Alinhamento da gestão de segurança da informação com as áreas de negócio: uma avaliação da contribuição das diretrizes da norma NBR ISO/IEC 27002:2005

Edison Luiz Gonçalves Fontes
Centro Estadual de Educação Tecnológica Paula Souza/CEETEPS – SP - Brasil
edison@pobox.com

Prof. Dr. Napoleão Verardi Galegale
Centro Estadual de Educação Tecnológica Paula Souza/CEETEPS - SP- Brasil
nvg@galegale.com.br

Resumo – A presente pesquisa teve por objetivo identificar as diretrizes da Norma NBR ISO/IEC 27002:2005 que possibilitam o alinhamento da gestão da segurança da informação com as áreas de negócio e faz parte do rol de pesquisas em andamento vinculadas a projeto de dissertação de Mestrado em Tecnologia. Foi realizado um levantamento na norma para identificar as diretrizes que exigem a participação das áreas de negócio. Como resultado foi identificado um conjunto de cinqüenta e uma diretrizes que requerem esta participação e, consequentemente, possibilitam este alinhamento. Conclui-se desta forma que a referida norma contribui para o alinhamento da gestão da segurança da informação com as áreas de negócio.

Palavras chave: segurança da informação, objetivos de negócio, alinhamento ao negócio, NBR ISO/IEC 27002.

Abstract – This research aimed to identify the guidelines of the Standard NBR ISO/IEC 27002:2005 that enable the alignment of the management of information security with business areas and is part of the list of ongoing research project linked to the Master's dissertation in Technology. A research was conducted to identify the standard guidelines that require the participation of business areas. A set of fifty-one guidelines that require such participation, and thus enable the alignment was identified. It is thus that this standard helps to align the management of information security with business areas.

Keywords: information security, business goals, aligning the business, NBR ISO/IEC 27002.

Introdução

Como parte do levantamento teórico e estado da arte no rol de pesquisas em andamento vinculadas ao projeto da dissertação de Mestrado em Tecnologia, provisoriamente intitulada: “Políticas e normas de segurança da informação: em busca de um padrão mínimo e efetivo para as organizações” foi desenvolvida

esta pesquisa que tem por objetivo identificar quais diretrizes da Norma NBR ISO/IEC 27002:2005 - 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.

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, [1]

> - 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.

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, [2].

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 apóiam e reforçam o uso da norma NBR ISO/IEC 27002:2005.

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

Esta norma declara no seu Item 0–Introdução, que a função da segurança é viabilizar os negócios e indica no seu item 5–Política de segurança da informação, que a política deve estar de acordo com os requisitos de negócio.

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 27002:2005 exige para o alinhamento do processo de segurança da informação com os objetivos das 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 diretrizes que possibilitam o alinhamento da gestão da segurança da informação com as áreas de negócio.

Este tema é significativo no campo da segurança da informação uma vez que 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. A Norma ISO/IEC 27002:2005 possibilita esta situação quando declara que os

requisitos de segurança da informação podem ser aplicados em todas as organizações e não depende do seu tipo, tamanho e natureza, [2].

Este artigo inicialmente aborda a Norma ISO/IEC 27002:2005 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 as diretrizes que possibilitam que a segurança da informação alcance o seu alinhamento com as áreas de negócio.

Por fim é apresentada a conclusão que contem as considerações finais e as observações sobre o trabalho realizado.

Norma NBR ISO/IEC 27002:2005

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.

A Norma NBR ISO/IEC 27002:2005 – 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 [3].

Esta norma é composta por um conjunto de ações (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. Algumas diretrizes indicam a participação direta ou indireta da área de negócio. A identificação das diretrizes que requerem a participação da área de negócio foi o objetivo desta pesquisa.

Na medida em que a área de negócio define ou participa da definição da segurança da informação em relação aos níveis de controle, à prioridade e ao

apetite de risco, a gestão da segurança da informação estará alinhada com as áreas de negócio e consequentemente com os objetivos das áreas de negócio.

A Norma NBR ISO/IEC 27002:2005 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, [3].

Alinhamento da segurança da informação ao negócio

A Norma NBR ISO/IEC 27002:2005 declara que a informação é um ativo essencial para o negócio de uma organização e necessita ser adequadamente protegida [3]. Porém, a proteção da informação não deve acontecer por si só. A proteção deve acontecer porque existem os objetivos de negócio. Peltier [4] [5] 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. 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 [6] afirma que os programas de segurança da informação precisam se mover da implantação tática da tecnologia para se tornar parceiros estratégicos do negócio. Peltier [4] [5] 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. Calder e Watkins [7] 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. Quando estivermos construindo uma arquitetura de segurança, Sherwood, Clark e Linas [8] 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. E não podemos esquecer que a segurança da informação vai afetar cada funcionário da organização em função das políticas e dos controles implantados [9].

Domeneghetti e Meir [10] 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.

Pensar em sustentabilidade e transparência nos leva ao conceito de governança. Tomando por base várias definições do IT Governance Institute [11]

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.

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 das diretrizes, aquelas que exigem a participação das áreas de negócio e consequentemente possibilitam esse alinhamento. A implantação destas diretrizes possibilita o alinhamento da segurança da informação com as áreas de negócio. A Norma ISO/IEC 27002:2005 possui enraizada no seu texto a exigência deste alinhamento, como é dito no seu início: “Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável levando-se em conta os objetivos organizacionais”, [3].

Identificação no conjunto das diretrizes, aquelas que possibilitam o alinhamento da gestão de segurança com os objetivos das áreas de negócio.

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 aquelas diretrizes, considerando o conjunto de diretrizes, que exigem a participação das áreas de negócio.

Seção 5: Política de Segurança da Informação, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

a) O documento de segurança da informação deve ser aprovado pela direção.

b) O documento de segurança da informação deve conter uma declaração do comprometimento da direção alinhada com os objetivos e a estratégia de negócio.

c) A revisão periódica da política de segurança da informação deve considerar as mudanças e as circunstâncias do negócio.

Estas diretrizes exigem o comprometimento da direção da organização e desta forma garantem que as orientações básicas do processo de segurança da informação estarão alinhadas com os objetivos de negócio e da organização.

Seção 6: Organizando a segurança da informação, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

a) A direção deve apoiar ativamente o processo de segurança da informação através de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação.

b) A direção deve fornecer um claro direcionamento e apoio para as iniciativas de segurança da informação.

c) Dependendo do tamanho da organização a direção pode definir um fórum de gestão

(exclusivo ou já existente) para o acompanhamento e coordenação dos resultados da implantação do processo de segurança da informação.
d) As atividades do processo de segurança da informação devem envolver representantes de diferentes partes da organização.
e) Os novos recursos de processamento de informação devem ter a autorização adequada por parte da administração dos usuários (área de negócios) permitindo seus propósitos e uso.
f) Quando da proteção do recurso de informação deve-se definir requisitos para a continuidade dos serviços de acordo com as prioridades do negócio da organização.

Estas diretrizes reforçam o comprometimento da direção e explicitam a participação e conseqüente comprometimento das diversas áreas da organização (áreas de negócio): na participação de atividades do processo de segurança da informação, na autorização de uso de novos recursos de processamento da informação e na definição do nível de disponibilidade. Desta forma as ações e o nível de rigidez do processo de segurança da informação serão direcionados pelos requisitos das áreas de negócio.

Seção 7: Gestão de ativos, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

a) As informações e os ativos associados com os recursos de processamento da informação devem ter um proprietário por uma parte definida da organização.
b) A classificação da informação e seus respectivos controles devem considerar os impactos nos negócios.

Estas diretrizes indicam que:

a) diferente do que historicamente ocorreu (ou ocorre) onde a área de TI 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 dos impactos nas áreas de negócio, isto é, os objetivos de negócio serão a razão do nível de classificação da informação.

Seção 8: Segurança em Recursos Humanos, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

a) As responsabilidades em relação à segurança da informação existem em todos os cargos da organização. Os papéis e responsabilidades em relação ao processo de segurança da informação dos funcionários, fornecedores e terceiros precisam estar definidos e documentos quando da contratação dessas pessoas.
b) É conveniente a existência de um código de conduta que contemple as responsabilidades dos funcionários, fornecedores ou terceiros em relação à ética e a proteção dos dados.
c) A conscientização, educação e treinamento em segurança da informação devem ser adequados aos papéis, responsabilidade e das pessoas.

Estas diretrizes explicitam que todos os cargos (e consequentemente todas as pessoas) possuem responsabilidades com o processo de segurança da informação e que orientações corporativas, como o código de ética, devem falar da proteção da informação, indicando dessa maneira que a segurança da informação deve ser uma preocupação da organização. Como preocupação organizacional, os objetivos de negócio dessa organização deverão ser considerados no processo de segurança da informação.

Seção 9: Segurança física e do ambiente

Para esta seção não foram identificadas diretrizes que explicitamente reforçam o alinhamento da Gestão da Segurança da Informação com os objetivos de negócio.

Seção 10: Gerenciamento das operações e comunicações, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

a) Todas as pessoas envolvidas em cada mudança devem ser comunicadas dos detalhes das mudanças.
b) Convém que sejam estabelecidos os procedimentos e responsabilidades gerenciais formais para garantir que haja um controle satisfatório de todas as mudanças.
c) As mudanças em sistemas devem ser realizadas apenas quando houver uma razão de negócio válida para tal.
d) As funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.
e) Os recursos que possuem um ciclo de renovação ou custo maior devem ser monitorados pelos gestores que devem identificar as tendências de utilização, particularmente em relação às aplicações do negócio, com o objetivo de identificar e evitar os potenciais gargalos e a dependência em pessoas chaves que possam representar ameaças à segurança dos serviços.
f) Quando de novos sistemas, atualizações e novas versões a aceitação formal deve considerar s requisitos de continuidade dos negócios.
g) Na proteção contra códigos maliciosos devem-se preparar planos de continuidade do negócio.
h) As cópias de segurança devem refletir os requisitos de negócio da organização e para tanto devem ter o nível necessário para a existência dessas cópias.
i) Deve-se prevenir contra a divulgação não autorizada, remoção ou destruição de recursos de informação que podem causar interrupção das atividades do negócio e as mídias as mídias removíveis devem estar habilitadas somente se houver uma necessidade de negócio.
j) Devem-se ter diretrizes de retenção e descarte para toda a correspondência de negócios.
k) Convém que os aspectos de segurança contidos nos acordos de troca de informação reflitam a sensibilidade das informações envolvidas no negócio.
l) Convém que as políticas e procedimentos sejam desenvolvidos e implantados para proteger as informações associadas com a interconexão de sistemas de informações do negócio.
m) Deve existir uma Gestão de Mudança que garanta um rígido controle das alterações que serão feitas no ambiente de processamento das informações, considerando os impactos potenciais e a comunicação dos detalhes das mudanças para todas as pessoas envolvidas.

Estas diretrizes são variadas, mas todas têm como base a participação das áreas de negócio ou a exigência de definições de segregação de função.

Seção 11: Controle de acessos, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

a) Convém que a política de controle de acesso seja estabelecida documentada e analisada criticamente tomando-se como base os requisitos de acesso dos negócios.
b) O acesso do usuário deve ser permitido apenas onde existe necessidade do negócio ou razões operacionais.
c) O nível de acesso concedido ao usuário deve ser apropriado ao propósito do negócio.
d) Para o usuário ter acesso ao sistema é necessário a autorização do proprietário do sistema.
e) O estabelecimento de perfis de acesso para usuário deve ser baseado nos requisitos dos negócios.

O acesso a informação exige que as áreas de negócio sejam as responsáveis para a liberação da informação do negócio para todas as áreas da organização.

Seção 12: Aquisição, desenvolvimento e manutenção de sistemas, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

> a) Convém que sejam especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas ou melhorias dos sistemas existentes.
> b) Convém que requisitos de segurança e controles reflitam o valor para o negócio dos ativos de informação envolvidos e os danos potenciais ao negócio que poderiam resultar de uma falha ou ausência de segurança.

Desde a etapa de desenvolvimento ou aquisição de sistemas de informação, as áreas de negócio precisam ser envolvidas. Os sistemas e posteriores controles de segurança existem para a realização do negócio.

Seção 13: Gestão de incidentes de segurança da informação, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

> a) Convém que os eventos de segurança da informação sejam relatados através dos canais da direção, o mais rápido possível.
> b) Deve existir um ponto de contato de conhecimento de toda a organização para receber as notificações de segurança da informação.

Neste item temos o uso de canal da direção e a ênfase para que toda a organização conheça o ponto de contato para relato de gestão de incidentes.

Seção 14: Gestão de continuidade de negócio, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

> a) Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização.
> b) Quando do entendimento dos riscos que a organização está exposta, no que diz respeito à sua probabilidade e impacto no tempo, deve-se considerar a identificação e prioridade dos processos críticos de negócio.
> c) Devem-se identificar os ativos dos processos críticos de negócio.
> d) Deve-se entender o impacto que os incidentes de segurança da informação terão sobre os negócios.
> e) Deve-se buscar garantir que a gestão da continuidade do negócio está incorporada aos processos estruturais da organização.
> f) Convém que as análises/avaliações de riscos de continuidade de negócio sejam realizadas com total envolvimento dos responsáveis pelos processos e recursos do negócio.
> g) Convém que a análise/avaliação de riscos identifique, quantifique e priorize os critérios baseados nos riscos e os objetivos pertinentes à organização.
> h) Deve-se ser definida uma abordagem estratégica para a continuidade dos negócios e a mesma deve ser validada com a direção da organização.
> i) Ao ser desenvolvido o plano de continuidade de negócios deve-se ser dada atenção especial à avaliação de dependências externas ao negócio e de contratos existentes.
> j) Convém que o processo de planejamento foque nos objetivos requeridos do negócio.

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.

Seção 15: Conformidade, ABNT [3].

Diretrizes que definem participação da área de negócio ou da direção:

> a) Convém que a direção aprove o uso de recursos de processamento de informação.

> b) Os recursos de processamento da informação de uma organização são destinados básica ou exclusivamente para atender aos propósitos do negócio.
> c) Se qualquer não-conformidade for encontrada como um resultado da análise crítica convém que os gestores determinem as causas da não conformidade; avaliem ações para que a não conformidade se repita; determinem e implementem ação corretiva apropriada e analisem a ação corretiva tomada.

Este item 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 deseje a garantia do cumprimento legal e contratual.

Seção 4: Análise/avaliação e tratamento de risco, ABNT [3].

A Norma NBR ISO/IEC 27002:2005 não considera a análise/avaliação e tratamento de risco como uma das categorias principais da segurança da informação. Entendemos que ela é uma espécie de ferramental que as categorias podem utilizar para identificar o impacto na organização caso o controle apresentado não esteja efetivo.

Porém a Norma deixa bem explícita a necessidade da participação da área de negócio quando declara, [3]:

> a) Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base me critérios para a aceitação dos riscos e dos objetivos relevantes para a organização.
> b) Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se me conta os objetivos organizacionais.

Conclusão

Como resultados desta pesquisa exploratória foram identificados em onze categorias, das doze categorias existentes na norma, cinqüenta e uma diretrizes que exigem a participação das áreas de negócio e consequentemente possibilitam o alinhamento da gestão da segurança da informação com as mesmas. Desta maneira, conclui-se que a Norma NBR ISO/IEC 27002:2005 contribui através das suas diretrizes para o alinhamento da gestão da segurança da informação com as áreas de negócio.

As informações deste artigo serão parte do levantamento teórico e estado da arte no rol de pesquisas em andamento vinculadas ao projeto da dissertação de Mestrado em Tecnologia, provisoriamente intitulada: “Políticas e normas de segurança da informação: em busca de um padrão mínimo e efetivo para as organizações”.

Referências

Livros e Teses

[2] ISO - International Organization for Standardization (2005) “Information technology — Security techniques — Code of practice for information security management - Final draft – ISO/IEC FDIS 17799”, ISO.

[3] ABNT – Associação Brasileira de Normas e Técnicas (2005) “Tecnologia da informação – Técnicas de segurança – Código de Prática para a gestão da segurança da informação – NBR ISO/IEC 27002”, ABNT, Brasil.

[4] Peltier, T. R. (2004) “Information Security Policies and Procedures”, Auerbach Publications, New York.

[5] Peltier, T. R., Peltier, J., Blackley, J., (2005) “Information Security Fundamentals”, Auerbach Publications, New York, USA.

[6] Wydler, J. (2004) “Strategic Information Security”, Auerbach Publications, New York.

[7] Calder, A., Watkins, S. (2005) “IT Governance – A Manager´s Guide to Data Security and BS17799”, Editora Kogan Page, London.

[8] Sherwood, J., Clark, A., Lynas, D. (2005) “Enterprise Security Architecture”, CMP Books, New York.

[9] Maiwald, E., Sieglein, W. (2002) “Security Planning & Disaster Recovery”, Mcgraw-Hill, New York.

[10] Domeneghetti, D., Meir, R. (2009) “Ativos Intangíveis”, Elsevier Editora, Rio de Janeiro.

[11] ITGI – Information Technology Governance Institute (2008) “Information Security Governance: Guidance for Information Security Managers”, ISACA, Rolling Meadows/USA.

Internet

[1] USP – UNIVERSIDADE DE SÃO PAULO (2010) “Política de Segurança da USPNet. Disponível em: <http://www.security.usp.br/normas_pseg00.html>. Acesso em: 15-junho-2010.

Contato

Edison Luiz Gonçalves Fontes, Alameda Santos, 1.293, Conjunto 84 – Cerqueira César – São Paulo, SP, CEP 01419-001. Setembro/2010.

Napoleão Verardi Galegale, R. Dr. Cândido Espinheira, 560, Conj. 81, Perdizes, São Paulo, SP, CEP 05004-000. Setembro/2010.