RESULTADOS OBTIDOS COM A APLICAÇÃO DA NORMA NBR ISO/IEC 17799:2000 NO CENTRO UNIVERSITÁRIO DE BRUSQUE – UNIFEBE

RESULTS ON THE APPLICATION OF IEC/ISO 17799:2000 STANDARD ON CENTRO UIVERSITÁRIO DE BRUSQUE – UNIFEBE

Rosiane Constante[1]

RESUMO: Assim como é importante manter documentos em papel sob proteção de roubo ou intempéries, é necessário preservar a informação quando armazenada em meio digital. Uma vez que a segurança plena para estes ativos é utópica, resta ao ser humano encontrar formas relativamente seguras de preservá-los. Este trabalho descreve a aplicação da Norma NBR ISO/IEC 17799:2000 "Código de Prática para a Gestão de Segurança de Informações" no Núcleo de Informática do Centro Universitário de Brusque – Unifebe. Foi realizada uma fundamentação teórica sobre segurança de informações para servir de base a uma coleta de dados. Em seguida, foi produzido um comparativo entre as premissas e recomendações da Norma com a realidade do Núcleo de Informática. Como resultado, obteve-se que, dos 127 controles possíveis, a Unifebe atende completamente a 51, parcialmente a 33, não atende a 41 e não se adequou a 2. Com base nesses números, foram geradas 5 recomendações consideradas as mais críticas para serem estabelecidas no departamento.

Palavras-chave: Segurança de Informação. Política de Segurança. NBR ISO/IEC 17799.

ABSTRACT*: Just as it is important to keep paper documents under the protection of theft or weather, it is necessary to preserve information when stored in digital media. Once the full security for these assets is utopian, it remains to humans find relatively safe ways to preserve them. The present paper describes the use of NBR ISO/IEC 17799 at the Information Tecnology facilities of Unifebe – Centro Universitário de Brusque. A complete review about information security was conducted to serve as the basis for a data collect. It was produced a comparison between ISO´s recommendations and the reality of the IT department. As result, it was observed that Unifebe is completely aligned on 51 of the 127 possible subjects, partially aligned on 33. Not aligned on 41 and finally, not appliable on 2. It was generated 5 critical recommendations to be established on the department to help improve security.*

Keywords*: Information Security. Security Policy. NBR ISO/IEC 17799.*

[1] Graduada em Sistemas de Informação pelo Centro Universitário de Brusque – Unifebe. E-mail: rosianesjb@hotmail.com

1 INTRODUÇÃO

A informática é uma ferramenta cada vez mais utilizada pelo homem, o qual procura constantemente realizar suas tarefas de modo mais fácil, rápido, eficiente e conseqüentemente mais competitivo, produzindo assim, os melhores resultados (NAKAMURA, 2007, p. 44). Esta crescente dependência de tecnologia faz surgir uma das fundamentais preocupações naturais do ser humano: a sua segurança.

Estar seguro é estar protegido contra as ameaças. Logo, um computador está seguro se não existem vulnerabilidades em sua arquitetura, desde o hardware até a aplicação. Infelizmente, as atuais arquiteturas não foram elaboradas para serem seguras por padrão, e por isso não é possível garantir sua segurança (LANDWEHR, 2001 apud BORTOLUZZI, 2004, p.13).

As informações são ativos importantes para os negócios, pois possuem valor para a organização e devem ser protegidas adequadamente. A segurança das informações as protege contra um conjunto de ameaças, a fim de assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais (NBR ISO/IEC 17799, 2000, p. 6).

Longo (2008) corrobora e destaca que, "a existência de uma norma permite que o usuário tome conhecimento do quão protegidas e seguras estarão as suas informações, possibilitando ao mesmo uma ferramenta que irá auxiliar na escolha de uma solução". Do ponto de vista dos profissionais técnicos, eles passarão a possuir uma ferramenta comum de trabalho, evitando assim que cada equipe tenha para si um padrão desarmônico das demais equipes, dificultando aos clientes a melhor escolha.

É na busca por este objetivo que o presente trabalho está direcionado, fundamentado no Padrão Internacional de Tecnologia da Informação - Código de Prática para a Gestão da Segurança de Informações (NBR ISO/IEC 17799:2000) para a busca de melhoria dos serviços de Segurança da Informação no Centro Universitário de Brusque – Unifebe.

2 METODOLOGIA

Todo o referencial teórico para o desenvolvimento desta pesquisa está disponível em livros, pesquisas e artigos da Internet. Entretanto, as principais atividades partem das recomendações trazidas na Norma NBR ISO/IEC 17799:2000.

Primeiramente foi feita uma análise documental sobre Segurança da Informação e a norma NBR ISO/IEC 17799:2000, com o intuito de compreensão do assunto. Em seguida foi

realizado um levantamento sobre a realidade do Núcleo de Informática, através da interação com a equipe de trabalho, com o objetivo de descrever seu real funcionamento. Logo após, foi realizada uma comparação entre as recomendações de segurança contidas na norma NBR ISO/IEC 17799:2000 e as práticas estabelecidas no Núcleo de Informática, verificando a quantidade de recomendações que não são atendidas, os motivos de não utilização e a viabilidade para implantá-las, resultando em um relatório com principais pontos de não adequabilidade e recomendações de mudanças.

O trabalho enquadra-se na abordagem qualitativa da pesquisa, utilizando a metodologia do estudo de casos, com o intuito de propor ações de segurança para o Centro Universitário de Brusque – Unifebe fundamentadas na Norma NBR ISO/IEC 17799:2000.

Os dados da pesquisa foram coletados a partir de aplicação de questionário com o Núcleo de Informática da Unifebe e responsáveis por suas respectivas áreas do Núcleo. Esse questionário foi baseado em cada recomendação trazida pela norma, verificando a existência e funcionamento de cada item.

3 SEGURANÇA DE INFORMAÇÕES

A Segurança da Informação não é um assunto novo, aliás, nota-se que desde o início da civilização humana há uma preocupação com as informações e com conhecimento presente nessas informações. Porém, foi na sociedade moderna, através do surgimento dos computadores, que se começou a dar uma atenção maior a segurança das informações (LONGO, 2008).

A Informação como qualquer outro ativo, é importante para a organização e necessita ser protegida adequadamente. A Segurança da Informação resguarda a informação contra várias ameaças, garantindo o seguimento dos negócios, diminuindo os danos e aumentando o retorno dos investimentos e oportunidades (FERREIRA, 2003).

Segundo Ferreira (2003), o gerenciamento da Segurança da Informação é uma arte, onde se cria e administra a Política de Segurança, pois só é possível gerenciar o que pode ser definido.

A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação, aumentam a dificuldade de se conseguir controle de acesso. Isso faz com que a Segurança da Informação se torne um assunto crucial para a sobrevivência das organizações (NBR ISO/IEC 17799, 2000).

Levando em conta que muitos sistemas de informação não foram projetados para serem seguros e que a segurança que pode ser obtida por meios técnicos é limitada, a norma NBR ISO/IEC 17799:2000 avigora que a Segurança da Informação deveria ser apoiada por um meio de gestão adequada, necessitando da participação de todos os envolvidos na organização.

A Segurança das Informações não pode ser considerada um assunto técnico, pois todo o processo de segurança tem seu início e seu término em um ser humano. Desta forma, não basta adquirir uma série de dispositivos de hardware e software para assegurar a informação, pois, sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários os hardwares não farão efeito (SILVA, 2008 apud OLIVEIRA, 2001).

Assim, o grande desafio para a implementação de procedimentos de segurança de acordo com Sêmola (2003), é arranjar ações que relatem a real situação da organização, destacando seus riscos, ameaças, vulnerabilidades, sensibilidades e impactos com a intenção de criar um plano de gestão das informações adequado.

A ISO 17799 aponta as melhores práticas para a proteção e controle da segurança das informações, sendo base para uma política concreta e oferecendo um abrangente conjunto de controles (LAUDON, 2007).

Sêmola (2003) enfatiza que a implantação de controles é feita com o intuito de se chegar a um grau de risco cômodo. Esta atividade está incluída em uma orientação obtida através das sugestões da norma ISO/IEC 17799.

3.1 Política de Segurança

"A política de Segurança é o apoio para todas as questões incluídas na proteção da informação, exercendo um papel importante em todas as organizações" (NAKAMURA, 2007, p. 188). "Tornando-se um grande pilar para a sustentação do equilíbrio do ambiente informatizado" (FERREIRA, 2003, p. 41).

A política de segurança aborda os aspectos humanos, culturais e tecnológicos de uma organização, englobando também processos, negócios e legislação local. Uma vez que a política de segurança faz parte da cultura da organização, ela auxilia na simplificação de todos os seus recursos (NAKAMURA, 2007).

Os regulamentos de segurança têm como objetivo fazer com que as informações em uma empresa sejam utilizadas de forma estruturada, fornecendo melhor direcionamento para implementações técnicas, evitando prejuízos causados pelo mau uso da informação.

"É necessário que uma Política de Segurança tenha uma abordagem pró-ativa estando bem defina e clara, para evitar futuros problemas à organização" (NAKAMURA, 2007, p. 189). De fato, de acordo com a pesquisa Modulo (2008), 33% das organizações não sabem quantificar as perdas causadas por falta de segurança das informações, e 22% sequer sabem identificar os responsáveis pelo problema.

"Para o processo de segurança da informação, tanto um funcionário quanto um prestador de serviço tem a mesma responsabilidade perante a organização, independente de sua ocupação na organização" (FONTES, 2006, p. 3).

Para que a política de segurança seja eficaz na organização, ela deve ter algumas características, tais como: ser verdadeira, complementada com a disponibilização de recursos, válida para todos, ser simples e ter o comprometimento da alta direção da organização (FERREIRA, 2003).

3.2 Norma NBR ISO/ IEC 17799:2000

O BSI (*British Standard Institute*) criou a norma BS 7799, um padrão internacionalmente reconhecido para a implementação de controles de segurança, considerado o mais completo padrão para o gerenciamento da Segurança da Informação no mundo. A ISO/IEC 17799 é uma versão internacional do BS 7799, adotada pela ISO (*International Organization for Standardization*) e pelo IEC (*International Engineering Consortium*) em dezembro de 2000, resultante de diversas sugestões e alterações. No Brasil, em agosto do ano seguinte, adotou-se esta norma como padrão, por meio da ABNT (Associação Brasileira de Normas Técnicas), e conferiu-lhe a denominação NBR ISO/IEC 17799, sendo uma tradução literal da norma ISO (FERREIRA; NAKAMURA, 2007).

Desta forma, a política de segurança pode ser defina com base em padrões de referência como a NBR ISO/IEC 17799:2000.

A Norma de Segurança da Informação NBR ISO/IEC 17799:2000, tem o foco em três premissas, que são confidencialidade, integridade e disponibilidade.

A Confidencialidade garante que as informações só estarão disponíveis as pessoas com permissão de acesso a elas. A Integridade garante a precisão das informações e aos métodos de processamento e a Disponibilidade garante que os usuários autorizados terão acesso às informações sempre que necessário.

A norma possui aproximadamente 127 controles distribuídos em 10 sessões, sendo elas: política de segurança, segurança organizacional, classificação e controle dos ativos,

segurança relacionada ao pessoal, segurança física e ambiental, gerenciamento de comunicações e operações, controle de acesso, desenvolvimento e manutenção de sistemas, gerenciamento da continuidade do negócio, obediência a exigências.

Diversas referências foram criadas para auxiliar as organizações nas melhores práticas da gestão da segurança da informação, neste trabalho foi utilizado a NBR ISO/IEC 17799:2000, que faz parte da família de padrões internacionais BS 7799, sendo a norma mais utilizada na atualidade no Brasil (BEAL, 2005).

4 PROJETO

O presente projeto teve como meta o desenvolvimento de ações de segurança para o Núcleo de Informática do Centro Universitário de Brusque - Unifebe. A finalidade foi destacar os pontos fracos na gestão da segurança das informações do Núcleo de Informática, dando ênfase nos pontos mais relevantes, sugerindo ações para a melhoria dos mesmos. Para o desenvolvimento do projeto utilizou-se uma pesquisa de caráter exploratório de abordagem qualitativa, utilizando como instrumento metodológico um estudo de casos.

“A pesquisa qualitativa pode ser usada para explorar áreas, a fim de ganhar maior entendimento sobre a mesma, produzindo resultados sem a utilização de procedimentos estatísticos, utilizando métodos como a interação” (STRAUSS, CORBIN, 2008, p.23).

No desenvolvimento do projeto foram gerados os seguintes produtos:

- Instrumento de coleta de dados;
- Texto comparativo entre as recomendações da norma NBR ISO/IEC 17799:2000 e a realidade do Núcleo Informática;
- Relatório dos principais pontos de não adequabilidade;

Neste trabalho não se buscou generalizar os dados da organização para todo o setor de TI (Tecnologia da Informação), porém teve a finalidade de exploração de um caso particular e específico com características bem interessantes para a organização, que foi foco do projeto.

4.1 Coleta de dados

Como instrumento de coleta de dados foi utilizado um questionário embasado na norma NBR ISO/IEC 17799:2000, onde cada recomendação da mesma foi repassada através de uma pergunta, já que a norma é muito abrangente em termos de quantidade de recomendações, o que dificultaria muito o alcance de uma posição para cada recomendação se não desta forma.

“A estrutura da norma NBR ISO/IEC 17799:2000 permiti que o questionário seja composto por questões abertas, possibilitando que o entrevistado exponha suas atitudes e suas opiniões que ajudam o pesquisador a interpretar suas respostas” (MALHOTRA, 2006, p. 298). “Por questões fechadas, onde são apresentadas várias respostas para uma pergunta, permitindo que o entrevistado escolha dentre as alternativas oferecidas as que se enquadram com a situação de resposta” (MALHOTRA, 2006, p. 298).

Deste modo, o questionário foi aplicado para facilitar a compreensão do funcionamento e importância de cada recomendação, possuindo a cautela de estar próximo do entrevistado, pois, como assinala Richardson (2008). A melhor situação para participar da mente de outro ser humano é a interação face a face, pois tem o caráter, inquestionável, de proximidade entre as pessoas, que proporciona as melhores possibilidades de penetrar na mente, vida e definição dos indivíduos.

Ressalta-se que a coleta de dados para um estudo de caso pode ser feita utilizando-se mais de um procedimento (RICHARDSON, 2008). No caso em tela, além do questionário aplicado, utilizou-se também documentos para fundamentar o estudo de caso e a observação de comportamento e atitudes dos integrantes do Núcleo de Informática da Unifebe.

4.2 DESENVOLVIMENTO DO PROJETO

Para o desenvolvimento da análise primeiramente foi feita a aplicação do instrumento descrito acima com os integrantes do Núcleo de Informática. O primeiro quadro de respostas foi obtido através da interação com o administrador de redes, que avaliou as perguntas e respondeu grande parte delas.

O questionário respondido pelo administrador de redes foi repassado ao coordenador do Núcleo Informática da Unifebe, o qual avaliou as respostas dadas pelo administrador de redes e complementou-as onde necessário, adicionando comentários e auxiliando nas questões mais gerenciais.

O instrumento de pesquisa e coleta de dados é uma forma de alcançar o máximo de informações necessárias para fazer uma boa fundamentação da proposta de melhorias para a segurança das informações. Desta forma, a interação com os integrantes do Núcleo de Informática foi de extrema importância, pois esclareceu dúvidas tanto entre acadêmica e o funcionamento real do Núcleo de Informática, quanto dúvidas dos integrantes do Núcleo de Informática em relação à necessidade de coleta de tais dados.

A segunda etapa foi a elaboração do texto comparativo entre as recomendações da norma NBR ISO/IEC 17799:2000 e a realidade do Núcleo de Informática. O texto foi formulado através das respostas obtidas com a aplicação do questionário, destacando o que a norma recomenda, e qual era ação real do Núcleo de Informática em relação tal recomendação.

A partir da descrição do funcionamento real do Núcleo de Informática em relação às recomendações da norma, foram identificados entre os comportamentos citados, quais deles poderiam gerar riscos a segurança das informações dentro da organização.

Logo após a identificação desses riscos foi documentado o relatório citando os principais pontos de não adequabilidade da norma NBR ISO/IEC 17799:2000 em relação ao funcionamento do Núcleo de Informática. Provendo a elaboração do relatório final, permitindo a busca e elaboração de ações e medidas de segurança ou correção, para amenizar os riscos da gestão de segurança do Núcleo de Informática, setor responsável pelas informações do Centro Universitário de Brusque - Unifebe.

A única dificuldade que tinha potencial de gerar algum risco na realização desse projeto era a falta de disponibilidade dos integrantes do Núcleo de Informática.

5 RESULTADOS

O questionário aplicado com os integrantes do Núcleo de Informática é formado por 278 questões divididas em 10 sessões, conforme a estrutura da norma NBR ISO/IEC 17799:2000. Essas questões abrangem 125 dos 127 controles apresentados pela norma, o que corresponde a 98% de aplicação do conteúdo proposto. Todas as questões propostas receberam respostas em conformidade com a norma.

O Gráfico 1 exibe a contabilização da avaliação de segurança separada em itens conforme o cumprimento dos objetivos que a norma propõe. As possibilidades são:

- Cumpre por completo (40%);
- Cumpre parcialmente (26%);
- Não cumpre (32%);
- Não se aplica à realidade da Unifebe. (2%).

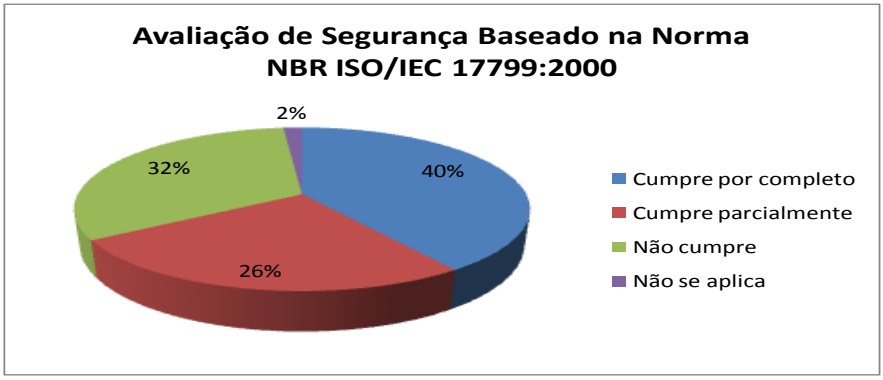

Grafico 1 – Avaliação de Segurança Baseado na Norma NBR ISO/IEC 17799:2000
Fonte: Pesquisa de Campo (2009)

Os itens da norma foram separados em quatro listas, uma de conformidade total, outra de conformidade parcial, outra de não conformidade e por fim uma de não adequabilidade. Através dessas listas foi possível visualizar todos os pontos sobre a Segurança de Informações que necessitam de melhorias no âmbito do Núcleo de Informática. Essas melhorias deverão ser tratadas conforme as possibilidades de tempo e orçamento do departamento.

As listagens de não conformidade e de conformidade parcial foram expostas ao coordenador de Núcleo de Informática, o qual avaliou junto à acadêmica a relevância de cada um dos itens a fim de evitar erros na priorização das atividades. Através deste mapeamento destacou-se os cinco principais itens para a melhoria da Segurança das Informações no Núcleo de Informática.

Com base nos dados coletados e na fundamentação das necessidades da segurança de informações para a continuidade dos negócios da organização, constatou-se que o primeiro item a ser reestruturado no Núcleo de Informática seria o documento da política de segurança de informações, devido a sua relevância e abrangência informativa, a política de segurança torna-se base para a implantação da gestão de segurança de informações dentro da organização.

Ficou entendido que para a realidade da Unifebe, a política de segurança deve dar prioridade a educação e treinamento de todos os colaboradores e usuários da organização, de modo a deixar clara a necessidade da gestão da segurança das informações bem como fornecer quais diretrizes deverão ser seguidas e obedecidas por todos os colaboradores e usuários em um geral.

Em seguida, a primeira diretriz técnica a ser imposta é a gestão de senhas, a fim de evitar quebras de segurança causadas por falta de confidencialidade do proprietário e usuário ou de má escolha no momento de cadastro.

Fica estabelecido que o Inventário de Ativos será realizado em seguida, para permitir a identificação de quais são os ativos do Núcleo de Informática, a importância e o valor referentes a cada um desses ativos e o provimento de níveis de segurança individuais para cada um de acordo com sua importância.

Por fim, fica constituído o uso de assinaturas digitais, para a melhoria do tempo de trabalho principalmente nas normativas e determinações dos conselhos (Consuni, CA e Curador), eliminando a coleta de assinaturas em ata com o uso das assinaturas digitais.

Abaixo segue um resumo destas ações em ordem lógica e de prioridade:

1. Documento da política de segurança de informações;
2. Educação e treinamento sobre segurança de informações;
3. Gerenciamento de senhas de usuário;
4. Inventário dos ativos;
5. Assinaturas digitais.

6 CONSIDERAÇÕES FINAIS

O desenvolvimento desse trabalho surgiu através de um acordo entre o coordenador do Núcleo de Informática, o orientador e a acadêmica para a realização de ações de reconhecimento do ambiente de trabalho a fim de destacar os pontos mais relevantes para a segurança das informações do Centro Universitário de Brusque – Unifebe.

A revisão bibliográfica permitiu elucidar a importância e a necessidade de se manter uma boa gestão da segurança das informações. A norma NBR ISO/IEC 17799:2000 foi interpretada literalmente e influenciou diretamente no conhecimento acadêmico e na fundamentação das necessidades do Núcleo de Informática em reconhecer seu ambiente, destacar suas vulnerabilidades e propor soluções efetivas a elas.

O questionário surgiu como a ferramenta ideal para a coleta de dados, mesmo sendo abrangente e necessitando de acompanhamento na hora de responder o questionário, o que causou uma demora até a finalização de toda a coleta de dados. O questionário foi projetado para que cada recomendação da norma fosse repassada através de uma pergunta com uma única resposta e resultou em 278 indagações pertinentes.

O resultado foi um diagnóstico real e pertinente do ambiente de trabalho do Núcleo de Informática, pois, apesar de ser utilizado apenas um questionário para a obtenção desse diagnóstico, ele retratou todos os itens da norma NBR ISO/IEC 17799 que é referencia tanto nacional quanto internacional de alto desempenho no que se trata de segurança de informações dentro das organizações. As interações de aplicação do questionário elucidaram os pensamentos sobre segurança e contribuíram para a priorização das melhorias a serem tomadas no departamento.

Dos 125 controles avaliados, 51 são atendidos completamente pelo Núcleo de Informática, o que significa 40% do total. Um índice aceitável, perante as recomendações da Norma NBR ISO/IEC 17799:2000, pois embora uma parcela significativa das recomendações seja atendida parcialmente ou não seja atendida, estas não foram identificadas como causadoras de alto risco para o mesmo.

O mapeamento de riscos do Núcleo de Informática em relação às recomendações da Norma NBR ISO/IEC 17799:2000 e os controles que não foram enquadrados na priorização de ações podem ser trabalhados conforme as possibilidades do departamento.

É esperado um posterior direcionamento para o trabalho apresentado e a criação de outros trabalhos relacionados, tendo em mente que a segurança de informações é um processo continuo e que precisa estar sempre atualizado, é necessário que o Núcleo de Informática mantenha-se atento e trabalhando encima do processo de gestão da segurança das informações, procurando dar continuidade aos objetivos alcançados com este trabalho.

REFERÊNCIAS

BORTOLUZZI, Fabrício, “Aplicação da Análise de Causa Raiz em Sistemas de Detectação de Intrusões” 105 f. **Dissertação** (Pós-Graduação em Ciência da Computação) – Universidade Federal de Santa Catarina, Florianópolis, 2004.

CERT. (2008) **Computer emergency and response team**: Cert/CC statistics: “number of incidents reported”. Disponível em: <http://www.cert.org/stats/cert_stats.html>. Acesso em: 02 de setembro de 2010.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna. 2003.

FONTES, Edson. **Segurança da Informação**. São Paulo: Editora Saraiva, 2006.

LONGO, Gustavo Dobkowski. **Segurança da Informação**. Universidade Estadual Paulista. Faculdade de Ciências Campus de Bauru. Disponível em: <http://www.firewalls.com.br/files/ArtigoCientifico.pdf. Acesso em: 02 de agosto de 2010.

MODULO. **10ª Pesquisa Nacional de Segurança da Informação**. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. 02 de agosto de 2010.

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec. 2007.

NBR ISO/IEC 17799:2000: T**ecnologia da Informação – Código de Prática para Gestão da segurança de Informações**. Rio de Janeiro, 2001.

SILVA, Moisés Benigno. Importância na Gestão da Segurança da Informação nas Instituições Particulares de Ensino Superior do Grande Recife. Disponível em: http://www.moisesbenigno.com/Artigo_MoisesBenigno.pdf. Acesso em: 02 de agosto de 2010.