# Segurança de Informação: Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005

# *Information Security: Adherence to the Standard ABNT NBR ISO/IEC 17799:2005*

Marcos de S. Vianez, Roberta H. Segobia e Vander Camargo

USCS - Universidade Municipal de São Caetano do Sul - São Caetano do Sul - SP - Brasil

soumarkos@gmail.com robertasegobia@yahoo.com.br vander.camargo@toledo.com.br

**Resumo:** Este artigo descreve o estudo realizado sobre segurança da informação com base na norma da ABNT NBR ISO/IEC nº 17.799:2005, que trata da Tecnologia da Informação – Técnicas de segurança – Código de prática para gestão da segurança da informação. A ABNT NBR ISO/IEC nº 17.799:2005 é um código de prática de gestão de segurança da informação, e sua importância pode ser dimensionada pelo número crescente de pessoas e organizações que a utilizam, devido à variedade de ameaças a que a informação é exposta na rede corporativa e de comércio eletrônico. Com base nessa norma, foi realizada uma pesquisa quantitativa com algumas empresas situadas na região do ABC, onde se mostrou se as empresas analisadas aderem à norma da ABNT como padrão para implementar e manter a segurança da informação dentro e fora das organizações. Demonstrou-se, ainda, o entendimento da informação como ativo importante para a organização, juntamente com os bens físicos e financeiros.

**Palavras-chave:** Segurança da Informação, Gestão de Ativo, Norma ABNT.

**Abstract:** This article describes a study about Information Security, based on ABNT standard NBR ISO/IEC 17799:2005 about Information Technology - Security Techniques - Code of Practice for Information Security management. The ABNT NBR ISO/IEC 1799:2005 is a code of practice for Information Security management and its importance can be measured by the increasing number of people and organizations that use it, due to the variety of threats that the information is exposed in the corporative network and e-commerce. Based on this norm a quantitative research was done with some companies located in the ABC region, where we show if these analyzed companies adhere the norm of the ABNT as standard for implement and to keep the Information Security inside and outside the companies. The understanding of the information as important active for organization, joined with physical and financial goods, was also shown.

**Keywords**: Information Security, Active Management, ABNT standard.

## 1 INTRODUÇÃO

A informação pode existir de várias formas, pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente (GONÇALVES, 2003).

Garantir a segurança da informação digital é uma tarefa difícil, pois envolve, além da informática, outras áreas de conhecimento, como o direito, o *marketing*, a matemática, a sociologia ou o comércio eletrônico. A variedade e a diversidade da informação que se pretende proteger são muito amplas, podendo ser bases de dados, fundos arquivísticos ou dados pessoais altamente sigilosos, entre muitos outros (PEREIRA, 2005).

A informação, para uma organização, é fundamental para a continuidade dos negócios. Para isso, é importante que seja adequadamente protegida, pois, com o crescimento da interconec-

tividade entre ambientes de trabalho, a informação ficou mais exposta a uma grande variedade de ameaças (SÊMOLA, 2003).

Hoje, a informação assumiu importância vital para a manutenção e o crescimento dos negócios, marcados pela economia globalizada e permanentemente *on-line*, de tal forma que não há organização humana que dependa da tecnologia de informação em maior ou menor grau, de maneira que o comprometimento do sistema de informação por problemas de segurança pode causar grandes prejuízos ou, mesmo, levar a organização à falência (GONÇALVES, 2005).

A necessidade de garantir a segurança da informação exige a proteção da informação contra vários tipos de ameaças conhecidas e desconhecidas pela organização, ajudando a minimizar os riscos para os negócios e procurando maximizar o retorno sobre os investimentos e as oportunidades de negócios (CHEROBINO, 2007).

Para facilitar o processo de seleção de controles a serem aplicados e garantir a segurança da informação, que nem sempre é fácil, existem ferramentas que auxiliam a identificar os possíveis problemas que a organização pode ter, e normas para auxiliar na resolução desses problemas ou, até mesmo, evitá-los antes que eles aconteçam. (GONÇALVES, 2007).

## 2 SEGURANÇA DA INFORMAÇÃO

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida (JÚNIOR, FONSECA & COELHO, 2006).

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade dos negócios, minimizar os riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios. Ela é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde e quando necessário, para garantir que os objetivos dos negócios e de segurança da organização sejam atendidos. Isso deve ser feito em conjunto com outros processos de gestão dos negócios (MORAES, 2003).

## 3 NORMA ISO/IEC Nº 17.799:2005

As normas contribuem para fazer com que os processos de fabricação e fornecimento de produtos e serviços sejam mais eficientes, seguros e limpos, facilitando os negócios entre fornecedores e clientes, seja no comércio local, seja no internacional, uma vez que estabelecem padrões a serem seguidos, garantindo interoperabilidade entre serviços, processos e produtos (CASANAS & MACHADO, 2006).

Conforme definidos pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização encontram-se explicitados nos itens seguintes.

- **Comunicação:** proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente, melhorando a confiabilidade das relações comerciais e de serviços.
- **Segurança:** proteger a vida humana e a saúde.
- **Proteção do consumidor:** prover a sociedade de mecanismos eficazes para aferir a qualidade de produtos.
- **Eliminação de barreiras técnicas e comerciais:** evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando, assim, o intercâmbio comercial.

A Associação Brasileira de Normas Técnicas (ABNT) é o fórum nacional de normalização. A norma brasileira *ABNT NBR ISO/IEC nº 17.799:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação* foi publicada em 31 de agosto de 2005 e entrou em vigor em 30 de setembro de 2005.

A ISO/IEC nº 17.799:2005 é um código de práticas com orientações para gestão de segurança da informação. Apresenta uma descrição geral das áreas consideradas mais importantes quando da implantação ou gestão de segurança da informação.

A norma ISO/IEC nº 17.799-2005 trata dos seguintes tópicos:

- política de segurança;
- organização da segurança da informação;
- gestão de ativos;
- segurança em recursos humanos;
- segurança física e do ambiente;
- gerenciamento das operações e comunicações;
- controle de acessos;
- aquisição, desenvolvimento e manutenção de sistemas de informação;
- gestão de incidentes de segurança da informação;
- gestão de continuidade de negócios;
- conformidade.

A ISO/IEC nº 17.799:2005 não fornece material definitivo ou específico para qualquer tópico de segurança. Ela serve como um guia prático para o desenvolvimento de padrões de segurança organizacional e auxilia na criação de atividades confidenciais interorganizacionais (SOUTO, 2006).

## 4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Segundo a referida norma da ABNT (ABNT, 2005), a política de segurança da informação deverá prover uma orientação e apoiar a direção, de acordo com os requisitos dos negócios, com as leis e as regulamentações relevantes.

Para a implementação da política de segurança da informação, é necessário que se tenha um documento que declare o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a política. Ela deverá ser comunicada por meio de toda a organização para os usuários, de forma que seja acessível e compreensível para o leitor em foco.

O documento da política de segurança da informação deverá ser parte de um documento da política geral da organização. Caso a informação seja distribuída fora da organização, ela deverá ser analisada cuidadosamente, para não revelar informações sensíveis.

A análise crítica da política de segurança da informação precisará ser analisada periodicamente e em intervalos planejados ou quando mudanças significativas ocorrerem, para garantir a contínua pertinência dos negócios, sua adequação e eficácia.

Conforme a norma da ABNT em estudo (ABNT, 2005), a política de segurança da informação precisará possuir um gestor que tenha a responsabilidade pelo desenvolvimento, pela análise crítica e pela avaliação da política de segurança da informação. A análise crítica deverá incluir a avaliação de oportunidades para melhoria da política de segurança da informação que tenha um enfoque para gerenciar a segurança da informação, em resposta às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais ao ambiente técnico.

## 5 ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO

Segundo a norma da ABNT em questão (ABNT, 2005), a organização da segurança da informação deverá gerenciar e assegurar que os procedimentos estipulados para segurança da informação sejam executados corretamente.

Uma estrutura de gerenciamento deverá ser estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Caberá à direção aprovar a política da segurança, atribuir as suas funções, coordenar e analisar criticamente a implementação da segurança da informação por toda a organização. Se necessário, uma consultoria especializada em segurança da informação poderá ser estabelecida e disponibilizada dentro da organização para iniciar e controlar as implantações.

Os contatos estabelecidos com especialistas ou grupos da área de segurança da informação que forem externos, incluindo autoridades relevantes, os contatos feitos para a organização se manter atualizada com as tendências do mercado, as normas de monitoração e os métodos de avaliação fornecerão apoio adequado, quando se estiver tratando de incidentes de segurança da informação. Convém, ainda, que um enfoque multidisciplinar na segurança da informação seja incentivado (ABNT, 2005).

### 5.1 Gestão de ativos

Segundo a norma da ABNT estudada (ABNT, 2005), a pessoa designada como responsável pelos ativos da organização deverá alcançar e manter a proteção adequada dos ativos, e garantir que todos os ativos estejam inventariados e tenham um proprietário responsável.

Esses proprietários dos ativos precisarão ser identificados e a eles deverá ser atribuída a responsabilidade pela manutenção apropriada dos controles do seu ativo.

A implementação de controles específicos poderá ser delegada pelo proprietário, conforme apropriado, porém o proprietário permanecerá responsável pela proteção adequada dos ativos (Asciutti, 2007).

### 5.2 Segurança em recursos humanos

Ainda segundo a norma da ABNT em foco (ABNT, 2005), a segurança da informação em recursos humanos deverá assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis dentro da organização, reduzindo o risco de roubo, fraude ou mal uso de recursos (Peixoto, 2004).

As responsabilidades pela segurança da informação em recursos humanos deverão ser atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.

Os candidatos ao emprego, fornecedores e terceiros serão adequadamente analisados, especialmente em cargos com acesso a informações sensíveis. Os funcionários, fornecedores, terceiros e usuários dos recursos de processamento da informação deverão assinar acordos sobre seus papéis e responsabilidades pela segurança da informação.

### 5.3 Segurança física

Segundo a norma em referência, a segurança física precisará prevenir o acesso físico não-autorizado, além de danos e interferências com as instalações e informações da organização.

As instalações de processamento das informações críticas ou sensíveis deverão ser mantidas em áreas seguras e protegidas por perímetros de segurança, com barreiras de segurança e controles de acesso, sendo importante que permaneçam fisicamente protegidas contra o acesso não-autorizado, danos e interferências.

Para os riscos identificados, a organização deverá oferecer uma proteção compatível, prevendo antecipadamente esses riscos e garantindo que estará preparada caso os riscos se tornem reais.

### 5.4 Gerenciamento das operações e comunicações

Segundo a norma em destaque, o gerenciamento das operações e das comunicações deverá garantir a operação dos recursos de processamento da informação de forma segura e correta.

Os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações terão de estar definidos, o que abrange o desenvolvimento de procedimentos operacionais adequados. Convém, ainda, que seja utilizada a segregação de funções quando apropriado, para minimizar o risco de mau uso ou de uso doloso dos sistemas (ABNT, 2005).

De acordo com a norma estudada, deverá ser controlado o acesso à informação, assim como recursos de processamento das informações e processos de negócios, com base nos requisitos de negócios e na segurança da informação, obedecendo às regras de controle de acesso e considerando as políticas para autorização e disseminação da informação.

A norma em pauta prevê que as aplicações críticas de negócios deverão ser analisadas criticamente e testadas quando sistemas operacionais forem mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.

### 5.5 Gestão de incidentes de segurança da informação

Segundo a norma mencionada, as notificações de incidentes têm o objetivo de assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Para isso, precisarão ser estabelecidos procedimentos formais de registro e escalonamento.

Todos os funcionários, fornecedores e terceiros também deverão estar conscientes dos procedimentos para notificação dos diferentes tipos de eventos e fragilidades que possam ter impactos na segurança dos ativos da organização, e que seja deles requerido que notifiquem os eventos de segurança da informação e fragilidades, tão logo quanto possível, ao ponto de contato designado.

Em conformidade com a norma citada, para garantir a continuidade, deverão ser identificados os eventos que podem causar interrupções nos processos de negócios, junto à probabilidade e ao impacto de tais interrupções e às conseqüências para a segurança de informação.

Existem planos de contingência, e estes deverão ser desenvolvidos e implementados para a manutenção ou a recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio, destacando que as atividades e os planos de gerenciamento de crise podem ser diferentes da gestão de continuidade de negócios, isto é, uma crise poderá acontecer e ser suprida por intermédio dos procedimentos normais de gestão.

### 5.6 Conformidade com normas, políticas de segurança da informação e técnicas

É importante que todos os gestores garantam que a política e as normas de segurança sejam seguidas. Mesmo assim, revisões periódicas deverão ser executadas para garantir o nível de conformidade com as normas. A periodicidade destas revisões está diretamente relacionada com a sua criticidade para o ambiente.

Periodicamente, a verificação de conformidade deverá ser executada de forma manual, e, sempre que possível, apoiada por *softwares* que possam gerar relatórios.

Os testes de conformidade poderão fazer uso de ferramentas que realizem verificações de possíveis vulnerabilidades, até mesmo testes de invasão, porém este tipo de teste somente deverá ser realizado por pessoas previamente autorizadas, visto que o mesmo poderá comprometer a integridade da segurança do sistema (GONÇALVES, 2005).

Segundo a referida norma da ABNT (ABNT, 2005), conformidade com normas, políticas de segurança da informação e conformidade técnica têm o objetivo de garantir conformidade dos sistemas com as políticas e as normas organizacionais de segurança da informação.

A segurança dos sistemas de informação deverá ser analisada criticamente em intervalos regulares, sendo que estas análises críticas deverão ser executadas com base nas políticas de segurança da informação apropriadas, de maneira que as plataformas técnicas e os sistemas de informação sejam auditados em conformidade com as normas de segurança da informação e estejam com os controles de segurança completos e documentados.

## 6 METODOLOGIA DA PESQUISA

Com base no conteúdo da ABNT NBR ISO/IEC nº 17.799:2005, realizou-se uma pesquisa exploratória por meio de entrevistas com algumas empresas situadas na região do ABC, a fim de descrever um percentual de organizações que utilizam da norma para implementação, manutenibilidade e garantia da segurança da informação.

### 6.1 Coleta de dados

A coleta de dados contou com respostas obtidas através da aplicação questionários estruturados, enviados via correio eletrônico corporativo.

No total, a pesquisa quantitativa teve uma mostra de dez questionários, compostos por 36 perguntas fechadas, de múltipla escolha, referentes às técnicas de segurança da informação.

Os profissionais de sistemas de informação que participaram deste estudo são responsáveis pela segurança da informação nas respectivas corporações em que atuam.

Por medidas de segurança e conforme acordo feito com os profissionais de segurança da informação das respectivas empresas que se dispuseram a responder ao questionário, o nome das empresas não será citado em nenhuma ocasião.

## 6.2 Apresentação e análise dos dados

A análise teve como objetivo organizar e sumarizar os dados de forma tal que possibilitem o fornecimento de respostas ao problema proposto para a investigação.

Os índices analisados são baseados nas respostas "sim" ou "não" do questionário elaborado com base na norma NBR ISO/IEC nº 17.799:2005, sendo que "sim" significa que a empresa está aderente aos itens da norma. As médias entre empresas e assuntos foram os parâmetros adotados para a análise comparativa.

A Figura 1 apresenta a média das empresas que seguem a norma da ABNT praticamente à risca para assegurar sua informação, tendo como parâmetro o índice, todas respostas, geral dos questionários.

Os resultados apresentados indicam que 50% das empresas estão de acordo com os procedimentos da norma para garantir a segurança da informação e se encontram acima da média (76%), e 24% estão abaixo da média. Todas as empresas pesquisadas estão acima de 50% de aderência aos requisitos da norma.

A Figura 2 mostra o nível de aderência ao tema política de segurança da informação, pesquisado entre as empresas, tendo como parâmetro as respostas à questão 1 do questionário.

Os resultados apresentados indicam que 30% das empresas procuram manter sua política de segurança com base na norma e estão acima da média (50%), e 70% estão abaixo da média. Entre as dez empresas, 70% estão abaixo de 50% de aderência e 30% estão acima dos 50%.

A Figura 3 apresenta o nível de aderência por empresa desse requisito da norma, tendo como parâmetro as respostas às questões 2 e 3 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média nesse requisito (78%) e 50% estão abaixo da média. Entre as dez empresas, 70% estão acima de 50% de aderência e 30% entre e abaixo de 50%.

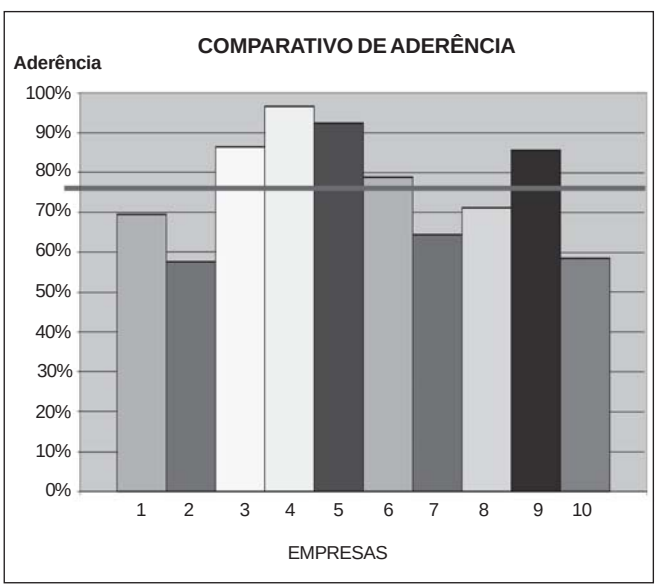


**Figura 1:** Comparativo de aderência por empresas

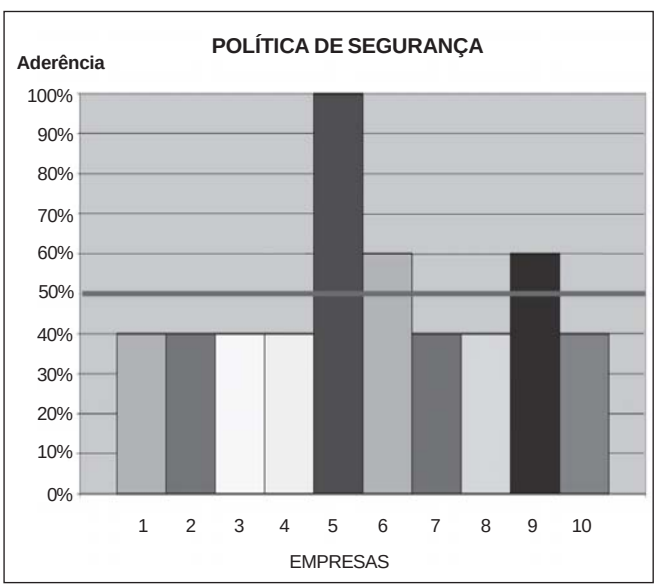


**Figura 2:** Política de segurança

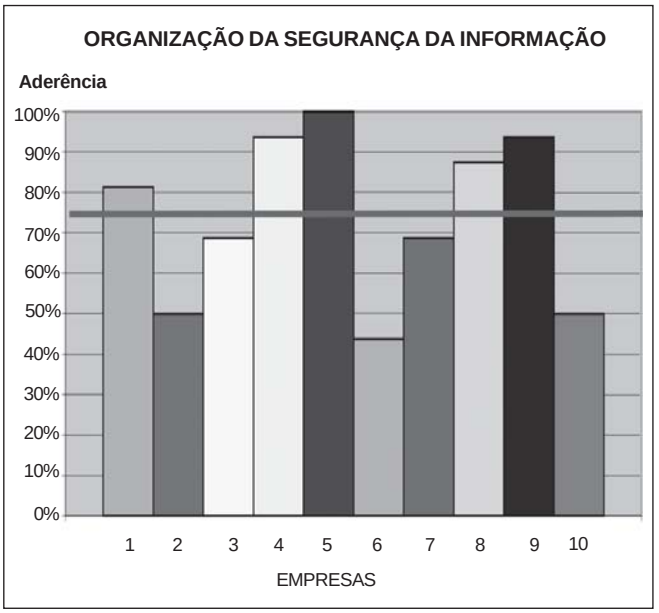


**Figura 3:** Organização da segurança da informação

A Figura 4 apresenta o nível de aderência na gestão de ativos por empresa, pesquisado entre as empresas, tendo como parâmetro as respostas às questões 4 e 5 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média, que foi de 78%, conforme as respostas obtidas, e 50% estão abaixo dessa média. Todas as empresas estão acima de 50% de aderência a esse requisito da norma.

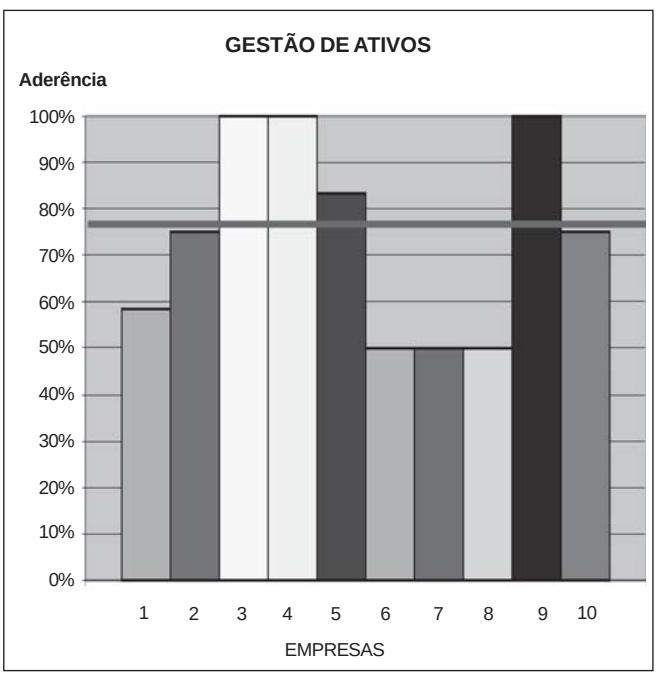


**Figura 4:** Gestão de ativos

A Figura 5 apresenta o nível de aderência no requisito segurança em recursos humanos, com base nos tópicos da norma que foi pesquisada entre as empresas, tendo como parâmetro as respostas às questões 6, 7 e 8 do questionário.

Os resultados apresentados indicam que 40% das empresas estão acima da média, que é de 78%, e 60% estão abaixo da média. Todas as empresas estão acima de 50% de aderência.

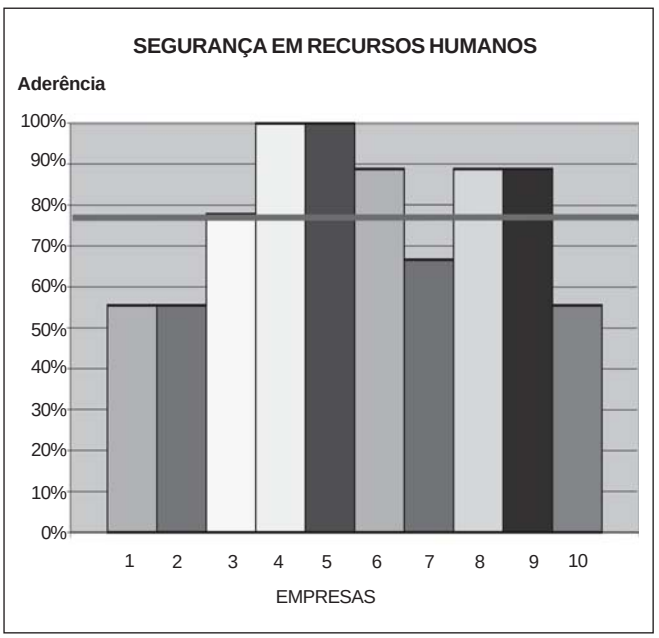


**Figura 5:** Segurança em recursos humanos

A Figura 6 apresenta o nível de aderência no requisito segurança física, pesquisado entre as empresas com base na norma, tendo como parâmetro as respostas às questões 9 e 10 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média de 81% de aderência, e 50% estão abaixo da média. Todas as empresas estão acima de 50% de aderência nesse requisito.

A Figura 7 apresenta o nível de aderência no gerenciamento das operações, pesquisado entre as empresas, tendo como parâmetro as respostas obtidas entre as questões 11 e 19 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média, que é de 74%, e 50% estão abaixo da média. Todas as empresas estão acima de 50% de aderência.

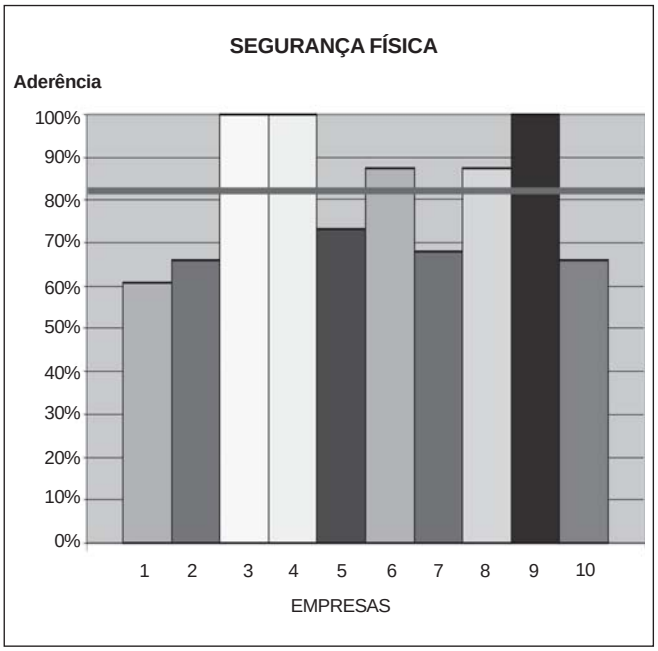


**Figura 6:** Segurança física

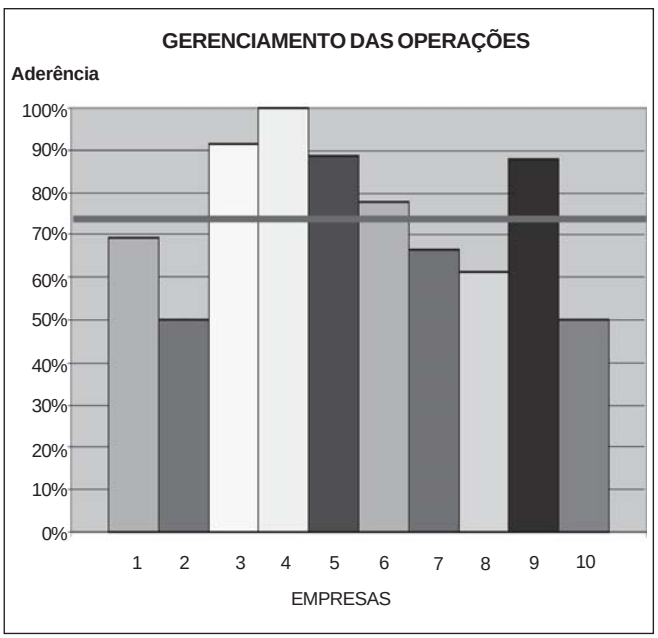


**Figura 7:** Gerenciamento das operações

A Figura 8 apresenta o nível de aderência das empresas ao requisito da norma que abrange o tema de monitoramento, pesquisado entre as empresas, tendo como parâmetro as respostas à questão 20 do questionário.

Os resultados apresentados indicam que 40% das empresas estão acima da média, que é de 87%, e 60% estão abaixo da média. Todas as empresas estão acima de 50% de aderência.

A Figura 9 apresenta o nível de aderência no requisito controle de acesso, pesquisado entre as empresas, tendo como parâmetro as respostas obtidas entre as questões 21 e 24 do questionário.

Os resultados apresentados indicam que 60% das empresas estão acima da média de 92%, e 40% estão abaixo da média. Todas as empresas estão acima de 50% de aderência.

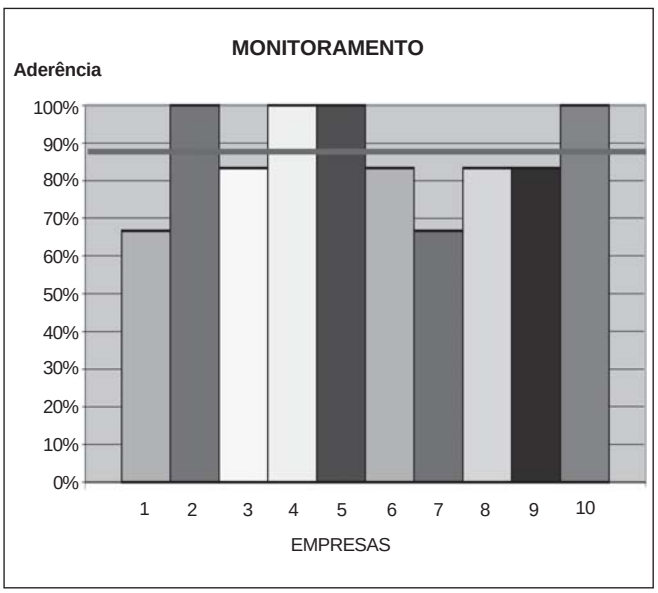


**Figura 8:** Monitoramento

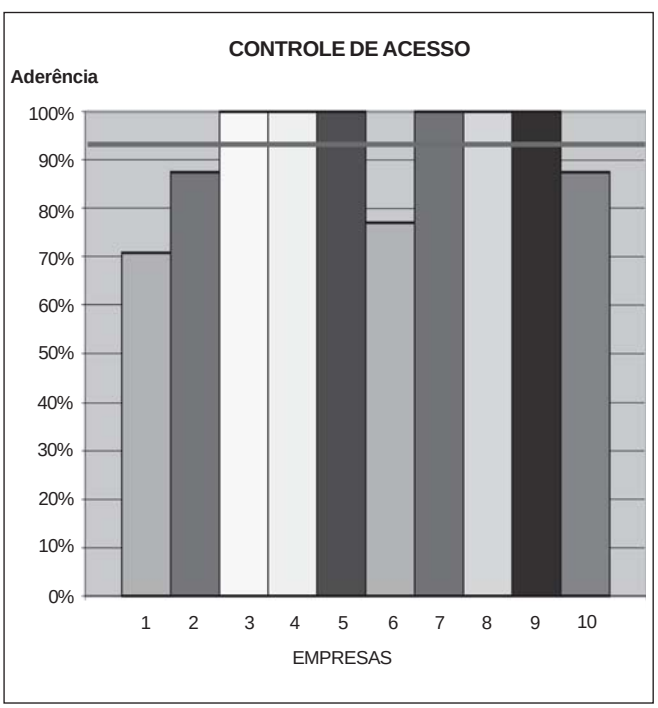


**Figura 9:** Controle de acesso

A Figura 10 apresenta o nível de aderência nos requisitos de segurança, pesquisado entre as empresas, tendo como parâmetro as respostas obtidas entre as questões 25 e 30 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média de 61%, e 50% estão abaixo da média. Entre as dez empresas, 70% estão acima de 50% de aderência e 30% estão abaixo.

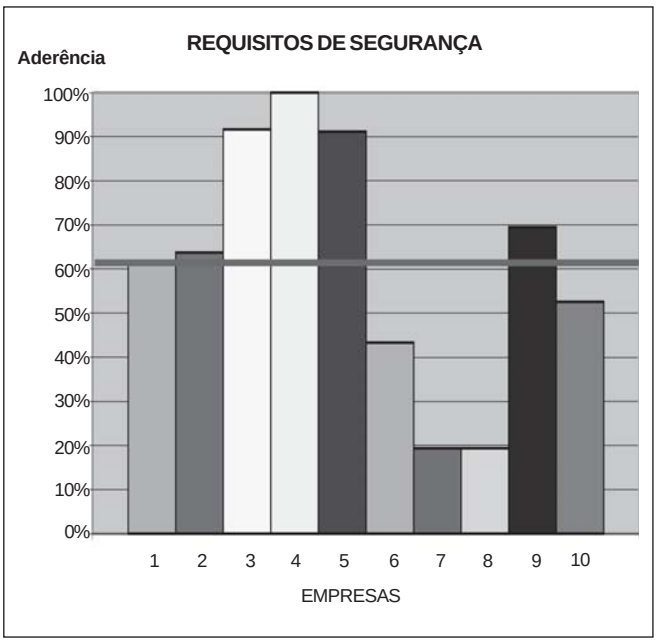


**Figura 10:** Requisitos de segurança

A Figura 11 apresenta o nível de aderência na gestão de incidentes, pesquisado entre as empresas, tendo como parâmetro as respostas às questões 31 e 32 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média de 78%, e 50% estão abaixo da média. Todas as empresas estão acima de 50% de aderência.

A Figura 12 apresenta o nível de aderência na gestão da continuidade do negócio, pesquisado entre as empresas, tendo como parâmetro as respostas à questão 33 do questionário.

Os resultados apresentados indicam que 60% das empresas estão acima da média (70%) e 40% estão abaixo da média. Entre as dez empresas, 60% estão acima de 50% de aderência e 40% estão abaixo.

A Figura 13 apresenta o nível de aderência na conformidade, pesquisado entre as empresas, tendo como parâmetro as respostas entre as questões 34 e 36 do questionário.

Os resultados apresentados indicam que 50% das empresas estão acima da média de 72%, e 50% estão abaixo da média. Entre as dez empresas, 70% estão acima de 50% de aderência e 30% estão a seguir.

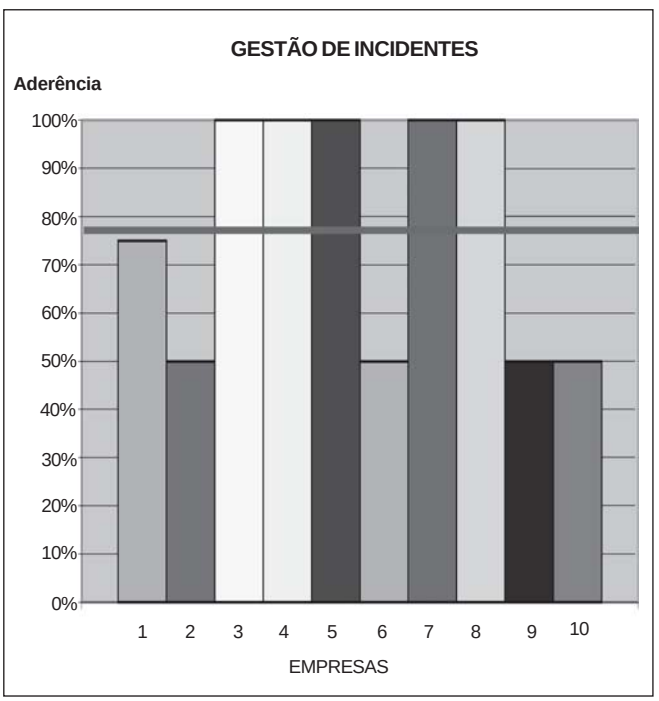


**Figura 11:** Gestão de incidentes

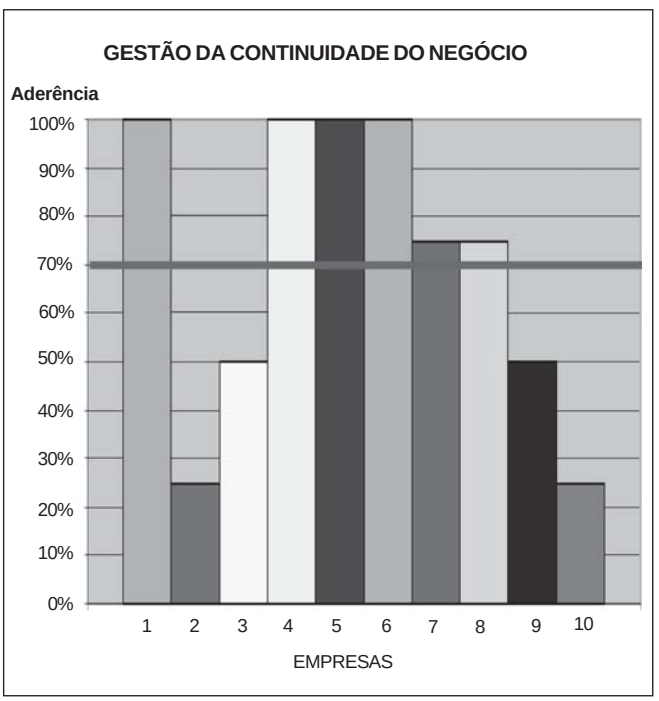


**Figura 12:** Gestão de continuidade do negócio

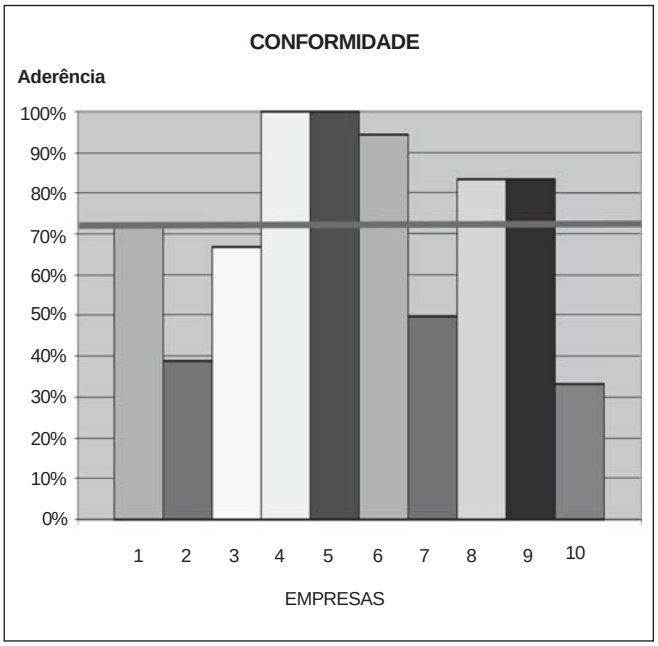


**Figura 13:** Conformidade

A Figura 14 apresenta o nível de aderência por assunto, pesquisado entre as empresas, tendo como parâmetro todas as questões do questionário.

Os resultados apresentados indicam que 75% das empresas estão iguais, ou seja, estão no mesmo nível de segurança ou acima de 50% de aderência, e 25% estão abaixo. O índice de 70% não foi ultrapassado em nenhum assunto. Pode-se observar, também, que o índice com maior problema é a política de segurança, pois está com 30% de aderência.

## 7 CONCLUSÃO

Este artigo teve o objetivo de fornecer conceitos tecnológicos voltados à segurança da informação, utilizando como base a norma ABNT NBR ISO/IEC nº 17.799:2005, e verificar qual a aderência de algumas empresas situadas na região do ABC aos requisitos da norma estudada. Assim, buscou-se fornecer o conhecimento de segurança da informação, auxiliando os interessados em aplicar a norma e avaliar como o mercado atual de empresas situadas na região do ABC encontra-se quando se fala de segurança da informação.

Para que o objetivo fosse alcançado, procurou-se conhecer os princípios de segurança de informação e da norma ABNT NBR ISO/IEC nº 17.799:2005, bem como a analisar a aderência das empresas aos requisitos da norma, seu conhecimento sobre os conteúdos principais da norma e sua aplicação no dia-a-dia.

Com isso, foram obtidos os seguintes resultados:

- o conceito de segurança da informação é bem disseminado na organização;

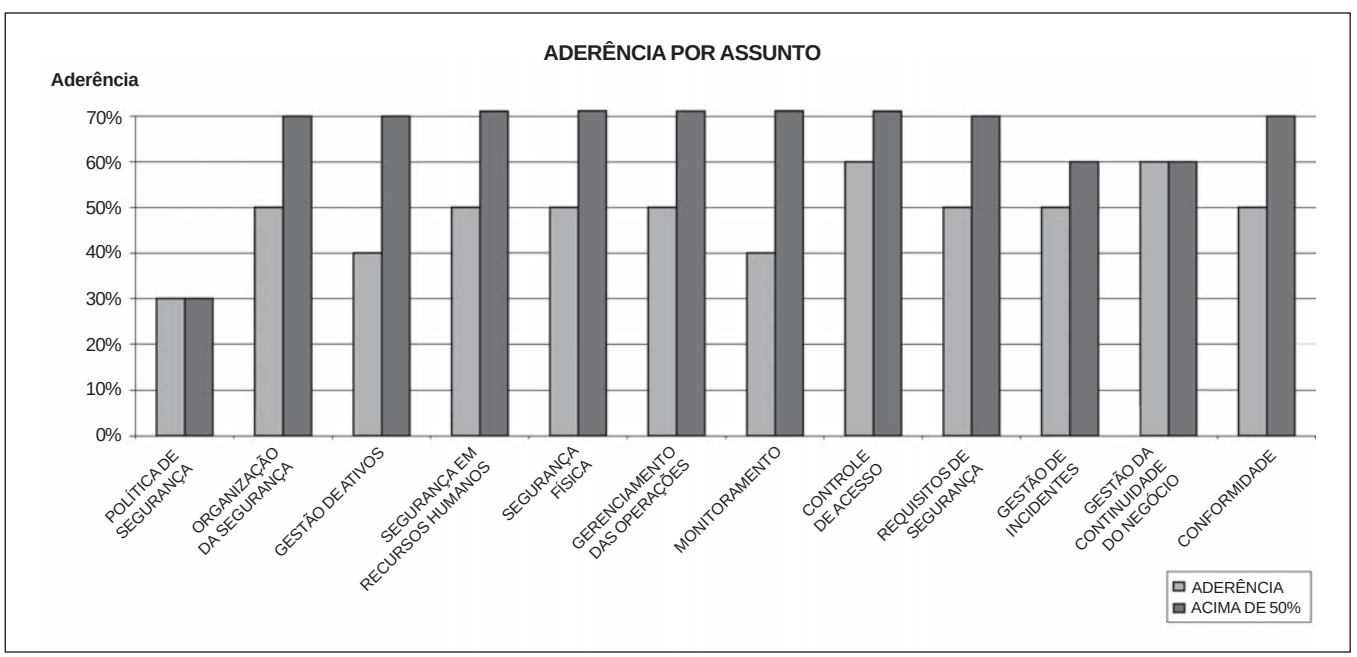


**Figura 14:** Nível de aderência das empresas

- a política de segurança é conhecida pela população da organização;
- a segurança é compreendida como ativo organizacional e intrínseco para o diferencial no mercado;
- os controles de segurança da informação são percebidos pela organização como fundamentais para a segurança da informação.

Baseado neste resultado, realizou-se um estudo aprofundado das respostas obtidas e foi avaliado que os pontos críticos são os que seguem: a publicação às partes externas, o espaço de tempo no qual a política é revisada, além do que dificilmente ela é alterada após mudanças significativas.

Porém, nesta análise detalhada por assuntos, também se obteve um resultado muito positivo, mostrando que 78% dos assuntos abordados são bem disseminados, e as empresas aderem à norma, e 22% delas não se mostraram aderentes, tendo como parâmetro 50% de aderência.

Com base em todos os temas levantados neste trabalho, foi possível instruir as organizações avaliadas sobre quais os pontos necessários para melhoria e/ou alterações.

Este estudo pode ser aprofundado, levando à comparação um maior numero de organizações e suas diversas localidades, com o aprofundamento dos temas considerados críticos e a necessidade de melhorias.

## 8 REFERÊNCIAS BIBLIOGRÁFICAS


ABNT – Associação Brasileira de Normas Técnicas. Tecnologia da informação – Técnicas de Segurança – Código de prática para gestão de segurança da informação. ABNT NBR ISO/IEC nº 17.799:2005, de 30/09/2005.

Asciutti, C. A. Alinhando ABNT NBR ISO/IEC nº 17.799 e nº 27.001 para a Administração Pública – USP. Disponível em: <http://www.security.usp.br/artigos/2-ESECOM_USP-09-11-2006-Artigo-By-Asciutti-Cesar-A-V1-04.pdf>. Acesso em: 01 de maio de 2007.

Casanas, A. D. G. & Machado, C. S. O impacto da implementação da norma NBR ISO/IEC nº 17.799. Fonte: *Modulo Security Magazine*. Publicado em 11 de maio de 2006. Disponível em: <http://www.modulo.com.br/artigos>. Acesso em: 30 de setembro de 2007.

Cherobino, V. Tendências 2007: segurança ainda é prioridade de TI nas empresas. Fonte: *Computerworld*. Disponível em:

<http://idgnow.uol.com.br/seguranca/2006/12/29/idgnoticia.2006-12-29.4183160774/IDGNoticia_view?pageNumber:int=1>. Acesso em: 01 de maio de 2007.

Gonçalves, L. R. O. Pequeno histórico sobre o surgimento das normas de segurança. Fonte: *Lockabit*. Publicado em: 18 de agosto de 2003. Disponível em: <http://www.modulo.com.br/artigos>. Acesso em: 30 de setembro de 2007.

_____. 2005. *Um modelo para verificação, homologação e certificação de aderência à norma nacional de segurança de informação – NBR ISO/IEC nº 17.799:2005*. Trabalho de conclusão de curso (Pós-Graduação) – Universidade Federal do Rio de Janeiro. Rio de Janeiro: UFRJ.

_____. O surgimento da Norma Nacional de Segurança de Informação [NBR ISO/IEC nº 1.779:2001]. Disponível em: <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=85>. Acesso em: 28 de setembro de 2007.

Júnior, A. R. S.; Fonseca, F. S. S. & Coelho, P. E. S. Entendendo e implementando a Norma ABNT NBR ISO/IEC nº 17.799:2005. Apostila desenvolvida pelo Instituto *On-line* em parceria com a Microsoft Informática Revisão 1.0. Publicado em março de 2006. Disponível em: <http://www.instonline.com.br/>. Acesso em: 20 de maio de 2007.

Moraes, P. B. Tutorial para o projeto da infra-estrutura de um *Internal Data Center*. Publicado em 17 de fevereiro de 2003. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialidc/pagina_4.asp>. Acesso em: 30 de setembro de 2007.

Peixoto, M. C. P. 2004. *Gestão da segurança da informação no contexto da vulnerabilidade técnica e*

*humana inserida nas organizações*. Monografia (Bacharelado) – Curso de Ciência da Computação – Pró-Reitoria de Ensino de Graduação do Centro Universitário do Triângulo. Uberlândia: Unitri.

PEREIRA, P. J. F. Segurança da informação digital. *Cadernos de Biblioteconomia Arquivística e Documentação* – Cadernos BAD, n. 1 – Associação Portuguesa de Bibliotecários, Arquivistas e Documentalistas (BAD), Lisboa, Portugal, p. 66-80, 2005.

SÊMOLA, M. *Módulo Security Solutions S/A*. Gestão da segurança da informação: visão executiva da segurança da informação aplicada ao *security officer*. Rio de Janeiro: Elsevier/Campus, 2003.

SILVA, R. P. 2005. *Engenharia de Software segura*: segurança em desenvolvimento de *software*. Monografia (Pós-Graduação *Lato Sensu*) – Programa de Pós-Graduação em Engenharia de *Software* da Universidade Candido Mendes. Rio de Janeiro: Ucam.

SOUTO, C. C.; SILVA, M. A. & LIMA, W. D. 2006. *Estudo da aplicação da Norma NBR ISO/IEC nº 17.799:2005 em segurança da informação*. Trabalho de conclusão de curso (Graduação) – Programa de Graduação em Sistemas de Informação do Centro Universitário Unieuro. Brasília-DF: Unieuro.