Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas

Alternative Title: Proposal for Simplified Security Model for Small and Medium Business

Gonçalo M. da Silva Neto
Afiliação do 1º autor
Núcleo de Tecnologia da Informação - UFRPE
Rua Dom Manoel de Medeiros, s/n, Dois Irmãos
CEP: 52171-900 – Recife - PE
goncalo@nti.ufrpe.br

Gliner Dias Alencar
Centro de Informática – UFPE / Supervisão de Serviço de Informática de PE – UE/PE - IBGE
Av. Jornalista Anibal Fernandes, s/n, Cidade Universitária
CEP: 50.740-560 - Recife - PE
gda2@cin.ufpe.br

Anderson Apolonio L. Queiroz
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (Campus Santa Cruz)
Rua São Braz, 304, Bairro Paraíso,
CEP: 59200-000 - Santa Cruz - RN
anderson.queiroz@ifrn.edu.br

RESUMO

A adoção de um modelo de segurança da informação, implementação de políticas e adequação a alguma norma de segurança da informação é algo raro para as Pequenas e Médias Empresas (PMEs) devido, muitas vezes, a complexidade das normas. Como essas organizações contribuem com boa parte da economia nacional, sendo os maiores empregadores do Brasil, se fez necessário pesquisar formas para tentar suprir esta carência. Para isto a presente pesquisa analisou, com amostra real de 48 PMEs, através de questionário, qual a visão das PMEs sobre segurança da informação e propôs um modelo simplificando os 133 controles da NBR ISO/IEC 27002 para apenas 22. Tal modelo simplificado foi, posteriormente, validado também via questionário com profissionais de TIC atuantes nas PMEs.

Palavras-Chave

Segurança da Informação. Pequenas e Médias Empresas. Modelo de Segurança da Informação. Normas de Segurança da Informação.

ABSTRACT

The adoption of information security model, implementation of policies and fitness for any information security standard is rare for Small and Medium Enterprises (SMEs) because, often, the complexity of the rules. As these organizations contribute to much of the national economy, being the largest employers in Brazil, it was necessary to research ways to try to fill the gap. For this purpose the present study analyzed with real sample of 48 SMEs, through a questionnaire, which the vision of information security for SMEs and proposed a model simplifying controls 133 of ISO / IEC 27002 for just 22. This simplified model was , later also validated via questionnaire with ICT professionals in SMEs.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
SBSI 2015, May 26–29, 2015, Goiânia, Goiás, Brazil.
Copyright SBC 2015.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security.

Keywords

Information Security. Small and Medium Business. Information Security Model. Information Security Standards.

1. INTRODUÇÃO

Atualmente, com o avanço tecnológico, as empresas encontram-se em uma realidade diferente, onde o mercado é disputado vorazmente em um alto nível de competitividade. Segundo [8] "com a popularização da tecnologia e o avanço da economia digital a TI encontra-se em posição de destaque no ambiente empresarial, exercendo papel decisivo nos negócios".

Neste ambiente, o aumento dos incidentes de segurança cresce aceleradamente em todo o mundo. Os ataques atingem diversos tipos de organizações, tanto as governamentais quanto empresas privadas de diversos portes e segmentos. Vem se tornando cada vez maior a lista de empresas, países e instituições governamentais que estão em um verdadeiro duelo contra "hackerativistas" [7].

A maioria das empresas pequenas subestima a preferência de bandidos por elas. Muitas vezes por desconhecer que todas as empresas são possíveis alvos, independente de seu porte. Os invasores focam-se em alvos específicos, realizando pacientemente várias etapas de um ataque, assim, melhorando as chances de sucesso [2]. No universo geral das empresas podemos destacar as Pequenas e Médias Empresas (PME), que, segundo Cadastro Central de Empresas [10] possuem as seguintes características: pequenas empresas têm entre cinco e 99 pessoas empregadas; médias empresas têm entre 100 a 499 pessoas empregadas; estão concentradas no setor de serviços; e são os maiores empregadores no Brasil. Segundo o Sebrae [23] [24], as PMEs representam, nacionalmente, 99% dos estabelecimentos,

52% dos empregos de carteira assinada, 40% dos salários pagos e 27% do PIB.

Os ataques a esta modalidade empresarial vem crescendo nos últimos anos. O número de ataques destinados a empresas com até 250 funcionários no ano de 2012 dobrou [14], em 2013 as PMEs tiveram o maior aumento em ataques dirigidos e responderam por 30% de todas as ofensivas em 2013 no mundo, conforme relatório disponibilizado em 2014 [25]. Os dados de 2014 e as tendências para 2015 demonstram que deve continuar crescente os ataques neste nicho de empresas [25] [26].

Por conta deste e de outros fatores, existem diversos padrões, normas e regulamentos para a implementação de um modelo de segurança. Esses modelos fornecem um conjunto de boas práticas para a garantia de um modelo de Gestão de Segurança da Informação (GSI). Porém, as empresas caracterizadas como PMEs geralmente não adotam nenhum dos modelos e normas disponíveis no mercado, nem mesmo parcialmente. Premissas básicas como identificação e classificação dos ativos organizacionais e análise e avaliação de riscos não são implantadas, ou até mesmo desconhecidas pelos gestores [12].

Para [9] o principal motivo da ausência de um modelo de segurança da informação nestas empresas deve-se ao nível formal de seus dirigentes, que geralmente são pequenos empreendedores. Outros motivos encontrados são barreiras financeiras e de acesso a crédito, como também o desconhecimento dos padrões, normas e algumas tecnologias. [9] ainda retrata o cenário de TI em pequenas e médias empresas no Brasil, onde pode-se destacar alguns pontos como: a infraestrutura de TI não é complexa; há limitações de habilidades de TI dentro da empresa; há muito foco em relação aos custos e existem poucos controles.

Diante deste contexto, o presente trabalho visa analisar a situação atual das PMEs do Grande Recife e, a partir destes dados, propor um modelo de segurança simplificado.

Para isto, o presente artigo está organizado, além da seção 1 já exposta, da seguinte forma: a seção 2 apresenta a fundamentação teórica, inserindo os principais pontos inerentes ao trabalho, que engloba uma introdução à segurança da informação, as Normas NBR ISO/IEC 27001:2006 [5] e NBR ISO/IEC 27002:2005 [4], assim como ao Business Model for Information Security [6]. Na seção 3, é classificada a pesquisa e a metodologia utilizada é apresentada. A seção 4 apresenta a análise dos dados obtidos e a proposta de modelo simplificado para as PMEs. Finalizando, tem-se a seção 5 com as considerações finais do trabalho.

2. REFERENCIAL TEÓRICO

Com o passar do tempo, a segurança da informação transformou-se em algo crítico e essencial para os negócios. Para manter a sustentabilidade da empresa é primordial a proteção dos ativos de valor e eficácia na gestão dos riscos, para que assim, possa maximizar os lucros e aumentar o valor da organização [6].

Segundo [11] existem alguns aspectos essenciais para o bom andamento da segurança nas organizações, que são a confidencialidade, integridade e disponibilidade.

Ciente que confidencialidade é propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados [5]; integridade é a propriedade de proteção à precisão e perfeição de recursos [5]; e disponibilidade é a propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada [5], torna-se evidente a sua necessidade aos sistemas atuais, indiferentes do porte da empresa. [11] corrobora com tal pensamento ao colocar que estes aspectos visam à manutenção do acesso às informações pertencentes à empresa, e acessada por usuários diversos, desta forma, fazendo com que toda informação chegue ao usuário de uma forma íntegra e confiável.

Um documento importante para a gestão da segurança da informação é a política de segurança da informação. É embasado nesta política que os procedimentos e normas são criados. Ela trata de aspectos ligados a cultura e tecnologia de uma empresa, levando em conta os processos organizacionais. Depois de implantada e incorporada à cultura da organização, a política funciona como uma facilitadora do gerenciamento dos seus recursos, pois é impossível gerenciar o que não podemos definir [11]. A política de segurança "tem como objetivo 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" [3].

Para servir de base para a implementação de procedimentos de segurança existem as normas e modelos relacionados. "Um modelo pode ser pensado como uma descrição teórica da forma como um sistema funciona. No entanto, muitas vezes tem de ser simplificado, em certa medida, como sendo úteis na prática". Já as normas de segurança são documentos formais de procedimentos [6]. Entre os documentos nesta área e correlacionados com o trabalho podemos citar o Business Model for Information Security (BMIS) e as normas ISO/IEC 27001 e 27002.

Tais procedimentos de segurança também poderão servir como ponto de apoio para melhor mensurar a segurança da informação no meio corporativo, visto que carece de estudos e métricas para uma melhor aferição como é debatido por [16].

2.1 Business Model for Information Security

Do mesmo elaborador do COBIT (Control Objectives for Information and related Technology), a ISACA (Information Systems Audit and Control Association), o BMIS é uma abordagem holística e de negócios para a gestão da segurança da informação e uma linguagem comum para a segurança da informação e de gestão de negócios, de forma que simplifica a comunicação entre as áreas distintas sobre o tema proteção de ativos de informação [6]. O BMIS é essencialmente um modelo tridimensional, onde todas os pontos tem igual teor e importância. É composto de quatro elementos e seis interconexões dinâmicas (DIs), conforme a Figura 1 [6].

O BMIS já é resultado da necessidade de se propor algo mais simplificado, na área de segurança da informação, de forma que pessoas externas e as internas à área de TIC (Tecnologia da Informação e Comunicação) possam se entender neste ramo, visto que é essencial a participação de todos para uma efetiva aplicação da segurança da informação corporativa [1].

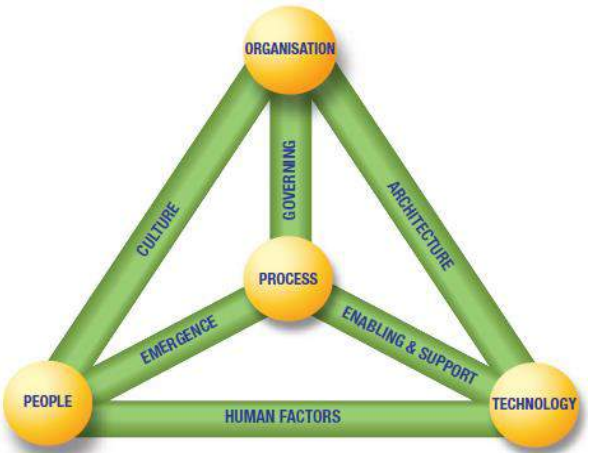

Figura 1. Modelo tridimensional em forma de pirâmide [6]

2.2 NBR ISO/IEC 27001:2006

A NBR ISO/IEC 27001 [5] é um modelo internacional para a gestão da segurança da informação, publicado em 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commision. A ABNT NBR ISO/IEC 27001:2006 [5] é baseada na norma BS 7799 (British Standard), que surgiu na década de 90 por uma iniciativa da instituição inglesa para padronizar os processos de segurança da informação e melhorar a qualidade dos dados. Segundo [9] a NBR ISO/IEC 27001 foi preparada para promover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar o sistema de gestão de segurança da informação, essa norma internacional pode ser usada visando avaliação da conformidade por partes interessadas internas e externas.

2.3 NBR ISO/IEC 27002:2005

A NBR ISO/IEC 27002 [4] surgiu em substituição a NBR ISO/IEC 17799 [3], onde são descritos um conjunto de práticas e controles para a segurança da informação, esse modelo e a norma NBR ISO/IEC 27001 [5] se complementam devendo ser utilizadas em conjunto para uma gestão de segurança da informação de qualidade. De acordo com [9] um dos principais benefícios desse modelo está na prevenção contra perdas financeiras que a organização pode ter no caso de ocorrências de incidentes de segurança da informação.

2.4 Trabalhos Correlatos

A pesquisa "Segurança da Informação - uma abordagem social" [18] e [19] faz referencia ao caráter social da segurança da informação, em um momento em que as redes sociais estão a cada dia mais inseridas no cotidiano das pessoas e das corporações, traz à tona a importância da preparação dos usuários para a obtenção de uma segurança da informação de qualidade, e apresenta a segurança da informação como um domínio multidisciplinar para as ciências sociais.

O trabalho "Método para aferir alinhamento e planejamento estratégico da tecnologia da informação e governança em tecnologia da informação" apresentado por [20], propõe uma ferramenta para verificação se as ações planejadas nas instituições pesquisadas estão em conformidade com a gestão de governança de tecnologia da informação proposta, no caso utilizou-se o COBIT na versão 4.1.

O trabalho de [21], "Sistema de gestão de segurança da informação em organizações da área de saúde", descreve o processo de implantação de um sistema de gestão de segurança da informação em uma instituição de saúde, onde pode ser comparado pelo autor, através da aplicação de questionários uma melhora nos controles implementados e uma redução dos riscos aos ativos e um aumento na conformidade com a norma de referência, no caso, utilizou-se a ISO/IEC 27001:2006.

O estudo realizado por [22] "A importância da implantação de sistemas de segurança da informação em pequenas e médias empresas", foi realizada através de uma pesquisa bibliográfica, e aborda em sua essência, a importância da implantação de sistema de segurança em pequenas e médias empresas. Propondo passos a serem seguidos na implantação de sistema de segurança.

Percebe-se que os trabalhos citados tem ligação com o presente, devido ao seu tema, assim como diversos outros poderiam ser aqui colocados. Porém o presente trabalho se diferencia pela proposta de elaborar um modelo simplificado de segurança da informação para a aplicação em pequenas e médias empresas através de uma pesquisa qualitativa objetivando desmistificar os paradigmas de custo exorbitante e da alta complexidade para a implantação de segurança da informação, assim como definir os tópicos essenciais de uma política de segurança de acordo com o ponto de vista das PMEs e validá-los. Fatos estes não encontrados em outras pesquisas na área.

Ciente da importância das PMEs para o contexto social e da diferenciação da presente pesquisa para as demais existentes, acredita-se ser relevante atualmente pesquisas como a aqui demonstrada.

3. METODOLOGIA

O presente trabalho parte de uma pesquisa descritiva com estudo de campo. Para isso, utilizou-se um questionário estruturado de abordagem quanti-qualitativo. Porém o foco principal da pesquisa enquadra-se como qualitativa, sendo quantitativa apenas a coleta de alguns pontos que irão auxiliar no embasamento do trabalho. Para a realização do estudo, a pesquisa foi restrita ao segmento de pequenas e médias empresas.

Não foi estabelecida nenhuma restrição quanto à atividade fim da empresa, podendo ser de diversos ramos de atividade, porém, tendo pelo menos uma equipe ou profissionais de TIC responsável pela área de TIC, pois caso contrário, acredita-se que não teria como foco a aplicação de uma política de segurança. Um deste profissional de TIC da empresa que deverá responder o questionário.

Outra restrição imposta foi quanto à localização geográfica, onde apenas empresas com sede ou escritório na capital pernambucana, Recife, ou cidades circunvizinhas, estavam aptas. Essa região é tratada no trabalho como "Grande Recife".

Para atingir os objetivos deste trabalho, os dados foram coletados através de um questionário estruturado disposto na Internet, com intuito de coletar informações que esclarecem alguns pontos específicos adotados pelas empresas como práticas de segurança, assim podendo ter uma visão superficial de como a segurança da informação é tratada dentro da organização.

Em uma segunda parte do mesmo questionário, que se enquadra como qualitativa, os controles de segurança retirados da norma

NBR ISO/ IEC 27002 foram submetidos à opinião das empresas quanto a sua importância para a organização em questão de forma a se selecionar quais os mais relevantes para as PMEs.

Com base na análise dos dados será proposto um modelo simplificado para aplicação de políticas de segurança nas PMEs e verificado sua aceitação via outro questionário.

Sabe-se da necessidade de uma análise de riscos para levantamento dos ativos críticos. Porém, esta etapa, mesmo que de forma simplificada, não faz parte do escopo deste trabalho.

4. RESULTADOS E DISCUSSÕES

4.1 Perfil das Empresas

A pesquisa atingiu 61 respostas no total, dessas, sete eram empresas públicas (11,5%), quatro empresas de grande porte (6,6%), uma foi desconsiderada por haver incoerência entre as respostas (1,6%), como, por exemplo, informar incorretamente o ramo de atividade da empresa, e houve uma resposta redundante (1,6%). Assim, a amostragem restante foi de 48 respostas consideradas em conformidade com os objetivos da pesquisa (78,7%). Sendo assim, todos os dados agora exibidos são oriundos, apenas, destas 48 PMEs.

Das empresas pesquisadas, observa-se que grande parte (60%) está situada no setor de prestação de serviços, estando as demais, distribuídas equilibradamente entre os setores de indústria, comércio, educação e outras áreas diversas, corroborando com o *ranking* apresentado em [13], onde mostra que 57% das PMEs que mais crescem no Brasil pertencem ao setor de serviços, assim como apontando que tal amostra tem características semelhantes ao retrato do Brasil.

Todos os respondentes eram da área de TIC. Ressalta-se que 32 deles (67%) eram responsáveis ou diretamente ligados a área de Segurança da Informação.

4.2 Política de Segurança e Conformidade com Normas

Os dados obtidos na pesquisa realizada apontam que quase metade das empresas (40%) alegou possuir uma política de segurança da informação informalmente implementada e 21% formalmente implementada, divergindo com indicadores da pesquisa de [1], onde 15% possuem uma política informal implementada e 35% uma política formal. De acordo [11], podemos identificar um problema com as empresas analisadas, pois mesmo tendo 40% delas com uma política de segurança informal implementada, é indispensável que esta seja aplicada e divulgada com a aceitação dos usuários, para que se possa controlar de forma efetiva as ações de não conformidade.

Os dados analisados confirmam o que foi exposto em [12], mostrando que 79% não estão em conformidade com alguma norma ou modelo de segurança. Os motivos para a não adequação às normas e padrões são vários, podendo destacar a cultura organizacional como um dos principais fatores (39%), ou seja, apesar do processo de informatização existente nas PMEs, ele se concentra, basicamente, em ações operacionais, baseadas em ferramentas e hardware. Ações gerenciais ou estratégicas, tais como uma política, ainda não é comum na cultura dessas empresas.

4.3 Ferramentas e Incidentes de Segurança

Ao questionar sobre as ferramentas e mecanismos de segurança utilizados, verificou-se que todas as empresas pesquisadas utilizam uma ferramenta de antivírus, e boa parte (83%) utilizam em conjunto também um *firewall*, conforme o Gráfico 1. Salienta-se que a soma dos valores ultrapassam os 100% devido a possibilidade de marcação de mais de uma ferramenta na mesma questão desta pesquisa.

No questionário foi incluída uma pergunta subjetiva, que indagava sobre os maiores problemas de segurança da informação encontrados na empresa. Entre os diversos problemas citados, os principais estão expostos no Gráfico 2.

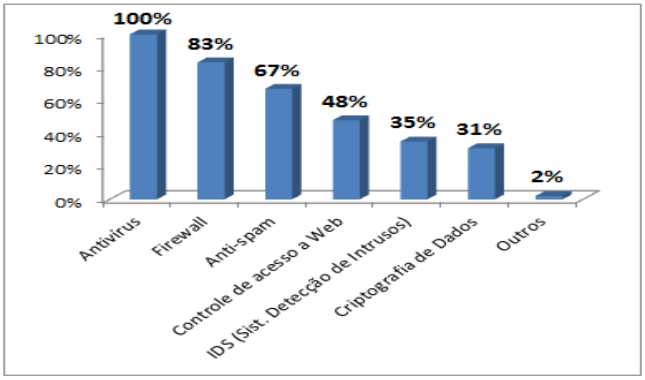

Gráfico 1. Ferramentas e mecanismos utilizados

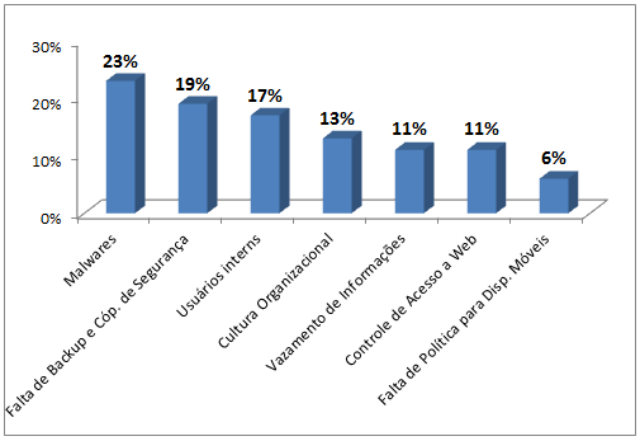

Gráfico 2. Principais Problemas citados

4.4 Análise Descritiva dos Dados

Na análise dos dados coletados na segunda parte do questionário, que se trata da parte qualitativa, foram inseridos os controles existentes na norma NBR ISO/IEC 27002 e submetidos a uma validação das empresas em uma escala de 1 (nenhuma importância) a 5 (muito importante), sendo a nota 3 categorizada como neutro na escala.

Após a análise de todos os 133 controles da norma, foram selecionados todos os controles que obtiveram médias superiores à 3, ou seja, que para a maioria era considerados importantes. Com este crivo, foram selecionados 20 controles (C1 a C20) relevantes às PMEs, exibidos na Tabela 1 e Tabela 2.

Tabela 1. Categorização dos controles de segurança da norma NBR ISO/IEC 27002 selecionados

SEÇÃO	Nº	CONTROLE
Alinhamento do negócio com segurança da informação	**C1**	Alinhamento da segurança da informação ao negócio.
Avaliar riscos da integração de novas soluções	**C2**	A.10.1 Documentação dos procedimentos de operação
	C3	A.10.2 Gestão de Mudanças
Gerenciamento da disponibilidade e da capacidade	**C4**	A.10.3.1 Gestão da capacidade
	C5	A.14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio
	C6	A.14.1.2 Continuidade de negócios e análise/avaliação de riscos
	C7	A.14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
	C8	A.14.1.4 Estrutura do plano de continuidade de continuidade do negócio
Rotinas de *Backup*	**C9**	A.10.5.1 Cópias de segurança das informações
Segurança física do *Data Center*	**C10**	A.9.1.1 Perímetro de segurança física
	C11	A.9.1.2 Controles de entrada física
	C12	A.9.1.6 Acesso do público, áreas de entrega e de carregamento
	C13	A.9.2.1 Instalação e proteção do equipamento
Segurança lógica	**C14**	A.11.1.1 Política de controle de acesso
	C15	A.11.2.1 Registro de usuário
	C16	A.11.2.2 Gerenciamento de privilégios
	C17	A.11.2.4 Análise crítica dos direitos de acesso de usuário
Gerenciamento da configuração e de inventário de recursos computacionais	**C18**	A.7.1.1 Inventário dos ativos
	C19	A.7.1.2 Proprietário dos ativos
	C20	A.7.1.3 Uso aceitável dos ativos

Pode-se dar destaque ao controle C9, com média 4,20, na mesma escala de 1-5, sendo a maior média de todos os controles propostos. Este também teve o maior percentual de empresas que o classificaram como muito importante (56%), conforme exposto no Gráfico 3.

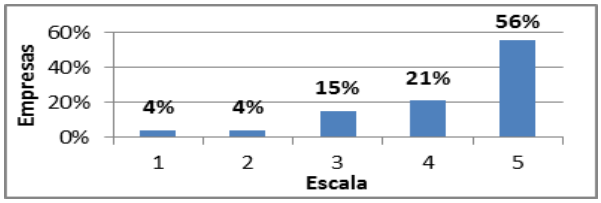

Gráfico 3. C9: Cópias de segurança das informações

Tabela 2. Detalhamento dos valores obtidos

Nº	MÉDIA	DESVIO PADRÃO	MEDIANA
C1	3,35	0,982	3
C2	3,45	1,045	4
C3	3,45	0,955	3
C4	3,60	0,920	4
C5	3,41	0,875	3,5
C6	3,45	0,920	4
C7	3,31	0,922	3
C8	3,35	0,911	3
C9	4,20	0,891	5
C10	3,39	1,195	3
C11	3,18	1,378	3
C12	3,45	1,292	3,5
C13	3,81	0,901	4
C14	3,79	1,043	4
C15	3,85	0,986	4
C16	4,02	0,775	4
C17	3,81	0,935	4
C18	3,47	1,106	4
C19	3,43	0,961	4
C20	3,39	0,820	3

4.5 Proposta Simplificada para as PMEs

Nesta seção será incluído um conjunto de controles considerados mais importantes no contexto pesquisado, conjunto este sugerido como uma proposta de modelo simplificado para pequenas e médias empresas contendo um conjunto de controles da norma NBR ISO/IEC 27002. Os 133 controles da norma NBR ISO/IEC 27002 foram reduzidos para 22. Os controles propostos serão colocados na sequência de implementação, porém as diretrizes para a implementação de cada controle deve ser consultada a partir das normas da ISO.

Para definir a sequência em que os controles foram dispostos no modelo a seguir, utilizou-se as médias obtidas na pesquisa, priorizando os controles que obtiveram as maiores médias, exceto em caso de pré-requisitos entre controles. É importante lembrar que alguns controles ou parte deles poderão ser omitidos, dependendo da necessidade da empresa.

1- Alinhamento da segurança da informação ao negócio: É importante que todos os esforços para implementação dos controles propostos por este modelo simplificado estejam de acordo com as características da empresa em questão. Segundo [17], um fator importante é que os planos de segurança da

informação estejam alinhados com a necessidade do negócio, estratégia e processos da empresa. Este é um fator enfatizado no BMIS e considerado por algumas normas um requisito, porém foi considerado um controle e colocado como primeiro item neste modelo simplificado para que seja seguido em todo o processo de implantação.

2- Cópias de segurança das informações: Este controle recomenda através da política de geração de cópias de segurança que sejam realizadas cópias de informações de negócio e de softwares e testes de efetividade regularmente. Convém que seja determinado o período em que se pretende manter a cópia das informações. Todo este processo pode ser automatizado através de diversas ferramentas de mercado, porém, devem-se testar periodicamente as mesmas [4].

3- Políticas de controle de acesso: Para implementação deste controle é recomendado que sejam criadas regras de controle de acesso, e estas devem estar incluídas na política de controle de acesso, como também que as regras sejam apoiadas e formalizadas, com a nítida definição das responsabilidades. É conveniente que sejam abordados aspectos de controle de acesso lógico e físico conjuntamente numa mesma política. É importante também que seja disponibilizado aos usuários e provedores de serviço uma declaração clara dos requisitos de negócio relativos a controle de acesso [4].

4- Registro de usuário: Com a política de controle de acesso definida, o próximo passo é o registro dos usuários, para a implementação deste controle convém que sejam definidos procedimentos formais de registro e cancelamento de usuários para todos os sistemas e serviços utilizados na empresa [4].

5- Gerenciamento de privilégios: Após o processo de controle de acesso e registro de usuários estarem funcionando efetivamente surge a necessidade de gerenciar os privilégios concedidos, que deve ser um processo constante, devido ao dinamismo das mudanças na organização. Para isto a norma NBR ISO/IEC 27002 [4] sugere que se restrinja e controle a liberação de privilégios.

6- Análise crítica dos direitos de acesso dos usuários: É interessante que seja conduzido a intervalos regulares a análise crítica dos direitos de acesso, este deve ser feito pelo gestor através de um processo formal [4].

7- Instalação e proteção dos equipamentos: Recomenda-se a reserva de um local protegido para a acomodação dos equipamentos associados a recursos computacionais, assim evitando diversas ameaças como perigos do meio ambiente e acesso não autorizado [4].

8- Gestão da capacidade: É recomendado que os recursos de sistemas sejam monitorados e ajustados quando necessário. É importante também que sejam realizadas projeções para necessidade de capacidade futura, no intuito de garantir o desempenho requerido do sistema [4].

9- Inventário dos ativos: Com gerenciamento de acesso dos usuários sobre controle, um próximo passo a seguir é o de controlar os ativos e recursos computacionais. Para isto, é importante utilizar inicialmente o controle de inventário dos ativos, que recomenda a identificação de todos os ativos, mantendo um inventário atualizado com o máximo de informações possíveis, como tipo do ativo, formato, localização, informações sobre licença e etc. [4].

10- Proprietário dos ativos: Este controle recomenda que para os ativos e as informações relacionadas a eles tenham um proprietário[1], este deve ser determinado por parte específica da organização [4].

11- Uso aceitável dos ativos: É importante que sejam estabelecidas e documentadas regras quanto à utilização dos ativos e recursos computacionais. Estas regras devem ser seguidas não apenas por funcionários internos, mas também por fornecedores e terceiros [4].

12- Documentação dos procedimentos de operação: É importante que sejam documentados, mantidos e atualizados todos os procedimentos de operação, estando sempre disponíveis a todos que precisem deles [4].

13- Gestão de mudanças: É recomendado que seja realizado um controle de todas as modificações nos recursos computacionais, sistemas e serviços [4].

14- Incluindo segurança da informação no processo de continuidade do negócio: É recomendado que seja elaborado, mantido e testado um processo de gerenciamento da continuidade do negócio em toda a organização, este deve contemplar os requisitos de segurança da informação [4].

15- Continuidade do negócio e análise/avaliação de riscos: É conveniente que os eventos que possam impactar nos processos de negócio, causando interrupções, sejam identificados e analisados para verificar a probabilidade e impacto das interrupções e quais as consequências para a segurança da informação [4].

16- Estrutura do plano de continuidade do negócio: É conveniente que se mantenha uma estrutura básica dos planos de continuidade do negócio, assim é possível assegurar a consistência dos mesmos. É importante também incluir os requisitos de segurança da informação e identificar as prioridades para testes e manutenção [4].

17- Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação: É importante que sejam elaborados e implementados planos para a recuperação das operações, assegurando a disponibilidade da informação no nível e na escala de tempo requerida, após eventos de interrupção nos processos de negócio [4].

18- Perímetro de segurança física: Todos esses controles implementados anteriormente seriam burlados em caso onde a segurança física é falha. Então, recomenda-se que sejam utilizados de alguma forma controles físicos, tais como, paredes, portões de entrada controlados por cartões, biometria entre outros, balcões com recepcionistas e etc., isto, para proteger áreas que possuem instalações e sistemas de processamento da informação [4].

19- Acesso do público, áreas de entrega e de carregamento: É recomendado que alguns pontos em que exista a circulação de pessoas não autorizadas sejam controlados e, caso possível, separados de áreas seguras [4].

---

[1] O termo proprietário, não significa que a pessoa realmente tenha direito de propriedade, mas apenas identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso ou a segurança dos ativos [4].

20- Controles de entrada física: Recomenda-se que controles de entrada apropriados sejam utilizados em áreas seguras, assegurando a entrada de pessoas autorizadas, apenas [4].

Após a realização da pesquisa, percebeu-se que seria interessante acrescentar ao modelo simplificado alguns outros dois controles não previstos, mas complementares aos demais inseridos, e essenciais para uma abraçar os principais pontos corporativos.

21- Conscientização, educação e treinamento em segurança da informação: percebeu-se pelo questionário que as empresas pesquisadas demonstraram uma imaturidade (falta de cultura na a área) ou falta de capacitação adequada aos profissionais quanto ao assunto segurança da informação. Com isso foi acrescentado ao modelo simplificado este controle, que está disposto na seção 8 da norma NBR ISO/IEC 27002 [4]. Este controle recomenda que sejam ministrados treinamentos adequados e conscientização sobre as políticas e procedimentos de segurança da informação para todos da organização de acordo com suas funções [4].

22- Política de Segurança da Informação: Este último controle adicionado está disposto na seção 5 da norma NBR ISO/IEC 27002 [4]. Sua inserção tornou-se necessária, pois é através deste documento que serão documentados efetivamente boa parte dos demais controles deste modelo simplificado. Este controle recomenda que o documento de política de segurança da informação tenha o apoio da alta direção sendo, aprovada, publicada e comunicada para todos da organização, incluindo partes externas relevantes. Na política de segurança da informação deve ser exposto o comprometimento da direção com o gerenciamento de segurança da informação [4].

Para validar a presente proposta de modelo simplificado, foi enviado para 51 profissionais da área de TIC de PMEs, o modelo simplificado proposto e um questionamento se o mesmo atendia as necessidades da empresa e se elas implantariam este modelo simplificado, assim como se solicitou a justificativa da resposta. Dos 51 questionários enviados, 38 foram retornados. Destes, apenas 1 afirmou que o modelo não atendia as necessidades da empresa. Ou seja, 97,4% dos respondentes afirmaram que os controles selecionados atendem a necessidade de sua empresa. Destes 37 apenas 1 afirmou que, mesmo atendendo as necessidades da empresa, não implantaria, visto que ainda se torna muito complexo. As demais 36 respostas, 94,7% dos respondentes, afirmaram ser viável e que implantariam tal proposta na empresa.

5. CONSIDERAÇÕES FINAIS

5.1 Análise Dos Resultados

Através da pesquisa, confirma-se que muitas das PMEs não estão em adequação com algum tipo de norma ou padrão de segurança da informação. Outro fator identificado foi que, a política de segurança, mesmo quando implementada, geralmente esta implementação é feita de maneira informal, isto representa um problema, pois como já foi dito por [11], para que se tenha efetividade e eficácia, a política de segurança deve ser formalmente implementada, além de ser imprescindível o apoio da alta direção.

Diante de diversos fatores a serem considerados para a não adequação as normas de segurança da informação, pode-se destacar a cultura organizacional das PMEs como um dos maiores fatores impeditivos. Percebeu-se também que algumas PMEs acreditam que a segurança da informação é desnecessária para a empresa, mesmo possuindo recursos de sistemas de informação, fator considerado para a elaboração do modelo.

A falta de cultura organizacional sobre o tema segurança da informação por parte das empresas pesquisada é um fator que as tornam vulneráveis a ameaças que exploram fatores humanos, como a engenharia social, que segundo [15] "pode ser entendida como uma arte para manipular pessoas fazendo-as tomar ações que normalmente não fariam para um estranho, normalmente cedendo algum tipo de informação".

Na pesquisa, os controles selecionados para o modelo atingiram de uma forma geral médias superiores a 3,18 em uma escala de 1-5, o que comprova uma importância no mínimo razoável quanto à implementação destes nas PMEs. Dos controles analisados, pode-se destacar o controle C9 (Cópias de segurança das informações), que obteve a maior média de todos os controles propostos (4,20), sendo assim, nos remete a importância das informações para empresas deste porte que lidam com sistemas de informações ligados ao negócio, pois, à medida que é dada ênfase a salvaguarda das informações armazenadas, subentende-se que essas são relevantes para a organização. Contribuindo com [1], que coloca que a segurança da informação deve ser entendida como uma responsabilidade de todos. Afinal a informação existe porque alguém irá precisar dela em algum momento.

Após a realização da pesquisa e análise dos dados foi julgada a necessidade da inclusão de alguns controles adicionais, como o que define o documento de política de segurança, retirado da seção 5 da norma NBR ISO/IEC 27002 [4], pois este é um controle que através de um documento único permite a implementação de boa parte dos demais controles contidos no modelo simplificado. Outro controle adicional foi o de conscientização, educação e treinamento em segurança da informação retirado da mesma norma (seção 8), para trabalhar a questão da imaturidade da organização em relação a SI, enfatizando sua importância para os negócios. Após a criação do modelo simplificado com 22 controles, foi validado com sucesso, também via questionário, com um conjunto de 38 representantes da área de TIC de PMEs.

5.2 Conclusões e Trabalhos Futuros

O intuito deste trabalho, "analisar normas NBR ISO/IEC 27001, NBR ISO/IEC 27002 e o BMIS, de forma a extrair os principais pontos para a elaboração de um modelo simplificado de segurança para pequenas e médias empresas" foi atendido após a análise das normas, seleção prévia dos controles de segurança e validação dos mesmos sob a perspectiva das PMEs e por fim, a elaboração do modelo simplificado contendo um conjunto de controles adaptados para pequenas e médias empresas.

Acredita-se que a implementação do modelo simplificado proposto neste trabalho, apesar de não ser por si só, suficiente para atingir um nível aceitável de segurança, é um grande passo para uma melhoria significativa. É possível concluir também por meio da observação dos dados, que há uma carência de práticas e modelos de segurança nas empresas deste porte, havendo assim, a necessidade de trabalhos e pesquisas direcionados a segurança da informação nas PMEs, visando melhorar a situação atual.

Por fim, com a situação descrita no trabalho, é visível que as PMEs carecem de um aprimoramento das práticas de segurança

da informação. Para isto, sugere-se a elaboração de trabalhos futuros mais aprofundados neste segmento que possam agregar e complementar informações encontradas nesta pesquisa, por exemplo, extrapolando o limite geográfico proposto ou estudando outros modelos e normas existentes, assim como as áreas de gestão continuidade e risco. Na área de gestão de risco, como forma complementar, acredita-se ser interessante realizar uma análise de risco prévia, de forma a confrontar os principais itens levantados com os selecionados neste modelo simplificado.

6. REFERÊNCIAS

[1] Alencar, G. D.; Queiroz, A. A. L.; De Queiroz, R. J. G. B. (2013). Insiders: Um Fator Ativo na Segurança da Informação. In: IX Simpósio Brasileiro de Sistemas de Informação (SBSI'13), p. 61-72.

[2] Trendlabs. (2014) "2Q 2012 Security Roundup", http://www.trendmicro.com.br/cloud-content/us/pdfs /security-intelligence/reports/rpt-its-big-business-and-its-getting-personal.pdf. Acesso: 28 de Agosto de 2014.

[3] ABNT. (2005a) NBR ISO/IEC 17799: Tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação.

[4] ABNT. (2005b) NBR ISO/IEC 27002: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.

[5] ABNT. (2006) NBR ISO/IEC 27001: Sistema de Gestão de Segurança da Informação – Requisitos.

[6] BMIS. (2007) "Business model for information security. IT Governance Institute", http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx. Acesso: 01 de Março de 2015.

[7] PWC. (2013) "Pesquisa global de segurança da informação 2013". http://www.pwc.com.br/pt/estudos-pesquisas/giss-2013.jhtml. Acesso: 13 de Dezembro de 2014.

[8] Diniz, I. J. D.; Medeiros, M. F. M.; Souza Neto, M. V. (2012) Governança de TI: a visão dos concluintes de Administração e Ciências da Computação. In: Revista Brasileira de Administração Científica, v.3, n.2, p.7-24.

[9] Fernandes, A. A.; Abreu, V. F. (2012), Implantando a governança de TI. Brasport, 3 ed.

[10] IBGE. (2010) "Cadastro Central de Empresas 2010", http://www.ibge.gov.br/home/estatistica/economia/cadastroempresa/2010/default.shtm. Acesso: 01 de Março de 2015.

[11] Nakamura, E. T.; Geus, P. E. (2007), Segurança de redes em ambientes cooperativos. Novatec.

[12] Computerworld. (2011) "PMEs não estão preparadas para desastres",http://computerworld.uol.com.br/seguranca/2011/01/31/pequenas-e-medias-empresas-nao-estao-preparadas-para-desastres/, Acesso: 01 de Março de 2015.

[13] Revista Exame Pme. (2012), 250 Pequenas e médias empresas que mais crescem. São Paulo: Abril, set 2012. ed. 53.

[14] Symantec. (2013) "PMEs: 7 previsões para proteger informações em 2013",http://www.symantec.com/connect/blogs/pmes-7-previsoes-para-proteger-informacoes-em-2013. Acesso: 01 de Março de 2015.

[15] Alencar, G. D.; Lima, M. F.; Firmo, A. C. A. (2013) O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing. In: IX Simpósio Brasileiro de Sistemas de Informação (SBSI'13), p. 254-259.

[16] Miani, R. S., Zarpelão, B. B., Mendes, L. S. (2014) Um estudo empírico sobre o uso de métricas de segurança em ambientes reais. In: X Simpósio Brasileiro de Sistemas de Informação (SBSI 2014), p. 699–710.

[17] Semola, M. Gestão da Segurança da Informação: Uma visão executiva. Rio de Janeiro: Editora Elsevier, 2003. 156 p.

[18] Marciano, J. L. P. Segurança da Informação uma Abordagem Social. 2006, 212p. Tese (Doutorado em Ciência da informação) – Universidade de Brasilia, Brasilia

[19] Marciano, J. L.; Marques. M. L. O Enfoque Social da Segurança da Informação. Ci. Inf. Brasília, v. 35, n. 3, p. 89-98, Dezembro 2006.

[20] Silva, Lucio Melre da. Método para Aferir Alinhamento e Planejamento Estratégico da Tecnologia da Informação e Governança em Tecnologia da Informação. 2011, 201p. Dissertação (Mestre em Gestão do Conhecimento e Tecnologia da Informação) – Universidade Católica de Brasília, Brasília

[21] Ribas, Carlos Eduardo. Sistema de Gestão de Segurança da Informação em Organizações de Saúde. 2010, 104p. Dissertação (Mestre em Ciências) – Universidade de São Paulo, São Paulo.

[22] Moraes, Samuel Nunes de. A Importância da Implantação de Sistemas de Segurança da Informação em Pequenas e Médias Empresas, 2011, 49p. Monografia (Especialista em Segurança da Informação) – Universidade Fumec, Belo Horizonte.

[23] SEBRAE/SP. (2015) "Pequenos Negócios em Números", http://www.sebraesp.com.br/index.php/234-uncategorised/institucional/pesquisas-sobre-micro-e-pequenas-empresas-paulistas/micro-e-pequenas-empresas-em-numeros. Acesso: 14 de Abril de 2015.

[24] SEBRAE/Nacional. (2015) "Em dez anos, os valores da produção gerada pelos pequenos negócios saltaram de R$ 144 bilhões para R$ 599 bilhões", http://www.sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/Micro-e-pequenas-empresas-geram-27%25-do-PIB-do-Brasil. Acesso: 14 de Abril de 2015.

[25] Santos, B. (2015) Segurança Digital - Segurança da informação como prioridade para as PMEs, http://segurancadigital.ig.com.br/2015/02/02/seguranca-da-informacao-como-prioridade-para-as-pmes/. Acesso: 14 de Abril de 2015.

[26] Decision Report. (2015) "Dicas de Segurança para PMEs" http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=18250&sid=41&tpl=printerview. Acesso: 14 de Abril de 201