1ºCONTECSI Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação
21-23 de Junho de 2004 USP/São Paulo/SP - Brasil

UM ESTUDO PROSPECTIVO SOBRE SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE TELECOMUNICAÇÕES SEGUNDO A NBR ISO/IEC 17799:2001

Décio Frederico Bueno Feijó, Eng.
Universidade Federal do Rio Grande do Norte
Programa de Engenharia de Produção, Centro de Tecnologia
Campus Universitário, Natal-RN
+55 84 211-9239 decio@digi.com.br

Anatália Saraiva Martins Ramos, D.Sc.
Universidade Federal do Rio Grande do Norte
Programa de Pós-graduação em Administração, Centro de Ciências Sociais Aplicadas
Campus Universitário, Natal-RN
+55 84 215-3536 anatalia@ufrnet.br

Palavras-chave: Segurança da Informação, Segurança Física e Ambiental, Certificação, ISO/IEC 17799, Telecomunicações.

Resumo

O presente artigo demonstra os resultados de uma pesquisa exploratória cujo objetivo foi identificar de forma prospectiva os pontos de controle da segurança da informação, documentados pela norma NBR ISO/IEC[i] 17799:2001 (Tecnologia da Informação – Um Código de Práticas para a Gestão da Informação), em seu item de Segurança Física e Ambiental, sob o prisma das práticas de controle hoje aplicadas em uma empresa do setor de telecomunicações. Os resultados indicam um baixo nível de segurança de área detectado em suas instalações, o que poderá comprometer o nível da qualidade do serviço e até mesmo sua competitividade empresarial. Recomenda-se uma adequada implantação das práticas propostas pela norma, iniciando-a pelo domínio da Segurança Física e Ambiental.

1. Introdução

O objetivo primordial da segurança da informação pode ser descrito como sendo a proteção da informação contra uma grande gama de ameaças, na forma em que assegura a continuidade dos negócios, minimiza os danos e maximiza o retorno dos investimentos e as oportunidades comerciais. Esta afirmação só se torna útil quando se compreende o valor da informação em nossos dias, uma vez que para muitos a informação se resume a um subproduto do processo produtivo e não seu bem mais valioso.

Nakamura e Geus (2002) entendem que uma gestão eficaz da segurança deve permitir as organizações buscar seus lucros, os quais são conseguidos através de novas oportunidades, resultando assim, na flexibilidade, facilidade e disponibilidade dos recursos de informática. Desta forma, considera-se que a segurança da informação não deve apenas ser tratada como uma proteção, mas como um elemento habilitador para a realização dos negócios.

Percebe-se nos dias atuais que os negócios das organizações – sejam elas empresas privadas ou instituições públicas - são, na grande maioria dos casos, sustentados pelas aplicações da Tecnologia da Informação (TI). A informação gerada pelos sistemas de informação possui seu valor e conseqüentemente necessidades de ser apropriadamente protegida (Cassa, 2003).

Quanto à revisão de literatura, identificaram-se muitos estudos no meio profissional e em periódicos internacionais. Porém, no cenário acadêmico nacional, os trabalhos em Gestão de Segurança da Informação são relativamente poucos, tendo em vista a área de Sistemas de Informação como um todo. Na pesquisa bibliográfica em congressos nacionais na área de Gestão de Segurança, destacam-se alguns trabalhos como os de Carvalho et al. (1999), Casanas e Machado (2001), Machado e Fischer (2002), Machado (2002a), Machado (2000B), Medeiros e Ramos (2002), Gabbay e Ramos (2003), Oliva e Oliveira (2003).

Espera-se que este artigo faça uma pequena contribuição ao avanço do conhecimento, principalmente aos interessados em pesquisar este assunto em seus trabalhos acadêmicos.

Conceitos básicos

A segurança da informação é um conjunto de medidas que se constituem basicamente de controles e política de segurança. Segundo Berinato e Scalet (2002), a segurança da informação pode ser visto como o processo da proteção das informações de acidentais ou propositais maus usos por pessoas de dentro ou fora de uma organização.

Para Benz (2000), os objetivos da Segurança da Informação são:

- Preservação do patrimônio da empresa;
- Manutenção dos serviços prestados pela empresa;

- Segurança do corpo funcional.

Moreira (2001) entende que os objetivos de segurança visam também aumentar a produtividade dos usuários através de um ambiente mais organizado, proporcionando maior controle sobre os recursos. Os benefícios obtidos pela segurança corporativa são:

- Redução de riscos contra vazamentos de informações confidenciais;
- Redução da probabilidade de fraudes;
- Diminuição de erros devido a treinamentos e mudança de comportamento;
- Manuseio incorreto de informações confidenciais.

Em caso de problemas, algumas ações são sugeridas, tais como detecção das causas e origens dos problemas no menor prazo possível, minimização das conseqüências dos mesmos, retorno às condições normais no menor prazo, com o menor custo e com o menor trauma possíveis.

Uma visão geral em todos os conceitos levantados de segurança da informação e seus objetivos leva a visualizar que, em todo escopo corporativo, a função da segurança da informação está associada com a "proteção do negócio da empresa". Para tanto, devem ser designados recursos e responsabilidades para tais ações. A existência da Segurança da Informação como um elemento da estrutura organizacional compatível com o porte e negócio da empresa, demonstra a seriedade do assunto para a organização (Fontes, 2001). Esta seriedade, uma vez conferida, pode e deve ser encarada como uma força competitiva, uma vez que demonstrações de bom uso e privacidade de informações, sem falar de suas próprias, se tornaram um diferencial na visão de negócio. Para isso, foram criadas normas internacionais com o intuito de se mensurar o grau de comprometimento, e orientar as empresas no rumo da segurança da informação. Tais normas, como a CEBIT, ISO/TR15369, BS 7799 e sua versão internacional ISO/IEC 17799 já contam com certificações internacionais, logrando grau de excelência na área de segurança a empresas e organizações. Bancos, instituições de crédito, seguradoras, dentre outros negócios que lidam com a informação já se encontram em um nível mais avançado de implementação de políticas de segurança de informação. No Brasil, destaca-se um dos maiores bancos privados, por suas ações pioneiras neste campo (Bradesco, 2002).

Para Restell (2000), a certificação oferece uma visão competente e imparcial do sistema de segurança da empresa. Ela é voltada para facilitar o comércio eletrônico, encoraja as organizações a se relacionar e promove a adoção de uma gestão comum de segurança por vários tipos de indústria. Organizações que completam com sucesso o processo de certificação podem garantir maior segurança, privacidade e ética na gestão de seus sistemas

de segurança e atestar aos seus parceiros comerciais o compromisso com os princípios fundamentais da segurança da informação: a confidencialidade, disponibilidade e integridade das informações.

Os primeiros indícios da necessidade da criação de normas que padronizem as ações de segurança nas empresas vieram com o advento dos sistemas informáticos, onde a informação ganhou maior grau de importância, graças ao descoberta de seu valor estratégico.

Em 1987 foi criado na Grã-Bretanha o Centro de Segurança de Informações do DTI (Departamento de Comércio é Indústria) com o intuito de se desenvolver uma norma de segurança das informações para o Reino Unido e códigos de segurança para os usuários da informação (Solms, 1998). Em 1989, foi publicado um Código para Gerenciamento da Segurança da Informação, cujo codinome é PD0003 e, posteriormente, em 1995, após ser revisado, foi publicado como a norma britânica - British Standard (BS), a BS7799:1995. Em dezembro de 2000, incorporadas diversas sugestões e alterações, a BS7799-1 ganhou status internacional com sua publicação na forma da ISO/IEC 17799:2000 (Hefferan, 2000).

Com a homologação oficial pela ISO/IEC da norma, vários paises, dentre eles o Brasil, acompanhando a tendência, seguiram seu exemplo e criaram normas nacionais de segurança. Em setembro de 2001, a ABNT – Associação Brasileira de Normas Técnicas – homologou a sua versão brasileira, denominada NBR ISO/IEC 17799:2001.

A ISO 17799 foi desenvolvida para ser usada como ponto de partida para o desenvolvimento de um programa empresarial específico. Nem todos os controles identificados na documentação podem ser aplicados em todas as empresas (Peltier, 2000).

Segundo Wynes (2000), o gerenciamento da segurança da informação habilita a informação para ser compartilhada, somando o quesito **proteção** com a vantagem da informática. Existem três componentes-chave para prover estas garantias:

i. Confidencialidade: assegurando que a informação esteja acessível somente para aqueles autorizados em ter acesso;
ii. Integridade: protegendo a precisão e a perfeição da informação;
iii. Disponibilidade: assegurando que pessoas autorizadas tenham acesso a informação e ao recurso associado quando requerido.

É com base nestes três princípios que foi construído o modelo ISO/IEC 17799:2000 e fundamenta todas as teorias e modelos de segurança.

A atual ISO/IEC 17799 não se limita a aspectos meramente técnicos de processamento, TI e redes, mas abrange todos os aspectos de segurança da organização

(Caruso, 2002). Os itens descritos pela norma são subdivididos em 12 seções, gerando 127 pontos de controle. Os itens da norma são (ABNT, 2001):

1. Escopo
2. Termos e Definições
3. Política de segurança;
4. Organização de segurança;
5. Classificação e controle de ativos;
6. Segurança aplicada a recursos humanos;
7. **Segurança física e de ambiente**;
8. Gerenciamento de operações e comunicações;
9. Controle de acesso;
10. Manutenção e desenvolvimento de sistemas;
11. Gerenciamento da continuidade do negócio e;
12. Conformidade.

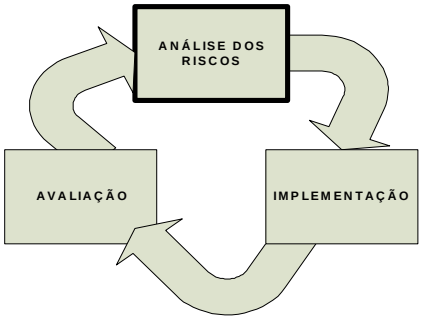
Além da visão abrangente e detalhada da Norma de segurança da informação, é necessário se implantar uma visão sistêmica de três elementos, conforme se apresenta na Figura 1:

1. Conduzir uma análise de riscos. Isso permitirá que a empresa possa identificar os riscos em uma atividade ou ativo, priorizando aqueles riscos ou ameaças e para identificar possíveis salvaguardas ou controles que possam reduzir o risco em um nível aceitável. É neste ponto que a ISO 17799 é mais útil.

2. Implementar os controles e treinar os empregados para que possam utilizá-los de forma apropriada.

3. Conduzir avaliações dos controles para garantir que eles continuam a permitir que os objetivos de negócios sejam atingidos.

Figura 1 - Ciclo da Segurança da Informação



Fonte: Peltier, 2003

A forma como os assuntos são abordados permite o entendimento das diversas dimensões do problema e nos leva a concluir que segurança da informação extrapola a esfera tecnológica, enveredando pelos problemas e vulnerabilidades associadas à infra-estrutura, ambientes físicos, aplicações, à própria tecnologia e às pessoas. Isso ratifica a mensagem de que segurança é a gestão inteligente da informação em todos os ambientes (Sêmola, 2001).

Neste estudo, será enfocado o ponto de vista da "**Segurança Física e Ambiental**, seção 7, especificamente avaliando o sub item: *Segurança de Área*" da norma NBR ISO 17799:2001, no caso de uma empresa do setor de Telecomunicações.

O principal objetivo da implantação de controles de segurança física é restringir o acesso às áreas críticas da organização, prevenindo os acessos não autorizados que podem acarretar danos a equipamentos, acessos indevidos à informação, roubos de equipamentos, entre outros (SCUA, 2003). Já para Moreira (1998), segurança física é compreendida como os aspectos de segurança relacionados com eventos em que existe contacto físico anormal com os equipamentos. Por vezes alguma proximidade física é suficiente, tal como acontece com falhas de confidencialidade por detecção à distância de sinais eletromagnéticos emitidos pelas linhas de comunicação ou monitores de vídeo.

O controle de acesso do tipo físico é toda e qualquer aplicação de procedimentos ou uso de equipamentos com o objetivo de proteger ambientes, equipamentos ou informações cujo acesso deve ser restrito. Esse tipo de controle envolve o uso de chaves, trancas, guardas, crachás, cercas, alarmes, vídeo, *smart cards*, biometria e outros meios, além da aplicação de normas e procedimentos utilizados pela empresa para esse fim (Haical, 2000).

A norma no item de Segurança Física e Ambiental possui três sub-divisões: Segurança de Área, Segurança de Equipamentos e Controles Gerais; cada uma possuindo vários pontos de controle propostos pela norma; no quesito Segurança de Área, os pontos segmentados pelo item abordado com seu quantitativo de controles são os seguintes:

- Perímetro de Segurança Física → 5 Controles
- Controle de Entrada Física → 4 Controles
- Protegendo escritórios, quartos e instalações. → 9 Controles
- Trabalhando em áreas seguras → 5 Controles
- Isolando áreas de carga e descarga → 5 Controles

Estes 28 pontos de controle apóiam a segurança da informação no sentido em que geram controles físicos padronizados. Estes pontos de controle somados às proteções estruturais reforçadas minimizam as interferências ambientais e alguns riscos humanos.

(Turban ,2003). Como mencionado, são os tópicos específicos sobre a Segurança de Área que o estudo foi realizado.

A seguir, será descrita a metodologia do estudo, para então apresentar alguns resultados do estudo de caso.

2. Metodologia

Trata-se de pesquisa exploratória em uma organização, com objetivo de descrever uma aplicação de conhecimentos na área de segurança de informação, realizando uma análise de uma empresa do setor de telecomunicações.

O estudo de caso refere-se a uma empresa de televisão por assinatura, do ramo de **TV a Cabo**, localizada na cidade do Natal, no Rio Grande do Norte. Caracterizando-se como um serviço de comunicação de massa, teve sua licença adquirida em 1998 por meio de licitação, então aberta pelo Ministério das Comunicações, Anatel, iniciando a implantação de sua base operacional em 1999, estando em operação efetivamente a partir de 2000. Esta licença compreende a comercialização de sistema de TV a Cabo em toda área da cidade do Natal, não podendo ampliar sua área para fora dos limites políticos do município. A TV hoje abrange grande parte da Zona Sul da cidade, com uma rede de distribuição HFC (Híbrida Fibra-Coaxial) com mais de 460Km. Oferece serviços de Televisão por Assinatura e, desde agosto de 2001, conta com o sistema de distribuição de Internet Banda Larga. A empresa conta com mais de 70 funcionários e três empreiteiras terceirizadas, responsáveis pelas instalações dos assinantes, centralizando suas operações em sua sede, onde o estudo foi realizado.

Em termos de procedimento de coleta de dados, esta pesquisa é de levantamento de dados, onde foram utilizadas algumas premissas criadas pela norma NBR ISO/IEC 17799:2001, em suas descrições de controles e gestões para os recursos da informação, tendo como base um estudo prospectivo de sua implantação futura.

Dada a extensão e a complexidade da norma, a qual compreende 12 seções de análise da segurança da informação, em todos os escopos de sua cadeia de evolução, descrevendo desde sua geração, armazenamento até sua disponibilização, foi escolhido apenas um destes escopos para aplicação neste artigo, focando o estudo na *Segurança Física da informação*, visualizando no contexto todos os itens que a influenciam.

Englobando todos os aspectos ressaltados pela norma com relação à segurança física, sob a responsabilidade da área de tecnologia de informação, este estudo levantou a primeira parte do Ciclo da Segurança da Informação, descrito por Peltier (2003), relativa à Análise dos Riscos.

Nesta pesquisa de estudo de caso, foi utilizada a técnica da triangulação (Yin, 2002), com a utilização dos recursos metodológicos da pesquisa documental, através de análise dos manuais de procedimento da empresa; entrevistas não estruturadas com funcionários e observação *in loco*. O período de coleta de dados compreendeu os meses de novembro e dezembro de 2003.

Para a tabulação dos dados, todos os pontos de controle estão apresentados segundo a Norma. Já a sua pontuação está de acordo com a avaliação do grau de comprometimento da empresa com relação ao determinado item de controle, observando-se aspectos objetivos e subjetivos nesta avaliação. A pontuação é numérica, com escala de intensidade medida de **0** - nenhum comprometimento, a **10** - total comprometimento. É apresentada a resposta **NA** quando o item da norma não se aplica neste caso. Caso a empresa atingisse a pontuação máxima dos itens avaliados, esta teria 270 pontos no total.

A análise dos dados se deu mediante uma abordagem qualitativa. Seus resultados estão descritos na seção correspondente deste trabalho.

3. Resultados do estudo de caso

As normas de segurança física e ambiental servem para garantir a segurança da área, do material, da documentação, das comunicações e dos recursos humanos relacionados com sua área de atuação, de forma a impedir o acesso indevido aos assuntos corporativos. O presente estudo de caso procurou avaliar os níveis de segurança deste tópico. Estes resultados serviram para a alta administração da empresa tomar decisões relativas à melhoria dos aspectos de segurança e traçar, no seu planejamento estratégico, as primeiras diretrizes da política de segurança corporativa.

Na Tabela 1, são apresentadas as pontuações obtidas em cada um dos controles relativos à Segurança de Área, referentes à avaliação realizada segundo a norma ISO/IEC 17799, sobre Segurança da Informação.

Tabela 1 – Controles de Segurança de Área

PERÍMETRO DE SEGURANÇA FÍSICA	Pontos da Empresa
a) O perímetro de segurança deve ser claramente definido	10
b) O perímetro de um edifício ou local que contêm instalações de processamento de informação deve ser fisicamente isolado (não deve haver nenhuma abertura no perímetro ou áreas onde uma ruptura possa ocorrer facilmente). As paredes externas do local devem ser de construção sólida e todas as portas externas devem ser protegidas adequadamente contra acesso sem autorização, por exemplo, mecanismos de controle, barras, alarmes, fechaduras etc.	7
c) Uma área de recepção tripulada ou outros meios de controle de acesso físico ao local ou prédio devem ser criados. Acessos aos estabelecimentos devem ser restritos apenas ao pessoal autorizado.	9

d) Barreiras físicas devem, se necessário, ser estendidas do chão ao teto para prevenir entrada sem autorização e contaminação ambiental, causadas por incêndios e inundações, por exemplo.	10
e) Todas as portas de incêndio no perímetro de segurança devem possuir alarmes e travas antipânico.	0
Sub-total	36

CONTROLE DE ENTRADA FÍSICA	Pontos da Empresa
a) Visitantes a áreas seguras devem ser supervisionados ou cancelados, com data e horário de entrada registrados	5
b) Acessos às informações sensíveis e instalações de processamento de informação devem ser controlados e restringidos apenas às pessoas autorizadas.	8
c) Deve ser exigido de todas as pessoas, o uso de alguma forma de identificação visível e devem ser encorajados a confrontar quaisquer estranhos não acompanhados e qualquer um que não esteja utilizando identificação visível.	9
d) Direitos de Acesso a áreas seguras devem ser regularmente revistos e atualizados.	3
Sub-total	25
PROTEGENDO ESCRITÓRIOS E INSTALAÇÕES	Pontos da Empresa
a) Instalações fundamentais devem estar sitiadas para evitar acesso pelo público.	10
b) Edifícios devem ser moderados e dar o mínimo de indicações de seu propósito, sem sinais óbvios, dentro ou fora do edifício identificando a presença de atividades de processamento de informação.	6
c) Funções de apoio e equipamentos, por exemplo, fotocopiadoras, máquinas de fac-símile, devem ser adequadamente situadas dentro da área segura para evitar fluxos de acesso que poderiam comprometer as informações.	1
d) Portas e janelas devem ser fechadas quando desacompanhadas e proteções externas devem ser consideradas para janelas, particularmente em nível do solo.	4
e) Um apropriado sistema de detecção de intrusos instalado com base em padrões profissionais e regularmente testados deve estar em um local que cubra todas as portas externas e janelas acessíveis.	0
f) Instalações de processamento de informação administradas pela organização devem ser separadas fisicamente daqueles controlados por terceiros.	10
g) Diretórios e listas telefônicas internas que identificam locais de instalações de processamento de informação sensíveis não devem ser prontamente acessíveis ao público.	10
h) Materiais perigosos ou combustíveis devem ser armazenados seguramente a uma distância segura de uma área segura. Não devem ser armazenados materiais volumosos, como papelaria, dentro de uma área segura até este ser requerido.	8
i) Equipamentos de redundância mídias de backup devem estar localizados a uma distância segura para evitar danos causados por um desastre no local principal.	9
Sub-total	58
TRABALHANDO EM ÁREAS SEGURAS	Pontos da Empresa
a) Pessoal deverá somente estar atento à existência de uma área segura na necessidade de tal conhecimento.	4
b) Trabalho não supervisionado em áreas seguras deve ser evitado tanto por razões de segurança como para prevenção das oportunidades para atividades maliciosas.	2
c) Áreas seguras desocupadas devem ser fisicamente fechadas e periodicamente conferidas.	NA
d) Pessoal de serviços terceirizado de apoio deve ter permissão de acesso restrito a áreas seguras ou instalações de processamento de informações sensíveis quando exigido. Este acesso deve ser autorizado e monitorado. Pode ser necessária a criação de barreiras adicionais e perímetros para controlar o acesso físico entre áreas com exigências de segurança diferentes dentro do perímetro de segurança.	6
e) Equipamento fotográfico, de vídeo, gravadores de áudio ou outros não devem ser permitidos, a não ser com autorização.	9
Sub-total	21

ISOLANDO ÁREAS DE CARGA E DESCARGA	Pontos da Empresa
a) Acesso a uma área externa da propriedade do complexo deve ser restringido o pessoal identificado e autorizado.	0
b) A área do complexo deve ser projetada de forma que materiais possam ser descarregados sem que o pessoal de entrega tenha acesso a outras partes do edifício.	7
c) A(s) porta(s) externa(s) da área da propriedade deve estar seguras quando a porta interna é aberta.	4
d) Os Materiais entrantes devem ser inspecionados contra potenciais perigos, antes de serem levados da área de carga a ponto de uso.	10
e) O material entrante deve ser registrado, se apropriado, na entrada para o almoxarifado.	10
Subtotal	31
TOTAL de pontos	**171**

Fonte: Pesquisa de campo

Somando-se todos os pontos obtidos pela empresa pesquisada, tem-se um total de 171 pontos. Isso significa um percentual de **63,3%** de conformidade, segundo o método de avaliação adotado, para o máximo de 270 pontos. Este grau de comprometimento com a segurança física é considerado baixo, uma vez que sistemas com grau superior a 85% são caracterizados como seguros e/ou orientados à segurança.

Em termos de riscos, há de se destacar que cada ponto deficiente de ação em segurança pode desencadear várias conseqüências não esperadas e indesejadas nesta organização. Portanto, cabe à gerência de TI desenvolver um plano de ação para implementar um código e as diretrizes apontadas pelas normas ISO/IEC 17799 e o ciclo de segurança da informação, apresentado por Peltier (2003).

4. Considerações Finais

A aplicação dos controles estabelecidos pela norma no confronto com a real situação da empresa estudada, demonstrou o baixo nível de segurança de instalações existente, quando na visão da segurança de informações.

Contudo, a norma de segurança ISO 17799, aqui utilizada como base teórica para o desenvolvimento da pesquisa, criou guias onde as empresas que desejam homologar suas ações ou criar metodologias de segurança, possam qualificar seus esforços e o grau de comprometimento com a segurança de suas informações corporativas. Certamente a certificação pode gerar diferenciais estratégicos devido à qualidade ofertada em segurança.

Para que a implementação de uma Gestão de Segurança da Informação seja vitoriosa, será necessário que as decisões sobre pontos polêmicos sejam validados pelos executivos, que estão diretamente preocupados com o rumo dos negócios da organização. Não se pode

esquecer que a segurança é responsabilidade e dever de todos e, como tal, deve ser de conhecimento de cada funcionário da empresa as estratégias definidas (Pereira, 2001).

A conscientização das pessoas com relação aos assuntos de segurança da informação é metade da batalha. Uma vez que os empregados estão sensibilizados sobre a importância e valor da informação, a administração pode-se começar a implantar uma variedade de políticas simples e procedimentos que podem ser seguidos facilmente por todos os empregados (Hill; Pemberton, 1995).

Por se tratar de um estudo de caso, os resultados não serão generalizados para o universo das empresas de telecomunicações, mas por ser uma pesquisa exploratória, lançou-se luz sobre o assunto, possibilitando o avanço do conhecimento na área de segurança, um tópico que cada vez mais tende a evoluir em termos de pesquisas no campo de Sistemas de Informação.

Como proposta para futuros trabalhos, sugere-se o estudo na perspectiva dos outros pontos apontados pela norma, o que pode assegurar uma política de segurança da informação mais global e efetiva e o aperfeiçoamento de escalas para medição da conformidade aos domínios da gestão de segurança da informação.

5. Referências

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: Tecnologia da informação – código de prática para a gestão da segurança da informação, 2001.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 11515**: Critérios de segurança física relativos ao armazenamento de dados. URL: www.abnt.org.br,1990.

BENZ, Karl H. **Segurança em Informação**. Acessado em 24/09/2003. URL: http://www.via-rs.com.br/pessoais/kbenz/seg03.htm, 2003.

BERINATO, Scott; SCALET, Sarah. **The ABCs of Security**. Acessado em 01/11/2003. URL: http://www.cio.com/research/security/edit/security_abc.html?action=print.March, 2002.

BRADESCO. **Segurança da Informação**. Acessado em 28/10/03. URL: http://www.bradesco.com.br/seguranca_informacao/ 2002.

CARLSON, Tom. **Information Security Management**: Understanding ISO 17799 – International Network Services White Paper. Acesso em 02/05/03. URL: http://www.lucent.com/livelink/209341_Whitepaper.pdf, 2001.

CARVALHO, Fábio C. A. de; CAGNIN, Cristiano H.; ABREU, Aline F. de; CASTRO, João E. E. Abordagem de sistemas de informação enfocando a segurança em ambientes Internet/Intranet/Extranet. Anais do **XIX Encontro Nacional de Engenharia de Produção**, Rio de Janeiro-RJ, 01 a 04 de novembro de 1999.

CARUSO, Carlos. **Gestão da Segurança da Informação**. Acessado em 06/11/2003. URL: http://www.securenet.com.br/, 2002.

CASANAS, Alex Delgado Gonçalves; MACHADO, César de Souza. O Impacto da Implementação da Norma NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação – nas Empresas. Anais do **XXI Encontro Nacional de Engenharia de Produção**, Salvador-BA, 17 a 19 de outubro de 2001.

CASSA, Mônica. **A Importância e a Implementação da Segurança da Informação no Âmbito das Atividades de Negócios**. Acessado em 20/10/03. URL: http://www.ietec.com.br/ietec/techoje/techoje/tecnologiadainformacao/ , 2003.

FONTES, Edison. **Segurança da Informação**: Investimento ou Custo Operacional. http://www.securenet.com.br/artigo.php?artigo=108. Portal SecureNet, 2001.

GABBAY, Max; RAMOS, Anatália S. M. Percepção de executivos e gerentes de TI quanto às práticas de segurança da informação: um estudo orientado para as diretrizes da Norma ISO/IEC 17799. Anais do **XXIII Encontro Nacional de Engenharia de Produção**, Ouro Preto-MG, 21 a 24 de outubro de 2003.

GAO/AIMD-98-68. **Executive Guide: Information Security Management**: Learning from Leading Organizations, 1998. Acessado em 25/10/03. URL: http://www.gao.gov/, 2003.

HAICAL, Cristiane. **Controle de Acesso Físico**. Módulo e-Security. Acessado em 24/09/03. http://www.modulo.com.br/. 2000.

HEFFERAN, Rosslynne. **BS 7799** – Information Security Management. http://www.istc.org.uk. Acessado em 25/10/2003. URL: http://www.istc.org.uk, Londres, 2000.

HILL, Lisa B.; PEMBERTON, J. Michael. Information security: An overview and resource guide for information managers. **Records Management Quarterly**, Vol. 29, n.1, p.14-25, 1995.

MACHADO, Cesar de Souza; FISCHER, Norberto. A Aplicação da Metodologia *Rummler Brache Group* na implantação da Norma ISO17799. Anais do **XXII Encontro Nacional de Engenharia de Produção**. Curitiba – PR, 23 a 25 de outubro de 2002.

MACHADO, César de Souza. O emprego da metodologia PMBOK para subsidiar a implantação da norma de segurança da informação ISO 17799. Anais do **XXII Encontro Nacional de Engenharia de Produção**, Curitiba-PR, 23 a 25 de outubro de 2002. 2002a.

MACHADO, César de Souza. Um modelo para gerenciamento da segurança da informação em sistemas de teletrabalho. Anais do **XXII Encontro Nacional de Engenharia de Produção**, Curitiba-PR, 23 a 25 de outubro de 2002. 2002b.

MEDEIROS, Sayonara; RAMOS, Anatália S. M. Gestão de segurança da informação em ambiente Internet: considerações sobre a utilização do correio eletrônico segundo a Norma ISO/IEC 17799. Anais **do XXII Encontro Nacional de Engenharia de Produção**, Curitiba-PR, 23 a 25 de outubro de 2002.

MOREIRA, Nilton Stringasci. **Segurança Mínima** - Uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

MOREIRA, André. **Segurança Física** – Instituto Politécnico do Porto – Porto/Portugal. Acessado em 10/11/03. URL: http://www.dei.isep.ipp.pt/~andre/documentos/seguranca-fisica.html, 1998.

O'BRIEN, J. **Sistemas de Informação** – as decisões gerenciais na era da Internet. 9.Ed. São Paulo: Saraiva, 2001.

OLIVA, Rodrigo Polydoro; OLIVEIRA, Mírian. Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em Relação às Recomendações da NBR/ISO17799. Anais em CDROM do **XXVI Reunião Anual da Associação Nacional de Programas de Pós-graduação em Administração** (ENANPAD), Atibaia-SP, 20 a 24 de setembro de 2003.

NAKAMURA, Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Editora Berkeley, 2002.

PELTIER, Thomas R and associates. **Preparing for ISO 17799**. Security Management Practices. Acesso em 15/11/03. URL: http://www.pelttech.com/issa/Preparing%20for%20ISO%2017799.pdf. Edição Jan/Fev 2003.

RIBEIRO, Mario Sérgio. **A Norma Brasileira para a Gestão da Segurança da Informação** (ISO/IEC 17799) SCUA Information Security. Acessado em 8/11/03. URL: http://www.scua.com.br/scuanews/pontodevista/scuanews.htm, 2004.

PEREIRA, Cristiane Santos. **Implementação de Políticas e Procedimentos de Segurança em Ambiente Internet**. Acesso na URL: http://www.modulo.com.br/pdf/cpereira.pdf. 2000.

SÊMOLA, Marcos. **O caminho para implementar a segurança da informação**. http://www.modulo.com.br/ Acessado em 06/11/2003, 2001.

SOLMS, Rossouw von. Information security management: the Code of Practice for Information Security Management (BS7799). **Information Management & Computer Security**, Vol. 6, n.5, p.224-225, 1998.

TURBAN, Efraim et al. **Administração da Tecnologia da Informação**. Rio de Janeiro: Campus, 2003.

WYNES, James. **Information Security Management Standard ISO 17799 / BS 7799** – White Paper Entirety Services. Acessado em 06/11/03. URL: http://www.entiretyservices.com/Security%20White%20Paper.pdf. 2000.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. Trad. Daniel Grassi, 2ª ed., Porto Alegre: Bookman, 2001.

[i] ISO – International Organization for Standardization - é uma organização internacional formada por um Conselho e Comitês com membros de diversos países; IEC - International Engineering Consortium - é uma organização internacional sem fins lucrativos dedicada ao progresso da indústria da informação.