Informação, no entanto, ela destaca que controles adicionais e recomendações não incluídos em seu corpo podem ser necessários dependendo das necessidades da organização. O objetivo da norma é estabelecer "diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização" (ABNT NBR ISO/IEC 27002:2005).

Antes de iniciar o capítulo 1 é feito uma introdução na qual é apresentada o conceito de segurança da informação, a importância do uso da segurança da informação, como estabelecer requisitos e analisar os riscos de segurança da informação, como selecionar controles, e quais são os fatores críticos de sucessos para uma boa gestão. Nos capítulos 1, 2 e 3 são apresentados, respectivamente, o objetivo da norma, termos e definições que são trabalhados no decorrer da norma, e um detalhamento da estrutura da norma. O capítulo 4 aborda a análise/avaliação e o tratamento de riscos. Nos 11 capítulos subsequentes são apresentados diversos tipos de Controles de Segurança para orientar os gestores na criação de uma Gestão de Segurança da Informação robusta capaz de impedir vários tipos de ameaças as quais colocam em cheque o futuro de uma organização.

Cada capítulo aborda um tipo de Controle de Segurança expondo de forma detalhada as ações a serem executadas a fim de implementar o controle ao qual se refere. No Quadro 2 é demonstrado com mais detalhes, quais são esses Controles de Segurança trabalhados do capítulo 6 ao 11, bem como seus respectivos objetivos.

Quadro 2: Controles de Segurança e seus respectivos objetivos

Controles de Segurança	Objetivos
Política de segurança da informação	Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes
Organizando a segurança da informação	Gerenciar a segurança da informação dentro da organização Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas
Gestão de Ativos	Alcançar e manter a proteção adequada dos ativos da organização Assegurar que a informação receba um nível adequado de proteção
Segurança em recursos humanos	Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano; Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada
Segurança física e do ambiente	Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização

Gerenciamento das operações e comunicações	Garantir a operação segura e correta dos recursos de processamento da informação; Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados; Minimizar o risco de falhas nos sistemas; Proteger a integridade do software e da informação; Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação; Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte; Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio; Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas; Garantir a segurança de serviços de comércio eletrônico e sua utilização segura; Detectar atividades não autorizadas de processamento da informação
Controle de acessos	Controlar acesso à informação; Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação Prevenir acesso não autorizado aos serviços de rede; Prevenir acesso não autorizado aos sistemas operacionais; Prevenir acesso não autorizado à informação contida nos sistemas de aplicação; Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto
Aquisição, desenvolvimento e manutenção dos sistemas de informações	Garantir que segurança é parte integrante de sistemas de informação; Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos Garantir a segurança de arquivos de sistema; Manter a segurança de sistemas aplicativos e da informação; Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas

Gestão de incidentes de segurança da informação	Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação
Gestão da continuidade do negócio	Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso
Conformidade	Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação; Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação

Fonte: ABNT NBR ISO/IEC 27002:2005

Como é possível observar são vários os objetivos que as ações propostas por esta norma buscam atingir o que deixa claro que se trata de uma norma que visa abranger os vários aspectos relacionados a Gestão da Segurança da Informação, aliás, ela traz recomendações voltadas não somente para os aspectos tecnológicos, mas também aos aspectos humanos, aspectos estes tratados no capítulo 9 cujo título é a Segurança em Recursos Humanos.

É muito difícil que a grande maioria das empresas estejam de acordo com esta norma haja vista a complexidade das orientações por ele dada. Em se tratando de pequenas e médias empresas isso torna-se mais difícil ainda, inclusive, sobre este assunto Netto e Silveira (2007, p. 395) já verificaram que há "uma baixa adequação das pequenas e médias empresas" em relação aos Controles de Segurança propostos pela norma ABNT NBR ISO/IEC 27002:2005.

Apesar disto, como se trata de uma norma referência na área de segurança da informação é extremamente relevante que a utilizemos como base para avaliar as ações de segurança da informação praticadas por qualquer tipo de empresa, desde aquelas de pequeno porte até aquelas consideradas como grandes empresas.

3 METODOLOGIA

Para o desenvolvimento desse trabalho foi realizado uma revisão bibliográfica com intuito de encontrar em livros, tese, artigos e normas, os conceitos necessários para a construção teórica que é indispensável na elaboração desta atividade acadêmica. Além disto é feito um estudo de caso numa microempresa localizada na cidade de Uiraúna-PB, a fim de verificar como é feito a gestão de segurança da informação na mesma.

Na elaboração do estudo de caso foi utilizado como uma das referências, algumas recomendações de Controle de Segurança dadas pela norma ABNT NBR ISO/IEC 27002:2005 as quais foram citadas anteriormente. Dentre os Controles de Segurança da informação colocados no Quadro 2, foram utilizados na aplicação do questionário os seguintes:

- Política de segurança da informação
- Segurança em recursos humanos
- Segurança física e do ambiente
- Controle de acessos

No Quadro 2 foi demonstrado apenas os Controles de Segurança e o seus respectivos objetivos, porém, no questionário foi optado por dar ênfase aos quatros controles listados acima, é interessante que se tenha um maior detalhamento destes.

A Política de Segurança da Informação é um documento que "[...]define normas, procedimentos, ferramentas e responsabilidades às pessoas que lidam com essa informação, para garantir o controle e a segurança da informação na empresa" (PIONTI e FERREIRA, 2013, p. 4). Conforme a ABNT NBR ISO/IEC 27002:2005, nela deve estar contido, dentre outras coisas, uma definição de segurança da informação, as metas globais que a empresa quer atingir, a importância da segurança da informação para a empresa, uma declaração do comprometimento da direção, uma estrutura para estabelecer os objetivos de controle e os controles, uma breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, e a definição das responsabilidades gerais e específicas na Gestão da Segurança da Informação.

Com relação a Segurança em Recursos Humanos a ABNT NBR ISO/IEC 27002:2005 divide este Controle de Segurança em três etapas, quais sejam: antes da contratação, durante a contratação e encerramento ou mudança da contratação. Um exemplo de ação realizada na fase antes da

contratação é: a empresa antes de contratar o funcionário deixa claro as suas responsabilidades funcionais e verifica se aquele concorrente a vaga tem realmente o conhecimento adequado para exercer a função. Um exemplo de ação realizada na fase denominada durante a contratação é: a empresa realiza treinamentos a fim de conscientizar sempre os funcionários de sua responsabilidade, bem como para atualização de conhecimentos. E por fim, um exemplo de ação realizada da fase última fase chamada de encerramento ou mudança da contratação é: o funcionário ao encerrar o contrato com a empresa ou ao mudar de contrato deve devolver os ativos da empresa que estão sobre a sua posse.

Quanto a Segurança Física e do Ambiente, a norma ABNT NBR ISO/IEC 27002:2005 lista vários requisitos dentre os quais foram procurados a trabalhar no estudo de caso, como os seguintes: a proteção do cabeamento de redes; a marcação que permite identificar cabos e equipamentos; a questão da documentação das conexões; a realização de varreduras técnicas e inspeções físicas; se empresa possui uma área de recepção, ou um outro meio para controlar o acesso físico ao local ou ao edifício; a questão da restrição de acesso aos locais restrito somente ao pessoal autorizado; a utilização de barreiras físicas para impedir o acesso físico não autorizado; os equipamentos apropriados de detecção e combate a incêndios; o monitoramento de condições ambientais; a proteção do edifício da empresa contra raios.

No que diz respeito ao Controle de Acesso, a norma ABNT NBR ISO/IEC 27002:2005 também menciona várias ações a serem praticadas, no entanto, no estudo de caso avaliamos esses: registro de usuário, gerenciamento de privilégios, gerenciamento de senha do usuário, política de mesa limpa e tela limpa, autenticação para conexão externa do usuário, identificação para equipamentos em redes, proteção de portas de comunicações e diagnósticos remotos, controle de conexão de rede, controle de roteamento de rede, procedimentos seguros de entrada no sistema operacional, identificação e autenticação do usuário, sistema de gerenciamento de senha, limite de tempo de sessão, limitação de horário de conexão ao sistema operacional, restrição de acesso à informação, procedimentos seguros para trabalho remoto.

A opção em utilizar apenas estes quatro dos onze Controles de Segurança propostos pela norma, justifica-se pelo fato de que eles se adequam mais com a realidade das pequenas empresas.

4 RESULTADOS E DISCUSSÃO

A empresa estudada trata-se de uma microempresa cujo ramo de atividade é o comércio. Ela atua no segmento do comércio varejista especificamente na comercialização de produtos de

segurança eletrônica residencial, não possui nenhum funcionário além dos 2 coproprietários os quais dividem o capital da mesma.

No que diz respeito ao Sistema de Informação usado pela microempresa trata-se de um sistema simples cujo componentes de hardware são um notebook e um desktop nos quais são armazenadas as informações tanto da microempresa como também dos seus clientes, dentre os componentes de software é utilizado alguns programas e um sistema básico para registro de dados dos clientes e outras operações, além disto existe o acesso à rede de Internet. O principal objetivo da utilização desse sistema é para agilizar as tarefas do dia a dia. Este sistema assemelha-se com o tipo de Sistema de Informação Transacional.

Com relação a Segurança da Informação a microempresa não possui departamento específico e nenhum profissional especializado nesta área, porém desenvolve ações, mesmo que mínimas, voltadas para a segurança das informações. Das ações de segurança praticadas, as quais possuem relação com os Controles de Segurança previstos na norma ABNT NBR ISO/IEC 27002:2005 que foram utilizados na aplicação do questionário, nota-se as seguintes:

- Com relação ao Controle de Acesso, a microempresa realiza registro de usuário, gerenciamento de senha de usuário e controle de conexão de redes;
- No que se refere a Segurança em Recursos Humanos que é dividida pela norma ABNT NBR ISO/IEC 27002:2005 em três etapas (antes da contratação, durante a contratação e no encerramento ou mudança da contratação), a microempresa mencionou que destas etapas aquela que é eventualmente praticada é a segunda a fim de renovar os conhecimentos;
- No tocante a política de segurança de informação a microempresa afirmou que não existe uma política robusta como a que é proposta pela norma ABNT NBR ISO/IEC 27002:2005, porém, existe uma política de backup das informações;
- No que tange a Segurança Física e do Ambiente o coproprietário entrevistado destacou que a proteção do cabeamento de redes por meio de canaletas a fim de evitar a interceptação não autorizada ou danos, e a utilização de barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado, são os dois tipos de ações adotadas.

Além destas ações, a microempresa utiliza como ferramenta de Segurança da Informação um antivírus a fim de minimizar possíveis ataques indesejados às informações. A utilização do antivírus, bem como a adoção de uma política de backup por parte da microempresa confirma o estudo realizado por Netto e Silveira (2007) sobre os fatores que influenciam as pequenas e médias

empresas a adotarem a segurança da informação, no qual ele constatou que a ferramenta mais utilizada é o antivírus, seguida por sistema de backup e *firewall*.

O coproprietário da microempresa classificou como parcial as seguintes assertivas colocadas nos questionários relativos às ações de segurança da informação: são capazes de garantir a proteção das informações manipuladas; tornaram-se uma necessidade para a empresa; auxiliam efetivamente na identificação de vulnerabilidades e riscos; garantem confidencialidade, integridade e disponibilidade; sempre que possíveis são atualizadas para acompanhar as mudanças tecnológicas. Além disso afirmou que as ações por ela praticada atendem ao esperado.

Segundo o entrevistado o que motiva a adoção destas ações de segurança que sempre foram praticadas desde o funcionamento da mesma é a necessidade de proteger as informações tanto da empresa como dos clientes de ataques, riscos e vulnerabilidades, a fim de que elas se mantenham sempre íntegras, disponíveis e não percam o seu caráter confidencial, obedecendo assim os três princípios básicos da Segurança da Informação.

O benefício gerado pela segurança da informação é que o planejamento e gerenciamento das informações ficaram mais compactos. Quanto aos efeitos negativos a microempresa nunca passou por nenhum inconveniente relativo a Segurança da Informação.

No que concerne a manutenção das ações de segurança a microempresa realiza apenas a atualização do antivírus utilizado nos computadores a fim de que os novos vírus que surgem diariamente sejam capturados e destruídos, evitando que eles ataquem as informações o que causaria prejuízo.

Sobre o nível de satisfação gerado pelo uso da segurança da informação no sistema de informação, o grau de importância da implantação da Segurança da Informação para a gestão, e o investimento na área de segurança da informação, o coproprietário da microempresa classificou, respectivamente, como regular, médio e baixo. De acordo com ele, a classificação de médio atribuída à importância da implantação da Segurança da Informação para a gestão da microempresa justifica-se pelo fato de que há uma preocupação com as informações que são guardadas no sistema de informação as quais são essenciais para o funcionamento da mesma.

Questionado acerca do que fundamenta as ações de segurança da informação, o entrevistado respondeu que nunca recorreu a nenhuma norma que versa sobre o assunto e que o conhecimento que possui é adquirido apenas em sites na internet os quais tratam sobre assuntos relacionados não

somente a segurança da informação, mas também sobre a área de tecnologia da informação no geral.

5 CONCLUSÃO

No decorrer do desenvolvimento do artigo foi abordado sobre os sistemas de informação e a segurança da informação a fim de construir um arcabouço teórico que nos permitisse avaliar a Gestão da Segurança da Informação da microempresa.

Sobre sistemas de informação foi demonstrado o conceito, o objetivo, o foco, um dos tipos de classificação e quais são os seus componentes.

Em relação a segurança da informação, apesar de ter sido desenvolvido a estrutura teórica baseada em vários autores que discorrem sobre o assunto, o foco maior deste trabalho esteve na norma ABNT NBR ISO/IEC 27002:2005 da qual foi extraída informações que subsidiaram a elaboração do questionário usado no estudo de caso sobre a Gestão da Segurança da Informação.

Da norma ABNT NBR ISO/IEC 27002:2005 foi utilizado apenas quatro dos onze Controles de Segurança por ela tratada, e com base nestes quatros controle notou-se que existe realmente uma baixa conformidade das ações de segurança praticadas pela microempresa em relação as orientações propostas pela norma ABNT NBR ISO/IEC 27002:2005, comprovando assim outros estudos já existentes sobre a Gestão da Segurança da Informação os quais colocam que pequenas e médias empresas não preocupam-se em implantar as muitas medidas de controles trazidas nesta norma.

Apesar disto, foi possível observar que existe uma preocupação com relação a proteção das informações manipuladas pela microempresa haja vista que algumas ações de segurança são realizadas a fim de evitar dados às informações e não comprometer a continuidade do negócio da mesma. De forma resumida estas ações são registro de usuário, gerenciamento de senha de usuário, controle de conexão de redes, política de backup das informações, utilização de antivírus, proteção dos cabos de redes e a utilização de barreiras físicas.

Deste modo, este trabalho mostrou que mesmo sendo pouquíssimas as recomendações da norma ABNT NBR ISO/IEC 27002:2005 seguidas pelas microempresas, ainda assim ela pratica ações de segurança da informação, o que demonstra que existe a necessidade no uso da segurança da informação mesmo nas mais pequenas empresas.

COSTA, Tássio Fernandes. COSTA, Rarysson Guilherme da. BARROS, Adriano David Monteiro de. **Gestão de segurança da informação: Um estudo de caso em uma microempresa de Uiraúna – PB.** Revista Interdisciplinar Científica Aplicada, Blumenau, v.11, n.3, p.69-87, TRI III 2017. ISSN 1980-7031

REFERÊNCIAS

ANDRADE, A.S. **Segurança da informação com foco em infraestrutura**: um estudo de caso em uma empresa do setor de tecnologia da informação. 2011. 89 f. Trabalho de Conclusão de Curso – Universidade Federal de Lavras, Lavras, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27001. **Tecnologia da informação – Técnicas de Segurança – Requisitos**. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002.**Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

BALDISSERA, Thiago André; NUNES, Raul Ceretta. Impacto na implementação da norma NBR ISO/IEC 17799 para a gestão da segurança da informação em colégios: um estudo de caso. **ENCONTRO NACIONAL DE ENGENHARIA DA PRODUÇÃO**, v. 27, 2006.

CHIAVENATO, I. **Introdução a Teoria Geral da Administração**. 7. ed. Rio de Janeiro: Elsevier, 2003.

COELHO, F.E.S; ARAUJO, L.G.S; BEZERRA, E.K. **Gestão da Segurança da Informação**. Rio de Janeiro: Escola Superior de Redes, 2014.

CORRÊA, R.M. **Um estudo de caso sobre a gestão da segurança da informação em uma empresa privada**. 2014. 177 f. Trabalho de Conclusão de Curso – Universidade Federal de Lavras, Lavras, 2014.

FALSARELLA, Orandi Mina; CHAVES, Eduardo O. C. **Sistemas de informação e sistemas de apoio à decisão**. Maio de 2004. Disponível em: http://www.chaves.com.br/TEXTSELF/COMPUT/sad.htm. Acesso em: 16 de Nov. de 2016.

NETTO, A.S; SILVEIRA, M.A.P. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v.4, n. 3, p. 375-397, 2007.

NOBRE, Anna Cláudia dos Santos; RAMOS, Anatália Saraiva Martins; NASCIMENTO, Thiago Cavalcante. Adoção de Práticas de Gestão de Segurança da Informação: um estudo com gestores públicos. **REUNA**, v. 16, n. 4, p. p. 95-113, 2011.

O'BRIEN, J.A. **Sistemas de Informação e as decisões gerenciais na era da internet**. 2. ed. São Paulo: Saraiva, 2004.

OLIVEIRA, M.S. et al. Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa. **Revista Eletrônica de Sistemas de Informação e de Gestão Tecnológica**, v. 6, n. 2, 2016.

PESSOA, R.A.M. **Um estudo de caso sobre a gestão da segurança da informação em uma instituição financeira**. 2012. 59 f. Trabalho de Conclusão de Curso – Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista, 2012.

COSTA, Tássio Fernandes. COSTA, Rarysson Guilherme da. BARROS, Adriano David Monteiro de. **Gestão de segurança da informação: Um estudo de caso em uma microempresa de Uiraúna – PB.** Revista Interdisciplinar Científica Aplicada, Blumenau, v.11, n.3, p.69-87, TRI III 2017. ISSN 1980-7031

PIONTI, Rodrigo; FERREIRA, D.P. Política de Segurança da Informação – Conceitos, Características e Benefícios. **PROFISSIONAISTI**, 19 de Agosto de 2013. Disponível em: <https://www.profissionaisti.com.br/2013/08/politica-de-seguranca-da-informacao-conceitos-caracteristicas-e-beneficios/>. Acesso em 19 de novembro de 2016.

PORTO, M.A.G.; BANDEIRA, A. A. O processo decisório nas organizações. **SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO**, São Paulo, Brasil, 2006.

REZENDE, D.A. **Engenharia de Software e Sistemas de Informação**. Rio de Janeiro: Brasport, 2005.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da Informação:** ***aplicada a sistemas de informações empresariais***. São Paulo: Editora Atlas S.A, 2003.

SILVA, P.M. **Segurança da informação nas microempresas**. 2011. 59 f. Trabalho de Conclusão de Curso – Faculdade de Ciências da Administração de Garanhuns, Garanhuns, 2011.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação / Tribunal de Contas da União**. – 4. ed. –Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. 108 p.