DOI: 10.5748/9788599693100-11CONTECSI/PS-714

ALIGNMENT OF INFORMATION SECURITY WITH BUSINESS AREAS - CONTRIBUTION OF NBR ISO/IEC 27002:2013

Edison Luiz Goncalves Fontes (Universidade Federal de Pernambuco, Pernambuco, Brasil) - edison@pobox.com

This research aimed to identify the controls of the NBR ISO/IEC 27002:2013 that guide the participation of the business areas in the process of information security. The alignment process of information security with business areas is required and in this context, the question arose: the controls of the standard require the participation of the business areas? The standard ISO/IEC 27002:2013 is the main regulation for the process of information security. A survey was conducted to identify the controls that require, directly or indirectly, participation of business areas. As a result, was identified a set of 28 controls of the 114 total controls, that requiring the participation of the business areas and thus enable the alignment of the process of information security with the organization goals. Then it was concluded that the NBR ISO/IEC 27002:2013 contributes to the alignment of the management of information security with business areas.

Keywords: information security; IT security; business objectives; information management; risk.

ALINHAMENTO DA SEGURANÇA DA INFORMAÇÃO COM AS ÁREAS DE NEGÓCIO - CONTRIBUIÇÃO DA NBR ISO/IEC 27002:2013

Esta pesquisa teve como objetivo identificar os controles da NBR ISO/IEC 27002:2013 que orientam a participação das áreas de negócio no processo de segurança da informação. O processo de alinhamento da segurança da informação com as áreas de negócio é necessária e, neste contexto, surgiu a questão: os controles da norma requerem a participação das áreas de negócio? A norma ISO/IEC 27002:2013 é o principal regulamento para o processo de segurança da informação. A pesquisa foi realizada para identificar os controles que exigem, direta ou indiretamente, participação das áreas de negócio. Como resultado, foi identificado um conjunto de 28 controles dos 114 controles totais, que exigem a participação das áreas de negócio e, assim, permitem o alinhamento do processo de segurança da informação com os objetivos da organização. Assim, concluiu-se que a NBR ISO/IEC 27002:2013 contribui para o alinhamento da gestão da segurança da informação com as áreas de negócio.

Palavras-chave: segurança da informação; segurança de TI; os objetivos de negócios; gestão da informação; risco.

1. INTRODUÇÃO

1.1 – Pesquisa realizada

Como parte do levantamento teórico e estado da arte no rol de pesquisas vinculadas ao projeto de estudo do tema segurança da informação e seu alinhamento aos objetivos da organização foi desenvolvida uma pesquisa que teve por objetivo identificar quais controles da Norma NBR ISO/IEC 27002:2013 - Tecnologia da informação – Código de prática para a gestão da segurança da informação, possibilitam o alinhamento da gestão da segurança da informação com as áreas de negócio e consequentemente com os objetivos da organização. Em 2013 a Norma NBR ISO/IEC 27002 teve uma nova versão com várias alterações nos seus controles, na sua abordagem e reduzindo a quantidade dos mesmos de 133 na versão do ano 2005, para 114 controles na versão do ano 2013.

Esta norma foi tomada como base para esta pesquisa, em função de ser um normativo internacional produzido pela ISO *(International Organization for Standardization)* e aceito como padrão para a gestão da segurança da informação nas organizações. Um exemplo de seu uso como base para a gestão da segurança da informação em uma organização de excelente reputação na área acadêmica e empresarial (Universidade de São Paulo), é o documento Política de Segurança da USPNet que cita a norma (utiliza a nomenclatura antiga, NBR ISO/IEC 17799:2005) ao indicar suas atribuições:

> *- Elaborar uma Política de Segurança que dê sustentação às atividades de proteção da informação eletrônica da Universidade;*
> *- Propor Planos de Segurança e de Contingência para os sistemas computacionais da Universidade, sempre que possível de acordo com a norma NBR ISO/IEC 17799. (USP, 2010: 00)*

Para se tornar um documento da ISO o texto precisa ser submetido a um grupo de trabalho formado por profissionais de várias organizações e de vários países, cumpre um processo estruturado de discussão e para sua aprovação precisa ter 75% de votos dos participantes do respectivo comitê técnico, (ISO, 2005)

Antes deste padrão, alguns países tinham regulamentos próprios e cada uma das grandes empresas de consultoria tinha seu padrão específico. Atualmente estas empresas de consultorias apoiam e reforçam o uso da norma NBR ISO/IEC 27002:2013.

A metodologia de pesquisa utilizada foi documental e foi realizada através da leitura detalhada da norma com o objetivo de identificar no conjunto dos controles, aqueles que exigem, direta ou indiretamente, para a sua implantação, a participação das áreas de negócio.

Esta norma declara no seu Item 0–Introdução, que ela deve ser usada como "uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão de segurança da informação" (ABNT-27002, 2013: x) e indica no seu item 5–Política de segurança da informação, que a política deve estar "de acordo com os requisitos de negócio da organização e com as leis e regulamentação relevantes" (ABNT-27002, 2013: 2).

Com base nestas duas declarações identifica-se que existe a necessidade de uma relação entre o processo de segurança da informação e os objetivos das áreas de negócio. Surge então a questão: o que a Norma NBR ISO/IEC 27002:2013 exige para o alinhamento do processo de segurança da informação com as áreas de negócio da organização?

A pesquisa realizada teve por objetivo responder a esta pergunta na medida em que ela identifica, em cada um dos controles da norma, as diretrizes que requerem a participação das áreas de negócio. É considerada a hipótese de que existem controles que orientam o alinhamento da gestão da segurança da informação com as áreas de negócio.

Este tema é significativo no campo da proteção da informação uma vez que sempre se busca o alinhamento da segurança da informação com as áreas de negócio. Esta importância aumenta na medida em que todas as organizações precisam desenvolver ou manter seus regulamentos de segurança da informação. Para tanto, a Norma ISO/IEC 27002:2013 declara que os requisitos de segurança da informação "podem ser aplicados em todas as organizações e não depende do seu tipo, tamanho e natureza", (ABNT-27002, 2013: x)

Este artigo inicialmente aborda a Norma ISO/IEC 27002:2013 e em seguida trata a questão de alinhamento da segurança da informação com as áreas de negócio identificando na literatura as orientações sobre este aspecto.

Na continuação são descritas os controles que possibilitam que a segurança da informação alcance o seu alinhamento com as áreas de negócio.

Em sequência é apresentada a conclusão que contém as considerações finais e as observações sobre o trabalho realizado.

Por fim são descritas as recomendações para o uso desta pesquisa no processo de segurança da informação e para futuras explorações sobre o tema.

1.2. A Norma NBR ISO/IEC 27002:2013

A Norma NBR ISO/IEC 27002:2005 tem sua origem na Norma Britânica BS-7799 que foi criada em 1993 pelo Órgão de Padrão Britânico (British Standard) que por sua vez se baseou em um código de boas práticas de segurança da informação do Governo do Reino Unido. Em 1995 este código foi republicado pelo BSI-British Standard International e foi criada a norma BSI-7799. No final da década de 1990, o BSI criou um programa para a certificação de empresas na Norma BS-7799. O reconhecimento da importância da segurança da informação aumentou e a Norma BS-7799 foi atualizada, reestruturada e dividida em duas partes: BS-7799-1(Código de prática) e BS-7799-2 (Requisitos para certificação). O próximo passo foi a transformação em Norma ISO. No ano 2000 a BS-7799-1 foi publicada pela *International Organization for Standardization* como ISO 17799. Em 2004, ocorreu uma nova revisão e foi publicada a Norma ISO/IEC 17799:2005. Logo depois a ISO dedicou a família 27000 ao tema segurança da informação e em 2007 trocou o nome da norma para ISO/IEC 27002:2005, mantendo exatamente o mesmo conteúdo. Anteriormente, a parte 2 da BS-7799 quando foi transformada em norma ISO, já utilizou a nomenclatura da nova família: ISO/IEC 27001:2005. Após estes fatos a ABNT – Associação Brasileira de Norma Técnicas publicou estas normas em português. Em 2013 a ISO divulgou a nova versão da Norma 27002 e neste mesmo ano a ABNT publicou a versão em português.

A Norma NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para a segurança da informação estabelece "as diretrizes e os princípios gerais para iniciar, implantar, manter e melhorar a gestão de segurança da informação em uma organização" (ABNT-27002, 2013: x).

Esta norma é composta por um conjunto de controles que tem como objetivo a proteção da informação. Para cada controle são definidas as suas diretrizes que indicam como deve ser implantado o respectivo controle. Alguns controles indicam a participação

direta ou indireta da área de negócio. A identificação dos controles que requerem a participação da área de negócio foi o objetivo desta pesquisa.

Na medida em que a área de negócio participa da definição da segurança da informação em relação à rigidez de cada controle, à prioridade para a implantação dos controles e ao apetite de risco, a gestão da segurança da informação estará alinhada com as áreas de negócio e consequentemente com os objetivos da organização.

A Norma NBR ISO/IEC 27002:2013 indica como um dos fatores críticos de sucesso para a implantação da segurança da informação o fato da política, dos objetivos e das atividades do processo de segurança da informação estarem aderentes aos objetivos das áreas de negócio. Outro fator que a norma destaca é o comprometimento e o apoio visível de todos os níveis gerenciais. A norma ainda descreve que o "processo de segurança da informação deve ser feito em conjunto com os outros processos de gestão de negócio" (NBR 27002, 2013: xi).

1.3 - Alinhamento da segurança da informação ao negócio

A Norma NBR ISO/IEC 27002:2013 declara que "a informação é um ativo essencial para o negócio de uma organização e necessita ser adequadamente protegida" (NBR 27002, 2013: x). Porém, a proteção da informação não deve acontecer por si só. A proteção deve acontecer porque existem os objetivos de negócio. Peltier enfatiza que a segurança da informação ajuda a organização a alcançar seus objetivos de negócio por intermédio de seus ativos tangíveis, de seus ativos intangíveis e deve dar suporte a realização da missão da organização, (Peltier, 2004 e 2005) Ele continua destacando que a alta direção é exigida para proteger os ativos da organização e deve tomar decisões baseadas em informações confiáveis. Isto nos indica que o processo de segurança da informação precisa ser posicionado de uma maneira menos operacional. Wylder afirma que os programas de segurança da informação precisam se mover da implantação tática da tecnologia para se tornar parceiros estratégicos do negócio (Wydler, 2004). Peltier complementa este pensamento quando afirma que só existem objetivos de negócio e a segurança da informação deve estar integrada em todos os processos de negócio, (Peltier, 2004 e 2005). Calder e Watkins reforçam quando afirmam que as organizações devem garantir que qualquer processo que seja implantado deva ser apropriado e construído sob medida para o ambiente da respectiva organização, (Calder e Watkins, 2005). Quando estivermos construindo uma arquitetura de segurança, Sherwood, Clark e Linas nos orientam indicando que a arquitetura corporativa de segurança deve ser guiada com base na perspectiva do negócio e deve considerar a variedade de requerimentos que inclusive podem conflitar entre si, (Sherwood, Clark, Lynas, 2005). E não podemos esquecer que a segurança da informação vai afetar cada funcionário da organização em função das políticas e dos controles implantados (Maiwald e Sieglein, 2002).

Domeneghetti e Meir incluem a segurança da informação como um ativo intangível de proteção de valor. Eles classificam os ativos da organização em ativos tangíveis e ativos intangíveis. Os ativos intangíveis são divididos em duas categorias de ativos em relação ao propósito econômico: ativos de geração de valor e ativos de proteção de valor. Estes autores declaram que para alcançar a sustentabilidade corporativa devem-se considerar os ativos tangíveis e os ativos intangíveis ao longo da vida da organização. (Domeneghetti, Meir, 2009).

Pensar em sustentabilidade e transparência nos leva ao conceito de governança. Tomando por base várias definições do IT Governance Institute pode-se consolidar uma

definição para a Governança de Segurança da Informação: é a estrutura de relacionamentos e processos para controlar a organização de maneira que ela alcance seus objetivos e minimize os seus riscos de segurança da informação contando com o envolvimento dos executivos de negócio nas decisões relativas à segurança da informação e que afetam ao negócio da organização. (ITGI, 2008).

Alinhar a segurança da informação aos requisitos de negócio é um elemento necessário para um efetivo processo de segurança da informação. Porém, ao se falar desse alinhamento fica a dúvida: como operacionalizar esse alinhamento?

A pesquisa apresentada neste artigo identificou no conjunto de controles, aqueles que exigem a participação das áreas de negócio e consequentemente possibilitam esse alinhamento. A implantação destes controles possibilita o alinhamento da segurança da informação com as áreas de negócio. A Norma ISO/IEC 27002:2013 possui no seu texto a exigência deste alinhamento, como é dito no seu início: "Os controles (de segurança) precisam ser estabelecidos, implantados, monitorados, analisados criticamente e melhorados quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos." (ABNT-27002, 2013: x).

2. METODOLOGIA

Para cada uma das seções em que a norma divide as categorias principais de segurança da informação, foi analisado o seu texto e foram identificadas aqueles controles que exigem a participação das áreas de negócio.

Foram considerados os controles que diretamente explicitam a necessidade de participação das áreas de negócio, bem como os controles que indiretamente fazem esta orientação ou exigência.

3. RESULTADOS

Para cada um dos capítulos da norma, foram encontrados os seguintes controles que orientam o processo de segurança da informação para o alinhamento com as áreas de negócio.

Capítulo 5 – Políticas de segurança da informação

Controle: Políticas para a segurança da informação.

> *5.1.1 - Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. (ABNT-27002, 2013: 2)*

Este controle exige o comprometimento da direção da organização e desta forma garante que as orientações básicas do processo de segurança da informação estarão alinhadas com os objetivos de negócio e da organização.

Capítulo 6 – Organização da segurança da informação

Controle: Responsabilidades e papéis pela segurança da informação.

> *6.1.1 – Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas. (ABNT-27002, 2013: 4)*

Controle: Segregação de funções.

> *6.1.2 - Convém que funções conflitantes e áreas de responsabilidades sejam segregadas para reduzir as oportunidades de modificação não autorizada ou*

> *não intencional, ou uso indevido dos ativos da organização. (ABNT-27002, 2013: 5)*

Controle: Segurança da informação no gerenciamento de projetos.

> *6.1.5 - Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto. (ABNT-27002, 2013: 7)*

Estes controles explicitam que o processo de segurança da informação deve ser considerado na estrutura da organização, tendo explicitado as suas responsabilidades e limites. Esta orientação afeta as áreas de negócio pois indica qual a autoridade da área de segurança da informação sobre alguns aspectos das áreas de negócio.

A exigência da segregação de função afeta diretamente as áreas de negócio e exige que estas áreas de negócio definam que funções devem ser segregadas. Esta definição de segregação de função é uma responsabilidade básica das áreas de negócio.

A participação inicial da área de segurança da informação nos diversos projetos da organização afeta as áreas de negócio pois todos os projetos devem considerar a segurança da informação.

Capítulo 8 – Gestão de ativos

Controle: Proprietário dos ativos.

> *8.1.2 - Convém que os ativos mantidos no inventário tenham um proprietário. (ABNT-27002, 2013: 17)*

Controle: Classificação da informação.

> *8.2.1 - Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. (ABNT-27002, 2013: 18)*

Estes controles indicam que:

a) diferente do que historicamente ocorreu (ou ocorre) onde a área de Tecnologia da Informação na prática assumia a função de proprietária da informação, é exigido que o proprietário da informação seja das diversas áreas da organização, isto é, seja da área (de negócio ou de apoio) que é responsável pela informação;

b) a classificação da informação existirá em função do seu valor, critério este que é de responsabilidade da área de negócio identificar este valor.

Capítulo 7 – Segurança em recursos humanos

Controle: Recursos Humanos - Seleção.

> *7.1.1 - Convém que verificações do histórico sejam realizadas para todos os candidatos a empregos, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos de negócio, aos riscos percebidos e à classificação das informações a serem acessadas. (ABNT-27002, 2013: 11)*

Controle: Recursos Humanos – Termos e condições de contratação.

> *7.1.2 - Convém que as obrigações contratuais com funcionários e partes externas declarem a sua responsabilidade e as da organização para a segurança da informação. (ABNT-27002, 2013: 12)*

Controle: Recursos Humanos – Responsabilidade da Direção.

> *7.2.1 - Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização. (ABNT-27002, 2013: 13)*

Controle: Recursos Humanos – Conscientização, educação e treinamento.

> *7.2.2 - Convém que todos os funcionários da organização e, onde pertinente, partes externas, recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções. (ABNT-27002, 2013: 13)*

Estes controles definem que qualquer pessoa, funcionário ou prestador de serviço, que utilize profissionalmente as informações da organização, necessitam ter suas obrigações definidas e precisam estar condizentes com as funções que vão exercer. Estes controles exigem uma série de responsabilidades para as pessoas em todas as áreas da organização, indicando que todos os gestores têm responsabilidade sobre as pessoas sob sua responsabilidade. É muito comum as áreas de negócio considerarem que apenas a área de segurança da informação é responsável por todas as pessoas da organização, no que diz respeito à proteção da informação.

Capítulo 11 – Segurança física e do ambiente

Controle: Perímetro de segurança física.

> *11.1.1 - Convém que perímetros de segurança sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis. (ABNT-27002, 2013: 38)*

Controle: Trabalhando em áreas seguras.

> *11.1.5 - Convém que sejam projetados e aplicados procedimentos para o trabalho em áreas seguras (ABNT-27002, 2013: 40)*

Estes controles definem proteção para o ambiente físico, inclusive as áreas de negócio. A rigidez destes controles precisam ser feitos em conjunto da área de segurança da informação com a área de negócio.

Capítulo 9 – Controle de acesso

Controle: Política de controle de acesso.

> *9.1.1 - Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios. (ABNT-27002, 2013: 23)*

Controle: Análise crítica dos direitos de acesso de usuário.

> *9.2.5 - Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários a intervalos regulares. (ABNT-27002, 2013: 28)*

Estes controles de acesso à informação indicam a necessidade de uma política de acesso que deve ser elaborada em conjunto com as áreas de negócio e explicita a necessidade do proprietário do ativo informação, que na maioria das vezes será da área de negócio.

Capítulo 12 – Segurança nas operações

Controle: Gestão de mudanças.

> *12.1.2 - Convém que mudanças na organização, nos processos de negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas. (ABNT-27002, 2013: 49)*

Controle: Gestão de capacidade.

> *12.1.3 - Convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema (ABNT-27002, 2013: 49)*

Controle: Cópias de segurança das informações.

> *12.3.1 - Convém que cópias de segurança das informações, dos software e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida. (ABNT-27002, 2013: 53)*

Estes controles exigem que:
- mudanças nos processos de negócio considerem a segurança da informação;
- a capacidade dos recursos seja monitorada, e a base da informação para este monitoramento deve ser fornecida pela área de negócio;
- existam cópias de segurança da informação, que precisam ser definidas pelas áreas de negócio.

Capítulo 13 – Segurança nas comunicações

Controle: Acordos de confidencialidade e não divulgação.

> *13.2.4 - Convém que os requisitos para a confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados. (ABNT-27002, 2013: 66)*

Este controle considera os acordos de confidencialidade reflitam as necessidades da organização, consequentemente reflitam as necessidades das áreas de negócio.

Capítulo 14 – Aquisição, desenvolvimento e manutenção de sistemas

Controle: Análise e especificação dos requisitos de segurança da informação

> *14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT-27002, 2013: 67)*

As áreas de negócio são as grandes demandadoras de novos sistemas de informação ou da melhorias em sistemas de informação existentes. Estas solicitações devem contemplar as questões de segurança da informação

Capítulo 15 – Relacionamento na cadeia de suprimento

Controle: Identificando segurança da informação nos acordos com fornecedores

> *15.1.2 - Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização, (ABNT-27002, 2013: 78)*

Controle: Cadeia de suprimento na tecnologia da informação e comunicação

> *15.1.3 - Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados à cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação. (ABNT-27002, 2013: 80)*

Estes controles definem regras para todos os fornecedores, inclusive os fornecedores das áreas de negócio. Elas devem identificar estes fornecedores e considerar as exigências destes controles também na contratação destes fornecedores.

Capítulo 17 – Aspectos de segurança da informação na gestão de continuidade do negócio

Controle: Planejando a continuidade da segurança da informação

> *17.1.1 - Convém que a organização determine seus requisitos para a segurança da informação e continuidade da gestão da segurança da informação em situações diversas, por exemplo, durante uma crise ou desastre. (ABNT-27002, 2013: 88)*

Controle: Implementando a continuidade da segurança da informação.

> *17.1.2 - Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa. (ABNT-27002, 2013: 89)*

Controle: Verificação, análise crítica e avaliação da continuidade da segurança da informação.

> *17.1.3 - Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas. (ABNT-27002, 2013: 90)*

Controle: Disponibilidade dos recursos de processamento da informação.

> *17.2.1- Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade. (ABNT-27002, 2013: 91)*

Este é o item da norma que mais fortemente acontece a participação da área de negócio. Fica bastante claro que um plano de continuidade deve existir para possibilitar a continuidade do negócio.

Capítulo 18 – Conformidade

Controle: Identificação da legislação aplicável e de requisitos contratuais

> *18.1.1 - Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes e o enfoque da organização para atender a esses requisitos sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização. (ABNT-27002, 2013: 91)*

Controle: Proteção e privacidade de informações de identificação pessoal

> *18.1.4 - Convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável (ABNT-27002, 2013: 94)*

Controle: Conformidade com as políticas e procedimentos de segurança da informação.

> *18.2.2 - Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidades, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação. (ABNT-27002, 2013: 96)*

Este controle tem como foco principal a necessidade da organização cumprir os regulamentos, a legislação e seus contratos. De uma maneira indireta, tudo que torna a organização não cumpridora das suas obrigações afetará a área de negócio. Sendo assim a área de negócio deve ser a unidade organizacional que mais exige a garantia do cumprimento legal e contratual.

4. CONCLUSÕES

Como resultados desta pesquisa exploratória foram identificados 28 (vinte e oito) controles que exigem (direta ou indiretamente) a participação das áreas de negócio e consequentemente possibilitam o alinhamento da gestão da segurança da informação com os objetivos da organização.

Estes controles identificados declaram no seu texto esta orientação da participação das áreas de negócio ou das áreas diretivas da organização. Este conjunto de controles constrói um direcionamento estratégico para o processo de segurança da informação, indicando que a segurança existe para atender e para estar adequada às necessidades das áreas de negócio, isto é, a rigidez da segurança precisa ser direcionada pelos objetivos de negócio.

Desta maneira, conclui-se que a Norma NBR ISO/IEC 27002:2013 contribui através das suas diretrizes e controles para o alinhamento da gestão da segurança da informação com as áreas de negócio e com os objetivos da organização.

5. RECOMENDAÇÕES

Uma das grandes dificuldades quando da implantação ou melhoria do processo de segurança da informação em uma organização é o envolvimento e comprometimento das áreas de negócio. Historicamente, com raras exceções, estas áreas de negócio não se envolvem com o aspecto da proteção da informação. Com a migração da maioria da informação para o ambiente digital, esta responsabilidade apareceu para a área de tecnologia da informação ou (de maneira acertada) para uma área independente de segurança da informação.

Os controles da norma identificados nesta pesquisa devem ser utilizados para demonstrar às áreas de negócio que elas são consideradas para participarem ativamente no processo de segurança da informação. Evidentemente, considerando que a organização deseja estar alinhada com os normativos relativos à segurança da informação.

Estes controles devem ser analisados e identificados a sua prioridade em relação a cada organização. É de responsabilidade do Gestor da Segurança da Informação utilizar esta pesquisa para melhor conduzir o processo de segurança da informação na sua organização.

O tema também pode ser mais explorando com a investigação de como as organizações que utilizam a norma implementam os controles identificados nesta pesquisa

considerando o alinhamento das áreas de negócio com o processo de segurança da informação.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT, **NBR ISO/IEC 17799 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

_____, **NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

____, **NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2008.

CALDER, Alan; WATKINS, Steve **IT Governance – A Manager´s Guide to Data Security and BS17799**. London: Editora Kogan Page, 2005

DOMENEGHETTI, Daniel; MEIR, Roberto. **Ativos Intangíveis**. Rio de Janeiro: Elsevier Editora, 2009.

ISO - International Organization for Standardization. **Information technology — Security techniques — Code of practice for information security management - Final draft** – ISO/IEC FDIS 17799, 2005

ITGI, **Information Security Governance: Guidance for Information Security Managers**, 2nd Edition, Rolling Meadows, Ilinois – USA: Information Technology Governance Institute, 2008.

MAIWALD, E., SIEGLEIN, W. **Security Planning & Disaster Recovery**, Mcgraw Hill, New York, 2002.

PELTIER, Thomas. **Information Security Fundamentals.** USA: Auerbach, 2005.

_____. **Information Security Policies and Procedures.** USA: Auerbach, 2004.

SHERWOOD, John; CLARK, Andrew; LYNAS, David. **Enterprise Security Architecture.** USA: CMP Books, 2005.

USP – UNIVERSIDADE DE SÃO PAULO. **Política de Segurança da USPNet.** Disponível em: <http://www.security.usp.br/normas_pseg00.html>. Internet. Acesso em: 15-junho-2010.

WYDLER, J. **Strategic Information Security,** Auerbach Publications, New York, 2004.