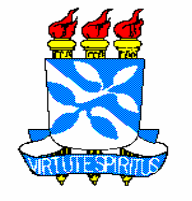


UNIVERSIDADE FEDERAL DA BAHIA

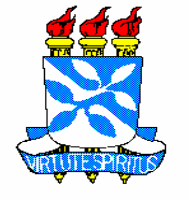
INSTITUTO DE CIÊNCIA DA INFORMAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

BIANKA CAPELATO LUCAS

A SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES DE SALVADOR.

Salvador 2005



UNIVERSIDADE FEDERAL DA BAHIA

INSTITUTO DE CIÊNCIA DA INFORMAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

BIANKA CAPELATO LUCAS

A SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES DE SALVADOR.

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Informação, Instituto de Ciência da Informação, Universidade Federal da Bahia, visando a obtenção do grau de Mestre em Ciência da Informação.

Orientadora: Profa. Dra. Kátia de Carvalho

Salvador 2005

L933 Lucas, Bianka Capelato

A Segurança da Informação em Organizações de Salvador / Bianka Capelato Lucas. – 2005.

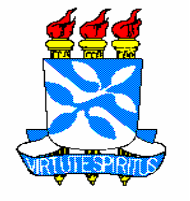
217f.; il.

Orientador: Profa. Dra. Kátia de Carvalho.

Dissertação (mestrado) – Universidade Federal da Bahia. Instituto de Ciência da Informação, 2005.

1. Informação. 2.Seguraça da Informação. 3.Organizações. I.Universidade Federal da Bahia. Instituto de Ciência da Informação. II.Carvalho, Kátia de. III.Título.

CDU:007



UNIVERSIDADE FEDERAL DA BAHIA

INSTITUTO DE CIÊNCIA DA INFORMAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

BIANKA CAPELATO LUCAS

A SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES DE SALVADOR.

BANCA EXAMINADORA

_____

Profa. Dra. Aida Varela

_____

Prof. Dr. Paulo Balanco

Orientadora: Profa. Dra. Kátia de Carvalho

Salvador 2005

Dedico primeiramente este trabalho a Deus, o principio de tudo, onde silenciosamente busco forças para superar os obstáculos.

Dedico também aos meus pais que com seus exemplos de vida sempre me mostram o caminho certo e cujos conselhos ate hoje são sábios e atuais.

Dedico também a meu marido e companheiro, que soube entender os momentos de ausência, tão necessários para o término deste trabalho e que sempre esteve ao meu lado nos momentos em que ele parecia de difícil conclusão.

AGRADECIMENTOS

À professora e orientadora Kátia de Carvalho cuja paciência e conselhos sempre vieram na hora certa e que não poupou esforços e preciosas horas de seu tempo em minha orientação.

Aos meus irmãos pelo amor sincero e conselhos sábios que também me ajudaram a superar obstáculos.

Aos meus amigos e sócios que sempre me ajudaram e sempre souberam suprir minha falta que se fizeram necessárias.

Aos meus amigos pela amizade e companheirismo, que também entenderam a minha ausência e cansaço.

Aos professores e colegas que com suas presença e companheirismo me incentivaram e proporcionaram-me vários momentos de aprendizagem.

Aquelas pessoas que mesmo em anonimato contribuíram de alguma forma para a efetivação deste trabalho.

SUMÁRIO

RESUMO 8
ABSTRACT 9
LISTA DE FIGURAS 10
LISTA DE ABREVIATURAS 11

1. INTRODUÇÃO 12

1.1 DEFINIÇÃO DO PROBLEMA..... 15
1.2 HIPÓTESES 15
1.3 OBJETIVOS 15
1.4 DELIMITAÇÃO DO TEMA 16
1.5 JUSTIFICATIVA 16
1.6 METODOLOGIA E FASES DA PESQUISA 17
1.7 FUNDAMENTAÇÃO TEÓRICA 19
1.8 ESTRUTURA DO TRABALHO 23

2. SOCIEDADE DA INFORMAÇÃO E O AMBIENTE DAS ORGANIZAÇÕES

2.1 INFORMAÇÃO, ORGANIZAÇÃO E AMBIENTE 25
2.2 INFORMAÇÃO EM UM CONTEXTO DE MUDANÇA 35
2.3 O PAPEL DAS TECNOLOGIAS DA INFORMAÇÃO NA SOCIEDADE 41
2.4 A SOCIEDADE DA INFORMAÇÃO 43

3. O USO DA INFORMAÇÃO E A NECESSIDADE DA SEGURANÇA DA INFORMAÇÃO

3.1 A NECESSIDADE DA INFORMAÇÃO SEGURA..... 50

3.2 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO 54
3.3 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO 55
3.4 MEDIDAS DE SEGURANÇA 77
3.5 BARREIRAS DA SEGURANÇA 81
3.6 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 83

4. A NORMA DE SEGURANÇA DA INFORMAÇÃO

4.1 A NORMA ISO/IEC 17799 / BS 7799: O HISTÓRICO 90
4.2 ASPECTOS IMPORTANTES DA NORMA 95
4.3 SISTEMA DE SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA 101

5 SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES DE SALVADOR E O USO DA NORMA

5.1 A SEGURANÇA DA INFORMAÇÃO NO BRASIL 117
5.2 A PESQUISA 119
5.3 METODOLOGIA 120
5.4 RESULTADOS OBTIDOS 123
5.4 O DEPOIMENTO DOS RESPONDENTES: 191
5.5 ANÁLISE DO USO DA NORMA ISO/IEC 17799/ BS 17799 195

6 CONSIDERAÇÕES FINAIS 200
7 REFERÊNCIAS 205

ANEXOS
Apêndice I – Questionário aplicado nas Organizações 212
Apêndice II – Lista da Organizações Pesquisadas 216

RESUMO

Atualmente, a informação é tratada como um ativo pelas organizações. E como qualquer outro ativo importante para os negócios, ela precisa ser devidamente protegida para garantir a continuidade dos negócios. O avanço tecnológico, que ao mesmo tempo agiliza e simplifica os trabalhos aumentando a produtividade, torna as organizações mais vulneráveis às ameaças de segurança.

Com o avanço da tecnologia e as grandes exigências do mercado, as organizações começam a preocupar-se em garantir a segurança da informação, e com a Norma ISO/IEC 17799/BS7799 que apresenta as melhores práticas para garantir a segurança, é possível garantir através de diretrizes que as informações sejam protegidas e sem riscos de acessos não autorizados. Nesta pesquisa é abordado os controles da Norma para a implantação de um Sistema de Gestão de Segurança da Informação visando abordar a implantação de um ambiente seguro para os negócios.

Este trabalho fundamenta-se sobre os conceitos de Segurança da Informação e a Norma internacional de segurança da informação ISO/IEC 17799/BS 7799. A presenta o resultado de uma pesquisa com o panorama da Segurança da Informação e o uso da Norma em organizações em Salvador.

Palavras Chaves: Segurança da Informação, Sistema de Gestão de Segurança da Informação, Tecnologia da Informação, ISO/IEC 17799/BS7799.

ABSTRACT

Nowadays, the organizations treat information like an asset. As well as any other important asset to business, it needs to be duly protected to guarantee business continuity. The technological advance, that at the same time speeds and simplifies the Works increasing the productivity, makes the organizations more vulnerable to security guard threats.

With the advance of the technology and the great requirements of the market, the organizations start to be worried in guaranteeing the security of the information, and with ISO/IEC 17799/BS7799 Norm that presents the best practices to guarantee the security, it is possible to guarantee through lines of direction that the information are protected and without risks of unauthorized accesses. In this research it is boarded the controls of the Norm for the implantation of a System of Management of Security of the Information aiming at to approach the implantation of an surrounding insurance for the businesses

This work bases on the concepts of Security of the Information and the international Norm of security of information ISO/IEC 17799/BS 7799. It presents the result of a research with the scene of the Security of the Information and the use of the Norm in organizations in Salvador sits down.

Key Words: Security of the Information, System of Management of Security of the Information, Technology of the Information, ISO/IEC 17799/BS7799.

LISTA DE FIGURAS

Figura 1 – O ambiente externo de uma organização 31
Figura 2 – Propriedades mais importantes da segurança 52
Figura 3 – Incidente de Segurança 67
Figura 4 – Impactos dos incidentes de segurança nos negócios 68
Figura 5 – Relação entre vulnerabilidade e incidente de segurança 69
Figura 6 – Ameaças 70
Figura 7 – Ciclo de segurança da informação 72
Figura 8 – Diagrama da equação do risco de segurança da informação..... 73
Figura 9 – Relação de dependência entre ativos, processos de negócios e o próprio negócio 74
Figura 10 – Preocupações básicas de segurança 77
Figura 11 – Fluxo de análise das ameaças e riscos..... 78
Figura 12 – Medidas de Detecção 80
Figura 13 – Medidas de Segurança Corretiva 81
Figura 14 – Diagrama de conceito dos componentes da política e pilares de sustentação 86
Figura 15 – Ilustração da relação entre a classificação e tratamento definido na política para o ciclo de vida da informação 87
Figura 16 – Modelo de SGSI – Sistema de Gestão de Segurança da Informação 102
Figura 17 – Modelo de Processo - PDCA (Plan-Do-Check-Act) 105

LISTA DE ABREVIATURAS

ISO – (*International Organization for Standardization*): organização internacional que desenvolve, sugere e define padrões.

IEC – (*International Electrotechnical Commission*): organização que, conjuntamente com a ISO, desenvolve, sugere e define padrões para protocolos de rede.

BS 7799 – Norma britânica de segurança da informação constituída de duas partes, sendo a primeira publicada em 1995, também referenciada como BSI (1995), e a segunda, em 1998. A primeira parte deu origem à norma ISO/IEC 17799:2000BS.

TI – (Tecnologia da Informação): conjunto de tecnologias utilizadas para desenvolver o processo de geração, processamento, disseminação e documentação das informações.

NTIC – Novas Tecnologias de Informação e Comunicação.

TIC – Tecnologia da Informação e Comunicação.

NBR – Norma Brasileira

CPD – Centro de Processamento de Dados: local onde estão localizados os equipamentos de maior porte que são responsáveis pelo processamento centralizado.

ABNT – Associação Brasileira de Normas Técnicas

SGSI – Sistema de Gestão de Segurança da Informação.

ACC – Ambiente Computacional Complexo

ISMS – (*Information Security Management System*): é o resultado de uma ação de gerenciamento explícito, expresso como uma coleção de políticas, princípios, objetivos, medidas, processos, formas, modelos, lista de verificações (*checklist)*, que juntos definem como os riscos de segurança de um ACC podem ser reduzidos.

PDCA – Modelo de processo (*Plan-Do-Check-Act*).

1 INTRODUÇÃO

> Na sociedade em que vivemos, onde a informação é grande fonte de riqueza (e, portanto, um dos principais ativos a serem protegidos), subestimar a importância da segurança pode custar a sobrevivência da organização no mercado. (NIMER (1998), p.24).

A Informação contempla qualquer conteúdo que possa ser armazenado ou transferido, servindo a determinado propósito e sendo útil ao ser humano permitindo a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais produtos da era atual, pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, pode ser armazenada para os mais variados fins, possibilitando a leitura, a modificação, e até a exclusão.

Desde a inserção do computador, na década de 40, como dispositivo auxiliar nas mais variadas atividades, até os dias atuais, temos observado uma evolução nos modelos computacionais e nas tecnologias usadas para manipular, armazenar e apresentar informações.

Considerando o cenário, há uma necessidade de oferecer suporte à colaboração de múltiplas organizações e comunidades, que muitas vezes, têm interesses sobrepostos. Em tal situação, o controle de acesso às informações é um requisito fundamental nas organizações atuais.

A grande maioria das informações, disponíveis nas organizações, encontram-se armazenadas e são trocadas e manipuladas entre os mais variados setores e sistemas de informações. Dessa forma, inúmeras vezes decisões e ações tomadas decorrem das informações manipuladas por esses sistemas. Dentro deste contexto, toda e qualquer informação deve ser correta, precisa e estar disponível a fim de ser armazenada, recuperada, manipulada ou processada, além de poder ser trocada de forma segura e confiável.

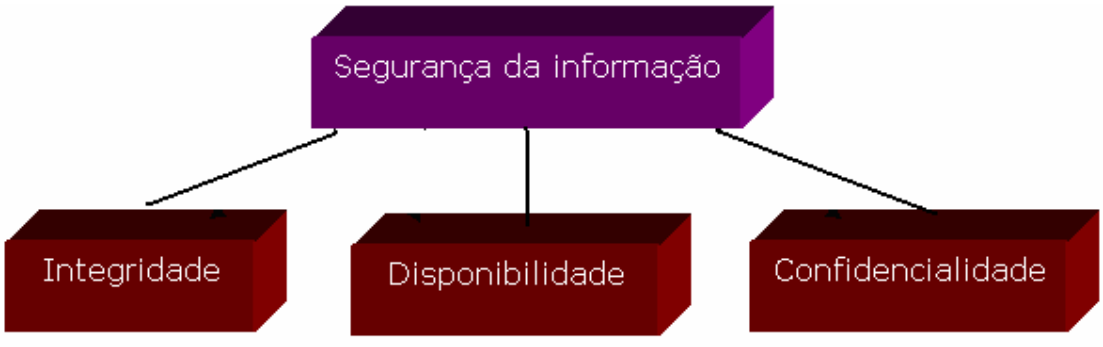
Nos dias atuais, a informação constitui uma mercadoria, ou até mesmo uma *commodity*, de suma importância para as organizações dos diversos segmentos. Por esta razão, segurança da informação tem sido uma questão de elevada prioridade nas organizações.

Nesse sentido, Segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade, e confidencialidade que constituem os pilares da Segurança da Informação. O uso desses pilares é feito em conformidade com as necessidades específicas de cada organização. Assim o uso desses pilares pode ser determinado pela suscetibilidade das informações ou sistemas de informações, pelo nível de ameaças ou por quaisquer outras decisões de gestão de riscos.

Esses pilares são essenciais no mundo atual, onde se tem ambientes de natureza pública e privada, conectados a nível global. Dessa forma, torna-se necessário dispor de uma estratégia, a fim de compor uma arquitetura de segurança que venha unificar os propósitos dos pilares. Neste contexto as organizações tendem a incluir em suas metas a criação de um Sistema de Gestão de Segurança da Informação.

Atualmente, numa era onde conhecimento e informação são fatores de suma importância para qualquer organização ou nação, segurança da informação é um pré-requisito para todo e qualquer sistema de informação e, há uma relação de dependência entre a segurança da informação e seus pilares, como ilustrado na Figura abaixo.

Nesse contexto, a confidencialidade oferece suporte a prevenção de revelação não autorizada de informações a pessoas sem privilégio de acesso. A integridade previne a modificação não autorizada de informações. E a disponibilidade provê suporte a um acesso confiável e prontamente disponível a informações. Isto implica em informações prontamente disponíveis e confiáveis.



Pilares da Segurança da Informação.

No mundo dos negócios, ágil e competitivo, as organizações não podem mais ficar indisponíveis para o acesso de seus clientes, mesmo que tenham problemas com seus processos de negócios e/ou com seus ambientes e tecnologias. Confidencialidade, Integridade e Disponibilidade são requisitos fundamentais previstos inclusive em normas internacionais como BS 7799 e sua congênere no Brasil, a NBR ISO/IEC 17799.

Assim, garantia contra vazamentos de dados, associados a controles rígidos garantindo que a informação somente possa ser alterada por quem realmente tenha autoridade para fazê-lo, e ainda velocidade de processamento e de decisões, altíssima disponibilidade, flexibilidade e foco em produtos/serviços de acordo com o mercado são fundamentais para a sobrevivência e sucesso de uma organização. Porém, se não houver planejamento adequado que envolva ações coordenadas de Segurança e um Sistema de Gestão de Segurança da Informação, alguns requisitos estarão ameaçados e consequentemente a organização estará ameaçada.

Como Analista de Sistemas as Tecnologias da Informação sempre nos orientaram na vivência profissional. Tendo uma formação técnica, faltava a experiência e o conhecimento para o desenvolvimento de um trabalho desta natureza. Com isso o Mestrado em Ciência da Informação contribui para o aumento do conhecimento e consequente amadurecimento diante deste tema.

O tema está centrado na Sociedade da Informação que agrega paradigmas que apresentam a realidade da aceleração do uso da informação. Esta questão envolve a necessidade de Segurança da Informação que é acelerada pelas tecnologias da informação. A Segurança da Informação é um tema novo e pouco explorado, fazendo-se necessário o seu estudo.

O objeto de estudo desta pesquisa será apresentar os principais conceitos da Segurança da Informação, a aplicabilidade destes conceitos que norteiam a Gestão da Segurança da Informação e a importância da aplicação das práticas nas organizações através das principais medidas a serem observadas para a elaboração de um projeto/processo de planejamento e implementação da Segurança da Informação; Pretende-se verificar como as organizações selecionadas em Salvador e região metropolitana estão incorporando a Segurança da Informação em seus processos, e se as ações que estas estão tomando para implantar a Segurança da Informação estão baseadas na Norma BS 7799:2002 2 / ISO IEC 17799.

1 DEFINIÇÃO DO PROBLEMA

Como as organizações estão incorporando a necessidade de implantação de mecanismos de Segurança da Informação, que visa a competitividade, e o uso da informação para a tomada de decisão. Convém salientar o uso das tecnologias que aceleram os processos e que necessitam de assegurar o uso da informação.

1.2 HIPÓTESES

- As organizações pesquisadas em Salvador consideram importante a Segurança da Informação nos seus ambientes.
- As organizações pesquisadas em Salvador estão trabalhando com rotinas de Segurança baseadas na Norma.

1.3. OBJETIVOS

O objetivo geral da dissertação é analisar se as organizações pesquisadas em Salvador acreditam na importância da informação e por isso usam as Normas de Segurança da Informação.

São objetivos específicos:

a) Identificar como as organizações de Salvador estão encarando o uso das Normas da Segurança da Informação.
b) Identificar se as organizações pesquisadas estão aplicando os conceitos de Segurança da Informação e se os padrões da Norma estão sendo seguidos de forma adequada.
c) Analisar a contribuição da Norma ISO IEC 17799/BS 7799 de Segurança da Informação para as organizações .

1.4 DELIMITAÇÃO DO TEMA

O universo da pesquisa é a cidade de Salvador-Ba e região metropolitana, onde se situam as organizações que serão pesquisadas.

1.5 JUSTIFICATIVA

Desde o início da civilização humana percebe-se a preocupação com o uso da informação onde somente as camadas superiores da sociedade tinham acesso à informação. Desde a antiga civilização egípcia, somente as classes superiores tinham acesso aos manuscritos da época, sendo que a maioria das pessoas não dominavam a escrita e a leitura

Os avanços das tecnologias ao longo do tempo vai exigindo outras medidas e condutas que asseguram a organização social. Na sociedade moderna, o uso das Tecnologias da Informação traz a tona as questões de Segurança da Informação. Os avanços tecnológicos têm proporcionado às organizações maior eficiência e rapidez na troca de informações e tomadas de decisões, os computadores cada vez mais rápidos são lançados em curto espaço de tempo, o que permite que agentes ameaçadores aos ambientes computacionais, em constante evolução, se ampliem em quantidade e em forma.

Entre estes agentes, novos vírus surgem em curto espaço de tempo, trazendo riscos às informações existentes nos arquivos das organizações. Ataques à rede interna da empresa podem ocasionar a quebra de sigilo de informações confidenciais, e/ou divulgação das mesmas. Pode-se perceber que as novas tecnologias, em virtude da aceleração de suas mudanças, têm afetado muitas organizações. Problemas de origem interna e externa têm marcado presença no dia-a-dia, principalmente, nas organizações que não possuem Políticas de Segurança implementadas.

Como a informação vem sendo considerada um dos principais ativos das organizações, Segurança da Informação tem-se tornado uma real necessidade no dia-a-dia dessas organizações, seja para proteger seus segredos de negócio, suas estratégias comerciais ou até mesmo na proteção do capital intelectual. Diante desse fato, pode-se afirmar que a informação é um bem e que o seu valor é perfeitamente possível de ser medido. Portanto, a informação

deve ser mantida em segurança, assim como os ambientes e os equipamentos utilizados para o seu processamento.

A Busca da Ciência da informação foi necessária para fazer-nos compreender a importância da informação nessa Sociedade da Informação e a necessidade de mecanismos de Segurança da Informação. Isto porque a Ciência da Informação investiga as propriedades e o comportamento da informação, seu fluxo e os meios de processá-la para otimizar a sua acessibilidade.

Justifica-se este trabalho para se as organizações estão atentas à necessidade das práticas de uso de normas de Segurança da Informação e porque usá-las? A resposta deste questionamento muito interessa visto que com a evolução das novas tecnologias a Segurança da Informação tem se tornado necessária em todas as organizações e por isso o aprofundamento dos conhecimentos chegando a certificação como Auditora na Norma BS7799 Guia de melhores práticas de Segurança da Informação. No entanto a Norma é relativamente nova e é necessário de saber como está sendo disseminada e aplicada em Salvador.

Pretende-se verificar como as organizações pesquisadas em Salvador estão encarando a Segurança da Informação, e como se estabelece as relações com a utilização das recomendações sugeridas pela Norma de Gestão de Segurança da Informação uso da Norma BS7799/ISO/IEC 17799 (Internacional Standardization Organization/ Internacional Electrical Technical Commission (ISO/IEC) 17799).

1.6. METODOLOGIA E FASES DA PESQUISA

O presente estudo tem um caráter exploratório e descritivo com um posicionamento interpretativo. Compreende-se uma pesquisa qualitativa, uma vez que a realidade e o conhecimento a ser investigado, objeto da pesquisa - Segurança da Informação em organizações de Salvador- é um tema recente, conseqüentemente pouco explorado.

Dada a especificidade do objeto utilizou-se a pesquisa bibliográfica e documental (Normas) em consonância com uma pesquisa de campo. Justifica-se essa opção, por priorizar a identificação de uma realidade complexa e recente, o estudo sobre a Segurança da Informação em organizações de Salvador.

O universo da pesquisa visa as organizações de Salvador. A amostra desse universo são as organizações com ambiente computacional complexo envolvendo diversas soluções com servidores de Banco de Dados, de acesso a Internet, de bloqueio de acesso como Firewall. Com um mínimo de 30 usuários de computador visto que a maioria das vulnerabilidades da Segurança da Informação envolvem as pessoas e o acesso a Internet.

A escolha das organizações se fez por que elas são sistemas organizacionais onde há uma demanda variada de vulnerabilidades, exigindo uma pluralidade de serviços. Pretende-se identificar como essas organizações de Salvador estão encarando a Segurança da Informação, com vistas a otimizar o sistema de Gestão da Segurança da Informação e conseqüentemente, se estão em consonância com as diretrizes da Norma ISO/IEC 17799 e BS 7799.

Para a coleta de dados aplicou-se a técnica de questionário semi-estruturado. Os sujeitos contemplados a contribuir com a presente investigação são: Gestores da área de Informática e da área de Segurança da Informação (Vide modelo de questionário no Anexo I). Esta coleta de dados foi escolhida em virtude da dificuldade encontrada para entrevistar pessoas face a face, com tempo limitado, em função da delicadeza e do sigilo solicitado pelo tema.

Quanto a análise dos dados, utilizou-se a ordenação e a classificação das respostas das entrevistas. A análise relaciona pontos de acordo com os objetivos e o referencial teórico, e, empregou-se as técnicas de: 1) Análise de documento - a Norma BS 7799 como um documento de referencia, fundamentando a análise qualitativa, objetivando a exploração dos dados coletados, em consonância com a análise temática de conteúdo, composta de três fases distintas: pré-análise, exploração dos dados, tratamento dos resultados, inferência e interpretação.

A metodologia utilizada visa conhecer o uso de Normas de Segurança da Informação nas organizações localizadas em Salvador mediante questionários, pesquisa documental e bibliográfica. Deste modo são etapas da pesquisa:

1 - Levantamento bibliográfico visando contribuir com a fundamentação teórica sobre o tema.

2. -Leitura de obras de base para a fundamentação da pesquisa.

3 - Seleção das organizações que possuem ambientes computacionais complexos e com variedades de serviços como Internet, Banco de Dados, Firewall.

4 – Aplicação de formulários com questionamento previamente estruturado nas organizações.

5 - Coleta dos dados nas organizações e Análise das informações.

6 - Consolidação das informações visando a valiação dos resultados.

7 - Elaboração do relatório final da pesquisa.

1.7. FUNDAMENTAÇÃO TEÓRICA

O homem ao buscar padrões de melhoria de qualidade de vida vai inventando técnicas e tecnologias cada vez mais refinadas, e em muitos casos introduzem novos paradigmas que potencializam a escrita e a leitura. Os avanços tecnológicos na área da agronomia amplia a economia e vai aos poucos criando novos modelos de vida societária. Mas é com a sociedade da informação que o uso da informação atinge um nível de necessidade nunca visto, e que o atual ambiente de negócios é caracterizado pelos mercados abertos em que a competição se torna cada vez mais acirrada, quando novas técnicas e paradigmas são rapidamente disseminados e as empresas precisam promover mudanças rápidas e eficazes.

A modernidade introduz nos quatro cantos do mundo novos padrões qualitativos que exigem criatividade, competência e flexibilidade. Controlar e reduzir custos, formar corretamente os

preços de venda dos serviços e arquitetar a estrutura operacional, eis a receita básica para o sucesso de uma organização.

Com o processo de globalização de mercados e a velocidade dos avanços tecnológicos, a busca por informação tornou-se alvo comum de toda sociedade. Naturalmente, emerge o conceito de sociedade da informação, onde o acesso à informação passa a ser um diferencial da nova era.

A Sociedade da Informação traz novas responsabilidades para todos os atores sociais, denota a responsabilidade desses atores para a provisão de um fluxo constante de informações que possibilite a geração de conhecimentos para a tomada de decisão nas muitas instâncias da sociedade.

É nesse ambiente de mudança da Sociedade da Informação, que se apresenta um desafio para adequar a sociedade às profundas mudanças resultantes. As manifestações da Sociedade da Informação rodeiam o nosso quotidiano, afetam o comportamento das empresas e organizações, e influenciam o pensamento estratégico das nações.

Vista sob esta ótica funcional, a informação pode ser entendida como recurso redutor de incertezas (WETHERBE, 1987; CHIAVENATO, 1999), e no que concerne ao desenvolvimento, ela pode viabilizar a elaboração, implementação e avaliação de políticas públicas com maior grau de eficácia e eficiência, a partir da análise da complexidade social, de suas demandas e contradições. Assim sendo, informação gera conhecimento, e este, por sua vez, gera mais informação, dentro de uma estrutura circular virtuosa. Por conseguinte, tal estrutura, geradora desse fluxo perene de informação tem levado estudiosos a atribuir-lhe o status de recurso fundamental para o desenvolvimento da sociedade, tendo adquirido essa posição em função das transformações tecnológicas que a tornam cada vez mais difusas.

Assim, para os diferentes atores da sociedade, a informação assume finalidades específicas. No âmbito do mercado, o acesso à informação visa a geração de vantagem competitiva sobre a concorrência, descoberta de novos nichos de consumidores; pesquisa e desenvolvimento de novos produtos e serviços, bem como o monitoramento do ambiente externo, a fim de identificar ameaças e/ou novas oportunidades de negócios para as empresas que o compõem. Por isso, cada vez mais, grandes corporações vêm realizando investimentos vultuosos em

sistemas de informação, objetivando interagir de forma mais rápida e dinâmica em áreas de produção, distribuição e comercialização de produtos estrategicamente espalhadas pelo planeta (FERREIRA, 2000).

Os avanços ocorridos das chamadas tecnologias da informação e da comunicação, alavancaram rapidamente esforços no sentido de organizar e analisar dados, de forma que sejam disponibilizados como informação, com valor agregado, para subsidiar processos de tomada de decisão. Ter a informação certa e adequada a determinada necessidade, no tempo correto e a um custo compatível é fundamental em uma sociedade em que se antecipar às expectativas do futuro passou a ser um diferencial para o sucesso e o retorno de uma demanda informacional tem que ser na velocidade e nos meios compatíveis com os novos tempos, sendo essencial a incorporação dos avanços das tecnologias de informação e comunicação nas organizações.

A informação, produto direto do capital do conhecimento humano é um bem de grande valia no novo panorama mundial. Por esta razão, o seu armazenamento e organização para uso eficiente e seguro deve ser objeto de preocupação de todos os segmentos da sociedade. Com isso, a segurança da informação tem deixado de ser tratada como um assunto técnico da área de informática e vem sendo considerada uma real necessidade nas organizações e instituições, passando a ser um requisito estratégico, que interfere na capacidade de realização de negócios e na agregação de valor de seus produtos no mercado.
A Informação segundo Moreira (2001), é um importante patrimônio para muitas organizações, daí a necessidade da implantação de Segurança da Informação, uma vez que a proteção destas informações não é uma atividade muito simples e diante desta realidade, tem sido um assunto que vem ganhando destaque e atenção, disseminada pelos meios de comunicação, palestras, congressos e seminários.

O aumento da confiança e da dependência nos sistemas computacionais é uma tendência natural nas organizações, que visam aumento de competitividade e de qualidade dos serviços prestados. Moreira (2001), diante destes fatos, comenta que o nível de exposição aos riscos destas empresas tende a aumentar e é nesse momento que surge a necessidade de um programa de segurança da informação, que tem como objetivo garantir a continuidade do negócio e minimizar os danos causados á organização através da prevenção e redução dos impactos gerados por incidentes de segurança.

O tema Segurança da Informação é amplo e requer uma definição. Sêmola (2003, p.43) define "como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas e sua indisponibilidade". De forma mais ampla, pode ser considerada como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Desta forma, o que se necessita é a definição de regras que incidem sobre cada etapa do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

Do ponto de vista de Caruso(1999), o ambiente de informações define medidas que garantem a segurança efetiva a um custo aceitável. Essas medidas devem estar claramente descritas na política global de segurança da organização, delineando as responsabilidades de cada grau da hierarquia da delegação de autoridade, e, devem estar claramente sustentadas pela alta direção. O caráter altamente dinâmico das atividades relacionadas com o processamento da informação adquire ao longo do tempo uma política de segurança de informações ampla e simples na execução.

O desafio corporativo da segurança envolve várias variáveis que tendem a crescer à medida que vão surgindo novas tecnologias, novos modelos de negócios e inovações no relacionamento comercial. Com esta motivação Sêmola (2003) se refere a Norma BS7799/ISO IEC 17799, que reúne as melhores práticas para o gerenciamento de segurança da informação. O objetivo principal da norma é orientar e, a partir disso, criar uma sinergia entre as empresas que estão diante do desafio do gerenciamento da segurança da informação.

A organização deve estar consciente que a Segurança da Informação deve representar preocupação de todos que integram a organização e sua cadeia de valor. Acionistas, executivos, funcionários, clientes, fornecedores e parceiros devem estar atentos em preservar seus ativos, preocupados com a proteção adequada de informações e sistemas da organização. Isso acontece porque a Segurança da Informação está se tornando um importante diferencial competitivo.

Por outro lado, a ausência de processos e controles de segurança pode acarretar dificuldades, que levam a perda de faturamento, custos e despesas que influenciam a perda de valor na

organização. No entanto, existe uma dúvida: como medir e verificar se as recomendações e controles usados são efetivos e completos.

Com base nessa necessidade, o BSI (British Standard Institute) criou a Norma BS 7799, que até então é considerada o mais completo padrão para gerenciamento da Segurança da Informação dando condições para implementar um sistema de gestão de segurança baseado em controles e práticas definidos por normas e práticas internacionais.

1.8. ESTRUTURA DO TRABALHO

O trabalho é apresentado em capítulos:
Inicialmente uma Introdução ao tema, os procedimentos metodológicos e a fundamentação teórica são apresentadas no capítulo.

O segundo capítulo: procura compreender o processo de adoção da necessidade da Segurança da Informação nas organizações, tornando-se necessário compreender a relação entre as organizações, seu ambiente e a informação na nova sociedade. Apresentam-se visões das organizações e seus ambientes, seguindo da nova realidade em que se encontram as organizações com base no seu ambiente e no papel da informação na Sociedade da informação.

O terceiro capítulo, contextualiza a informação e o uso das tecnologias da informação na sociedade, o uso da informação e a necessidade de Segurança da Informação, tece comentários sobre a necessidade da informação segura, seus objetivos e conceitos utilizados juntamente com os aspectos importantes.

O quarto capítulo, trata da Segurança da informação, seu aporte teórico para conceitualizar os aspectos e a necessidade da Segurança nas organizações e apresenta-se a Norma BS 7799/ISO IEC 17799, que norteia a Segurança da Informação nas organizações, bem como seus controles e a sua aplicabilidade, a partir de um referencial.

O quinto capítulo versa sobre a Segurança da Informação em organizações de Salvador e a aderência dos controles da Norma BS 7799/ISO IEC 17799 com os processos das organizações pesquisadas.

O sexto e último capítulo, reune as considerações finais baseadas nas hipóteses e objetivos que nortearam esta dissertação.

O sétimo capítulo relaciona as Referêncas das obras básicas que embasaram o trabalho.

Como apoio ao trabalho o Apêndice I traz a complementação necessária ao texto ao relacionar o questionário utilizado na pesquisa com as organizações e o anexo é a minuta da Norma BS 7799.

2. SOCIEDADE DA INFORMAÇÃO E O AMBIENTE DAS ORGANIZAÇÕES

2.1 INFORMAÇÃO, ORGANIZAÇÃO E AMBIENTE

Com a crescente onda de mundialização da economia, passamos a ter, por mais distintas que sejam as estruturas sociais, econômicas e culturais, uma aproximação muito grande com os acontecimentos de várias partes do mundo. As organizações, públicas e privadas, sentem cada vez mais de perto as conseqüências dessa movimentação.

A organização pode ser definida como um sistema de atividades conscientemente coordenadas de duas ou mais pessoas onde, devido a limitações pessoais, os indivíduos são levados a cooperarem uns com os outros para alcançar certos objetivos que a ação individual isolada não pode alcançar. Portanto, as organizações se constituem nessa interação que faz com que elas sejam dinâmicas e complexas, ou seja, um organismo vivo. Assim, pode-se compreender porque a definição etimológica do termo é *organom* = órgão.

Segundo Srour(1998), podemos definir organização como "agentes coletivos, à semelhança das classes sociais, das categorias sociais e dos públicos" que "são planejadas de forma deliberada para realizar um determinado objetivo" (SROUR, 1998:108). O Novo Dicionário Aurélio, em uma de suas definições, enuncia que seja "associação ou instituição com objetivos definidos" (FERREIRA, 1975:1005).

Pode-se citar, primordialmente, as organizações públicas, as privadas, as sem fins lucrativos, as filantrópicas e as ONG's - organizações não governamentais. Todas têm em seu interior características muito específicas que as diferenciam, como também, aquelas que pertencem a uma mesma categoria.

Entre as muitas concepções sobre organização, a visão mecanicista encara a organização como uma estrutura rígida e tem sido deixada de lado por alguns estudiosos - a exemplo de Fritjof Capra - e por algumas organizações, que propõem a chamada visão sistêmica, pela qual se encaram as organizações como organismos vivos, que desenvolvem-se e adaptam-se aos impulsos da realidade.

Ao ingressar em um sistema organizacional produtivo, o indivíduo busca, de modo geral, satisfazer tanto suas necessidades de pertencer a um grupo social quanto de se auto- realizar. No entanto, sabe-se que estes objetivos nem sempre são alcançados, visto que existem inúmeros fatores que permeiam as relações de trabalho e influenciam a satisfação dessas necessidades. Pode-se dizer, ainda, que um dos fatores mais complexos e potentes nesse sentido é a própria subjetividade humana, ou seja, as motivações, interesses, valores, história de vida, modo de relacionar-se, enfim a singularidade de cada sujeito que influencia o grupo como um todo. Confirmando essa visão Moscovici (1997) afirma que:

> A maneira de lidar com as diferenças individuais cria um certo clima entre as pessoas e tem forte influência sobre toda a vida em grupo, principalmente nos processos de comunicação, relacionamento interpessoal no comportamento organizacional e na produtividade.

Sendo assim, o relacionamento interpessoal e o clima dos grupos podem trazer satisfações ou insatisfações pessoais ou grupais, repercutindo na organização. Nesse sentido é que o conjunto de preceitos, políticas administrativas, valores e crenças é que dão forma ao modo especial e único de como as pessoas agem e interagem dentro de uma organização e conseqüentemente colaboram para o estabelecimento de uma cultura e clima organizacional adequado.

Para que se possa compreender e intervir melhor em uma organização se faz necessário investigar e estudar sua cultura e clima organizacional considerando o contexto histórico e cultural em que ela está inserida. É importante pontuar que existe uma interferência real da cultura nacional, regional e até mesmo inter-regional na cultura da organização propriamente dita, que se dá nos relacionamentos, padrões de conduta, forma de administração, enfim, preceitos de cada organização.

Torna-se possível entender como o poder não só o que se manifesta no interior da organização mas também a troca de influências e ainda, como a inter-relação delas atua no conjunto e nos resultados. Pode-se considerar, que a interdependência, seja diretamente ampliada à medida que os processos de globalização - ou influências globais - da economia seja ampliado. A cultura, por sua vez, deveria estar relacionada ao significado da organização, ou, numa leitura mais adequada, a imagem de uma organização deve refletir seus traços culturais, como sincero retrato da sua identidade.

Assim sendo, uma organização é um sistema de recursos que procura realizar objetivos ou conjuntos de objetivos. Além de objetivos ou propósito e recursos, conforme propõe Maximiniano(1997), as organizações configuram outros dois elementos importantes a divisão do trabalho e a coordenação.

Numa organização, cada pessoa e cada grupo de pessoas tem um papel específico que converge para a realização do propósito. Assim como as organizações possuem determinadas competências, as pessoas e os grupos que nelas trabalham também são especializadas em determinadas tarefas e é através da divisão de trabalho que é possível superar as limitaçoes individuais.

As diversas tarefas especializadas precisam estar combinadas e interadas porque elas são interdenpendentes, para realizar uma, é necessário realizar outra. Interdependência e convergência são palavras-chave no processo de coordenação, a atividade que procura fazer as peças especializadas se encaixarem umas às outras, de modo que o conjunto consiga cumprir sua finalidade.

As organizações são deliberadamente orientadas para a realização de objetivos que podem ser classificados em duas categorias principais: produtos e serviços. As organizações na medida em que tenham o que oferecer ao mercado esperam estabelecer uma relação de troca com este. Em função do tipo de relação de troca de produtos e serviços por um preço, por impostos ou uma contribuição, as organizações conseguem estabelecer algum tipo de vantagem no jogo da competitividade.

As organizações vistas pela visão burocrática se reporta a palavra burocracia que identifica as organizações que se baseiam em regulamentos. Há uma razão extremamente importante para entender o que é burocracia porque a sociedade organizacional é, também, uma sociedade burocratizada sendo a burocracia um estágio na evolução das organizações e tendem a apresentar disfunções que interferem em seu desempenho, por isto é de grande importância estudar as organizações sob a perspectiva de sua natureza burocrática.

As organizações formais, ou burocráticas, apresentam três características principais, que as distiguem dos grupos informais ou primários: formalidade, impessoalidade e profissionalismo. Essas três características formam o chamado tipo ideal de burocracia, criado

por Max Weber. O tipo ideal é um modelo abstrato que procura retratar os elementos que constituem qualquer organização formal do mundo real.

- Formalidade - As burocracias são essencialmente sistemas de normas. A figura da autoridade é definida pela lei, que tem como objetivo a racionalidade da coerência entre meios e fins.
- Impessoalidade - Nas burocracias, os seguidores obedecem à lei. As figuras da autoridade são obedecidas porque representam a lei.
- Profissionalismo - As burocracias são formadas or funcionários. Como fruto de sua participação, os funcionários obtêm os meios para sua subsistência. As burocracias operam como sistemas de subsistência para os funcionários.

O tipo ideal por Marx Weber procura evidenciar as características das organizações burocráticas em sua forma pura. Todas as organizações reais contêm os três elementos do tipo ideal, em maior ou menor grau. Paradoxalmente, são, também, diferentes do tipo ideal, porque apresentam disfunções, que as fazem ser ineficientes e ineficazes. As disfunções existem porque as organizações são sistemas humanos e não mecânicos, estritamente regidos pelas leis.

Após estudar as organizações como sistemas regidos por regulamentos que aplicam tecnologia para transformar recursos em produtos e serviços, merece destaque as pessoas que fazem parte delas. Deixando de lado as máquinas e os equipamentos, os laboratórios, as normas e os regulamentos, faz-se necessário acompanhar o comportamento humano.

Usando um enfoque comportamental, Bateman & Snell (1999) consideram ser possível observar que dentro de qualquer organização formal existe uma organização informal, que tem grande influência sobre o desempenho e cujos elementos mais importantes são:

- Cultura organizacional: que compreende as normas de condutas, os valores, os rituais e hábitos;
- Clima organizacional: que compreende os sentimentos manifestos por pessoas e grupos em relação a empresa.
- Grupo informal: que compreende os grupos formados por motivos de interesses ou amizade.

O ambiente das organizações é abordado de diferentes maneiras e em níveis diferenciados considerando a profundidade e a abrangência pelas várias correntes de pensamento que compõem o corpo teórico da Teoria das Organizações.

A sistematização do conhecimento no campo da administração define a organização como um sistema fechado e não sendo atribuida uma importância relevante ao ambiente nas análises organizacionais. No entanto, segundo Motta, já admitindo a influência do ambiente, "o trabalhador é uma pessoa cujas atitudes e eficiência são condicionadas pelas demandas sociais, tanto dentro como fora da fábrica" (MOTTA, 1984, p.26),.

A abordagem behaviorista amplia o campo da administração da empresa para a organização, com a incorporação da sociologia da burocracia. Neste sentido, o ambiente assume um papel fundamental considerando a sua influência, tanto no nível interno como externo e que limita as alternativas disponíveis para a ação.

Outra corrente da Escola Estruturalista, considera uma preocupação sistemática da relação entre organizações e ambiente, uma vez que seus teóricos "vêem a organização como um sistema deliberadamente construído e em constante relação de intercâmbio com seu ambiente" (MOTTA, 1984, p.66). Para esta corrente, a organização poderia ser definida por suas relações de importação e exportação com o ambiente, tanto do subsistema social (valores e aspirações), como do subsistema técnico (insumos, equipamentos).

Na análise das relações entre as unidades organizacionais e o ambiente, o autor Motta, F.(2001), identifica de acordo com o nível de certeza/incerteza, estabilidade/instabilidade, uma maior ou menor necessidade de diferenciação dessas unidades para se adequarem a essa relação. O ambiente é diferenciado e cada subsistema da organização se relaciona com setores especializados do entorno, que, de acordo com o grau de diferenciação, vão exigir maior diversidade do subsistema organizacional e mecanismos de integração diferentes.

Uma vez que as relações da organização e ambiente se dão através de interlocutores privilegiados, os teóricos do neo-institucionalismo analisam a construção de um *meio ambiente negociado* através da interação e inter-estruturação de mecanismos que regulam a percepção dos atores sobre seu contexto de ação e que acabam por influenciar a reestruturação desse setor (MOTTA, F., 2001).

O ambiente de qualquer organização pode ser dividido em duas grandes dimensões. Em primeiro lugar, encontra-se o ambiente imediato, em que estão os segmentos que interessam diretamente à organização ou que influenciam diretamente seu desempenho. O ambiente imediato faz parte do macro-ambiente, ao qual pertencem os segmentos que influenciam todas as organizações semelhantes e a comunidade das organizações em geral. Nos dois casos, ambiente imediato e macro-ambiente, os segmentos podem-se organizar de modo complexo, formando sistemas externos, que interagem com os sistemas internos.

Inseridas em um ambiente externo, as organizações podem ser vistas como um sistema aberto já que mantém intercâmbio com o seu ambiente. Isso faz com que as organizações sofram influências internas de tudo que ocorre externamente, nesse ambiente. Segundo Tarapanoff o ambiente é complexo, e envolve toda a organização, ele pode ser analisado em dois segmentos: o ambiente geral e o ambiente tarefa. O ambiente geral é genérico e comum a todas as organizações, afetando-as, assim, direta ou indiretamente. Esse ambiente é constituido de condições semelhantes a todas as organizações, formando um campo dinâmico de forças que interagem entre si e apresentam um efeito sistêmico. As principais condições são: tecnológicas, legais, políticas, econômicas, demográficas, ecológicas, sociais e culturais. (TARAPANOFF 2001)

O segmento do ambiente geral do qual uma determinada organização extrai as suas entradas e deposita as suas saídas é o ambiente de operações de cada organização. Este ambiente é constituído por fornecedores, clientes ou usuários, concorrentes e entidades reguladoras (órgãos governamentais, sindicatos e associações de classe). (TARAPANOFF 2001)

O ambiente tarefa é o mais próximo e imediato de cada organização. Uma organização estabelece o seu domínio no ambiente tarefa e isto porque o domínio depende das relações de poder ou de dependência de uma organização quanto as suas entradas ou saídas. Quando a sua decisão afeta as decisões de fornecedores de entradas ou consumidores de saída, a organização tem poder sobre seu ambiente tarefa, e quando suas decisões dependem dos fornecedores e consumidores, a organização tem dependência em relação ao ambiente. As organizações procuram aumentar o seu poder e diminuir a sua dependência quanto ao seu ambiente e estabelecer o seu domínio. Vide figura 1

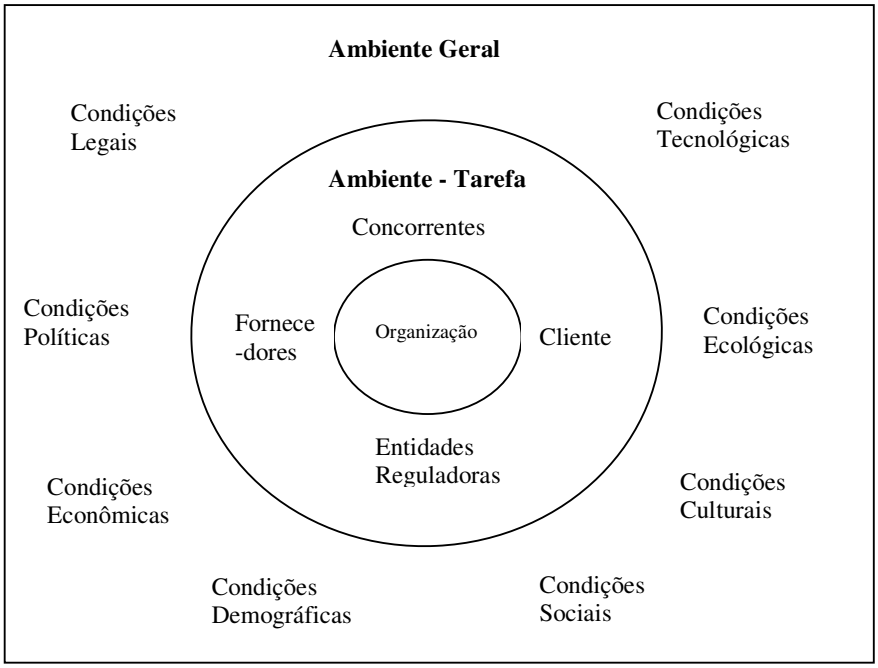


FIGURA 1 – O ambiente externo de uma organização.

Fonte: TARAPANOFF (2001)

A interconexão causal entre os elementos do ambiente pode estar associada a idéia de turbulênca ambiental e a instabilidade ou grau de complexidade, já que não se pode definir com clareza até que ponto os elementos possuem capacidade de influência mútua. Uma mudança econômica específica de um setor, por exemplo, pode ter ramificações econômicas, políticas ou mesmo tecnológicas, do mesmo modo que pode transferir os seus efeitos por todo sistema social, bem como causar mudanças em outros setores.

Portanto, o ambiente externo compreende os diversos fatores que os administradores devem estar preparados para enfrentar, e assim, poder auxiliar suas organizações a competir com eficácia e se manterem ativas no mercado. Com isso, diante da dinâmica das condições ambientais, torna-se difícil aos administradores, desenvolver e adaptar as organizações para concorrer com êxito. A evolução da ciência e da tecnologia e a internacionalização dos mercados influenciam o ritmo das mudanças no ambiente externo. O resultado disto é uma crescente necessidade de adaptação para as organizações, uma vez que o ambiente externo se caracteriza por incerteza e turbulência e passa por constantes mudanças.

Segundo a teroria dos sistemas, as organizações não são auto-suficientes nem independentes; elas trocam recursos com o ambiente externo e dele dependem, pois captam seus insumos,

transformam-nos em produtos ou em serviços e logo os mandam de volta para o ambiente externo. A tarefa executada por uma organização pressupõe o seu relacionamento e interdependência com inúmeras outras organizações e pessoas, comprovando assim, que elas dependem uma das outras para o seu funcionamento.

Para Chiavenato(1999), o ambiente é uma grande fonte de recursos e pode, igualmente, ser uma fonte de muitas pressões. Dessa forma, as organizações procuram aproveitar as influências positivas do ambiente, tirar vantagem das oportunidades que surgem e procurar eliminar a influências negativas ou adaptando-se a elas para manter sua sobrevivência e crescimento. À medida que as organizações se adaptam às circunstâncias ambientais, conseguem crescer pois aprendem a aproveitar as oportunidades positivas e amortecer as coações e contigências que lhes são impostas pelo ambiente.

O ambiente de negócios atualmente está voltado para o desenvolvimento, armazenamento e segurança do ativo de grande importância para as organizações: Informação e Conhecimento. Diante desta realidade as organizações têm-se aproveitado das influências deste mercado para desenvolver-se tecnologicamente, no sentido de atualizar-se e adaptar-se ao novo ambiente e assim tirar proveito das oportunidades positivas que podem surgir.

O histórico da explosão da informação tem um início após a I Gerra Mundial onde o capitalismo sofre transformações que se caracterizam pela participação do estado na vida econômica, gerando ruptura parcial e aparente do liberalismo clássico. Esse periodo, intitulado neocapitalismo e amadurecido após a crise de 1929, constitui-se em falsa mudança, ja que preservou a hegemonia burguesa, com os princípios básicos do capitalismo: propriedade particular, lucro e desigualdade social.

O desenvolvimento científico e tecnológico, proveniente de esforços da guerra dos anos 30, passou a permear o capitalismo industrial, que se deparou com o crescimento exponencial da informação.Tal mudança ocorreu em decorrência de novas exigências para a reprodução capitalista, onde a informação assume novas funções. Esse momento caracteriza a denominada explosão da informação, em que a informação se torna balisar para o progresso econômico.

A transição para uma era da informação e do conhecimento vem exigindo a constituição de novos espaços e instrumentos de regulação política e jurídico-normativa que respondem às múltiplas questões (de caráter economico-comercial, político, tecnológico, sócio-cultural e ético), colocadas a partir das mudanças que conduzem e expressam essa passagem.

Comércio eletrônico, privacidade e ética na Internet, ampliação e reformulação das garantias de direitos de propriedade intelectual, novas regulamentações no campo das telecomunicações, no mundo do trabalho e da educação, são apenas algumas das áreas nas quais se impõem a necessidade de novas regras e normas que ordenem os processos de geração, acesso, fluxo, disseminação e uso de informação e conhecimento, bem como a regulação de novas práticas e relações que se estabelecem em torno dessas atividades. Sem falar nos fluxos financeiros, transfronteiras, na prática de fluxos informacionais, cujos desequlíbrios causados nas economias nacionais e internacionais provocam o debate sobre a importância de se estabelecerem regulações neste campo.

Do mesmo modo, a dinâmica institucional emergente contribui, em grande medida, para moldar, de modo positivo ou restritivo, o perfil do novo padrão sócio-técnico-econômico. Tal dinâmica se define a partir da criação de uma série de intitutos normativos - leis, normas padrões, políticas, códigos de conduta e convenções, os quais irão incidir, direta ou indiretamente, sobre as atividades de informação e conhecimento.

Ao mesmo tempo, a medida que o processo de globalização, avança, recoloca-se o papel dos aparatos e instrumentos reguladores. Cabe-lhes administrar e normatizar as relações internacionais que se intensificam, ora medindo seus conflitos, ora impondo-lhes soluções. Cabe-lhes também criar condições político institucionais, no âmbito dos países, para que estes se ajustem a nova realidade sócio-econômico-politico, incluídas as transformações tecnológicas. De modo geral, no entanto, o espaco institucional tende a privilegiar os pontos de vista das partes de maior poder político e econômico no cenário mundial, o que frequentemente não coincide com a perspeciva dos países e segmentos sociais que se encontram em posição periférica.

A realidade vivida pelas organizações hoje, é pouco confortável e extremamente complexa, pois nada é constante e previsível. Nesse contexto é possível detectar altos níveis de incerteza,

de transformações e de competitividade globalizada, em que as formas tradicionais de gestão e de funcionamento não bastam mais para que as empresas consigam sobreviver em um ambiente de turbulência.

As práticas organizacionais e os antigos modelos não atendem mais as necessidades das empresas que têm enfrentado um grande desafio. Neste momento, busca-se vantagens competitivas num ambiente em freqüente e constante mutação, caracterizado por um conjunto de transformações políticas, econômicas e sociais.

Nesse novo contexto, as organizações com condições de sobreviver e se desenvolver são aquelas que tem a capacidade de reação a estas situações e, ao mesmo tempo, antecipem as mudanças a partir de estratégias adequadamente definidas. Isto traz a necessidade da criação de novas ferramentas e mecanismos para práticas organizacionais. Neste sentido, percebe-se uma forte tendência de reorganização dos fatores produtivos das empresas com altas taxas de incorporação de tecnologia.

A administração da tecnologia sendo considerada um processo relativamente complexo por vários autores, exige que os seus gestores entendam não só como as tecnologias surgem, mas também como se desenvolvem e afetam a forma das organizações competirem e como os seus membros desempenham as atividades. Para muitos especialistas, entender as forças que movem os desenvolvimentos tecnológicos pode auxiliar administradores na antecipação, monitoramento e gerenciamento das tecnologias de forma mais eficaz e eficiente.

A informação teve uma valorização crescente a partir da década de 70, do século XX, apoiada pelo desenvolvimento acelerado das Novas Tecnologias de Informação e Comunicação (NTIC's). Essa situação cunhou o novo paradigma social, o tecno-econômico-informacional, no qual, as práticas de produção, comercialização e consumo de bens e serviços, cooperação e competição entre os agentes sociais, privilegiam a recuperação da informação por meio das NTIC's (CASTELLS, 1999).

Esse paradigma imprime na sociedade a necessidade de desenvolver ainda mais a habilidade de integrar o humano e o tecnológico nos diferentes processos de trabalho (SARACEVIC, 1995) e, também, efetivar políticas construídas em conjunto, Estado e Sociedade, viabilizando esse novo *modus operandis* , a Informação e a Informática nos processos produtivos.

As organizações gerenciadas nos moldes taylorianos estão cada vez mais cedendo espaço a novas formas de gestão. O foco nos bens tangíveis cede lugar a outros bens, os intangíveis. Dos bens intangíveis relevantes para o gerenciamento das organizações, destacamos o dado, a informação e o conhecimento como subsídios essenciais à comunicação e tomada de decisão. Para que as decisões organizacionais sejam tomadas com rapidez e qualidade, é importante que as organizações disponham de um sistema de comunicação eficiente, que permita a rápida circulação da informação e do conhecimento, sendo, para isso, indispensável o suporte da tecnologia.

Para Drucker (1995), a época atual é um período de transformação que envolve toda civilização, em que o conhecimento, é o principal recurso para os indivíduos e a economia em geral. Neste sentido, o acesso, a disponibilidade, o tratamento e a efetiva utilização da informação é de fundamental importância, uma vez que a informação é a matéria prima do conhecimento.

É nesse ambiente de mudança que se insere a Segurança da Informação que tem por objetivo discutir inovações que marcam a sociedade atual e se refletem na pertinência da Sociedade da Informação neste novo contexto.

2.2 INFORMAÇÃO EM UM CONTEXTO DE MUDANÇA

O objeto "Informação" é identificado como a alavanca do comportamento humano em sociedade, associada ao processo de comunicação, que tem nos meios de transmissão da informação um novo sistema de comunicação que fala cada vez mais uma linguagem universal digital, promovendo a integração global da produção (CASTELL: 2000). A gestão da informação auxiliada pelas TIC's é cada vez mais considerada nas organizações como um fator estratégico na gestão organizacional.

Dado, informação e conhecimento são elementos fundamentais para a comunicação e tomada de decisão nas organizações, mas seus significados não são tão evidentes. Eles formam um

sistema hierárquico de difícil delimitação. Davenport (1998) corrobora esse posto de vista colocando a resistência em fazer essa distinção, por considerá-la nitidamente imprecisa.

Entretanto, existe um consenso de que os dados são elementos brutos, sem siginificado, desvinculados da realidade. Segundo Davenport (1998, p.19) são observações sobre o estado do mundo. São símbolos e imagens que não dissipam nossas incertezas. Eles constituem a matéria-prima da informação. Dados sem qualidade levam a informações e decisões da mesma natureza. O dado, é considerado a matéria-prima para a informaçãoe as informações são dados com significado. “São dados dotados de relevância e propósito” (DAVENPORT, 1998, p.18). Para Lussato(1991) são o resultado do encontro de uma situação de decisão com um conjunto de dados, ou seja, são dados contextualizados que visam a fornecer uma solução para determinada situação de decisão.

A informação pode assim ser considerada como dados processados e contextualizados que para Sveiby(1998) a informação também pode ser considerada como “desprovida de significado e de pouco valor,” sendo, ainda, considerada por Malhotra(1993) como “matéria prima para se obter conhecimento.”

Mas o que é conhecimento? “Conhecimento é a informação mais valiosa (...) é valiosa precisamente porque alguém deu à informação um contexto, um significado, uma interpretação (...)” (DAVENPORT ,1998, p.19),. O conhecimento pode então ser considerado como a informação processada pelos indivíduos e o valor agregado à informação depende do conhecimento anterior desses indivíduos e do uso da informação nas ações. Desta forma, o conhecimento está associado ao indivíduo; ele está estritamente relacionado com a sua percepção.

O conceito de conhecimento pode ser entendido com um sentido mais complexo que o de informação. “Conhecer como um processo de compreender e internalizar as informações recebidas, possivelmente combinando-as de forma a gerar mais conhecimento” (GONÇALVES, 1995, p.31). Conhecimento útil para tomada de decisões não é representado somente através de dados, este constitui o início do processo. O grande desafio dos tomadores de decisão é o de transformar dados em informação e informação em conhecimento, minimizando as interferências individuais nesse processo de transfornação.

Para Norbert Wiener, a informação é um requisito para nossa sobrevivência. Permite necessário intercâmbio entre nós e o ambiente em que vivemos.

> Viver efetivamente é viver com informação adequada. A comunicação e o controle, portanto, são integrantes da essência da vida interior do homem, na mesma medida em que fazem parte de sua vida em sociedade (WIENER 1954).

A importância da informação é resumida por Sagan (1977) em uma única frase: " informação e alimento são as condições necessárias à sobrevivência do ser humano". A informação, na verdade, é indispensável para toda e qualquer atividade humana, sendo cada vez mais, vista como uma força importante e poderosa a ponto de dar origem a expressões como: sociedade da informação, indústria da informação, revolução da informação, sociedade do conhecimento.

A informação não é, na verdade, um conceito único, singular, mas sim uma série de conceitos conectados por relações complexas. Nesta perspectiva, informação é o veículo de inter-relações e interações entre objetos e conteúdos. Belkin e Robertson (1976) procuraram a noção básica contida no termo e chegaram a conclusão de que a única noção comum à maioria ou a todos os usos da informação é a idéia de estruturas sendo alteradas, propondo, a seguinte definição: informação é o que é capaz de transformar a estrutura. Se informação é tudo aquilo que altera e transforma estruturas, então:

> ... a informação é a mais poderosa força de transformação do homem. O poder da informação, aliado aos modernos meios de comunicação de massa, tem capacidade ilimitada de transformar culturalmente o homem, a sociedade e a própria humanidade como um todo. (ARAÚJO, 1991)

A organização na luta pela sobrevivência, precisa, em especial, inovar e mudar constantemente para se adaptar ao seu ambiente, principalmente no que se refere às implicações da mudança tecnológica. Coutinho & Ferraz (1995) mostram que, a partir de meados dos anos 70, a inovação tecnológica acelera-se, exigindo que as estruturas e processos organizacionais sejam transformados em função do impacto da veloz difusão de novas tecnologias de informação baseados na microeletrônica e nas telecomunicações. Para os autores, a emergência de um novo paradigma tecnológico e a globalização financeira são os traços mais marcantes nos últimos anos. (COUTINHO & FERRAZ 1995).

A informação exerce um papel cada vez mais importante na organização. Spinola & Pessoa (1997), consideram a informação, ferramenta poderosa para as organizações em geral, uma vez que, a partir dela pode-se ter um domínio dos parâmetros que regem a sua dinâmica. Constitui-se como um elemento integrador das diversas atividades e processos organizacionais, tanto no que se refere aos seus níveis (seja operacional, gerencial ou estratégico) como na sua relação com o ambiente onde a informação está inserida.

Neste contexto, é crescente a utilização das novas tecnologias de informação e a aplicação de sistemas de informações nas organizações, devido ao grande desenvolvimento tecnológico da informática e uma contínua queda de seu custo. Para ser competitivo na Era do Conhecimento, o segredo não reside somente na capacidade que a organização tem em reconfigurar seus processos de acordo com as novas realidades do mercado, mas, também, nas informações disponíveis acerca do seu ambiente interno e externo.

A cada dia, torna-se mais claro o papel econômico da informação como insumo para o desenvolvimento de produtos, captação de recursos, conhecimento de mercado e sobrevivência de muitas empresas. A capacidade de uma empresa captar e absorver informação correta e de forma ágil determina suas possibilidades de inovação, aumentanado a lucratividade e atendendo ao cliente, sendo competitiva no mercado altamente instável e ágil.
Os investimentos em produtos e serviços de informação em muitas organizações no nosso país ainda são tímidos, muitas ainda não percebem como fazer negócios e decidir os seus rumos tendo como insumo a informação. A indústria brasileira, em função disso e de outros aspectos significativos, tem sofrido bastante para acompanhar as contínuas mudanças de uma economia que exige qualidade de produtos, agilidade de processos e que sofre ameaças constantes do mercado.

Para que seja possível acompanhar as transformações atuais, é fundamental conhecer os concorrentes e parceiros, produtos, fornecedores, dados financeiros e econômicos, bem como questões legais. Para isso, é necessário que estejam organizados e disponíveis produtos e serviços de informação que supram as empresas dos dados necessários para acompanhar o mercado.

As empresas necessitam, de informação disponibilizada com rapidez e precisão, que demonstre o contexto atual do mercado e da economia nacional e internacional. As empresas

brasileiras buscam informações sobre fontes de financiamento, processos de produção, controle de qualidade, gestão organizacional, bem como sobre fornecedores de máquinas e equipamentos, conforme resultado de pesquisa desenvolvida pela Confederação Nacional da Indústria.

A informação para negócios, definida como aquela que diz respeito a mercado, companhias, produtos, estatísticas e legislação, é uma área de conhecimento recente, e precisa ser consolidada em termos de conhecimentos teóricos, de organização de fontes de informação e produtos/serviços de informação. Além disso, ressalta-se que, à medida que se define uma área de estudos, torna-se possível capacitar pessoas para o exercício de atividades inerentes a essa área. Esse aspecto deve ser desenvolvido com urgência, uma vez que o mercado carece de profissionais que dominem especificamente a área de informação para negócios.

Os autores Borges e Campello (1997) levantam uma questão conceitual quando afirmam que o termo informação para negócios, antes considerado como aquele que substitui o termo informação para indústria, por ser mais abrangente – traz, na realidade, uma perspectiva maior para a agregação estratégica e geradora de conhecimento organizacional.

Os grandes serviços de informação que compõem hoje a indústria de informação para negócios, apresentam-se especializados, como informa a Simba Information, empresa americana que afirma que os maiores faturamentos em termos de informação se deram com corretagem, notícias financeiras e pesquisas de crédito.

Para a prestação de serviços de informação para negócios, Abell (1990) define uma estratégia básica que consiste, inicialmente, em identificar necessidades, promover meios confiáveis de captação e manipulação dessas informações, bem como promover o acesso à informação, tanto para o "staff" que planeja, como para o operacional.

Segundo CRAWSHAW (1991), a maior parte do valor agregado da informação está em sua precisão. Outra grande parcela desse valor agregado está na diversificação das possibilidades de formatos de saída (impresso, eletrônico, audiovisual, etc.) para o produto/serviço de informação.

Deve-se estar atento à organização dos recursos disponíveis da informação, identificando-se não só as necessidades de informações, mas inclusive, a tecnologia disponível para gerenciá-las. Nesse sentido, a tecnologia de informação, destaca-se como um recurso cada vez mais fundamental de competitividade empresarial, oferecendo um amplo leque de oportunidades, especialmente, quando aliadas às tecnologias de comunicações.

A interpretação dos fenômenos que marcam a sociedade atual, tem como referência inicial Daniel Bell, com a publicação do livro O Advento da Sociedade Pós Industrial, (1974) que estabelece a primazia da economia e da tecnologia, ao afirmar que:

> "conceito de sociedade pós-industrial lida sobretudo com as mudanças na estrutura social, com a maneira segundo a qual a economia está sendo transformada e como está sendo remanejado o sistema ocupacional, e com as novas relações entre a teoria e o empirismo, particularmente entre a ciência e a tecnologia."

A maior ênfase dada ao conhecimento científico e tecnológico, gerador de inovação, como fonte de valor e de crescimento da sociedade, acarreta vários desdobramentos a teoria da sociedade pós-industrial definida por Bell, sendo o mais difundido e popularizado o da sociedade da informação. Muitos autores consideram que, apesar da maior visibilidade das informações e das inovações, o cerne é mesmo o conhecimento, sem o qual não é possível decodificar o conteúdo das informações e transformá-las em conhecimento. O maior destaque dado ao conhecimento, deve-se também, ao fato de que as tecnologias de ponta dessa fase são resultados de enormes esforços de pesquisa e desenvolvimento.

Durante as últimas décadas, uma série de inovações científicas e tecnológicas passou a convergir, vindo a se constituir, segundo muitos, em um novo paradigma tecnológico baseado nas tecnologias de informação e comunicação, abreviadamente chamada de TIC.

2.3 O PAPEL DAS TECNOLOGIAS DA INFORMAÇÃO NA ORGANIZAÇÃO E NA SOCIEDADE

As organizações de pequeno porte podem competir com ferramentas ou estratégias tão potentes quanto às de grande porte. A informação, que marca a competição nesta nova sociedade, é um recurso disponível e democrático. No entanto, é preciso definir previamente os rumos da organização para que as ferramentas, estratégias e informações sejam bem utilizadas.

Em algumas organizações a informatização não tem efeito positivo pois uma ferramenta tão poderosa como a tecnologia de informação não deve ser implantada sem que haja planejamento ou foco adequado, pois muitas dessas organizações não definem os equipamentos e sistemas antes de comprá-los; se não forem absolutamente adequados para uma finalidade específica, não vão resolver o problema.

Uma empresa com um sistema totalmente informatizado, funcionando eficiente e eficazmente, proporcionará grandes vantagens, seja com relação ao tempo otimizado, à organização, à facilidade de obtenção de informações, à previsão e muitos outros aspectos que contribuirão para o sucesso da empresa. Assim, a informatização das organizações possibilita que elas ganhem eficiência e eficácia melhorando, assim, sua competitividade e aumentando sua lucratividade porque melhora as informações para tomada de decisões.

A grande motivação para que as organizações estejam buscando adquirir recursos da tecnologia da informação é a sua sobrevivência num mercado cada vez mais global e competitivo. Ao adquirirem modernas tecnologias para tratamento de informações, as organizações tendem a melhorar significativamente a sua agilidade e flexibilidade, além do aumento da qualidade de seus produtos.

Com o advento da revolução digital e da concorrência em escala global, muitas organizações começam a explorar as novas oportunidades de mercado, desenvolvendo áreas de negócio até então inexistentes. O crescimento do mercado das comunicações móveis, a explosão da Internet, a emergência do comércio eletrônico, o desenvolvimento da indústria de conteúdo em ambiente multimídia, a convergência dos setores das telecomunicações, dos computadores e da multimídia, demonstram o enorme potencial das tecnologias de informação para gerar novas oportunidades de emprego, estimular o investimento e o desenvolvimento acelerado de novos setores, criando um Novo Ambiente e uma Nova Economia. E, para Castells:

> O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso. (...) As novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos. (...) Pela primeira vez na história, a mente humana é uma força direta de produção, não apenas um elemento positivo do sistema produtivo. (CASTELLS, 1999, p.36).

A informação é a matéria-prima: "são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como nas revoluções tecnológicas anteriores." (CASTELLS, 1999).

A era da informação é centrada nas tecnologias de telecomunicações e informática, possibilitando a construção de sistemas computacionais e de comunicação cada vez mais potentes e eficientes, realizando uma transformação social profunda e uma nova sociedade denominada sociedade da informação.

Novas teorias e acontecimentos estão formatando o mundo para uma sociedade centrada em redes de comunicação, que permitem ao indivíduo o acesso a mais informações, a custos cada vez menores. A falta de fronteiras são evidentes e o recurso estratégico deixa de ser capital e passa a ser a informação.

A partir da incorporação de novos conhecimentos, desenvolve-se novos produtos, serviços, ferramentas e processos de produção mais modernos, a nova tecnologia sendo produzida. Esses avanços tecnológicos provocam o crescimento econômico, gerando bens e serviços, induzindo assim transformações políticas e sociais que tendem a proporcionar a melhoria da qualidade de vida da sociedade. Essas transformações nascem e evoluem impondo novos conceitos e comportamentos sociais.

Quando aparece uma inovação tecnológica, ocorrem mudanças na sociedade e a velocidade de produção e consumo é grande, sendo a desatualização da informação bastante acentuada. A concorrência leva muitas empresas a começar a explorar novas oportunidades de mercado, desenvolvendo áreas de negócio até então inexistentes.

As tecnologias da informação e das comunicações já integram o quotidiano das organizações. Oferecem instrumentos úteis para as comunicações pessoais e de trabalho, para o processamento de textos e de informação sistematizada, para acesso a bases de dados e à informação distribuída nas redes eletrônicas digitais, além de integradas em numerosos equipamentos do dia-a-dia, em casa, no escritório, na fábrica, nos transportes, na educação e na saúde, introduzindo uma nova dimensão no modelo das sociedades modernas.

2.4 A SOCIEDADE DA INFORMAÇÃO

Castells (1999) comenta as mudanças do modo de desenvolvimento industrial para o modo informacional, que decorre da convergência das mudanças sociais com as tecnológicas. Esta passagem para a sociedade da informação resulta de um processo social de desenvolvimento científico e tecnológico, cujas forças motrizes geram implicações técnicas, sociais, culturais, políticas, econômicas cumulativas e irreversíveis, que mudam as formas de discutir, produzir e organizar, enfim, de movimentar e representar a sociedade.

As mudanças de conceitos e idéias levam à percepção da necessidade de uma profunda transformação em nossa visão de mundo. Da máquina à revolução industrial e desta para uma economia de serviços, culminando na revolução pós-industrial, todas as mudanças sócio-econômicas e culturais, desde a energia a vapor até a era da informação afetam, de certa forma, nossa existência.

Castells (1999, v.1, p.49) considera a história da vida como uma série de situações estáveis, pontuadas em intervalos raros por eventos importantes, que ocorrem com rapidez e ajudam a estabelecer a próxima era estável. Para ele, no final do século XX, vivemos um desses raros intervalos na história, cuja característica é a transformação de nossa cultura material pelos mecanismos de um novo paradigma tecnológico, que se organiza em torno da tecnologia da informação. Na perspectiva do autor, tecnologia é entendida como o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de maneira reproduzível.

Na sociedade da informação, são diversos os estudos sobre as mudanças ocorridas, a abordagem da informação como produto econômico, o uso do computador e das

Telecomunicações, os novos produtos/serviços e as novas profissões até às conseqüências econômicas, políticas e sociais.

Na sociedade da informação ocorrem transformações, provocando a mudança de enfoque em relação ao fator de produção e ao fator de desenvolvimento econômico. A base dessa transformação é que o setor de informação é intensivo em conhecimento e não em mão-de-obra. Nessa mudança o valor agregado do conhecimento ou do segmento tecnológico é progressivamente mais importante, quando incorporado ao bem, provocando a transformação industrial da matéria prima pelo valor agregado. O valor econômico da informação parte do pressuposto de que a informação gera conhecimento e esse, quando acumulado, possibilita a produção científica e tecnológica, responsável pela geração de bens e serviços.

Castells (1999, v.1, p.174-176) é de opinião que a economia informacional se caracteriza pelo desenvolvimento de uma nova lógica organizacional, que está relacionada com o processo atual de transformação tecnológica, mas não depende dele. Defende que a convergência e a interação entre um novo paradigma tecnológico e uma nova lógica organizacional constituem o fundamento histórico da economia informacional. Ao explicar os pontos fundamentais de sua análise sobre as trajetórias organizacionais, destaca que o objetivo principal das transformações é lidar com a incerteza causada pelo ritmo veloz das mudanças no ambiente econômico, institucional e tecnológico da empresa, aumentando a flexibilidade em produção, gerenciamento e marketing.

Vislumbra-se uma excelente oportunidade para os profissionais da informação, que se ocupam com a geração, seleção, tratamento, organização, disseminação e uso da informação. Isto porque, na sociedade da informação, as unidades de informação devem assumir sua ampla responsabilidade em relação à oferta de produtos e prestação de serviços informacionais.

A informação precisa ser estudada como o fator essencial que permitirá a verdadeira transformação da sociedade da informação. Como atributos da informação podem ser considerados o seu uso horizontal e vertical, seu consumo com valor agregado, seu re-processamento e re-empacotamento. Esses aspectos devem ser melhor explorados pelos profissionais da informação, em especial pelos responsáveis pela oferta e prestação de serviços informacionais.

Entretanto, o contexto evolutivo do enfoque da informação e a visão do novo paradigma, preconizando e dando prioridade ao acesso à informação precisam ser considerados, quando se pensa na atuação desses profissionais nas unidades de informação brasileiras para que eles possam desempenhar, efetivamente, suas atividades nessa nova sociedade.

Segundo Castells (1999, v.1, p.497), a atuação em rede, de modo geral, ainda que enfrentando alguns problemas ao longo do tempo, tem sido considerada entre os profissionais da informação como mecanismo adequado para otimização de recursos e esforços, tanto para minimizar gastos, quanto para ampliar possibilidades de melhor atendimento a um número cada vez maior de usuários. Espera-se, que cada vez mais, a evolução da Telemática proporcione melhoria das condições de estabelecimento de novas redes e que as unidades de informação superem os obstáculos que enfrentam, de modo a que se possa contar com o quantitativo e qualitativo crescimento das redes informacionais em todos os setores e áreas do conhecimento.

Nessa perspectiva, é exigida atuação efetiva das unidades de informação, o que certamente implicará, entre outros requisitos a serem satisfeitos, no interesse em conhecer e satisfazer as necessidades de informação dos usuários e a preocupação com o constante aprimoramento do desempenho profissional dos prestadores de serviços de informação. Será preciso, buscar a melhor maneira de atuar, avaliando sempre para manter a atualização.

Expressões como sociedade pós-industrial, sociedade da informação, sociedade do conhecimento, são usadas nas análises e interpretações das mudanças sociais. São expressões que se proliferam na tentativa de descrever as características emergentes da realidade contemporânea. São conceitos provenientes de enfoques teóricos distintos, mas que apresentam vetores comuns de mudança como as tecnologias de informação e comunicação; produção informação-conhecimento intensiva; globalização; flexibilização; a descentralização produtiva e diversificação.

Sociedade da informação substitui o conceito complexo de sociedade pós-industrial e como forma de transmitir o conteúdo específico do novo paradigma técnico-econômico. A realidade que os conceitos das ciências sociais procuram expressar refere-se às transformações técnicas, organizacionais e administrativas que têm como fator-chave não mais os insumos baratos de

energia – como na sociedade industrial – mas os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e telecomunicações. Esta sociedade pós-industrial ou informacional, como profere Castells(1999), está ligada à expansão e reestruturação do capitalismo desde a década de 80 do século que terminou. As novas tecnologias e a ênfase na flexibilidade – idéia central das transformações organizacionais – têm permitido realizar com rapidez e eficiência os processos de desregulamentação, privatização e ruptura do modelo de contrato social entre capital e trabalho característico do capitalismo industrial.

As transformações em direção à sociedade da informação, em estágio avançado nos países industrializados, constituem uma tendência dominante mesmo para economias menos industrializadas e definem um novo paradigma, o da tecnologia da informação, que expressa a essência da presente transformação tecnológica em suas relações com a economia e a sociedade. Esse novo paradigma tem, segundo Castells(1999) as seguintes características fundamentais:

- A informação é sua matéria-prima: as tecnologias se desenvolvem para permitir o homem atuar sobre a informação propriamente dita, ao contrário do passado quando o objetivo dominante era utilizar informação para agir sobre as tecnologias, criando implementos novos ou adaptando-os a novos usos.
- Os efeitos das novas tecnologias têm alta penetrabilidade porque a informação é parte integrante de toda atividade humana, individual ou coletiva e, portanto todas essas atividades tendem a serem afetadas diretamente pela nova tecnologia.
- Predomínio da lógica de redes. Esta lógica, característica de todo tipo de relação complexa, pode ser, graças às novas tecnologias, materialmente implementadas em qualquer tipo de processo.
- Flexibilidade: a tecnologia favorece processos reversíveis, permite modificação por reorganização de componentes e tem alta capacidade de reconfiguração.
- Crescente convergência de tecnologias, principalmente a microeletrônica, telecomunicações, optoeletrônica, computadores, mas também e crescentemente, a biologia. O ponto central aqui é que trajetórias de desenvolvimento tecnológico em diversas áreas do saber tornan-se interligadas e transformam-se as categorias segundo as quais pensamos todos os processos.

O foco sobre a tecnologia pode alimentar a visão ingênua de determinismo tecnológico segundo o qual as transformações em direção à sociedade da informação resultam da tecnologia, seguem uma lógica técnica e, portanto, neutra e estão fora da interferência de fatores sociais e políticos. Nada mais equivocado: processos sociais e transformação tecnológica resultam de uma interação complexa em que fatores sociais pré-existentes, a criatividade, o espírito empreendedor, as condições da pesquisa científica afetam o avanço tecnológico e suas aplicações sociais. Para Castells:

> É provavel que o fato da constituição desse paradigma ter ocorrido nos EUA e, em certa medida, na Califórnia e nos anos 70, tenha tido grandes consequências para as formas e a evolução das novas tecnologias da informação. Por exemplo, apesar do papel decisivo do financiamento militar e dos mercados nos primeiros estágios da indústria eletrônica, da década de 40 à de 60, o grande progresso tecnológico que se deu no início dos anos 70 pode, de certa forma, ser relacionado à cultura da liberdade, inovação individual e iniciativa empreendedora oriunda da cultura dos *campi* norte-americanos da década de 60...Meio incoscientemente, a revolução da tecnologia da informação defundiu pela cultura mais significativa de nossas sociedades o espírito libertário dos movimentos dos anos 60. (CASTELLS, 2000, pp.25)

Além do indevido determinismo, incorre-se muitas vezes também em despropositado evolucionismo na discussão de novo paradigma tecnológico quando a sociedade da informação é vista como etapa de desenvolvimento. Como muito bem alerta Agudo Guevara (2000), melhor será referir-se a sociedade da informação, no plural, para identificar, numa dimensão local, aquelas nas quais as novas tecnologias e outros processos sociais provocaram mudanças paradigmáticas. A expressão sociedade da informação, no singular, seria melhor utilizada, numa dimensão global (ou mundial), para identificar os setores sociais, que participam "como atores de processos produtivos, de comunicação, políticos e cultutais que têm como instrumento fundamental as tecnologias de informação e comunicação e se produzem – ou tendem a se produzir – em âmbito mundial"(AGUDO GUEVARA, 2000, p.4).

O maior destaque dado ao conhecimento, deve-se também ao fato de que as inovações tecnologicas resultam de enormes esforços de pesquisa e desenvolvimento, numa geração sistemática de conhecimento. Nesse contexto, é postulado que durante as últimas décadas, uma série de inovações científicas e tecnológicas passou a convergir, vindo a se constituir, segundo muitos, em um novo paradigma tecnológico baseado nas Tecnologias de Informação e de Comunicação, abreviadamente chamadas de TIC.

Por que razão as Nações alteram o seu rumo e as empresas têm necessidade de refletir estrategicamente em função deste novo estágio da sociedade? Como será possível retirar o máximo proveito da revolução da informação em curso? Alcançando benefícios desta nova forma de organização da sociedade?

A expressão Sociedade da Informação pode-se referir a um modo de desenvolvimento social e econômico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conduz à criação de conhecimento e a satisfação das necessidades dos cidadãos e das organizações. Esta sociedade é marcada por um crescente funcionamento de redes digitais de informação. Esta alteração do domínio da atividade econômica e dos fatores determinantes do bem-estar social é resultante do desenvolvimento das novas tecnologias da informação, do audiovisual e das comunicações, com as suas importantes ramificações e impactos no trabalho, na educação, na ciência, na saúde, no lazer, nos transportes e no ambiente, entre outras.

Se a questão dos anos 80 se baseia na qualidade, a dos 90 se apóia na reengenharia, a questão deste século, a velocidade: com a rapidez a natureza dos negócios pode mudar, e as transformações comerciais; o acesso à informação pode alterar os estilos de vida dos consumidores e as expectativas em relação aos serviços e produtos. A melhoria da qualidade e do aperfeiçoamento dos processos empresariais podem ocorrer muito mais depressa. Essas mudanças podem ocorrer devido a uma idéia muito simples e baseada na tecnologia: o fluxo de informação digital.

Quatro mudanças de paradigmas têm impactado às organizações nos dias de hoje: as novas tecnologias (novas metas para a tecnologia da informação, computação em rede, aberta e centrada em usuários), o novo ambiente empresarial (mercado dinâmico aberto e competitivo), a nova empresa (organização aberta com atuação em rede e fundamentada na informação, e a nova ordem geopolítica (realidade mundial aberta, volátil e multipolar)). Estas mudanças convergem para uma maior quebra de paradigmas e uma nova sociedade surge com nova estrutura, novos canais de comunicação, novas formas de atuação social e de trabalho.

Novos referenciais sociais, econômicos, tecnológicos e culturais, provocam um conjunto significativo de mudanças de enfoque no âmbito das sociedades e de suas organizações, em que a informação constitui a principal matéria prima, um insumo comparável à energia que alimenta um sistema; o conhecimento é utilizado na agregação de valor a produtos e serviços; a tecnologia constitui um elemento vital para as mudanças em especial o emprego da tecnologia sobre acervos de informação; e a rapidez, a efetividade e a qualidade constituem fatores decisivos de competitividade.

A nova sociedade da informação e do conhecimento atribui ao seu objeto de estudo – a informação, o conceito de bem ou recurso, econômico e estratégico, que pode ser traduzido em vantagem competitiva. E para sobreviver em um ambiente de negócios cada vez mais competitivo, as empresas devem estar dispostas a se reinventarem constantemente, e para isso devem ter o conhecimento necessário para o domínio dos seus negócios.

Ao mesmo tempo que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes, e com isso, a segurança da informação tornou-se um ponto relevante nesse contexto.

3. O USO DA INFORMAÇÃO E A NECESSIDADE DA SEGURANÇA DA INFORMAÇÃO

De início, uma importante questão estratégica para o sucesso de qualquer organização nos dias de hoje é a sua capacidade de analisar, planejar e reagir, rápida e imediatamente, às mudanças nas condições de seus negócios. Para que isso aconteça, é necessário que se disponha de mais e melhores informações pois elas constituem a base desses processos.

3.1 A NECESSIDADE DA INFORMAÇÃO SEGURA

A informação é um dos principais patrimônios de grande parte das organizações, e deve ser tratada como tal, devendo ser protegida nos seus aspectos de disponibilidade, integridade e confidencialidade. Isto porque a segurança de informação é um elemento chave dentro desse conceito, e não deve ser vista apenas como guarda de informações disponíveis em um cofre, e sim como políticas de proteção de informação visando evitar maiores riscos e vulnerabilidades.

Segundo Dias(2000) Segurança pode ser entendida como a proteção de informações, sistemas, recursos e serviços contra desastres, erro e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes. Para isso é necessário possuir uma boa política de segurança da informação, na qual deve ser composta por regras claras, praticáveis e sintonizadas com a cultura e o ambiente tecnológico da empresa. Deve proteger não só as informações confidenciais, mas também motivar as pessoas que as manuseiam, mediante a conscientização de todas as pessoas envolvidas direta e indiretamente.

A segurança da informação tem deixado de ser tratada como um assunto técnico da área de informática e vem sendo considerada uma real necessidade nas empresas e instituições, passando a ser um requisito estratégico, que interfere na capacidade das organizações de realizarem negócios e no valor de seus produtos no mercado.

Segundo Moreira (2001), a informação é um ativo digital valioso para qualquer organização, independente da atividade. Tudo gira em torno de como é valiosa a informação, o quanto ela representa para o seu negócio. Por esta razão, prover proteção aos recursos da empresa (sistemas, pessoas, informações, equipamentos) tem a finalidade de diminuir o nível de exposição aos riscos existentes em todos os ambientes para que a organização possa estender a segurança aos seus produtos e serviços, resultando em uma maior satisfação por parte dos clientes.

Um aspecto que amplia a necessidade de segurança da informação e é apresentado por Nakamura(2003) é o aumento das autorizações financeiras eletrônicas, seja pessoalmente em comércio eletrônico e internet banking, seja nos sistemas de gestão empresarial. Assim a segurança da informação que é trocada ou armazenada para posterior utilização, é um dos aspectos determinantes na aceleração do desenvolvimento das relações de comércio, prestação de serviços e das demais relações empresariais.

O domínio da informação sempre teve fundamental importância para as corporações, sendo indispensável arma, do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa ter um suporte imbatível para a tomada ágil e eficiente de decisão.

Obviamente, da forma como hoje é manipulada e armazenada, quando se faz extensivo uso dos meios e equipamentos eletrônicos, a informação passou a ser objeto de preocupação dos profissionais de Tecnologia da Informação, responsáveis pelos métodos de tratamento e pela sistematização dos dados, de modo a formar a referida base confiável para processos decisórios. (CARUSO,1999).

A Tecnologia da Informação Segundo Nakamura(2003) é um instrumento cada vez mais utilizado pelo homem, o qual busca incessantemente realizar trabalhos de modo mais fácil, mais rápido, mais eficiente e mais competitivo, produzindo,assim, os melhores resultados. A rede é uma das principais tecnologias, permitindo conexões entre todos os seus elementos, que vão desde roteadores até servidores que hospedam site na Internet da organização e o banco de dados dos clientes, passando ainda por sistemas financeiros e de gestão de relacionamento com clientes. Esses recursos disponibilizados pela rede representam, na Era da Informação, até mesmo o próprio negócio das organizações. Isso faz com que a flexibilidade e facilidade de uso resultem em maior produtividade e na possibilidade de

criação de novos serviços e produtos, e consequentemente em maiores lucros para a organização.

Contudo, a confidencialidade, integridade e disponibilidade dessa estrutura de rede passa a ser essencial para o bom andamento das organizações, fazendo com que elas precisem ser protegidas. A proteção visa, a manutenção do acesso às informações que estão sendo disponibilizadas para os usuários. Isso significa que toda informação deve chegar aos usuários de uma forma íntegra e confiável. Para que isso aconteça, todos os elementos de rede por onde a informação flui, até chegar ao seu destino, devem estar disponíveis, e devem também preservar a integridade das informações. O sigilo também é importante, com isso forma-se os três pilares com as propriedades mais importantes para a segurança. (Fig. 2)

FIGURA 2. Propriedades mais importantes da segurança

Fonte: NAKAMURA(2003)

A informação, os processos de apoio, sistemas e redes segundo a Norma NBR ISO/IEC 17799 (Norma Internacional Standardization Organization/Internacional Electrical technical Commission (ISO/IEC) 17799), são importantes ativos para os negócios. Confidencialidade, Integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado.

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças à segurança da informação de uma variedade de fontes, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou

inundação. Problemas causados por vírus e *hackers* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A dependência nos sistemas de informação e serviços significa que as organizações estão vulneráveis às ameaças de segurança. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída dificulta a implementação de um controle de acesso centralizado realmente eficiente.

Um dos grandes desafios dos profissionais envolvidos com os problemas técnicos relativos à segurança da informação é a necessidade de buscar a segurança, mas sem ir de encontro à enorme tendência de flexibilização e de agilidade que vivem os mercados, de forma que as transações sejam realizadas de maneira mais conveniente e segura possível. A segurança da informação sempre foi tratada de forma romântica e estereotipada, seja nos filmes que falam de fraudes extraordinárias, seja nas histórias sobre *hackers* e vírus de computador.

Do ponto de vista de Caruso(1999), a necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios.

Nos últimos anos, muito tem se feito nas organizações de forma a eliminar o estigma que transforma Segurança da Informação em sinônimo de Segurança em TI, fazendo-a operar descolada da Segurança Física ou Patrimonial. Pouco a pouco, as organizações percebem que, a partir do momento que encaramos a segurança como uma garantia de que a empresa está protegida contra ameaças que possam causar impacto no funcionamento normal dos negócios, deixamos de ter uma visão pontual e centralizada para adotarmos uma visão mais holística do assunto. (NAKAMURA 2003).

Organizações de todos os tipos estão percebendo que, quando o assunto são ameaças em potencial que podem atrapalhar os objetivos da empresa, estamos basicamente falando sobre risco e, a gerência deste risco define, em última instância, a habilidade que a organização tem

para lidar com adversidades de percurso. Existem diversos fatores que afetam a preocupação com a segurança, sendo que alguns deles são quase imperceptíveis.

Segundo Moreira(2001), ter a visão focada para além dos problemas mais cotidianos da Segurança da Informação ajuda a antever cenários e fatores que podem influenciá-la no futuro, permitindo também que estejamos preparados para os problemas antes que eles aconteçam, regra básica quando o assunto é proteção. No mais, tal atitude também estimula o aprendizado e a leitura para além dos limites dos boletins de vulnerabilidades.

3.2 ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

Alguns elementos segundo Sêmola (2003) são considerados essenciais na prática da segurança da informação, dependendo do objetivo que se pretende alcançar. São eles:

Autenticação – Processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica, que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos.

Legalidade – Característica das informações que possuem valor legal dentro de um processo de comunicação, aonde todos os ativos estão de acordo com ás cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

Autorização – Concessão de uma permissão para o acesso às informações e funcionalidades das aplicações aos participantes de um processo de troca de informações (usuário ou máquina), após a correta identificação e autenticação dos mesmos.

Auditoria – Processo de coleta de evidências de uso dos recursos existentes, afim de identificar as entidades envolvidas num, processo de troca de informações, ou seja, a origem, destino e meios de tráfegos de uma informação.

Autenticidade – Garantia de que as entidades (informação, máquinas, usuários) identificadas em processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser, e que a mensagem ou informação não foi alterada após o seu envio ou validação. Normalmente, o termo autenticidade é utilizado no contexto de certificação digital, onde recursos de criptografia

e *hash* são utilizados para atribuir um rótulo de identificação às mensagens ou arquivos enviados entre membros de uma infra-estrutura de chave pública, visando garantir princípios/aspectos de: irretratabilidade, identidade, autenticidade, autoria, originalidade, integridade e confidencialidade.

Severidade – Gravidade do dano que um determinado ativo pode sofrer devido à exploração de uma vulnerabilidade por qualquer ameaça aplicável.

Relevância do ativo – Grau de importância de um ativo para a operacionalização de um processo de negócio.

Relevância de processo de negócio – Grau de importância de um processo de negócio para o alcance dos objetivos e sobrevivência de uma organização.

Criticidade – Gravidade referente ao impacto ao negócio causado pela ausência de um ativo, pela perda ou redução de suas funcionalidades em um processo de negócio, ou pelo seu uso indevido e não autorizado.

Irretratabilidade – característica de informações que possuem uma identificação do emissor que o autentica como o autor de informações por ele enviadas e recebidas. Sinônimo de não-repúdio.

Diante do que foi exposto alguns conceitos mais aprofundados sobre a segurança da informação são observadas no contexto das organizações e as medidas de segurança que devem ser adotadas diante dos riscos e ameaças apresentados.

3.3 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

A Segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, visando minimizar os danos e maximizar o retorno dos investimentos e as oportunidades de negócio. A Segurança da Informação na Norma NBR ISO/IEC 17799 é caracterizada pela preservação de Confidencialidade, Integridade e Disponibilidade.

Segundo Sêmola(2003) Segurança da Informação pode ser definida como uma área de conhecimento dedicada a proteção de ativos da informação contra acessos não autorizados,

alterações indevidas ou sua indisponibilidade. Pode-se também considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação. Desta forma, estaríamos falando de definição de regras que incidiram sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

Sêmola (2003) apresenta o termo segurança como ambíguo, podendo assumir dupla interpretação, sendo assim, coloca-se que ao utilizar este termo, deve-se ter consciência da ambigüidade, a fim de se identificar o conceito mais apropriado a ser abordado. Por exemplo:

Segurança como " meio " – A segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, a impossibilidade de que agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a comunidade dos negócios.

Segurança como " fim " – A segurança da informação é alcançada por meio de práticas e políticas voltadas a um adequada padronização operacional e gerencial dos ativos, e processos que manipulam e executem a informação.

Na definição de Moreira(2003) a Segurança é a base para dar às empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma a proporcionar confidencialidade, integridade e disponibilidade das informações.

Segundo Dias(2000) quando se pensa em segurança de informações, a primeira idéia que vem à mente é a proteção da mesma, não importando onde ela esteja (no papel, na memória do computador, em um disquete ou trafegando pela linha telefônica). Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado, porém, segurança é um conceito que vai muito além disso. É expectativa de todos que a informação armazenada em um sistema computacional permaneça lá, sem que pessoas não autorizadas tenham acesso a seu conteúdo. Ou seja, é expectativa de qualquer usuário que as informações estejam em local adequado, disponíveis no momento desejado, que sejam

confiáveis, corretas e permaneçam protegidas contra acessos indesejados. Essas expectativas podem corresponder aos objetivos da segurança.

A Segurança da Informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação desta prática, são eles: busca da disponibilidade, confidencialidade e integridade dos seus recursos e da própria informação.

Confidencialidade para Sêmola (2003) é a proteção da Informação de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

Moreira(2001) conceitua a Confidencialidade como a propriedade que visa manter o sigilo, o segredo ou a privacidade das informações evitando que pessoas, entidades ou programas não autorizados tenham acesso às mesmas. A perda de confidencialidade existe quando pessoas não autorizadas obtêm acessos às informações confidenciais e passam a revelar a terceiros.

Segundo Dias(2000) Confidencialidade consiste em proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação, isto é, as informações e processos são liberados apenas a pessoas autorizadas.

O conceito de Integridade de dados para Sêmola(2003) é: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

Integridade para Dias(2000) consiste em evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. O conceito de dados nesse objetivo é mais amplo, englobando dados, programas, documentação, registros. O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas. Em termos de comunicação de dados, integridade restringe-se à detecção (e subseqüente correção) de alterações (deliberadas ou acidentais) nos dados transmitidos. A integridade de dados também é um pré-requisito para outros aspectos de segurança. Enquanto o objetivo da confidencialidade está mais voltado à leitura de dados, a integridade preocupa-se mais com a gravação ou alteração de dados. Consiste em proteger a informação contra qualquer tipo de alteração sem a autorização explícita do autor da mesma.

Para Moreira(2001) Integridade de dados consiste em proteger a informação contra qualquer tipo de alteração sem a autorização explícita do autor da mesma.

A perda de integridade, é a alteração ou modificação de conteúdo ou do status, remoção da informação, alteração do conteúdo de um e-mail, programas, etc. Pode ser intencional ou não. Independente da forma ou motivo, a questão é: Quanto a empresa vai gastar para recuperar ou reconstituir os dados?

Na verdade, quando uma empresa perde a informação, além do valor desta, a empresa deverá levar em conta o custo de sua re-criação, substituição ou até mesmo de sua restauração. O problema da perda da integridade das informações pode ser catastrófico para qualquer empresa.

Com relação a Disponibilidade, Moreira(2001) conceitua como os esforços da empresa em proporcionar a disponibilidade dos seus recursos, sejam eles sistemas, informações ou processos, ocorrem quando estes necessitam de acesso contínuo e ininterrupto, ou seja, a informação deve estar disponível para a pessoa certa e no momento em que ela precisar. Portanto, a empresa deve identificar as soluções existentes voltadas a esta necessidade.

Sêmola(2003) simplifica a definição de Disponibilidade como toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Segundo o autor Sêmola (2003), informação é um conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processo comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolva, por exemplo, a transferência de valores monetários). A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvo de proteção da segurança da informação.

Complementando os conceitos de Segurança da Informação, alguns elementos devem ser definidos:

Ativos

Ativo

Para Moreira(2001), ativos são elementos que manipulam direta ou indiretamente, uma informação, inclusive a própria informação dentro da organização e que devem ser protegidos contra ameaças para que o negócio funcione corretamente. Uma alteração, destruição, erro ou indisponibilidade de algum dos ativos podem comprometer os sistemas e, em decorrência, o bom funcionamento das atividades de uma empresa. Portanto, um dos passos da Análise de Risco é o de identificar todas as coisas que podem ser afetadas por um problema de segurança e que, neste caso, precisam ser protegidas.

Ativo para Sêmola(2003) é todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

O termo ativo possui esta denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada.(NBR ISO/IEC 17799).

Risco

Todos os dias nos deparamos com riscos. Alguns com maior, outros com menor grau de periculosidade. Mas afinal, o que vem a ser um risco? Um risco existe quando uma ameaça, com potencial para causar algum dano, possui um vulnerabilidade correspondente com alto índice de probabilidade de ocorrência no ambiente computacional e um baixo nível de proteção. Para Moreira(2001), Risco pode ser entendido como tudo aquilo que pode afetar os negócios e impedir o alcance dos objetivos, corresponde a um grau de perda ou a possibilidade de um impacto negativo para o negócio.

Para Sêmola(2003), risco pode ser considerado como probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios.

Os níveis de riscos são indicativos importantes para a empresa. Portanto é muito importante que a empresa tenha claramente o seu nível de risco desejado, para que possa ter uma visão da priorização dos investimentos de segurança.

Vulnerabilidade

Segundo Moreira(2003), a vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações. Condição causada, muitas vezes, pela ausência ou ineficiência das medidas de proteção utilizadas com o intuito de salvaguardar os bens da empresa.

Todos ambientes são vulneráveis, partindo do pressuposto de que não existem ambientes totalmente seguros, muitas vezes, as medidas de segurança implementadas pelas empresas possuem vulnerabilidades. Neste caso, a ineficiência de medidas de proteção é uma das causas, em função de configurações inadequadas. A identificação de vulnerabilidades que podem contribuir para a ocorrência de incidentes de segurança é um aspecto importante na identificação de medidas adequadas de segurança.

Os riscos não podem ser determinados sem o conhecimento de até onde um sistema é vulnerável, contribuindo então para a ação das ameaças. Em um processo de análise de segurança, deve-se identificar os processos críticos vulneráveis e saber se os riscos a ele associados são aceitáveis ou não.

O nível de vulnerabilidades decai, à medida em que são implementados controles e medidas de proteção adequadas, diminuindo também os riscos para o negócio. Pode-se dizer que os riscos estão ligados ao nível de vulnerabilidades que o ambiente analisado possui, pois para se determinar os riscos, as vulnerabilidades precisam ser identificadas.

Vulnerabilidade para Sêmola(2003), é a fragilidade presente ou associada a ativos que manipulam e/ou processam informações que ao serem exploradas por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade. O autor apresenta alguns exemplos de vulnerabilidade:

Físicas – Instalações prediais fora do padrão; sala de CPD mal planejada; falta de extintores, detectores de fumaça e de outros recursos de combate a incêndio em sala com armários e fichários estratégicos; risco de explosão, vazamento ou incêndio.

Naturais – Computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura.

Hardware – falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.

Software – Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamentos de informações, perda de dados ou indisponibilidade do recurso quando necessário.

Mídias – Discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.

Comunicação – Acesso não autorizado ou perda de comunicação.

Humanas - Falta de treinamento, compartilhamento de informações confidenciais, ausência de execução de rotinas de segurança, erros ou omissões; ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras.

As vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são ameaças.

As ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidade e, consequentemente, causando impactos aos negócios de uma organização. Sêmola(2003), classifica as ameaças quanto a sua intencionalidade, e podem ser divididas nos seguintes grupos.

Naturais – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição.

Involuntárias – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia.

Voluntárias – Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Para Moreira(2001) as ameaças são fatores/ocorrências que podem violar sistemas e causar incidentes de segurança e, dessa forma, danos aos negócios da empresa. Comenta que as ameaças crescem em virtude das novas tecnologias e da Internet terem criado um novo universo de possibilidades. Dentro deste contexto, prover um nível de segurança aceitável à altura das necessidades dos negócios da empresa é uma importante ação contra as inúmeras ameaças existentes. Conhecer as ameaças potenciais ao ambiente da empresa é fundamental, quando se fala de investimento na área de segurança, é recomendável saber como identificar soluções adequadas, para atingir os seus objetivos e necessidades do negócio

Sem essa análise, a probabilidade de se perder tempo e recursos financeiros é grande. Em alguns casos, as ações implementadas podem não reduzir de forma adequada os atuais níveis de risco, fazendo com que continuem expostas a inúmeras ameaças e com a falsa sensação de segurança, mesmo após todo o investimento efetuado.

Diante do exposto Moreira(2001) conclui que todos os ambientes computacionais são vulneráveis a incidentes de segurança e, portanto, a ação de ameaças. Alguns com maior, outros com menor probabilidade de ocorrência, devido ao grau de eficiência das medidas de segurança implementadas. O autor classifica as ameaças como os tipos mais comuns:

Ameaças intencionais – Variam desde o uso de técnicas e ferramentas simples até os ataques mais sofisticados. Realização de uma exploração de uma vulnerabilidade intencional.
Ameaças Acidentais – Não estão associadas à intenção premeditada, ocorrem por mero desconhecimento, falta de atenção ou treinamento.
Ameaças Passivas – Não resultam em qualquer modificação nas informações contidas em um sistema, em sua operação ou em seu estado.
Ameaças Ativas – Envolvem a alteração da informação ou modificação em seu estado ou operação, como exemplo, o virus eletrônico; funcionário insatisfeito; software pirata na empresa; divulgação de senhas; espionagem industrial; sabotagem.

Outros exemplos de ameaças, cada uma com sua probabilidade de ocorrência em função da região, localização, tipo de negócio, tipo de equipamento, entre outros, serão apresentados a seguir.

Catástrofes – incêndio; alagamento; explosão; desabamento parcial ou total do prédio; sobrecarga na rede elétrica ou relâmpagos; terremotos; guerras; falha na energia elétrica; pane nos equipamentos de comunicação; pane nos sistemas de informações; pane na rede de computadores; problemas no Sistema Operacional.

Comportamento anti-social – paralisações e greves; piquetes; invasões; alcoolismo e drogas; falta de espírito de equipe; inveja pessoal/profissional; rixas entre funcionários.

Ação criminosa - furtos e roubos; fraudes; sabotagem; terrorismo; atentados; sequestros; espionagem industrial; engenharia Social.

Segundo Moreira(2001) as ameaças podem ter duas origens: interna e externa, mas qual a real importância de se saber a origem das ameaças? Serve para que se possa realizar medidas de proteção adequadas, porque muitas vezes, a causa pode estar dentro da organização e neste caso deve-se reforçar os avisos e os treinamentos para que haja mudança na maneira de pensar e agir dos funcionários.

As ameaças de origem interna estão presentes no dia-a-dia das organizações independente de estarem conectadas ou não à Internet. Sua existência é prejudicial para os negócios, cada qual com o seu grau de periculosidade, podendo ser desde um procedimento inadequado de um funcionário até uma ação intencional, com o intuito de interromper a execução de um processamento em determinado sistema.

Alguns exemplos de ameaças internas:

- Contaminação por vírus de computador através de um simples disquete;
- Pirataria de software;
- Incêndios;
- Funcionários mal treinados para a utilização de sistemas críticos;
- Instalação elétrica sem aterramento ou aterramento inadequado;

- Funcionários de empresa terceirizada não familiarizados com a política de segurança da organização;
- Divulgação das senhas de funcionários;
- Falta de definição clara de responsabilidades;
- Uso indevido dos serviços de Internet em nome da empresa;
- Falta de rotina/procedimentos para *Backup e Recovery*;
- Falta de procedimento de Contingência.

As ameaças de origem externa representam todos os ataques oriundos de fora do ambiente da organização, com o objetivo de explorar as vulnerabilidades de um determinado sistema computacional, para uma finalidade qualquer. Representam um alto grau de participação nas pesquisas sobre ataques a sistemas computacionais. Com o advento da Internet e das práticas do comércio eletrônico, o número e as formas de ataques aumentam a cada dia. Mas quem são os invasores e quais as razões para os ataques ?

Uma análise profunda da Organização Social Computer Underground demonstra que alguns problemas de ordem social, econômica e política, proporcionam cada vez mais a proliferação de agentes do mundo inteiro a se manifestarem. Existem vários motivos que encorajam pessoas a utilizarem seus conhecimentos com ferramentas e técnicas para burlarem esquemas de segurança computacional. São eles: ganhos financeiros; vingança; necessidade de aceitação ou respeito; idealismo; curiosidade ou busca de emoção; anarquia; aprendizado; ignirância; espionagem industrial.

O termo genérico para identificar quem realiza o ataque em um sistema computacional é *hacker*. Essa generalização, porém, tem diversas ramificações, pois os ataques aos sistemas apresentam objetivos diferentes e o seu sucessso depende do grau de segurança de seus alvos e da consequente capacidade do *hacker* em atacá-los. Isso significa que os sistemas bem protegidos são mais difíceis de sofrerem ataques, o que faz com que uma maior habilidade seja exigida para a concretização dos ataques.

Os *hackers*, segundo Nakamura(2003), por sua definição original, são aqueles que utilizam seus conhecimentos para invadir sistemas, sem o intuito de causar danos às vítimas, mas como um desafio as suas habilidades. Eles invadem os sistemas, capturam ou modificam arquivos para provar sua capacidade e depois compartilham suas proezas com os colegas. Não

têm a intenção de prejudicar, mas sim de apenas demonstrar que conhecimento é poder. Exímios programadores e conhecedores dos segredos que envolvem as redes e os computadores, eles geralmente não gostam de ser confundidos com *crackers*.

Moreira(2001) conceitua *hacker* como indivíduo que quer saber mais, investiga extensivamente os sistemas para detectar más comfigurações e buracos nas configurações que permitem ganhar acesso aos sistemas. Ao contrário do cracker, o *hacker*, depois de entrar no sistema, não altera a informação pois esta atitude vai contra a ética dos *hackers*. Só entram no sistema para explorar e se divertir, utilizar recursos ou como ponto de passagem.

O termo *hacker* já se encontra associado à pirataria digital, ao invasor de sistemas e criminoso. Segundo o "The New Hacker's Dictionary"(http://www.ccil.org/jargon), o *hacker* é um pessoa que gosta de explorar os detalhes dos sistemas e descobrir como obter o máximo de sua capacidade, em oposição à maioria dos usuário, que preferem aprender apenas o mínimo necessário.

Seguindo o vocabulário do meio, o *hacker* que se dedica a roubar arquivos confidenciais ou destruir dados recebe o nome *cracker*. Esses sim são perigosos e muito confundidos pelas pessoas que usam o termo hacker no lugar de *cracker*.

Moreira(2001) define *cracker* como *hacker* mal intencionado, isso porque eles invadem computadores e *homepages*, não por divertimento, mas por interesses próprios para desviar a conexão para outra página(concorrente, por exemplo), tirar algum serviço do ar. São usuários que usam seus conhecimentos para destruir sistemas e trapacear com novos usuários e o autor afirma que todos os *crackers* são *hackers*, mas nem todos os *hackers* são *crackers* e que ambos têm objetivos de aprendizagem comuns, mas intenções diferentes.

Com o advento da Internet, porém, os diversos ataques pelo mundo foram atribuídos a *hackers*, mas eles refutam essa idéia, dizendo que *hackers* não são *crackers*. Os *crackers* segundo Nakamura(2003) são elementos que invadem sistemas para roubar informações e causar danos às vítimas. O termo *cracker* também é uma denominação utilizada para aqueles que decifram códigos e destroem proteções de *softwares*.

Atualmente, no entanto, com o crescimento da Internet e a consequente facilidade em se obter informações e ferramentas para ataques, mudou a definição de *hacker*. A própria imprensa mundial tratou de modificar esse conceito. Agora, qualquer incidente de segurança é atribuído a *hackers*, em seu sentido genérico. A palavra *cracker* não é mais vista, a não ser como *cracker* de senhas, que é um *software* utilizado para descobrir senhas ou decifrar mensagens cifradas.

É importante lembrar, que não são apenas os *hackers* que causam problemas de segurança nos sistemas. Os usuários, autorizados ou não, mesmo sem intenções malévolas, também podem causar danos aos serviços de redes, por meio de seus erros e de sua própria ignorância.

Após a discussão sobre as ameaças e as vunerabilidades, Moreira (2001) conclui que cada vulnerabilidade existente pode ser explorada por ameaças e podem permitir a ocorrência de determinados incidentes de segurança.

Incidentes de Segurança

Segundo Sêmola(2003) incidente é um fato decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando a perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Gera impactos aos processos de negócio da empresa, sendo ele o elemento a ser evitado em uma cadeia de gestão de processos e pessoas.

Segundo Moreira(2001), um incidente de segurança é qualquer evento que prejudica o bom andamento dos sistemas, das redes ou do próprio negócio. O incidente pode ser resultado de uma violação de segurança concretizada, um acesso não autorizado a determinadas informações confidenciais ou até mesmo um site tirado do ar pela ação de um *hacker*.

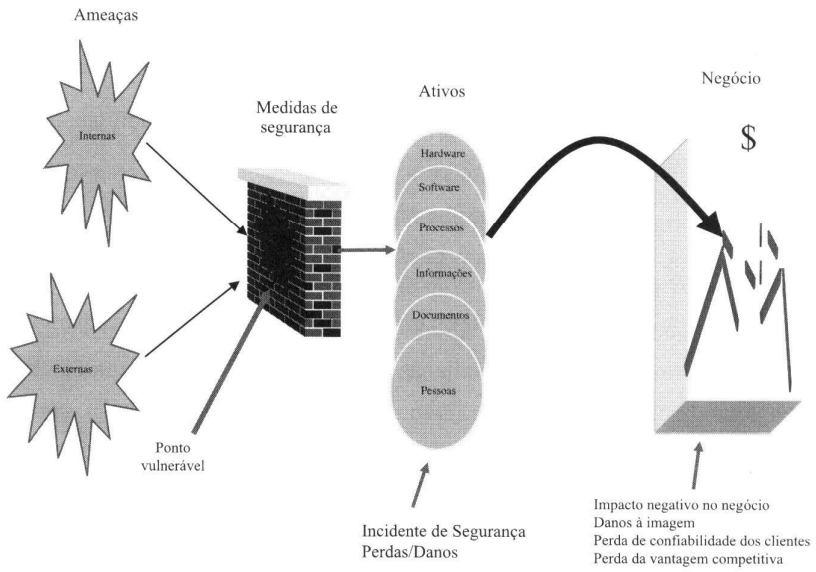


FIGURA 3 - Incidente de segurança.

Fonte: Moreira(2001)

Antigamente, tínhamos os *mainframes*(computadores de grande porte) isolados, os incidentes de segurança possuíam como origem os funcionários internos e tinham como causa o descontentamento, vingança ou qualquer outro motivo. Hoje, com o advento da Internet, temos as facilidades para transações comerciais fraudulentas e espionagem industrial.

O fato é que o número de usuários da rede interna de uma empresa é muito menor do que as milhões de pessoas conectadas diariamente na Internet, mas, conforme inúmeras pesquisas, as maiores ocorrências referentes a incidentes de segurança ainda estão dentro das empresas.

Os incidentes de segurança ocorrem pela ação efetiva de uma determinada ameaça através de uma vulnerabilidade encontrada. Logo, pode-se afirmar que os incidentes de segurança somente podem ser concretizados quando existem ambientes propícios, ou seja, vulnerabilidades. (MOREIRA 2001).

RELAÇÃO ENTRE VULNERABILIDADE, AMEAÇA E INCIDENTE DE SEGURANÇA

Cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança. Por estar numa condição vulnerável, pessoas mal intencionadas podem explorar as fraquezas de uma má configuração de um *firewall* ou de uma versão antiga do *kernel* de um Sistema Operacional, e entrar na rede interna de uma empresa para copiar informações e apagar outras. Dessa forma Moreira(2001) conclui que as vulnerabilidades são as principais causas das ocorrências de incidentes de segurança, conforme apresenta a Figura 4.

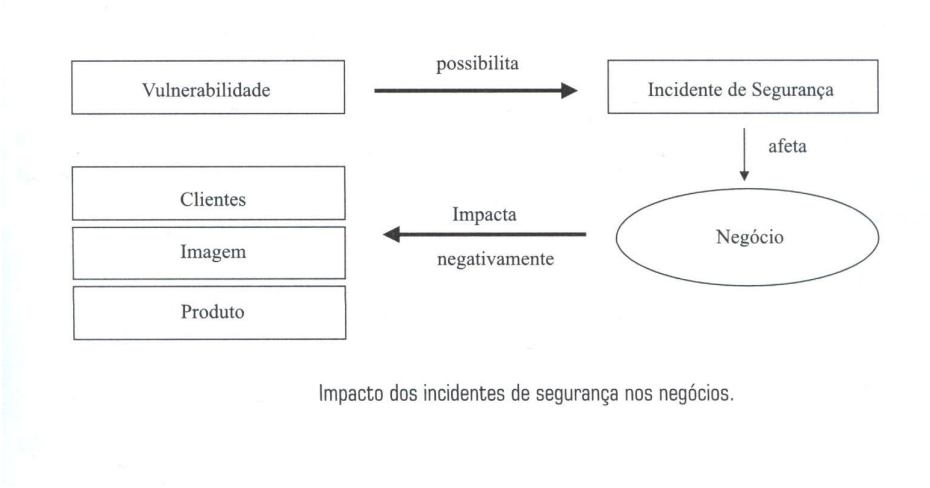


FIGURA 4 - Incidente de segurança.

Fonte: Moreira (2001)

Devido a inúmeras vulnerabilidades em redes conectadas à Internet, muitos incidentes têm marcado presença no dia-a-dia das empresas. A Figura 5 demonstra que são vários os tipos de ocorrências. Desde as mais simples até a parada de um site. Uma invasão que explora uma vulnerabilidade pode ocasionar as seguintes ocorrências:

- documentos confidenciais divulgados na Internet;
- funcionários divulgando material pornográfico;
- contas e senhas roubadas para posterior utilização;
- linhas de comunicação grampeadas e informações sigilosas da empresa ficam comprometidas;
- Servidores podem entrar em pane através do recebimento de inundação de pacotes.

Os danos e as perdas causados por um incidente de segurança existem também em decorrência dos pontos vulneráveis em seu ambiente computacional.

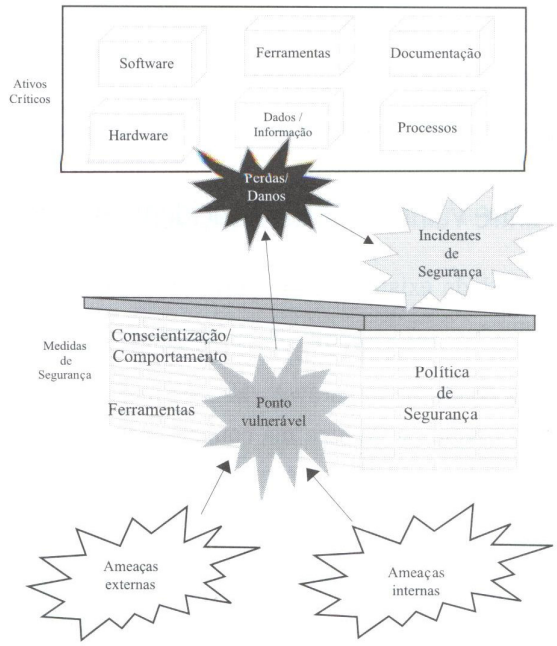


FIGURA 5 Relação entre vulnerabilidade e incidente de segurança.

Fonte: Moreira(2001)

Toda ameaça, quando concretizada, causa uma perda ou um dano a algum recurso, não representa perda concreta, mas quando existe uma vulnerabilidade relacionada a ela e a situação propicia, um incidente ocorre. Cabe a empresa avaliar o impacto negativo causado para os seus negócios.

Pode-se dizer que, para cada ameaça, tem-se vários incidentes de segurança a eles associados. Por exemplo: Um vírus eletrônico quando infecta um computador, pode causar:

- Lentidão na máquina afetada;
- Corrupção de um ou mais arquivos;
- Perda de informações
- Parada de um sistema;
- Atrasos na entrega de um serviço devido à indisponibilidade da informação.

A Internet é um importante veículo de negócios para as empresas e também para a ação de ameaças. Independente das medidas de segurança adotadas pela empresa, as ameaças existem, e não só na Internet, mas também no ambiente interno da empresa. É fundamental entendê-las para que seja possível propor medidas de segurança voltadas a eliminar a causa do problema.

As ameaças se tornam potencialmente perigosas a partir do momento em que existam vulnerabilidades nestes ambientes, podendo causar danos e perdas.

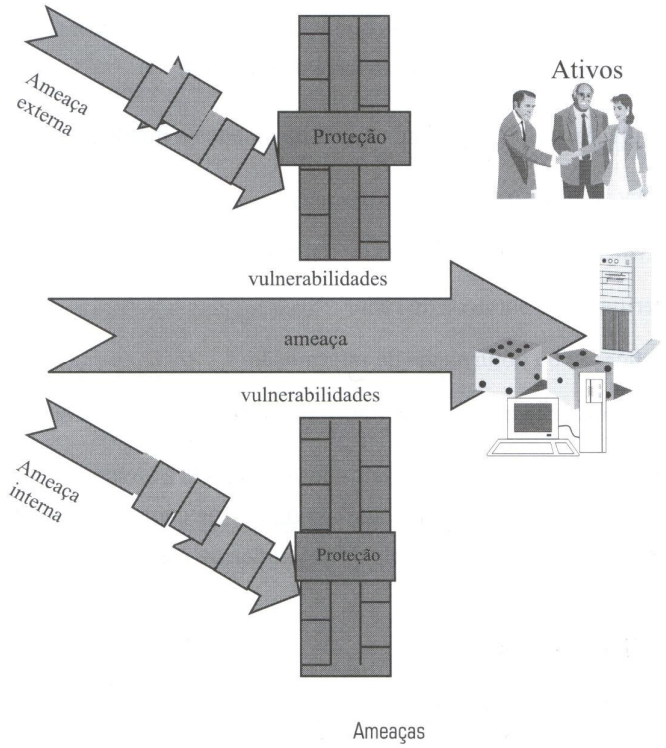


FIGURA 6 - AMEAÇAS.

Fonte:. Moreira(2001)

Algumas ameaças têm uma relação direta com aspectos econômicos. Em situações de recessão econômica e aumento de competitividade é comum termos a sensação de que valores morais e éticos ficam um pouco em baixa e cresce um aumento da competitividade. Isto leva, muitas vezes, a conflitos de interesses, sendo estes um grande motivador para eventuais

problemas de segurança, como tentativas de espionagem e obtenção de informações privilegiadas, em benefício próprio ou de terceiros.

Cada ambiente computacional possui a sua realidade e não se pode dizer que uma determinada ameaça é perigosa de fato e que afeta o ambiente computacional de todas as empresas, uma vez que existem: ambientes computacionais diferentes, níveis de informatização diferentes e exigências de segurança também diferentes.

COMO SURGEM OS RISCOS?

Segundo Caruso(1999) após o advento dos equipamentos de processamento de informações e também dos modernos computadores eletrônicos, a concentração em um único lugar e o grande volume de informações passaram a ser um problema sério para a segurança. Os riscos agravaram-se após o aparecimento dos microcumputadores, redes e Internet e a disseminação da cultura de informática em segmentos expressivos da sociedade.

As organizações, cada vez mais, tornam-se dependentes de informações armazenadas em computadores. Aproveita-se a grande velocidade e a capacidade de cruzamento de informações que os computadores possuem para obter benefícios como tomada de decisões rápidas ou mudança rápida de estratégia e/ou tática. Mas, a mesma facilidade proporcionada pelos computadores também implica em um alto risco de violação, pois o mesmo programa usado para emitir relatório de projeção de vendas, destinado ao diretor de marketing pode ser usado por um espião para emití-lo para o diretor de marketing do concorrente.

Nem todos os riscos relacionados com o processamento de informações surgiram com o advento dos computadores, entretanto, estes contribuíram muito para o seu agravamento. Esses riscos são decorrentes principalmente de fatores que, em maior ou menor grau, aparecem em todas as organizações humanas e, de forma geral, não dependem do tipo e tamanho dos equipamentos.

Todos os ativos da empresa estão sujeitos a vulnerabilidade em maior ou menor escala e, proporcionam riscos para a organização causada, muitas vezes, por falhas nos seus controles. Logo, pode-se dizer que os riscos surgem em decorrência da presença dessas fraquezas.

Por outro lado, Moreira(2001) afirma que as ameaças exploram as vulnerabilidades existentes devido às falhas de configuração ou inexistência de medidas de proteção adequadas. Neste caso, os danos causados pela ação das mesmas causam impactos negativos no negócio aumentando ainda mais os riscos.

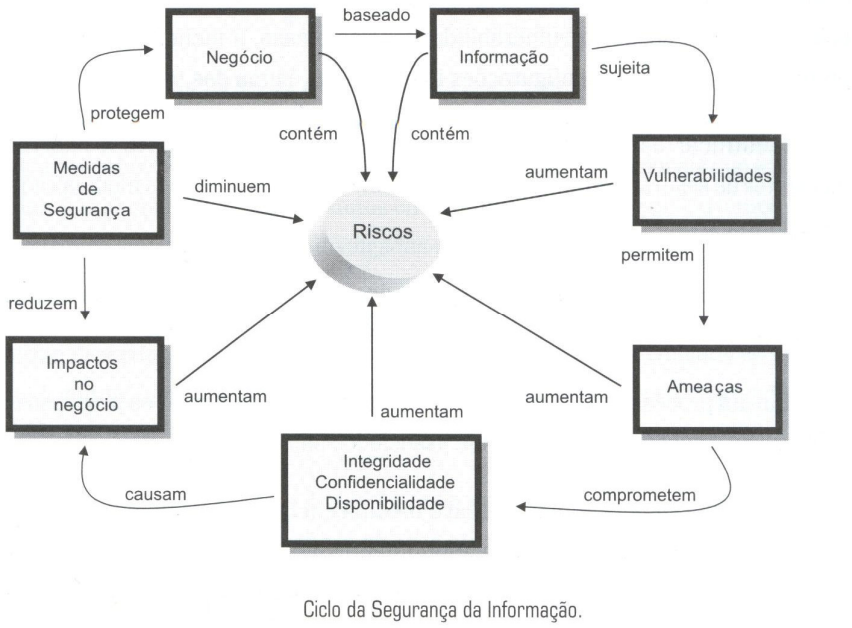


FIGURA 7 - Ciclo de segurança da informação.

Fonte: Moreira (2001)

Em contrapartida, medidas de proteção adequadas protegem os ativos, diminuindo então os riscos. A Figura 7 apresenta os fatores que contribuem para a existência e diminuição dos riscos.

Equação do Risco

Cada negócio, independente de seu segmento de mercado e seu *core business*, possui dezenas, talvez centenas, de variáveis que se relacionam direta e indiretamente com a definição do seu nível de risco. Identificar estas variáveis passa a ser a primeira etapa do desafio.

O risco é a probabilidade de que agentes, que são as ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos nos negócios. Estes impactos são limitados por medidas de segurança que protegem

os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

$$R_{\text{RISCO}} = \frac{V_{\text{VULNERABILIDADES}} \times A \times I_{\text{IMPACTOS}}}{M_{\text{MEDIDAS DE SEGURANÇA}}}$$

FIGURA 8 - Diagrama da equação do risco de segurança da informação.

Fonte: Sêmola(2003)

É fundamental que todos tenham a consciência de que não existe segurança total e, por isso, devemos estar bem estruturados para suportar mudanças nas variáveis da equação, reagindo com velocidade e ajustando o risco novamente aos padrões pré-especificados como ideal para o negócio.

Diante disso, Sêmola(2003) conclui que não há um resultado R (risco) igual para todos. Sempre será necessário avaliar o nível de segurança apropriado para cada momento vivido pela organização, como se tivéssemos de nos pesar em períodos regulares para definir a melhor dose de ingestão calórica (dose de segurança) do período, a fim de buscar aproximação com o peso ideal (nível de risco) para o momento. A análise de risco possibilita ajuda na definição dessas doses.

Realizar uma análise de segurança já é prioridade para a grande maioria das organizações, o que vem demonstar a percepção da necessidade de diagnosticar os riscos. Contudo, ainda há dúvidas no entendimento do que é uma análise de risco de verdade.

Voltando aos pilares de sustentação do negócio, vemos iniciativas de mapeamento de vulnerabilidades concentradas puramente nos ativos tecnológicos, ou seja, instrumentos destinados a analisar e identificar falhas de computadores, redes e sistemas. Evidente que são atividades importantes mas não suficientes para, isoladamente, diagnosticar com precisão os

reais riscos que envolvem a operação da organização. Muitos outros pilares convivem com os pilares tecnológicos e, dependendo da natureza do negócio, estes podem ser ainda mais relevantes para a sustentação. Veja figura 9.

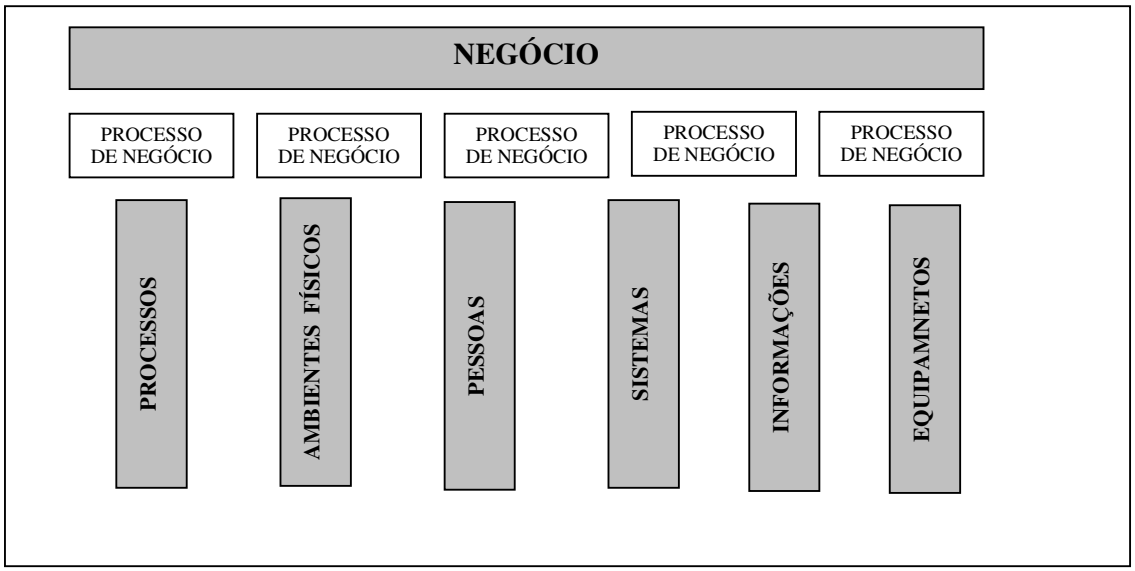


FIGURA 9 - Relação de dependência entre ativos, processos de negócios e o próprio negócio

Fonte:Sêmola(2003)

Há uma quebra de paradigma ao compreender que os riscos de uma organização não estão apenas associados ao volume de falhas tecnológicas, à qualificação das ameaças que poderiam explorá-las, ou ainda, aos impactos potenciais. Para Sêmola(2003) diagnosticar o risco envolve a análise de variáveis endógenas que extrapolam os aspectos tecnológicos; portanto, devem considerar, também os aspectos comportamentais dos recursos humanos, os aspectos físicos, legais e, ainda, um grande leque de variáveis exógenas que interferem direta ou indiretamente na proteção do negócio. Uma mudança estratégica, a presença de um novo concorrente ou, ainda, um fator representativo da economia podem provocar oscilações no nível de risco do negócio tirando a organização de seu ponto de conforto.

Diante disso, a Análise de Risco para Sêmola(2003) tem de ser encarada como um instrumento fundamental para diagnosticar a situação atual de segurança da organização, através da sinergia entre o entendimento dos desafios do negócio, o mapeamento das funcionalidades dos processos

de negócio e o relacionamento deles com a diversidade de ativos físicos, tecnológicos e humanos que hospedam falhas de segurança.

Para Moreira(2001) a análise de risco é de fundamental importância e consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios.

Toda análise de risco bem estruturada deve considerar, no mínimo, alguns componentes básicos. Pode-se destacar a identificação de ameaças, vulnerabilidades e o risco como os pilares do processo.

Através da aplicação deste processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado. Proporciona também informações para que se possa identificar o tamanho e o tipo de investimento necessário de forma antecipada aos impactos causados pela perda ou indisponibilidade dos recursos fundamentais.

Como é impossível prever em termos de variedade e freqüência os inúmeros acontecimentos que podem ocorrer, este tipo de análise nos aponta os possíveis perigos e as conseqüências em virtude das vulnerabilidades presentes no ambiente computacional de muitas empresas. Por outro lado, sem um processo deste tipo, não é possível identificar a origem das vulnerabilidades, nem visualizar os riscos.

Alguns fatores podem contribuir para o sucesso do trabalho, a técnica utilizada, a abrangência do mapeamento, possibilitando uma visão maior do negócio e, dos riscos presentes.

Para Moreira(2001) as medidas de segurança não podem assegurar 100% de proteção, e a organização deve analisar a relação custo/benefício sendo necessário encontrar o nível de risco ao qual estará disposta a correr. Este processo deve, no mínimo, proporcionar as seguintes informações:

- Pontos vulneráveis do ambiente;

- Ameaças potenciais ao ambiente;
- Incidentes de segurança causado pela ação de cada ameaça;
- Impacto negativo para o negócio a partir de cada incidente de segurança;
- Medidas de proteção adequadas para impedir ou diminuir o impacto de cada incidente.

Alguns fatores são cruciais e devem ser identificados a fim de mapear todo o negócio da empresa com o intuito de detectar a presença de riscos, são eles: identificar os produtos e bens produzidos que são críticos; os processos produtivos que geram bens e serviços críticos; e os ativos (hardware, software, dados, recursos humanos, instalações, equipamentos) utilizados também nos processos críticos.

Os maiores riscos são aqueles que não vemos ou não conhecemos; assim o conhecimento do ambiente e das suas reais necessidades, tem um papel tão ou mais importante do que as ferramentas que eventualmente venhamos a utilizar.

Moreira(2001) complementa que a Análise de Risco é peça fundamental para a obtenção da qualidade em um Programa de Segurança, pois ajuda a identificar todos os pontos críticos e falhos de proteção em todos os processos, configurações, documentações, enfim, tudo que é considerado valioso para a atividade da Organização.

Esta atividade dará os direcionamentos para a identificação das medidas de segurança necessárias para que o ambiente computacional da empresa possa atingir o nível de segurança desejado. Assim como a segurança é importante para uma Organização, a Análise de Risco e Vulnerabilidades são para um Programa de Segurança Corporativo.

Muitas empresas gastam fortunas investindo em ferramentas caríssimas com a ilusão de que todos os problemas estarão resolvidos. Estas indagações servem para enfatizar a necessidade de um Programa de Segurança Corporativo que vise a avaliação de todo o ambiente computacional como: documentação, licenças de software, manuais, instalação, configuração, controle de acessos, treinamento de usuários. A segurança não se resolve apenas com as tecnologias como *firewall* ou com software antivírus, envolve muito mais recursos da organização, principalmente as pessoas e os processos.

3.4 MEDIDAS DE SEGURANÇA

Segundo Caruso(1999) a finalidade da análise do risco econômico para a seguraça é obter a medida da segurança existente em determinado ambiente. A etapa final da análise de risco é a geração do plano de segurança da organização. Qualquer plano de segurança deve ser montado, sob medida, em função da organização para qual se aplica. O enfoque de segurança para cada caso deve ter como preocupações básicas os ítens listados na figura abaixo, relaciona-se as preocupações básicas com as medidas necessárias para evitar ou impedir as ocorrências:

- Evitar a ocorrência ou sinistro
- Detectar e/ou combater os danos provocados por sinistros.
- Minimizar os danos, recompondo a função original.

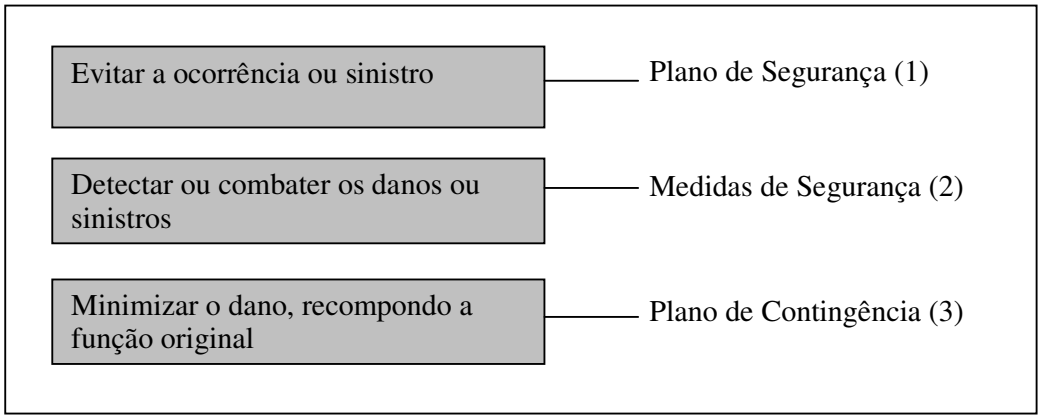


FIGURA 10 - Preocupações básicas de segurança.

Fonte: Caruso(1999)

O Plano de Segurança (1) deve preocupar-se com medidas e procedimentos para que falhas ou sinistros não ocorram e já prover a forma de detecção e combate através das medidas de segurança(2). O plano de contingência(3) deve servir para minimizar os efeitos ou danos ocorridos se o plano de segurança e as medidas de segurança não conseguirem evitá-los.

Caruso(1999) apresenta algumas considerações relacionadas a segurança de ativos de informações, a primeira é a relação custo/benefício. Não se despendem recursos em segurança

que não tenham retorno à altura, isto é, não se gasta mais dinheiro em proteção do que o valor do ativo a ser protegido. Ainda que existam exceções a essa regra, ela é válida em praticamente todos os casos.

O segundo ponto a ser considerado é que, ainda que o principal fator deva ser a análise da relação custo/benefício, a mesma envolve bom senso. Mesmo nos casos em que não é possível uma análise direta da relação custo/benefício, há meios indiretos de se obterem valores bem próximos dos reais.

Com frequência é difícil identificar, segurança sempre segue parâmetros lógicos, mesmo quando reage a situações de risco criadas por seres humanos; os investimentos relacionados com segurança podem facilmente chegar à casa de milhões de dólares com o consequente custo indireto relacionado. A forma mais eficiente de se efetuar a análise custo/benefício é fazer com que os usuários finais de cada sistema de informações avaliem o valor das mesmas para a organização; quem trabalha com as informações no seu dia-a-dia é o mais indicado para fazer a análise de risco.

FIGURA 11 - Fluxo de análise das ameaças e riscos.

Fonte: Caruso(1999)

Segundo Moreira(2001), medidas de segurança são esforços como procedimentos, software, configurações, *hardware* e técnicas empregadas para atenuar as vulnerabilidades com o intuito de reduzir a probabilidade de ocorrência da ação de ameaças e, por conseguinte, os incidentes de segurança.

Sêmola(2003) define medidas de segurança como as práticas, procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma. As medidas de segurança são consideradas controles que podem ter as seguintes características:

Preventivas – Medidas de segurança que tem como objetivo evitar que incidentes venham ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança na instituição. Como exemplo podemos citar as políticas de segurança, instruções e procedimentos de trabalho, especificação de segurança, campanhas e palestras de conscientização de usuários; ferramentas para implementação da política de segurança (*firewall*, antivírus, configurações adequadas de roteadores e dos sistemas operacionais). Este tipo de estratégia possui como foco a prevenção da ocorrência de incidentes de segurança. Todos os esforços estão baseados na preocupação e, por esta razão, o conjunto de ferramentas e/ou treinamentos estão voltados para esta necessidade.

Detectáveis – Medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. Alguns exemplos são: análise de risco, sistema de detecção de instrução, alertas de segurança, câmeras de vigilância, alarmes. É a estratégia utilizada quando se tem a necessidade de obter auditabilidade, monitoramento e detecção em tempo real de tentativas de invasão. Alguns exemplos segundo Moreira(2001): monitoramento de ataques; controle sobre os recursos; controle das atividades de usuários; auditoria em logs, documentação.

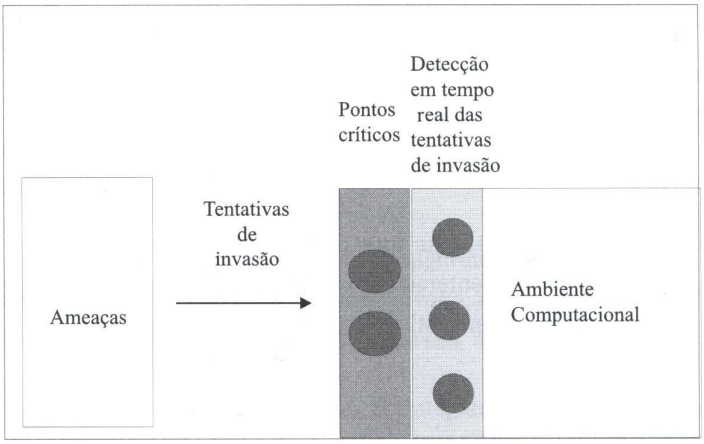


FIGURA 12 - Medidas de Detecção

Fonte: Moreira(2001)

Corretivas – Ações voltadas à correção de uma estrutura tecnológica e humana para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos: equipes para emergências, restauração de *backup,* plano de continuidade operacional, plano de recuperação de desastres.

Muitas das medidas de segurança podem possuir mais uma característica, isto é, um plano de continuidade de negócios, é tanto um ação preventiva (quando da sua criação) quanto uma corretiva (quando da sua aplicação). Logo, esta categorização serve apenas para identificação do foco que o trabalho de segurança está se propondo, quando o mesmo está sendo realizado.

Medidas corretivas segundo Moreira(2001) suplementam uma estratégia de correção/ continuidade, ou seja, propõem mecanismos e procedimentos necessários para a recuperação e a continuidade das operações de uma empresa.

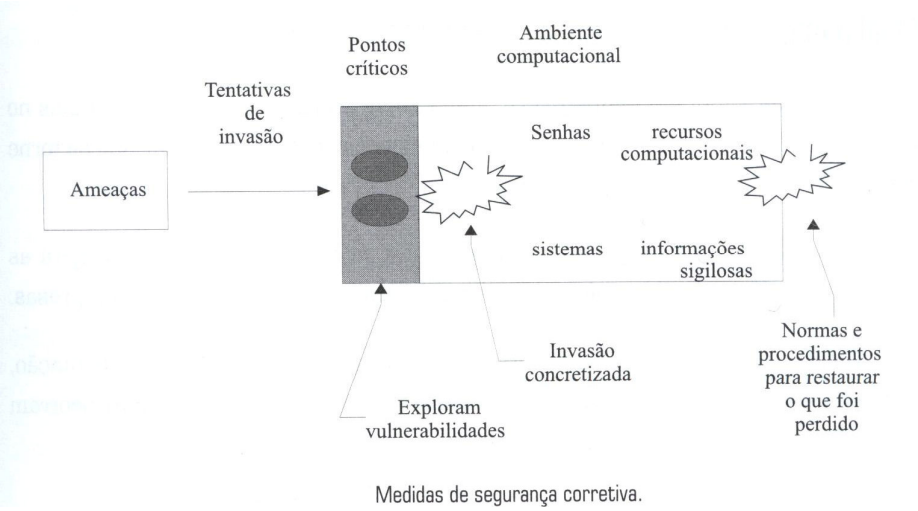


FIGURA 13 – Medidas de Segurança Corretiva

Fonte: Moreira(2001)

3.5 BARREIRAS DA SEGURANÇA

Conceitualmente, diante da amplitude e complexidade do papel da segurança, é necessário estudar os desafios detalhadamente, para tornar mais claro o entendimento de cada uma das fases. Sêmola(2003) conceitua as fases como seis barreiras de segurança, cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos, e por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita interação e integração, como se fossem peças integradas de um jogo. São elas:

Barreira 1: Desencorajar - Esta é a primeira das seis barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Essas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos e humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas, já são efetivos nesta fase.

Barreira 2: Dificultar – Visa complementar a anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Como exemplo, podemos citar os dispositivos de autenticação para acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, senhas e certificados digitais, além da criptografia, firewall entre outros.

Barreira 3: Discriminar - O importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e bancos de dados. Os processos de avaliação e gestão do volume de uso dos recursos, como email, impressora, ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos desse elemento.

Barreira 4: Detectar - Mais uma vez agindo de forma complementar detectar é munir a solução de segurança de dispositivos que sinalizem, alertem e instrumentem os gestores da segurança nas situações de risco. Seja em uma tentativa de invasão, uma possível contaminação por vírus, o descumprimento da política de segurança da empresa, ou a cópia e envio de informações sigilosas de forma inadequada. A exemplo do sistema de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e o sistema de detecção de intrusos, que reduzem o tempo de resposta a incidentes.

Barreira 5: Deter - Representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.

Barreira 6: Diagnosticar - Esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança da informação. Pode parecer o fim, mas é o elo de ligação com a primeira barreira, criando um movimento cíclico e contínuo. Devido a esses fatores esta é a barreira de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa.

Importante notar que um trabalho preliminar de diagnóstico mal conduzido ou executado sem uma metodologia adequada e instrumentos confiáveis que confiram maior precisão ao processo de levantamento e análise de riscos, pode distorcer o entendimento da situação atual de segurança e simultaneamente a situação desejada. Desta forma, aumenta a probabilidade de se dimensionar inadequadamente estas barreiras, distribuindo os investimentos de forma desproporcional e de forma ineficaz. O retorno sobre os investimentos não corresponde às expectativas e a empresa não atinge o nível de segurança adequado à natureza de suas atividades.

Diante da complexidade das questões levantadas, a necessidade de políticas voltadas para o uso adequado de Segurança da Informação vai aprimorar a atuação da organização.

3.6 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança pode ser entendida como sendo um conjunto de normas e diretrizes destinadas à proteção dos ativos da organização. Neste documento deve estar escrito a forma como a organização deseja que seus ativos sejam protegidos, manuseados e tratados.(MOREIRA, 2001).

Nakamura(2003) considera política de segurança como a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. A necessidade de estabelecer uma política de segurança é um fato realçado unanimemente em recomendações provenientes tanto do meio militar(como o Orange Book do Departamento de Defesa dos Estados Unidos) como do meio técnico (como o Site Security Handbook [Request for Coments – RFC] 2196 do Institute Engineering Task Force, IETF) e, mais recentemente, do meio empresarial (Norma Internacional Standardization Organization/Internacional Electricaltechnical Commission (ISO/IEC) 17799).

Seu desenvolvimento é o primeiro e o principal passo da estratégia de segurança das organizações. É por meio dessa política que todos os aspectos envolvidos na proteção dos recursos são definidos e, portanto, grande parte do trabalho é dedicado à sua elaboração e ao

seu planejamento. No entanto, vê-se que as maiores dificuldades estão mais na implementação do que no planejamento e elaboração.

A política de segurança trata dos aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos e os negócios, além da legislação local. É com base nessa política de segurança que as diversas normas e os vários procedimentos devem ser criados.

Além de seu papel primordial nas questões relacionadas com a segurança, a política de segurança, uma vez fazendo parte da cultura da organização, tem uma importante função como facilitadora e simplificadora do gerenciamento de todos os seus recursos. De fato, o gerenciamento de segurança é a arte de criar e administrar a política de segurança, pois não é possível gerenciar o que não pode ser definido.

À medida que o tempo passa, aumenta-se a dependência das organizações no uso de computadores e sistemas. Esta dependência é necessária para que se torne eficiente e a partir daí, gere mais negócios. A informação passa a ter um valor estratégico e tático para a organização e passa a ser considerado o ativo mais valioso para muitas empresas.

Diante deste cenário, a política de segurança passa a ter uma importante função, visando a proteção dos ativos da organização para que os negócios não sejam interrompidos e ocorram dentro de um ambiente harmônico e seguro, podendo ser entendida como um conjunto de normas e diretrizes destinadas à proteção dos ativos da organização.

O objetivo de qualquer política de segurança segundo Moreira(2001) é o de definir as expectativas da organização em relação ao uso dos seus recursos, estabelecendo procedimentos com o intuito de prevenir e responder a incidentes relativos à segurança. Uma boa política de segurança da informação deve ser composta por regras claras, práticas e sintonizadas com a cultura e o ambiente tecnológico da empresa. Deve proteger as informações confidenciais e também motivar as pessoas que as manuseiam, mediante a conscientização e envolvimento de todos. Garantir a segurança corporativa é um grande desafio que passa por todas as pessoas envolvidas direta ou indiretamente.

Segundo Sêmola(2003) a política de segurança estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a organização, portanto, a política deve ser personalizada.

Com o propósito de fornecer orientação e apoio a decisões de gestão de segurança, a política tem um papel fundamental e assume grande abrangência. Para Sêmola(2003), é subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional.

As diretrizes têm papel estratégico, precisam expressar a importância que a organização dá para a informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança na sua cultura organizacional.

É notória a necessidade do envolvimento da alta direção, refletida pelo caráter oficial com que a política é comunicada e compartilhada junto aos funcionários. Este instrumento deve expressar as preocupações dos executivos e definir as linhas de ação que orientarão as atividades táticas e operacionais.

Com caráter tático, as normas são o segundo nível da política, detalhando situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações. Baseado em ordens de grandeza, podemos estimar 10 a 20 diretrizes em organizações de qualquer porte, mas têm de multiplicar este número por 100 ou mais para estimar o volume de normas aplicáveis. Este volume tende a ser proporcional ao porte da empresa, à heterogeneidade de seus ativos físicos, tecnológicos e humanos,e, ainda, ao grau de detalhamento necessário para levar a organização a operar sob o nível de risco adequado.

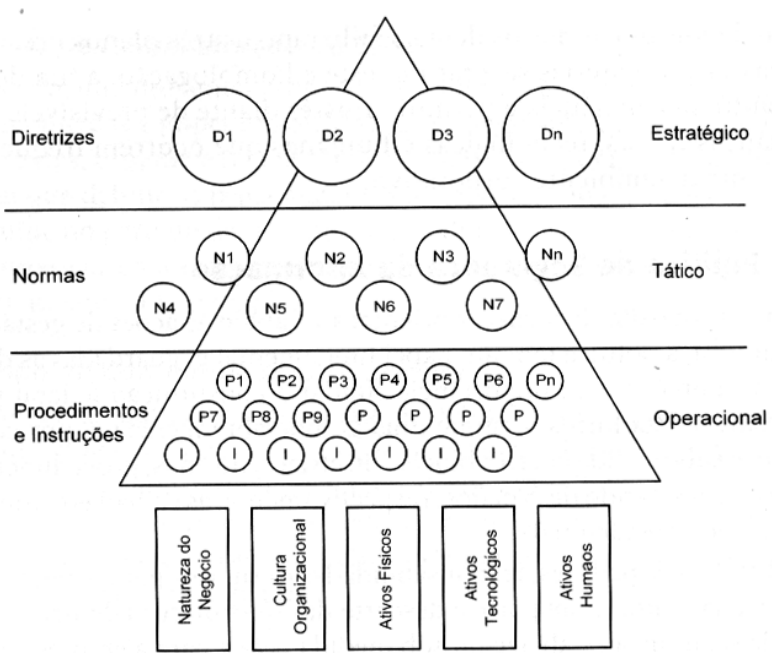


FIGURA 14 - Diagrama de conceito dos componentes da política e seus pilares de sustentação.

Fonte: Sêmola(2003).

Critérios normatizados para a admissão e demissão de funcionários; criação e manutenção de senhas; descarte de informação em mídia magnética; desenvolvimento e manutenção de sistemas; uso da Internet; acesso remoto; uso de notebook; contratação de serviços de terceirizados; e a classificação da informação são bons exemplos de normas de uma típica política de segurança.

Em especial, a norma de classificação da informação é fator crítico de sucesso porque assume a responsabilidade por descrever os critérios necessários para sinalizar a importância e o valor das informações, premissa importante para a elaboração de praticamente todas as demais normas. Não há regra preconcebida para estabelecer esta classificação, mas é preciso entender o perfil do negócio e as características das informações que alimentam os processos e circula no ambiente corporativo para que os critérios sejam personalizados.

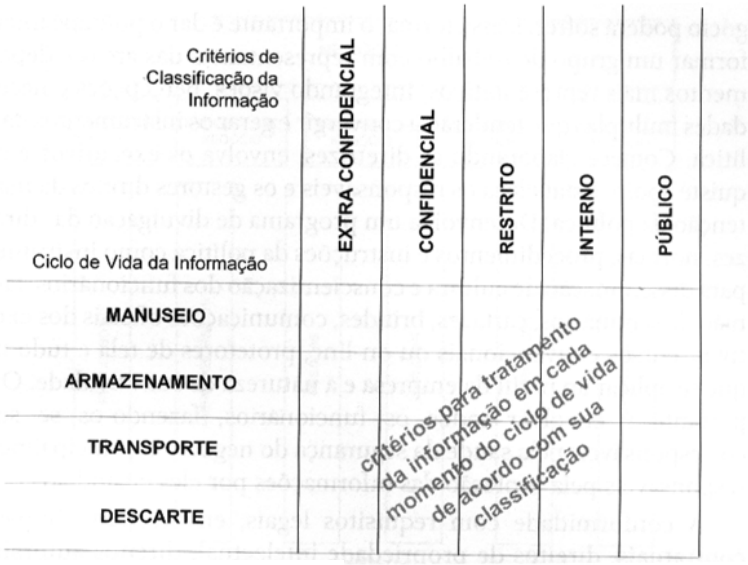


FIGURA 15 - Ilustração da relação entre a classificação e tratamento definido na política para o ciclo de vida

Fonte:Sêmola(2003).

Procedimentos e instruções devem estar presentes na política em maior quantidade por seu perfil operacional, onde é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso das informações. Como exemplo: enquanto a diretriz orienta estrategicamente para a necessidade de salvaguardar as informações classificadas como confidenciais e a norma define que estas devem ser criptografadas em tempo de envio de e-mail, o procedimento e a instrução específica para esta ação tem de descrever os passos necessários para executar a criptografia e enviar o e-mail. A natureza detalhista deste componente da política pressupõe a necessidade de manutenção ainda mais freqüente.

Entre as diretrizes para uma política de segurança Moreira(2001) apresenta orientações:

- Ser flexível com relação às mudanças necessárias;
- Ser simples na comunicação;
- Ser objetiva e curta;
- Conter regras simples;
- Ser consistente, de acordo com as outras políticas da corporação;
- Ser aplicável utilizando os equipamentos e tecnologias de rede existentes;
- Estar de acordo com as leis locais, estaduais e federais;
- Ser facilmente acessível a todos os membros da Organização;

- Definir um conjunto claro de metas de segurança;
- Definir sobre que circunstâncias determinado item é aplicável;
- Definir regras e as responsabilidades dos membros da Organização com respeito a cada uma das diretivas definidas;
- Descrever ou associar as conseqüências do não cumprimento da Política descrita, preferencialmente com punições já existentes na empresa;
- Indicar informações para contato, mais detalhes e esclarecimentos de qualquer uma das diretivas;
- Definir as expectativas de privacidade dos usuários;
- Incluir a responsabilidade sobre a definição de temas não especificamente definidos para a resolução de impasses.

O documento da política deverá ser aprovado pela direção, publicado e comunicado a todos da organização. Deve ser revisada regularmente, e nos casos de mudanças significativas, ser adequadamente ajustada.

Diante disso, já é possível perceber como é complexo desenvolver e, principalmente, manter atualizada a política de segurança da informação com todos os seus componentes. Esta percepção torna mais latente se considerar o dinamismo do parque tecnológico de uma organização e, ainda, as mudanças previsíveis e imprevisíveis que o negócio poderá sofrer. Dessa forma, o importante é iniciar o processo formando um grupo de trabalho com representantes das áreas e departamentos mais representativos, interagindo visões, percepções e necessidade múltiplas que tendem a convergir e gerar os instrumentos da política.

A conformidade com requisitos legais, envolvendo obrigações contratuais, direitos de propriedade intelectual, direitos autorais de *software* e todas as possíveis regulamentações que incidam sobre o negócio da organização devem ser respeitados e, portanto, deve ser a linha de conduta da construção da política de segurança.

4. A NORMA DE SEGURANÇA DA INFORMAÇÃO

A evolução da Segurança da Informação tem acompanhado a evolução tecnológica englobando os computadores e as tecnologias resultantes, pois juntamente com as inovações surgem novas necessidades e consequentemente novas ameaças e vulnerabilidades de acordo com novo cenário em que estiver inserida.

Esta evolução é composta por quatro estágios que tange a segurança da informação: o primeiro estágio na década de 70, com os computadores de grande porte, chamados "mainframes", em que o fabricante do equipamento, além de fornecer o hardware e software, também se preocupava em garantir a segurança. Na década de 80, vieram as redes e os microcomputadores, o que gerou uma época de incertezas, pela falta de sistemas e métodos de segurança. A partir da década de 90 surge a Internet, nesse momento a necessidade de segurança se amplia e a sua importância passa a ser considerada pelos executivos e usuários. Surgem produtos e serviços cada vez mais especializados e as empresas e os governos aumentam suas equipes de segurança.

Atualmente acredita-se na necessidade de regulamentação da segurança da informação. Setores da economia passam a atender determinações das agências reguladoras que exigem proteção da informação, garantindo sigilo, integridade, privacidade e disponibilidade. As novas tecnologias, aumentam o alcance e a exposição das informações, como as redes sem fio, equipamentos portáteis integrados com celular, Voz sobre IP (VoIP) e a TV Digital. Diante destas exigências, cada vez mais se faz necessário o uso de Normas para orientação de melhores práticas de Segurança de Informação.

Entre as iniciativas conhecidas vale ressaltar a Norma NBR ISO/IEC 17799 que vem sendo considerado o padrão a ser deguido.

4.1. A NORMA ISO/IEC 17799 / BS 7799: HISTÓRICO

A aceleração de acesso à informação movida pelas novas tecnologias e o uso da informação de forma competitiva para a tomada de decisão no meio empresarial torna a segurança da informação uma questão de fundamental importância. A questão da segurança no âmbito dos computadores ganhou força com o surgimento das máquinas de tempo compartilhado, também conhecidas como computadores "time-sharing", ou seja, permitem que mais de uma pessoa ou usuário faça uso do computador ao mesmo tempo.

O time-sharing permite que vários usuários possam acessar as mesmas informações, contudo, este acesso não gerenciado pode gerar efeitos indesejáveis, tal como: um estagiário ter acesso aos dados do presidente da firma. Neste sentido, nasce a necessidade da implementação de ferramentas que implementem o fornecimento de mecanismos para minimizar o problema do compartilhamento de recursos e informações de forma insegura.

Caracteriza-se que o problema clássico de computadores, o qual pode ser resumido na expressão: Como fazer com que usuários autorizados possam ter acesso a determinadas informações, ao mesmo tempo em que os usuários não autorizados não possam acessá-las?

Em outubro de 1967, surge nos Estados Unidos a primeira possibilidade para solucionar a situação de como fazer com que usuários autorizados possam ter acesso a determinadas informações, ao mesmo tempo em que os usuários não autorizados não possam acessá-las. Isto se deu com a criação de uma força tarefa, que resultou em um documento intitulado *Security Control for Computer System: Report of Defense Science Boad Task Force on computer Security*, este documento foi editado por W. H. Ware, e representa o início do processo oficial de criação de um conjunto de regras para segurança de computadores, expressa na publicação de uma norma internacional de segurança da informação, no ano de 2000.

Em outubro de 1972, J. P. Anderson escreve um relatório técnico denominado: *Computer Security Technologes Planning Study*, no qual ele descreve todos os problemas envolvidos no processo para se fornecer os mecanismos necessários para salvaguardar a segurança de computadores.

Em 1977, o Departamento de Defesa dos Estados Unidos formulou um plano sistemático para tratar do Problema Clássico de Segurança, o qual daria origem ao *DoD Computer Security Initiative*, que, por sua vez, desenvolveria um centro para avaliar o quanto seguro eram as soluções disponibilizadas.

A construção do Centro gerou a necessidade da criação de um conjunto de regras a serem utilizadas no processo de avaliação. Este conjunto de regras ficou conhecido informalmente como *The Orange Book* (O livro Laranja), devido a cor da capa deste manual de segurança, e o Coronel Roger Shell foi o primeiro diretor deste centro.

O processo de escrita do *Orange Book (*livro Laranja), conhecido oficialmente como *Trusted Computer Evaluation Criteria - DoD 5200.28-STD* (Critério de Evolução da confiança dos computadores), teve o seu início ainda no ano de 1978. No mesmo ano foi publicada a primeira versão *Draft* (rascunho) deste manual, entretanto somente no dia 26 de dezembro de 1985 foi publicada a versão final deste documento.

Graças a operações e ao processo de criação do Centro de Avaliação e do *Orange Book* (livro Laranja) tornou-se possível a produção de uma larga quantidade de documento técnicos, que representam o início da formação de uma norma coesa e completa sobre a segurança de computadores.

Mesmo que o *Orange Book* (livro Laranja) seja considerado, atualmente, um documento ultrapassado, pode-se considerá-lo como o marco inicial de um processo mundial e contínuo de busca de um conjunto de medidas que permitam a um ambiente computacional ser qualificado como seguro.

Pode-se concluir que o processo de busca de soluções para os problemas de segurança em ambientes computacionais envolve a necessidade do desenvolvimento de padrões, utilizados no apoio à construção de sistemas computacionais seguros como também para a sua avaliação.

A existência de uma Norma permite o usuário possa tomar conhecimento do nível de proteção e segurança das suas informações, possibilitando ao mesmo uma ferramenta que auxilie a escolha de uma solução. Do ponto de vista dos profissionais técnicos, eles passam a possuir

uma ferramenta comum de trabalho, evitando assim que cada equipe tenha para si um padrão desarticulado dos utilizados pelas equipes, dificultando aos clientes a melhor escolha.

O *Orange Book*(Livro laranja) representou o marco zero, do qual nasceram vários padrões de segurança, cada qual com a filosofia e métodos próprios, visando uma padronização mundial. Houve um esforço para a construção de uma nova norma, mais atual e que não se detivesse somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação.

Este esforço foi liderado pela *International Organization for Standardization* (ISO), e teve no final do ano de 2000, o primeiro resultado desse esforço apresentado, que é a Norma Internacional de Segurança da Informação ISO/IEC-17799:2000 (*International Standardization Organization/Internacional Electricaltechnical Commission* 17799), a qual já possui uma versão aplicada aos países de língua portuguesa, denominada NBR ISO/IEC-17799.

Os esforços relacionados com a busca de melhores mecanismos para salvaguardar a segurança culminam com a homologação da Norma Internacional de Segurança da Informação denominada ISO/IEC 17799:2000. Esta Norma trata da segurança das informações e não somente dos dados que trafegam pela rede ou que residem dentro de um sistema computacional.

A ISO se origina de um esforço do governo britânico, que de acordo com Gamma(2000) em 1987, através do Departamento de Indústria e Comércio do Reino Unido (*UK - Departamente of Trade Center - DTI*) criou o Centro de Segurança de Computação Comercial (*Comercial Computer Security Centre - CCSC*), que dentre as suas atribuições, teve a tarefa de produzir um código com as melhores práticas de segurança em tecnologia da informação, com a finalidade de auxiliar os usuários na implantação de sistemas de segurança em seu Ambiente Computacional complexo - ACC. Desse esforço, que foi realizado conjuntamente com o Centro de Computação Nacional dos EUA (*National Computing Centre – NCC*), resultou um "Código de práticas para usuários" (Users Code of Pratice), que foi publicado em 1989.

Para fazer uma avaliação desse código, do ponto de vista do usuário, foi formado um grupo de trabalho ligado à indústria britânica. O resultado dessa avaliação foi a publicação de um guia de segurança denominado documento PD 0003 e intitulado um código de práticas para gerenciamento de segurança da informação (*A code of practice for information security management*). Após um período de consulta pública, foi publicada, em 1995, a versão final desse documento, intitulado Padrão Britânico (*British Standard*) BS7799:1995.

Em 1995, o código é revisado, ampliado e publicado como Norma Britânica (BS – British Standard), intitulado BS7799-1:1995 (Tecnologia da informação – Código de prática para a gestão da segurança da informação). Em 1996, essa Norma foi proposta a ISO para homologação e rejeitada. Conforme Haical (2000), já nesta sua primeira versão, o padrão despertava interesse de organizações ao redor do mundo, apesar de apresentar algumas limitações para sua expansão mundial, como, por exemplo, a legislação voltada para os padrões britânicos. Para superar essas limitações, uma extensiva revisão e uma consulta pública foram iniciadas em novembro de 1997, culminando com a publicação da primeira revisão do padrão, o BS7799:1999, em abril de 1999. Para a revisão, foram solicitadas opiniões de vários países como forma de melhorar a Norma.

Ainda de acordo com Haical (2000), com essas contribuições, a BS 7799 atingiu dois objetivos: tornou-se mais flexível diante da necessidade de cada país e foi amplamente divulgada. Como conseqüência, a Normafoi adotada não apenas pela Inglaterra – cujo governo a recomendou como parte de seu Ato de Proteção aos dados de 1999, e que foi efetivado em março de 2000 – como também por outros países da comunidade britânica, tais como Austrália, Nova Zelândia e África do Sul, além da Holanda e Noruega. A segunda parte desse documento – criada em resposta à necessidade de certificação da segurança implantada em um ACC (Ambiente Computacional Complexo), seguindo os códigos da primeira parte – foi apresentada em novembro de 1997 para consulta publica e avaliação. E, em fevereiro de 1998, o documento final foi publicado como BS7799-2:1998.

Em Abril de 1999, as duas Normas (a de 1995 e a de 1998) foram publicadas, após uma revisão, com o nome de BS7799-1999; adotada por outros países, está acessível, traduzida para várias línguas entre as quais pode-se destacar o Francês, o Alemão e o Japonês.

Neste mesmo ano a primeira parte deste documento foi submetida à ISO para homologação. Em maio de 2000 a BSI – *British Standard Institute* homologou a primeira parte da NormaBS7799. Em outubro na reunião do comitê da ISO em Tóquio, a Norma foi votada e aprovada pela maioria dos representantes. Os representantes dos países ricos, excluindo a Inglaterra, foram todos contra a homologação; mas em primeiro de dezembro de 2000 houve a homologação desta Norma BS como ISO/IEC 17799:2000.

A Norma BS7799-2 foi submetida a um processo de revisão em 2001 e em janeiro de 2002 publicou-se o primeiro *draft* (rascunho) para acesso e avaliação pública. Esta revisão visa ajustar BS7799-2 com normas internacionais, tais como a ISO9001 e a ISO14001, e remover aspectos locais próprios da lei britânica. Os controles da ISO/IEC 17799 foram adicionados a um anexo desta versão, permitindo uma correspondência entre a numeração em ambas. A BS 7799-2:2002 foi publicada no dia 5 de setembro de 2002.

4.2 ASPECTOS IMPORTANTES DA NORMA.

O mercado atingiu um nível de automação, de compartilhamento de informações e de dependência tal, que motivou a elaboração e compilação de uma norma específica para orientar a padronização de uma base comum voltada para a gestão de segurança da informação, a BS7799: parte 1, que possui uma versão brasileira – NBR/ISO17799:1.

A Norma de Segurança da Informação trouxe mais do que vários controles de segurança, ela permitiu a criação de um mecanismo de certificação das organizações, semelhante às certificações ISO já existentes, contudo esta nova certificação afirma que a organização certificada manipula seus dados e os dos clientes de forma segura, independente da forma como eles estão armazenados.

A primeira parte da Norma Britânica BS7799 deu origem à versão ISO 17799:1 após avaliação e proposição de pequenos ajustes. Em seguida, foi traduzida e disponibilizada pela ABNT – Associação Brasileira de Normas Técnicas. Tem o objetivo de definir na parte 1 um Código de Práticas para a Gestão de Segurança da Informação. São, ao todo, 10 domínios, reunidos em 36 grupos que se desdobram em um total de 127 controles. Por se tratar de um código de práticas, esta parte da norma não é objeto de certificação, mas recomenda um amplo conjunto de controles que subsidiam os responsáveis pela gestão corporativa de segurança da informação.

A parte 2 da BS7799, que especifica um *framework* de segurança chamado SGSI – Sistema de Gestão de Segurança da Informação está em consulta pública, a fim de gerar a versão da ISO correspondente, e será, quando concluída, a base para a certificação das empresas. Enquanto isso não ocorre, a alternativa é buscar a conformidade e certificação da BS 7799, que já pode representar uma pré-certificação para a ISO 17799.

Possuir o certificado ISO/IEC 17799 é o diferencial que está sendo almejado por várias instituições. Ao ser certificada a organização mostra estar apta a tratar dados de forma sigilosa. O sigilo e a integridade das informações é o objeto de desejo de todo o mercado consumidor que está cada vez mais preocupado com a segurança das suas informações.

A ABNT Associação Brasileira de Normas Técnicas, que é a responsável pelo Fórum Nacional de Normalização, em abril de 2001, disponibilizou para consulta pública o Projeto 21:204.01-010, que daria origem à Norma nacional de segurança da informação: NBR ISO/IEC 17799:2000;.

A versão final da NBR ISO/IEC-17799, que é uma tradução literal da NormaInternacional de Segurança da Informação - ISO/IEC-17799:2000, foi homologada em Setembro de 2001 e sua publicação inclui oficialmente o Brasil no conjunto de países que, de certa forma, adotam e apóiam o uso da norma de Segurança da Informação ABNT 2001. E esta versão da ISO/IEC 17799 vem sendo utilizada por vários outros países, como é o caso de Portugal e Angola. A Versão 2005 da ABNT NBR ISO IEC17799:2005 – Código de Prática para Gestão da Segurança da Informação foi lançada no dia 24 de Agosto de 2005.

A Norma BS7799:1999 – Primeira Parte, descreve o código de melhores práticas para o gerenciamento de segurança da informação. Ela está dividida em dez títulos principais, com 127 controles de segurança e mais de 500 subcontroles, que visam manter e gerir a segurança da informação na organização, sendo o foco geral o gerenciamento de riscos, cujo objetivo é ajudar a organização a planejar a sua política de segurança. Como, normalmente, nem todos os controles precisam ser aplicados, a própria norma ajuda a organização a identificar os controles relevantes para seus negócios. No processo de certificação, a organização deverá especificar os controles que não estão incluídos na sua política de segurança e justificar sua exclusão.

Os dez títulos principais cobrem todas as formas pelas quais se pode obter uma informação, sejam mensagens de voz ou escritas, transmitidas por telefones móveis, fixos, fax ou circuitos de comunicação de dados. Identificam também as novas formas de se fazer negócios, tais como *e-commerce*, Internet, terceirização, computação móvel etc. Haical (2000) afirma que a grande flexibilidade da norma está justamente em tratar a segurança de informações independentemente dos meios nos quais a mesma se apresente. Estes dez títulos estão assim divididos:

- Política de Segurança;
- Segurança Organizacional;
- Classificação e Controle dos Ativos da Informação;
- Segurança em Pessoas;
- Segurança Física e do Ambiente;
- Gerenciamento de Operações e Comunicações;
- Controle de Acesso;
- Desenvolvimento da Segurança de Sistemas;
- Gestão da Continuidade do Negócio;
- Conformidade.

Já a Norma BS7799-2 – Segunda Parte especifica os passos necessários que as organizações devem seguir para obter a certificação de acordo com a norma. Para isso, define os requisitos necessários para estabelecer, implementar, documentar e avaliar um Sistema de Gerenciamento de Segurança da Informação (*Information Security Management System* – ISMS). DVN (2000) define um ISMS como o resultado de uma ação de gerenciamento

explícito, expresso como uma coleção de políticas, princípios, objetivos, medidas, processos, formas, modelos, lista de verificações (*checklist*) etc, que, juntos, definem como os riscos de segurança de um ACC podem ser reduzidos. Para Gamma (2000), ISMS é o meio através do qual os responsáveis pelo gerenciamento da segurança monitoram e controlam os sistemas de segurança, minimizando os riscos e garantindo que a segurança implantada satisfaz à organização, aos clientes e aos aspectos legais.

Ramos (2000) aponta que o importante é que o conceito de ISMS pode ser aplicado em qualquer organização, independente do seu tamanho. E esse conceito pode ser utilizado ainda que a organização não deseje submeter-se à certificação, mas apenas implementar um bom sistema de segurança para suas informações. A certificação serve para complementar o processo de implementação da segurança, atestando a prática da melhor política de segurança da informação, uma vez que é baseada no relato de auditores externos, portanto, supostamente imparciais. Após a certificação, as auditorias contínuas irão manter sempre os sistemas de segurança atualizados com as últimas vulnerabilidades e melhores práticas.

Após a BS7799: 1999 – Primeira parte (1999) ter sido publicada, ela foi submetida à ISO para se tornar um padrão internacional. A proposta para sua homologação foi apresentada pelo mecanismo de *Fast Track*, para um trâmite rápido, uma vez que qualquer norma leva em torno de cinco anos para ser avaliada e homologada pela ISO. Em outubro de 2000, na reunião do Comitê da ISO em Tóquio, a Norma foi votada e aprovada pela maioria dos representantes, muito embora os países ricos, exceto a Inglaterra, fossem contra sua homologação. Assim, em 1º de dezembro de 2000, ela foi publicada como ISO/IEC 17799: 2000.

Afirmar que um ambiente é aderente à Norma de Segurança da Informação significa dizer que o mesmo utiliza os recursos adequados para garantir a Disponibilidade, Confidencialidade e a Integridade de suas informações.

Mas para isto devem ser aplicados ao ambiente alguns ou todos os controles existentes na norma de segurança. Contudo, a lista dos controles que devem ser aplicados depende de características do próprio ambiente, como por exemploa forma e local de armazenamento das informações, valor das informações armazenadas, quem pode acessá-las, quais servidores

estão instalados, que tipo de serviços são disponibilizados aos usuários da rede interna e da rede externa.

De acordo com o nível de segurança necessário um conjunto de Controles de Segurança deve ser implementado. Mas a NBR é composta por 137 controles distintos, e o processo de seleção dos controles a ser aplicado nem sempre é fácil de ser realizado. Para facilitar o processo de seleção de controles podemos utilizar algumas ferramentas como por exemplo: a Análise de Risco de um ambiente, a Legislação Vigente, os Objetivos e Necessidades da organização.

A Análise de Risco de um ambiente baseia-se na avaliação do impacto de uma falha de segurança nas atividades da organização, bem como na sua probabilidade de ocorrência. O resultado desta análise apontará os principais pontos a serem trabalhados e a prioridade das informações a serem protegidas.

Sendo o resultado da Análise de Risco dependente das características atuais do ambiente e como o mesmo não é estático, este resultado representa as melhores ações a serem aplicadas em um determinado momento no ambiente. Conseqüentemente, análises de risco periódicas devem ser realizadas, mesmo quando um ambiente não tenha se modificado. Neste caso, a nova análise é justificada pelo fato de que novas vulnerabilidades e ameaças surgem no cotidiano.

Contudo, independente do ambiente, dos riscos e das ameaças que foram indicadas pelo resultado da Análise de Risco, existe um conjunto mínimo de controles, que segundo a NBR, sempre devem ser implementados. Este conjunto segundo a NBR engloba os seguintes aspectos:

- Política de segurança da informação: este é um documento que descreve quais atividades os usuários estão autorizados a realizar, como e quando podem ser realizadas. É de vital importância que a alta administração apóie o uso da Política e demonstre o seu comprometimento com a aplicação de suas penalidades cabíveis;

- Definição das responsabilidades de segurança: este controle visa esclarecer a quem *pertence* cada ativo da organização, bem como quem deve ser contactado em caso de problemas de segurança relacionados a ativo em questão;

- Processo de treinamento: a melhor forma de evitar mal uso das informações é educar seus usuários, assim é de vital importância que todo e qualquer usuário passe por um treinamento antes de ter acesso as informações contidas no ambiente.

- Relatórios dos incidentes: estes documentos permitem a criação de uma base de conhecimento que poderá ser utilizado para identificar e evitar futuros incidentes de segurança;

- Gestão da continuidade das atividades do ambiente: este controle diz respeito ao processo de se manter a informações, íntegras, sempre acessíveis mesmo em caso de parte do ambiente esteja comprometido.

4.3 SISTEMA DE SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA BS 7799

A gestão da segurança é um fator crítico de sucesso para as organizações, pois permite a proteção eficaz da informação de ameaças externas ou internas à organização. Esforços consideráveis devem ser canalizados para o melhoramento da gestão da segurança, tendo como base as melhores práticas presentes na Norma BS7799.

O BS7799 é a Norma oficial de Segurança da Informação desenvolvido pelo governo Britânico com o objetivo de criar um conjunto de boas práticas comum, que permita às organizações públicas e privadas desenvolver, implementar e avaliar as suas práticas de gestão da segurança da informação. Resulta do trabalho conjunto do Departamento de Comercio e Indústria e de várias organizações privadas, reunindo as suas práticas de segurança da informação, sendo uma Norma reconhecida internacionalmente. Esta se encontra dividida em duas partes, sendo o BS7799-1 um conjunto de políticas sugerindo um conjunto de boas práticas a adotar pelas organizações que desejem gerir a segurança da informação de uma forma eficaz. A primeira parte foi constituída como Norma internacional

pelo International Standards Organization - ISO, sendo denominado por ISO/IEC 17799:2000.

A segunda parte da Norma, o BS7799-2:2002, é um documento que especifica um conjunto de requisitos necessários para a implementação de um Sistema de Gestão de Segurança da Informação permitindo às organizações obterem uma certificação de segurança.

A Norma BS 7799 é um padrão de excelência que orienta a organização de um Sistema de Gestão de Segurançada Informação. A preparação para certificação representa a preocupação da empresa em demonstrar sua capacidade em atender aos controles necessários para garantir os requisitos de segurança sobre os ativos da informação considerados críticos para o seu negócio e submeter-se a avaliação por partes externas, que seriam os organismos certificadores.

A Versão BS7799:2002 da Norma BS 7799 apresenta a evolução compatível com as demais normas da implementação de um sistema integrado de gestão, aos moldes da versão 2000 da Norma ISO/IEC 9000.

Como implementar um sistema de segurança da informação com base na BS7799?
A implementação do sistema de segurança da informação deve ser orientado pelos passos previstos no *framework* apresentado na BS 7799 parte 2 de 2002. O *framework* de segurança definido pela parte 2 da Norma britânica BS7799 estabelece um SGSI – Sistema de Gestão de Segurança da Informação que, somado ao conjunto de controles sugeridos pela primeira parte da norma, serve de objeto para certificação. Desta forma, as organizações podem conduzir as ações de segurança sob a orientação de uma base comum proposta pela Norma, além de se prepararem indiretamente para o reconhecimento de conformidade aferido por órgãos credenciados.

A certificação de segurança, similar aos reflexos obtidos pela conquista da certificação de qualidade ISO 9000, promove melhorias nas relações “business-to-business” e “business-to-consumer”, além de adicionar valor à empresa por representar um diferencial competitivo e uma demosntração pública do compromisso com a segurança das informações de seus clientes. Este diferencial se potencializa por estar restrito a pouco mais de 1050 empresas em

todo o mundo até o momento e apenas 4 no Brasil, o que demonstra a posição de destaque, inovação e maturidade da empresa certificada.

Contudo, o caminho que conduz ao reconhecimento da conformidade é longo, pouco pavimentado e requer esforços dedicados ao planejamento, seleção de controles aplicáveis e a coordenação das atividades que irão preparar o objeto da certificação. Como ocorre na prática, o objeto de certificação não precisa necessariamente ser toda a empresa, devendo começar por um escopo restrito, normalmente um processo representativo para a natureza da atividade da empresa.

Os trabalhos iniciam e desdobram-se em seis fases principais:

1 - Definição da Política de Segurançada Informação – documento que contém de forma clara e resumida as premissas e diretrizes do Sistema de Gestão de Segurança da Informação SGSI.

2 - Definição do Escopo do Sistema de Gestão de Segurança da Informação – que é o perímetro de abrangência que define os ativos que serão contemplados no SGSI, sejam eles sistemas, dispositivos físicos, processos ou ações do pessoal envolvido;

3 - Análise de Risco – Que abrange a identificação de ameaças e vulnerabilidades para os ativos cobertos pelo escopo definido, seus possíveis impactos no negócio. A metodologia utilizada para elaboração desta análise deve ser documentada; os critérios para identificação dos riscos precisam ser registrados e inseridos no sistema de documentação;

4- Gestão do Risco – definição do processo de gestão dos riscos identificados e critérios para atribuição das prioridades e relação de custo benefício de cada ação recomendada;

5 – Seleção dos objetos de controle e dos controles a serem implementados;

6 – Preparação da declaração de Aplicabilidade – que é a justificativa clara de quais itens da Norma BS7799 são aplicáveis e serão desdobrados dentro do Sistema de Gestão de Segurança da Informação da organização. Este passo resume os passos anteriores e complementa o escopo para certificação. É também um norte para evitar que se definam controles em excesso ou que se deixe desprotegido algum ativo importante para a organização.

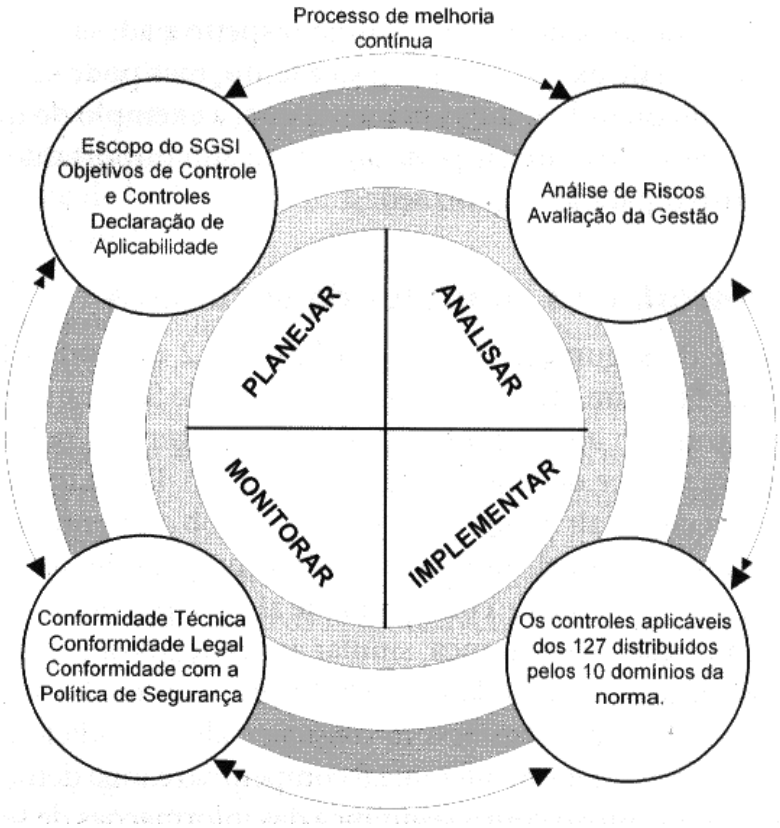


FIGURA 16 - Modelo de framework SGSI – Sistema de Gestão de Segurança da Informação.

Fonte: Sêmola(2003).

A Norma representa uma trilha que orienta as organizações dispostas a se estruturar para gerir os riscos de segurança da informação; por isso, limita-se a indicar o que deve ser feito sem, no entanto, dizer como deve ser feito. Pelo envolvimento de múltiplas especialidades e competências gerenciais e técnicas, recomenda-se que as organizações que submetam-se à preparação para a certificação, contem com o apoio externo a fim de agregar experiências, Know-how acumulados pela execução de outros projetos e, principalmente, pela visão isenta de vícios que adicionam qualidade ao trabalho.

O direcionamento da Norma busca a sintonia com padrões adotados pela Norma de qualidade ISO 9000. Este elemento agregou facilidade por permitir o aproveitamento das experiências vividas pelo processo de preparação, que requer o registro de controles e a construção do manual de qualidade, viabilizando a convergência das duas certificações.

Portanto, para certificação em segurança as organizações devem seguir as orientações do modelo apresentado apresentado pela Norma BS7799 e definir o SGSI - Sistema de Gestão de

Segurança da Informação com base nos elementos da Norma. Os elementos da Norma BS7799:2002 incluem:

1 – Escopo
2 – Referências Normativas
3 – Termos e Definições
4 – Requisitos do sistema de gerenciamento de segurança da informação
5 – Responsabilidades da Alta Gestão
6 – Gerência da revisão do SGSI
7 – Melhoria do SGSI
Anexo A – Objetivos de Controle e Controles A1 a A12.
- A.1 Introdução
- A.2 Guia de Melhores Práticas
- A.3 Política de Segurança
- A.4 Segurança Organizacional
- A.5 Classificação e controle dos ativos de informação
- A.6 Segurança em Pessoas
- A.7 Segurança Física e do ambiente
- A.8 Gerenciamento das operações e comunicações
- A.9 Controle de Acesso
- A.10 Desenvolvimento e Manutenção de sistemas
- A.11 Gestão da continuidade do negócio
- A.12 Conformidade

1 – Escopo

Generalidades – O escopo é o perímetro de abrangência que define os ativos que serão contemplados no Sistema de Gestão de Segurança da Informação, sejam eles sistemas, dispositivos físicos, processos ou ações do pessoal envolvido.

Aplicação - Esta parte da BS 7799 especifica os requisitos para estabelecimento, implementação e documentação de um sistema de Gerenciamento de Segurança da Informação(SGSI). A norma especifica os requisitos para controle de segurança a ser

implementado de acordo com as necessidades específicas de cada organização. Exclusões de requisitos podem ser realizadas contanto que não afetem a habilidade e/ou responsabilidade da organização em prover informações seguras de acordo com a Análise de Risco e Leis Aplicáveis.

2 – Referência Normativa

A ISO 17799:2001 – Tecnologia da Informação – Código de Prática para a Gestão da Segurança da Infromação;

A ISO 9001:2000 – Sistema de Gestão da Qualidade - Requisitos

ISO Guide 73:2002 – Gerenciamento do Risco – Vocabulário

3 – Termos e Definições

Os termos e definições constantes da ISO 17799 são válidos para dirimir eventuais dúvidas. Para os efeitos da Norma BS 7799-2, aplicam-se as definições especificadas no item 4 a 7 descritas a seguir.

4 – Requisitos de Gerenciamento de Segurança da Informação (Aspectos Gerais)

4.1 Generalidades

A organização deve estabelecer, documentar, implementar e manter um Sistema de Gerenciamento da Segurança de Informações (SGSI ou ISMS em inglês), sendo que este deve identificar os ativos a serem protegidos, o gerenciamento do risco, os objetivos e controles e o grau de qualidade requerido pela Organização. Seguindo o modelo proposto no PDCA (Plan, Do, Check, Act) ilustrado na figura abaixo:

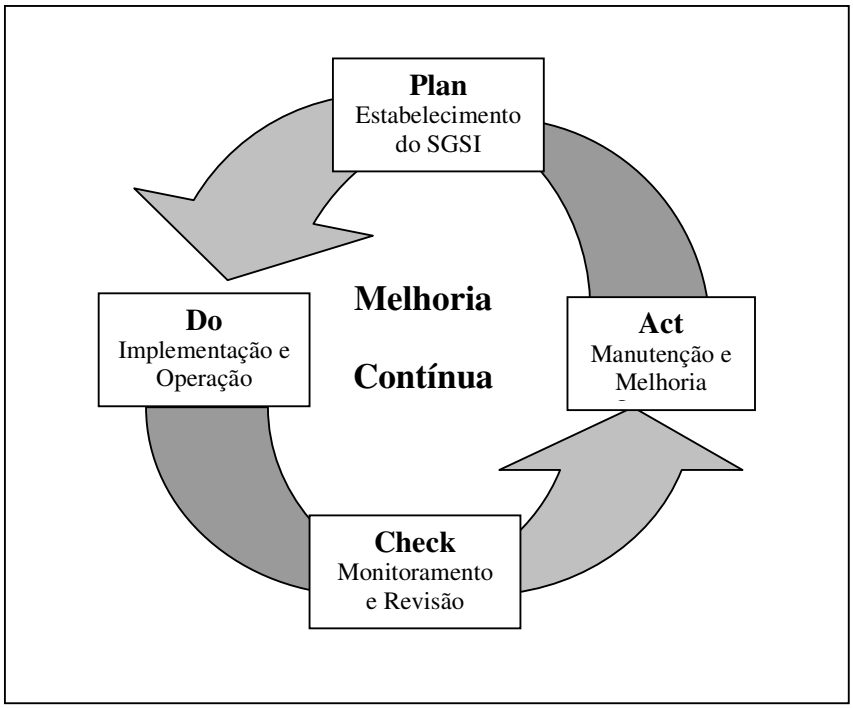


FIGURA 17 - Modelo de Processo - PDCA (Plan-Do-Check-Act), Norma BS7799

Fonte: Norma BS7799

4.2 Processo

4.2.1 PLAN – Estabelecendo o Gerenciamento do SGSI

a) Definição do Escopo e da Política do Sistema de Gestão de Segurança da Informação – SGSI

- ✓ A política de segurança é o documento que contém de forma clara e resumida as premissas e diretrizes do SGSI;
- ✓ O escopo é o perímetro de abrangência que define os ativos que serão contemplados no SGSI, sejam eles sistemas, dispositivos físicos, processos ou ações do pessoal envolvido.;

b) Definir Sistemática de Avaliação de Risco: identificar um método para Análise de Risco, que sirva ao SGSI. Direcionando a política e objetivos do SGSI para reduzir riscos a níveis aceitáveis. Determinando tais critérios. A metodologia utilizada para elaboração

desta análise deve ser documentada, os critérios para identificação dos riscos precisam ser registrados e inseridos no sistema de documentação;

c) Análise de Risco – a identificação das ameaças e vulnerabilidades para os ativos cobertos pelo escopo definido, seus possíveis impactos no negócio;

d) Avaliação do Risco – definição do processo de gestão dos riscos identificados e critérios para atribuição das prioridades e relação custo benefício de cada ação recomendada. Avaliar os possíveis danos sofridos com a perda de confidencialidade, integridade e disponibilidade dos ativos; avaliar a probabilidade de que as falhas de segurança ocorram independente dos controles implementados prevalecendo as ameaças e vulnerabilidades e impactos associados aos ativos; estimar os níveis de risco; determinar se o risco é aceitável ou requer o tratamento utilizando critério pré-estabelecido;

e) Seleção dos controles – selecionar e documentar os controles a serem implementados e seus respectivos objetivos de acordo com os controles do Anexo A desta norma e a sua escolha deve ser justificada;

f) Preparação da declaração de aplicabilidade – que é a justificativa clara de quais os itens da Norma BS7799 são aplicáveis e serão desdobrados dentro do Sistema de Gestão de Segurança da Informação da organização. Esse passo resume os passos anteriores e complementa o escopo para certificação;

g) Aprovação formal do SGSI – Deve-se obter nesta fase a aprovação da alta direção em documento formal de identificação dos riscos, considerando os riscos residuais, e os controles que deverão ser implementados para garantir a segurança sobre os ativos da informação cobertos pelo escopo.

4.2.2 DO – Implementação e Operação do SGSI

Os controles devem ser implementados efetivamente pela organização. A efetividade dos procedimentos utilizados para implementação dos controles selecionados deve ser verificada

por revisões de acordo com o estabelecido em Monitoramento e Revisão do SGSI. A organização deve executar:

- ✓ Um plano de tratamento de risco para identificar as ações, responsabilidades e prioridades de gerenciamento apropriadas;
- ✓ Implementar um plano de tratamento de risco para realizar os objetivos dos controles identificados, que consideram a profundidade, regras e responsabilidades;
- ✓ Implementar os controles selecionados a fim de atingir os objetivs destes controles;
- ✓ Implementar programa de Treinamento;
- ✓ Gerenciar operações;
- ✓ Gerenciar recursos;
- ✓ Implementar procedimentos e outros controles capazes de detectar e responder prontamente a incidentes de segurança.

4.2.3 CHECK – Revisar e Monitorar o SGSI

A organização deve:

a) Executar procedimentos e outros controles para:

- ✓ Detectar erros resultantes de processos;
- ✓ Identificar falhas, quebras de segurança e incidentes prontamente;
- ✓ Habilitar um Gerenciamento que permita avaliar se as atividades de segurança delegadas ou se tecnologia de informação implementadas são executadas conforme expectativa;
- ✓ Determinar as ações a serem tomadas para resolver quebras de segurança que afetem as prioridades do negócio.

b) Realizar revisões regulares da efetividade do SGSI, incluindo o atendimento a política e objetivos de segurança e controles adotados, resultados das auditorias de segurança, incidentes, sugestões e retornos de partes interessadas;

c) Revisar o nível de risco residual e risco aceitável, considerando as implicações:

- ✓ No negócio da Organização;

- ✓ Na Tecnologia;
- ✓ Nos processos e objetivos do Negócio;
- ✓ Identificação de Ameaças;
- ✓ Eventos Externos(mudanças de legislação);
- ✓ Conduzir auditorias de forma planejada;

d) Desenvolver um procedimento de gerenciamento para verificar se os procedimentos de segurança estão sendo cumpridos e se os dispositivos de segurança estão sendo utilizados a contento;

e) Executar revisão Gerencial do SGSI de forma regular para garantir que o escopo continua adequado e as melhorias do SGSI são identificadas.

f) Efetuar registros das ações e eentos que tiveram impacto na efetividade ou performance do SGSI.

4.2.4 – ACT – Manutenção e Melhoria do SGSI

A organização deve regularmente realizar:

a) Medir a performance do SGSI através de reuniões formais visando obter subsídios para melhoria da política e dos objetivos de controle do risco;
b) Identificar melhorias no SGSI e efetivamente implementá-las;
c) Tomar ações corretivas e ou preventivas adequadas de acordo com os itens 7.2 e 7.3 e aplicar o aprendizado com as experiências de segurança ocorridas na própria e em outras organizações;
d) Comunicar os resultados e ações decorrentes as partes interessadas;
e) Revisar o SGSI todas as vezes que for necessário, incentivando todos os envolvidos a fazê-lo de forma participativa e integrada;
f) Garantir que as melhorias implementadas atinjam aos objetivos.

4.3 Documentação

4.3.1 Generalidades

O Sistema de Gerenciamento de Segurança da Informação deve possuir:

a) Declaração da Política de Segurança e dos objetivos de controle e o escopo do SGSI, os procedimentos e controles que sustentam o SGSI;
b) O manual do SGSI, os procedimenos utilizados, as responsabilidades e ações relevantes;
c) Relatório de Análise de Risco;
d) Plano de Tratamento de Risco;
e) Procedimentos documentados necessários para que a organização garanta a efetividade planejada, operação e controles do processo de Segurança de Informações;
f) Evidência das ações tomadas;
g) Declaração de aplicabilidade, incluindo um sumário dos controles implementados;

Todos os documentos devem estar disponíveis de acordo com especificação da Política de Segurança. E os documentos citados acima(a) e (b) podem ser um único documento parte do Manual da Política de Segurança.

4.3.2 Controle de Documentos

Os documentos requeridos pelo SGSI devem ser protegidos e controlados. Um procedimento documentado deve ser estabelecido a fim de definir as ações necessárias para:

a) Aprovação da documentação;
b) Revisão, atualização e re-aprovação dos documentos quando necessário;
c) Garantir que mudanças e que o status da versão dos documentos seja identificada;

d) Garantir que a última versão dos documentos relevantes estarão disponíveis nos locais de uso;
e) Garantir que os documentos sejam legíveis e prontamente identificáveis;
f) Garantir que os documentos de origem externa sejam identificados;
g) Garantir que a distribuição dos documentos seja controlada;
h) Prevenir o uso não intencional de documentos obsoletos e aplicar identificação adequada caso estes documentos devam ser retidos por algum motivo.

4.3.3 Controle de Registros

- ✓ Registros devem ser estabelecidos e mantidos para demosntrar evidências de conformidade dos requisitos e da efetividade operacional do SGSI;
- ✓ O SGSI deve considerar qualquer registro legal relevante;
- ✓ Os registros devem ser controlados e permanecer legíveis, identificáveis e recuperáveis;
- ✓ Os controles necessários para identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição devem ser documentados

5. Responsabilidade da Direção

A direção deve prover evidências do seu comprometimento em estabelecer, implementar, operacionalizar, monitorar, revisar, manter e melhorar o SGSI através da:

- ✓ Definição da Política de Segurança de Informações;
- ✓ Garantindo que os objetivos para segurança de informações e os respectivos planos são estabelecidos;
- ✓ Estabelecendo regras e responsabilidades para Segurança de Informações;
- ✓ Comunicando a organização a importância em atender aos objetivos e política de Segurança de Informações, das responsabilidades perante as leis e da necessidade da melhoria contínua;
- ✓ Prover recursos suficientes para desenvolver, implementar, operar e manter o SGSI;

- ✓ Decidir o nível de risco aceitável;
- ✓ Conduzir revisões gerenciais do SGSI.

5.2 - Gerenciamento de Recursos

5.2.1 - Provisão de Recursos

A organização deve determinar e prover os recursos necessários para:

- ✓ Estabelecer, implementar, operar e manter o SGSI;
- ✓ Garantir que os procedimentos de Segurança de Informação suportam as necessidades do negócio;
- ✓ Identificar os regulamentos, leis, requisitos contratuais e ou legais de segurança;
- ✓ Manter a segurança adequada através da correta aplicação de todos os controles implementados:
- ✓ Executar revisões quando necessário e tomar ações apropriadas de acordo com o resultados destas revisões;
- ✓ Onde requerido, aprimorar a efetividade do SGSI.

5.2.2 - Treinamento, Consciência e Competências

A organização deve garantir que todo pessoal que tenha responsabilidades definidas no SGSI é competente para executar as tarefas conforme requerido:

- ✓ Determinando as competências necessárias para performance pessoal do trabalho que afetam ao SGSI;
- ✓ Prover treinamento e se necessário empregar pessoal competente para satisfazer estas necessidades;
- ✓ Avaliar a efetividade dos treinamentos fornecidos e das ações tomadas;
- ✓ Manter registros de educação, treinamento, habilidade, experiencia e qualificação.

A organização deve garantir ainda que o pessoal envolvido tenha consciência da relevância e importância das suas atividades relacionadas a segurança de informações e como eles podem contribuir para aprimorar os objetivos do SGSI.

6 - Revisão da Direção do SGSI

A direção deve revisar o SGSI a intervalos planejados para garantir a sua conveniência, adequação e efetividade contínua. A revisão deve incluir oportunidades de melhoria e necessidades de mudança do SGSI, incluindo a Política e os Objetivos de Segurança. Os resultados desta revisão devem ser claramente documentados e registros devem ser mantidos.

6.2 - Dados de Entrada

- ✓ Resultados das Auditorias Internas do SGSI;
- ✓ Retomo das partes interessadas;
- ✓ Técnicas, produtos ou procedimentos, que podem ser usados pela organizacao para aprimorar a performance e efetividade do SGSI;
- ✓ O status das ações corretivas e preventivas;
- ✓ Vulnerabilidades ou ameaças não adequadamente endereçadas na análise de risco anterior;
- ✓ Acompanhamento das ações das revisões gerenciais anteriores;
- ✓ Qualquer mudança que possa afetar o SGSI;
- ✓ Recomendações para melhoria.

6.3 - Dados de Saída

Os dados de saída da revisão gerencial devem incluir qualquer decisão e ação de acordo com:

- ✓ Melhoria e efetividade do SGSI;
- ✓ Modificações nos procedimentos que afetem a segurança de informações, quando necessário, para responder a eventos internos ou externos que possam impactar no SGSI, incluindo mudanças:
- ✓ Requisitos do Negócio;
- ✓ Requisitos de Segurança;
- ✓ Processos de Mercado repercutindo nos requisitos existentes da Organização;
- ✓ Regulamentos ou ambiente legal;
- ✓ Níveis de Risco e/ou níveis de aceitação de risco;
- ✓ Recursos Necessários.

6.4 - Auditoria Interna do SGSI

A organização deve conduzir auditorias internas a intervalos planejados para determinar se os objetivos dos controles, controles, processos e procedimentos do SGSI:

- ✓ Estão em conformidade com os requisitos desta Norma. Da legislação ou regulamento relevante;
- ✓ Estao em conformidade com os requisitos de Segurança de Informações identificados;
- ✓ Foram efetivamente implementados e são mantidos;
- ✓ São executados conforme expectativa.

Uma auditoria deve ser planejada levando em consideração o status e a importância dos processos e áreas a serem aditadas, bem como o resultado das auditorias anteriores. Os critérios de auditoria, escopo, frequência e método devem ser definidos.

A seleção dos auditores e a condução da auditoria devem garantir a objetividade e imparcialidade do processo de auditoria. Os auditores não podem auditar o seu próprio trabalho.

As responsabilidades e requisitos para planejar e conduzir auditorias, reportar os resultados e manter registros devem ser definidos em um procedimento documentado.

O responsável pela área auditada deve garantir que as ações são tomadas em tempo hábil para eliminar as não conformidades detectadas e suas causas.

Atividades de melhoria devem incluir a verificação das ações tomadas e o relatório da verificação dos resultados.

7 - Melhoria do SGSI

7.1 - Melhoria Contínua

A organização deve melhorar continuamente a efetividade do SGSI através do uso da Política de Segurança de Informações, Objetivos de Segurança, Resultados de Auditoria. Analise de Eventos Monitorados, Ações Corretivas e Preventivas e Revisão da Direção.

7.2 - Ações Corretivas

A organização deve tomar ações corretivas para eliminar as causas das não conformidades associadas a implementação e operação do SGSI de forma a evitar a recorrência dos problemas. Um procedimento documentado deve:

- ✓ Identificar não conformidades da implementação e/ou operação do SGSI;
- ✓ Determinar as causas das não conformidades;
- ✓ Avaliar a necessidade de ações para garantir que as não conformidades não reincidam;
- ✓ Determinar e implementar as ações corretivas necessárias;
- ✓ Registrar os resultados das ações tomadas;
- ✓ Revisar as ações corretivas tomadas.

7.3 - Ações Preventivas

A organização deve determinar ações para evitar futuras não conformidades de forma a prevenir sua ocorrência.

Ações preventivas tomadas devem ser apropriadas ao impacto dos problemas potenciais. Um procedimento documentado para ações preventivas deve ser definido considerando:

- ✓ Identificar não conformidades potenciais e suas causas;
- ✓ Determinar e implementar ações preventivas necessárias;
- ✓ Registrar os resultados das ações tomadas;
- ✓ Revisar as ações preventivas tomadas;
- ✓ Identificar mudanças de riscos e garantindo atenção significante sobre estas mudanças de risco;
- ✓ A prioridade das ações preventivas deve ser baseada nos resultados da análise de riscos.

O processo de implantação de um sistema de Gestão da Segurança da Informação baseado na Norma de Segurança BS 7799 em um determinado ambiente não é simples e envolve a implantação e o acompanhamento de muitos controles como vimos neste capítulo.

5. A SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES DE SALVADOR E O USO DA NORMA.

A questão da segurança da informação tornou-se um tema importante na sociedade contemporânea. De grandes empresas que guardam nos computadores os segredos de seus negócios, até indivíduos que trocam correspondências eletrônicas de caráter pessoal, todos têm o legítimo direito de esperar que os dados confiados às máquinas sejam mantidos intactos e confidenciais, acessíveis apenas às pessoas autorizadas.

Embora tenha tomado proporções maiores no final do século passado e início deste, essa questão é praticamente tão antiga quanto a própria humanidade. O homem se desenvolveu procurando criar um mundo cada vez melhor. Na sociedade atual as tecnologias da informação aceleram as mudanças e a segurança da informação é impositiva.

Capturar informações alheias sem autorização é sempre um crime, mas nem sempre o infrator tem por objetivo obter algum ganho financeiro com isso. Muitas vezes, é a curiosidade e a vontade de quebrar padrões que estimulam os *hackers*. Entender essa particularidade é importante tanto para as empresas como para os cidadãos que se preocupam com o assunto. Trata-se de um problema que não deve ser visto apenas do ponto de vista técnico, de programação ou infra-estrutura de redes de comunicação. É um problema cultural e social.

Embora haja hoje um bom nível de consciência de empresas e consumidores a respeito dos perigos dos vírus e dos ataques de *hackers*, em alguns casos as ações para evitar os problemas não acontecem como deveriam. Ainda é comum ver empresas que compram equipamentos e *software* de última geração, mas cometem erros básicos de configuração, ou não se preocupam como deveriam com as atualizações. Os programas de computador são como carros, precisam de manutenções, revisões e cuidados constantes. Ter um *software* de ponta e não cuidar da manutenção e configuração é como comprar carro blindado e andar de janela aberta ou portas destravadas. O número é alarmante: mais de 80% dos problemas de segurança poderiam ser evitados se os programas estivessem devidamente configurados e atualizados.

O Brasil, que soube rapidamente perceber as vantagens e potencialidades da Internet, é por conseqüência um dos países mais expostos aos problemas de segurança digital. Segundo

relatório da Conferência de Comércio e Desenvolvimento das Nações Unidas (Unctad), o Brasil tem a segunda Internet mais vulnerável do mundo, perdendo apenas para os Estados Unidos. A solução não é simples e envolve uma regulamentação maior por parte do governo, uma continuidade do esforço das empresas de tecnologia e uma educação e conscientização maior por parte dos usuários, técnicos ou leigos. Só assim cada um de nós, e o país como um todo, poderá tirar proveito de todas as potencialidades do mundo digital, sem temer pela integridade de suas informações.

5.1 A SEGURANÇA DA INFORMAÇÃO NO BRASIL

A Empresa Módulo Security realiza uma pesquisa anual que representa um importante norteador do segmento de Segurança da Informação no Brasil. A 9ª Pesquisa Nacional de Segurança da Informação realizada em 2003 e divulgada em 2005 apresenta um panorama das principais tendências do mercado nacional, indicadores, melhores práticas, além de uma análise comparativa entre as pesquisas de 2002 e 2003.

Os resultados da 9ª Pesquisa Nacional de Segurança da Informação realizada pela Módulo Security Solutions permite concluir que as empresas brasileiras estão cada vez mais conscientes da importância de se investir em segurança para reduzir os riscos operacionais e atender requisitos legais compatíveis com a natureza de seus negócios.

A coleta de dados para 9ª Pesquisa Nacional de Segurança da Informação contou com respostas presenciais e via on-line. No total, a pesquisa quantitativa teve uma amostra de 682 questionários, coletados entre março e agosto de 2003, junto a profissionais ligados às áreas de Tecnologia e Segurança da Informação.

Serão apresentados os principais destaques da pesquisa para nortear e situar o Brasil no cenário de Segurança da Informação:

- ✓ Para 78% dos entrevistados, as ameaças e os riscos e os ataques deverão aumentar em 2004.

- ✓ 42% das empresas tiveram problemas com a Segurnaça da Informação nos seis meses anteriores à pesquisa.
- ✓ 35% das empresas reconhecem que tiveram perdas financeiras. Já o percentual de empresas que não conseguiram quantificar essas perdas diminuiu de 73% em 2002, para 65% em 2003.
- ✓ Vírus (66%), funcionários insatisfeitos(53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informações(47%) foram apontados como as cinco principais ameaças à segurança das informações nas empresas.
- ✓ O percentual de empresas que afirmam ter sofrido ataques e invasões subiu de 43% em 2002, para 77% em 2003.
- ✓ 32% dos entrevistados apontam os *hackers* como os principais responsáveis por ataques e invasões de sistemas corporativos.
- ✓ 26% das empresas não conseguem sequer identificar os responsáveis pelos ataques.
- ✓ 48% não possuem nenhum plano de ação formalizado em caso de invasões e ataques.
- ✓ 60% indicam a Internet como principal ponto de invasão em seus sistemas.
- ✓ 58% dos entrevistados senten-se inseguros para comprar em sites de comércio eletrônico por causa da sensação de falta de segurança.
- ✓ A falta de consciência dos executivos é apontada por 23% dos entrevistados como o principal obstáculo para implementação da segurança.
- ✓ 63,5% dos entrevistados adotam a ISO 17799 como principal Norma que norteia suas empresas.
- ✓ Política de Segurança formalizada já é realidade em 68% das organizações.
- ✓ Apenas 21% das empresas afirmaram possuir um Plano de Continuidade de Negócios(PCN) atualizado e testado.
- ✓ 60% das empresas fazem Planejamento de Segurança, sendo que 27% possuem Planejamento para até 1 ano.
- ✓ A área de Tecnologia (49,5%) continua sendo a principal responsável pelo genreciamento da Segurança da Informação nas empresas, seguidas pela área específica, Securite Office (Responsavel pela Segurança), com 25,5%.
- ✓ Pelo terceiro ano consecutivo, antivírus (90%), sistema de backup (76,5) e firewall (75,5%) foram apontados como as três medidas de segurança mais implementadas nas empresas.

- ✓ 60% afirmam que os investimentos de suas empresas em Segurança para o ano seguinte vão aumentar.

Apesar da pesquisa ter sido realizada em 2003, é um grande referencial da Segurança da Informação no Brasil e após analisar o resultado da pesquisa verifica-se a existência de uma forte tendência de que as empresas adotem a ISO/IEC 17799 / BS 7799 como padrão de segurança para as organizações e em alguns casos, a Norma seja também utilizada para certificação das empresas. Esta certificação vem sendo adotada em mais de 20 países trazendo maior confiança nas relações e, muitas vezes, sendo considerada também um importante diferencial competitivo.

Atualmente, pelo mundo, o *International User Group*, que gerencia uma lista atualizada e completa das empresas que obtiveram a certificação na Norma BS 7799, contabiliza 1.050 organizações certificadas. No Brasil, já são quatro empresas. Dentre elas, está a Modulo Security a primeira empresa brasileira a obter a certificação, o Serasa, o Banco Matone, primeira instituição financeira das Américas a conquistar a BS 7799-2, e a Samarco Mineração S.A. que é a quarta empresa brasileira - e a primeira do setor industrial do país - a obter certificação na Norma internacional de segurança BS7799.

Após apresentar uma síntese da Segurança da Informação no Brasil, a pesquisa realizada em Salvador irá apresentar o cenário da Segurança da Informação em organizações de Salvador focando o uso da Norma BS7799 como síntese das melhores práticas de Segurança da Informação.

5.2 A PESQUISA

Após apresentar os conceitos de Segurança da Informação, a aplicabilidade destes conceitos para a implantação de um Sistema de Gestão de Segurança da Informação baseado na Norma BS 7799 e o cenario da Segurança da Informação no Brasil, a pesquisa direcionou-se para a realidade local, considerando o cenário apresentado acima. Foram pesquisadas 62

organizações selecionadas em áreas de atuação distintas de Salvador e região metropolitana para poder ser mapeado a situação atual da Segurança da Informação em Salvador.

Para realizar a entrevista foram levantados alguns requisitos que classificaram a organização como apta a responder a pesquisa. Em virtude da complexidade e da abrangência de um Sistema de Gestão de Segurança da Informação foram selecionadas organizações que possuíssem um ambiente computacional desenvolvido, com mais de um servidor, incluindo *Firewall,* acesso a Internet dedicado e um número mínimo de 30 usuários, visto que as maiores vulnerabilidades das informações encontram-se nos sistemas computacionais e nas pessoas envolvidas no processo de manipulação da informação.

O intuito desse questionário foi verificar como estas organizações de Salvador, vide Apêndice II, estão incorporando a necessidade da Segurança da Informação e quais as ações ou diretrizes que estas estão tomando para implantar ou de manter a Segurança da Informação com base na Norma BS 7799:2002 2 / ISO IEC 17799, que é a Norma que norteia este tema.

Sendo assim, o questionário foi elaborado com base nos controles existentes da Norma para traçar um panorama atualizado do nível de conhecimento da mesma pelas organizações e se esta está sendo utilizada na prática como referência para a Gestão da Segurança da Informação nas organizações de Salvador.

5.3 METODOLOGIA

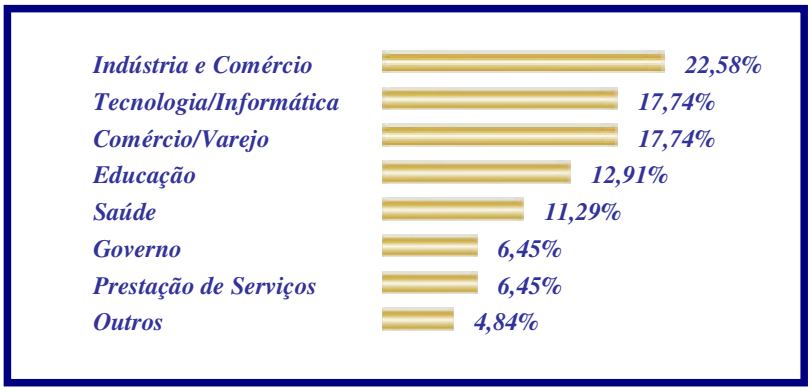
Para ter a informação com relação ao uso da Norma BS 7799 em Salvador foram aplicados 200 questionários para levantar os dados nas organizações através de respostas presenciais, via e-mail e por contato telefônico. No total, a pesquisa quantitativa teve uma amostra de 62 questionários respondidos, coletados entre 10 de agosto a 20 de setembro de 2005, junto a profissionais ligados às áreas de Tecnologia e Segurança da Informação.

As organizações que participaram deste estudo estão distribuídos em diversos segmentos, como: Indústria e Comércio (20%), Tecnologia/Informática (17,5%), Comércio/Varejo

(17,5%), Educação (12,5%) e Saúde (10%), Governo (7,5%), Prestação de Serviços (7,5%), Outros (5%). (vide lista no Apêndice II)

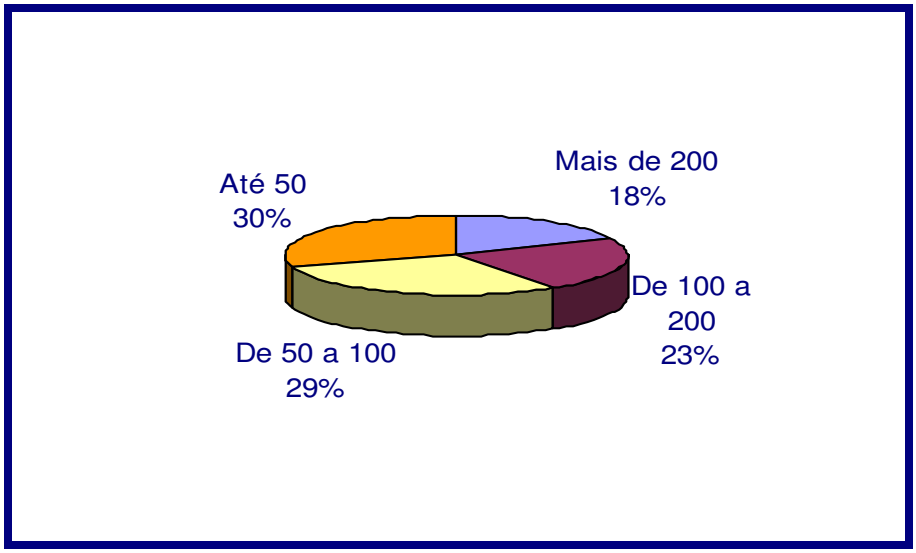
Perfil das Organizações Pesquisadas:

As organizações pesquisadas por ramos de atividade estão arroladas em ordem decrescente como se segue:

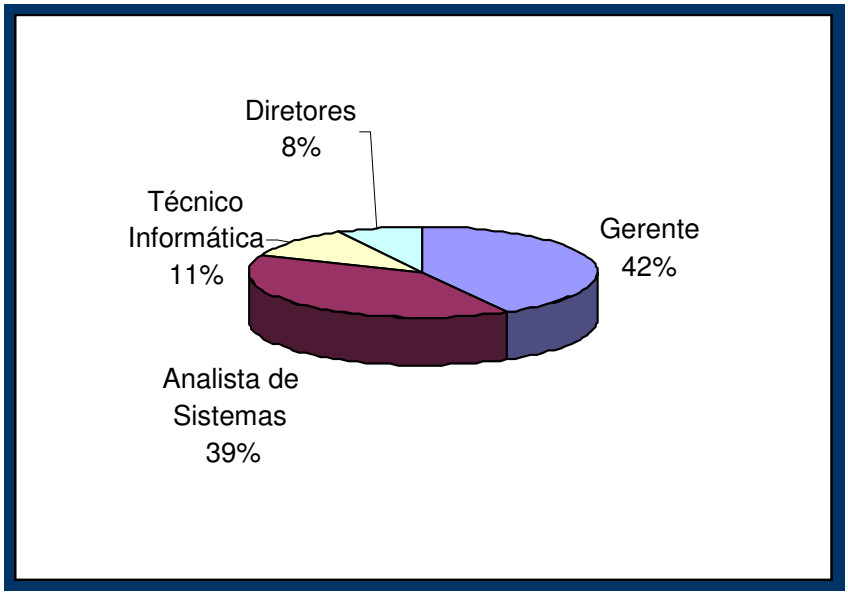


A capacidade do parque computational das organizações pesquisadas esta representada em número de computadores com: (30%) até 50 computadores, (29%) de 50 a 100 computadores, (23%) de 100 a 200 computadores e (18%) acima de 200 computadores.

As organizações pesquisadas por capacidade do parque computacional, número de computadores, estão apresentadas em quatro faixas como apresenta o gráfico abaixo:



O perfil profissional dos entrevistados está representado com: 42% Gerentes, 39% Analistas de Sistemas, 11% Técnicos em Informática, 8% Diretores. Como apresenta o gráfico abaixo:



5.4 RESULTADOS OBTIDOS

O questionário foi composto por 42 questões objetivas (vide Apêndice I), divididas e agrupadas em 11 tópicos com assuntos relativos aos controles da Norma. As respostas foram fechadas, podendo ser SIM ou NÃO. Cada um dos 11 tópicos possuem subtópicos com questionamentos relativos a um assunto específico com referência ao tópico que é agrupado. Para melhor visualização do resultado, ao final dos questionamentos de cada tópico apresenta-se uma média aritmética e um gráfico com o percentual de todos os questionamentos relacionados ao mesmo tópico.

Foram computadas somente as perguntas efetivamente respondidas e o resultado obtido na pesquisa foi baseado em processos que as organizações pesquisadas possuem. Analisando os questionários chega-se aos resultados que esclarecem o uso da Segurança da Informação nas organizações de Salvador. Foi usado a representação quantitativa para apoiar os elementos qualitativos do trabalho.

Primeiramente apresenta-se o resultado por ramo de atividade para possibilitar uma visão setorial do uso da Segurança da Informação nas organizações de Salvador e depois o resultado global.

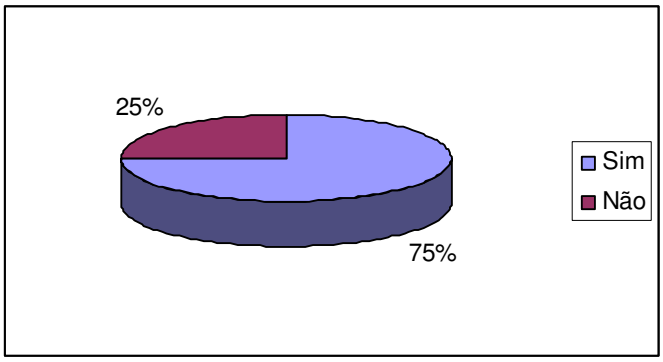
RESULTADO POR RAMO DE ATIVIDADE

- ✓ **Industria e Comercio**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	11	78,57%	3	21,43%
Algum responsável pela Gestão da Política	10	71,42%	4	28,58%

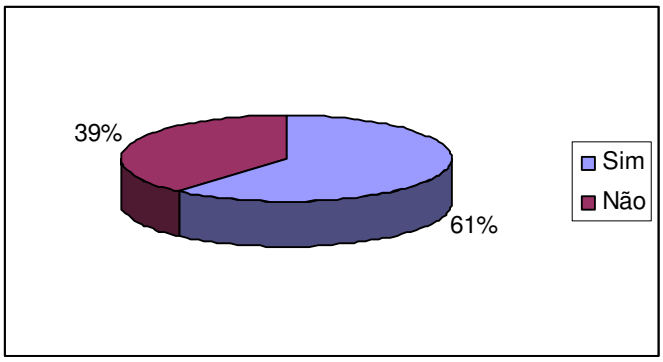
Média de Política de Segurança da Informação	75%	Sim	25%	Não



2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	10	71,42%	4	28,58%
Fórum de segurança formado pelo corpo diretor	5	35,71%	9	64,28%
Definição clara das atribuições associadas a segurança	9	64,28%	5	35,71%
Identificação dos riscos no acesso a prestadores de serviço	9	64,28%	5	35,71%
Controle de acesso específico para os prestadores de serviço	10	71,42%	4	28,58%
Requisitos de segurança dos contratos de terceirização	8	57,14%	6	42,86%

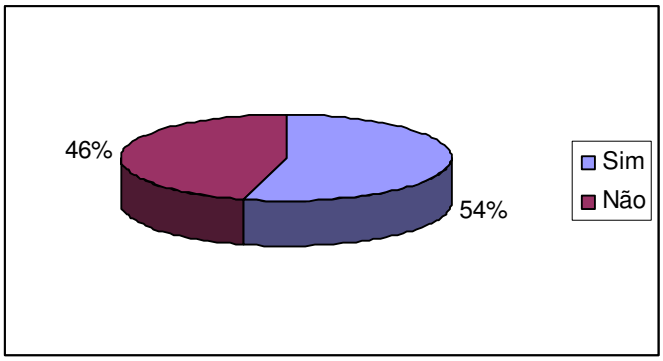
Média de Segurança Organizacional	60,7%	Sim	49,3%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	9	64,28%	5	35,71%
Critérios de classificação da informação	6	42,85%	8	57,14%

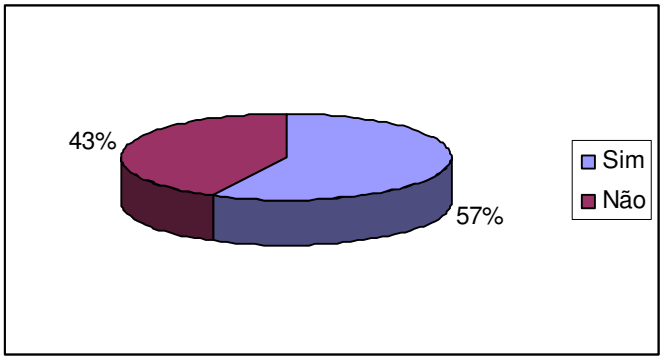
Média de Classificação e Controle dos ativos de Informação	53,56%	Sim	45,44%	Não



4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	10	71,42%	4	28,58%
Acordo de confidencialidade, termos e condições de trabalho	7	50%	7	50%
Processos para treinamento e capacitação de pessosas	9	64,28%	5	35,72%
Estrutura para notificar e responder aos incidentes de segurança	6	42,85%	8	57,14%

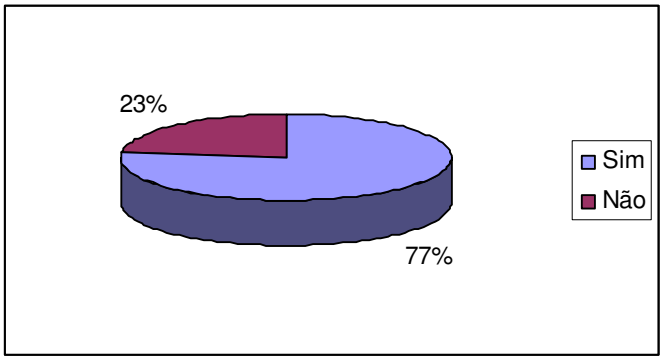
Média de Segurança em Pessoas	57,13%	Sim	42,87%	Não



5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	8	57,14%	6	42,86%
Recursos para segurança e manutenção dos equipamentos	12	85,71%	2	14,29%
Estrutura para fornecimento adequado de energia	11	78,57%	3	21,43%
Segurança de cabeamento de rede	12	85,71%	2	14,29%

Média de Segurança Física e de Ambientes	76,78%	Sim	23,22%	Não

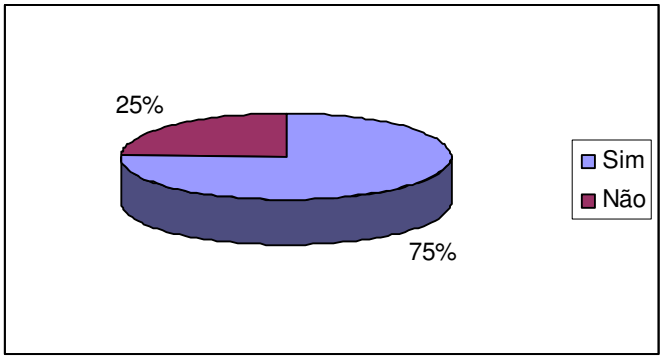


6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	12	85,71%	2	14,29%

Controles de mudanças operacionais	9	64,28%	5	35,72%
Segregação de funções e ambientes	8	57,14%	6	42,86%
Planejamento de aceitação de sistemas	13	92,85%	1	7,15%
Procedimento para cópia de segurança	12	85,71%	2	14,29%
Controles de gerenciamento de rede	13	92,85%	1	7,15%
Mecanismos de segurança e tratamento de mídias	8	57,14%	6	42,86%
Procedimentos para documentação de sistemas	9	64,28%	5	35,72%
Mecanismo de segurança do correio eletrônico	12	85,71%	2	14,29%

Média de Gerenciamento da Operações e Comunicações	75,39%	Sim	24,61%	Não

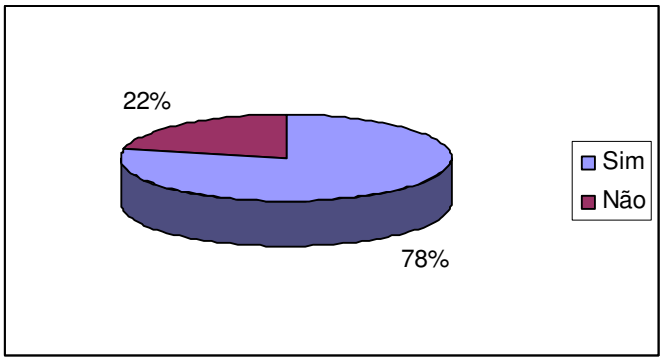


7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	9	64,28%	5	35,72%
Gerenciamento de acessos dos usuários	13	92,85%	1	7,15%
Controle de acesso a rede	12	85,71%	2	14,29%
Controle de acesso ao sistema operacional	14	100%	0	0%
Controles de acesso a aplicações	12	85,71%	2	14,29%
Monitoração de uso e acesso ao sistema	11	78,57%	3	21,43%

Critérios para computação móvel e trabalho remoto	6	42,85%	8	57,14%

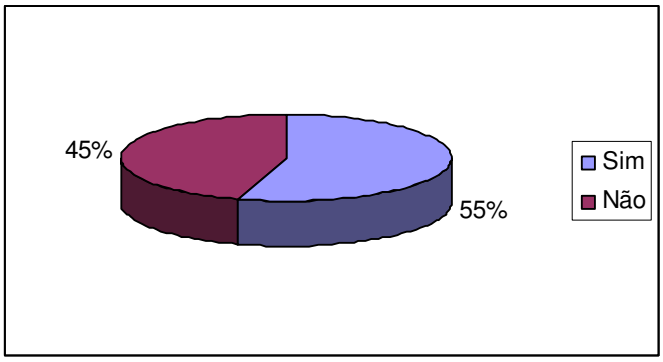
Média de Controle de Acesso	77,54%	Sim	22,45%	Não



8 - Desenvolvimento e manutenção de sistemas

As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	10	71,42%	4	28,58%
Controle de criptografia	5	35,71%	9	64,28%
Mecanismo de segurança nos processos de desenv. e suporte	8	57,14%	6	42,86%

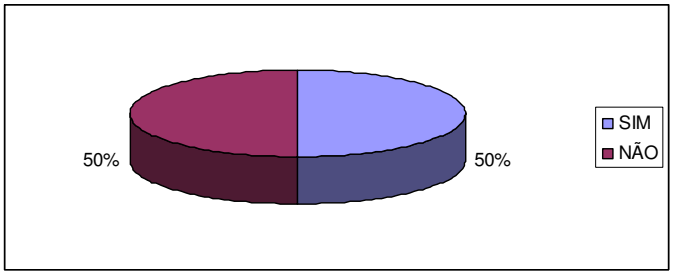
Média de Desenvolvimento e manutenção de sistemas	54,75%	Sim	45,25%	Não



9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	7	50%	7	50%

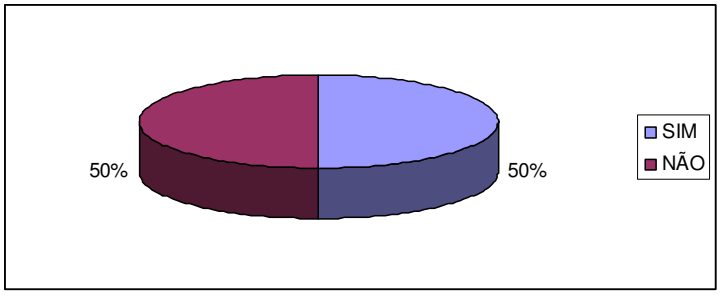
Média de Gestão da continuidade do negócio	50%	Sim	50%	Não



10 – Conformidade

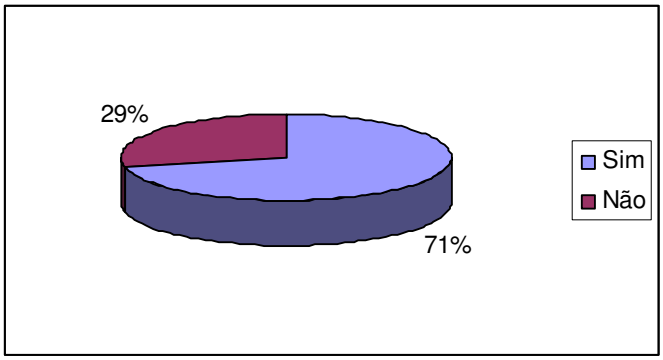
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	8	57,14%	6	42,86%
Recursos e critérios para auditoria de sistemas	6	42,86%	8	57,14%

Média de Conformidade	50%	Sim	50%	Não

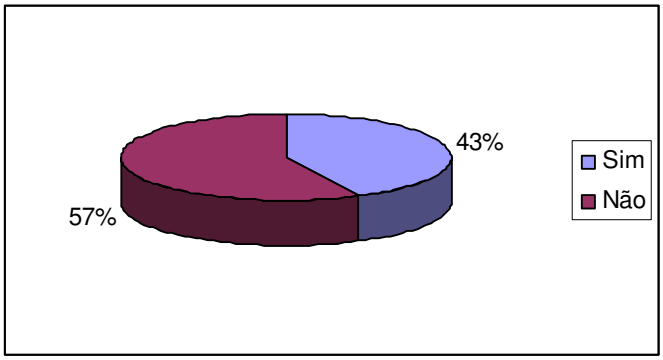


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	10	71,42%	4	28,58%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	6	42,85%	8	57,14%



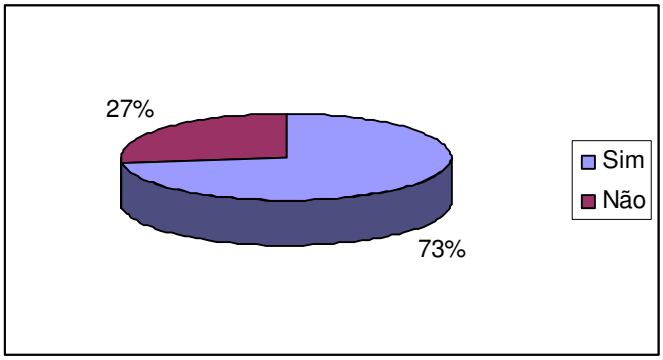
✓ **Tecnologia e Informática**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%

Política de Segurança	8	72,72	3	27,28%
Algum responsável pela Gestão da Política	8	72,72%	3	27,28%

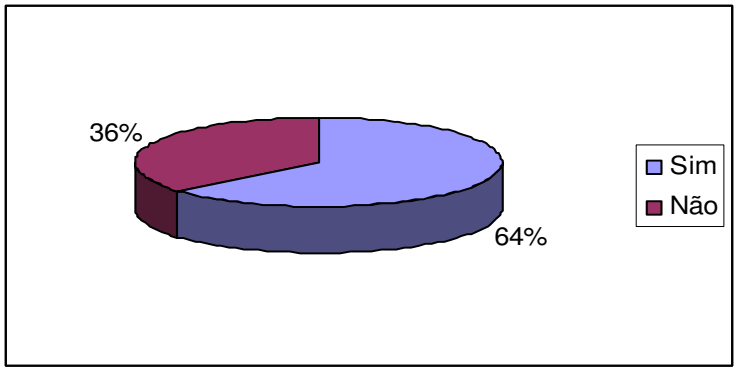
Média de Política de Segurança da Informação	72,72%	Sim	27,28%	Não



2 - Segurança Organizacional:

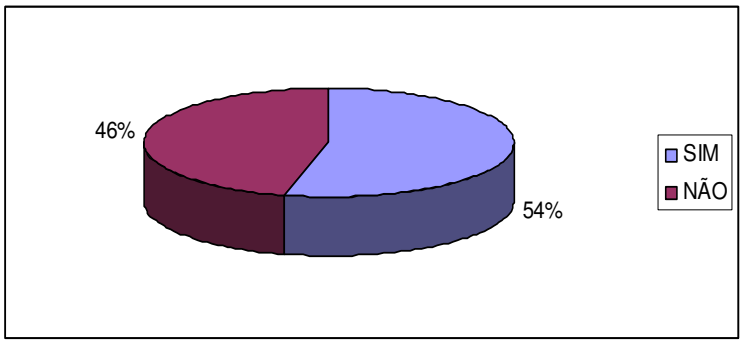
As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	9	81,81%	3	18,19%
Fórum de segurança formado pelo corpo diretor	4	36,36%	7	63,64%
Definição clara das atribuições associadas a segurança	7	63,63%	4	36,37%
Identificação dos riscos no acesso a prestadores de serviço	7	63,63%	4	36,37%
Controle de acesso específico para os prestadores de serviço	8	72,72%	3	27,28%
Requisitos de segurança dos contratos de terceirização	7	63,63%	4	36,37%

Média de Segurança Organizacional	63,63%	Sim	36,37%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	7	63,63%	436,37%	
Critérios de classificação da informação	5	45,45%	654,55%	
Média de Classificação e Controle dos ativos de Informação	54%	Sim	46%	Não

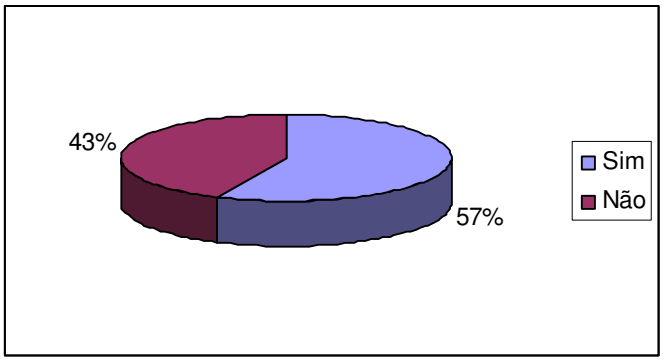


4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	7	63,63%	4	36,37%
Acordo de confidencialidade, termos e condições de trabalho	6	54,54%	5	45,56%
Processos para treinamento e capacitação de pessosas	7	63,63%	4	36,37%

Estrutura para notificar e responder aos incidentes de segurança	5	45,45%	6	54,55%

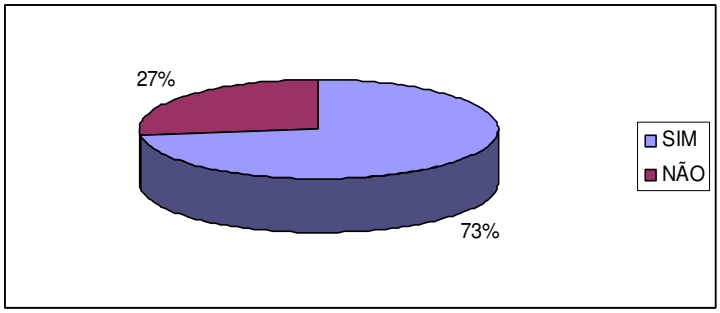
Média de Segurança em Pessoas	56,8%	Sim	43,2%	Não



5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	6	54,54%	5	45,56%
Recursos para segurança e manutenção dos equipamentos	9	81,81%	2	18,19%
Estrutura para fornecimento adequado de energia	9	81,81%	2	18,19%
Segurança de cabeamento de rede	8	72,72%	3	27,28%

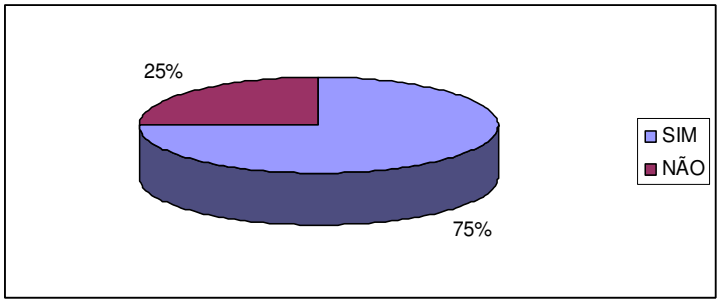
Média de Segurança Física e de Ambientes	72,72%	Sim	27,28%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	10	90,90%	1	9,10%
Controles de mudanças operacionais	7	63,63%	4	36,37%
Segregação de funções e ambientes	6	54,54%	5	45,56%
Planejamento de aceitação de sistemas	10	90,90%	1	9,10%
Procedimento para cópia de segurança	10	90,90%	1	9,10%
Controles de gerenciamento de rede	10	90,90%	1	9,10%
Mecanismos de segurança e tratamento de mídias	6	54,54%	5	45,56%
Procedimentos para documentação de sistemas	7	63,63%	4	36,37%
Mecanismo de segurança do correio eletrônico	9	81,81%	2	18,19%

Média de Gerenciamento da Operações e Comunicações	74,74% Sim	25,26% Não

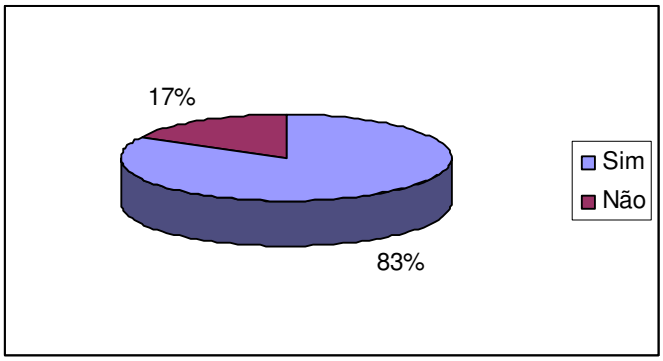


7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	7	63,63%	4	36,37%
Gerenciamento de acessos dos usuários	11	100%	0	0%
Controle de acesso a rede	10	90,90%	1	9,10%
Controle de acesso ao sistema operacional	11	100%	0	0%

Controles de acesso a aplicações	11	100%	0	0%
Monitoração de uso e acesso ao sistema	8	72,72%	3	27,28%
Critérios para computação móvel e trabalho remoto	6	54,54%	5	45,56%

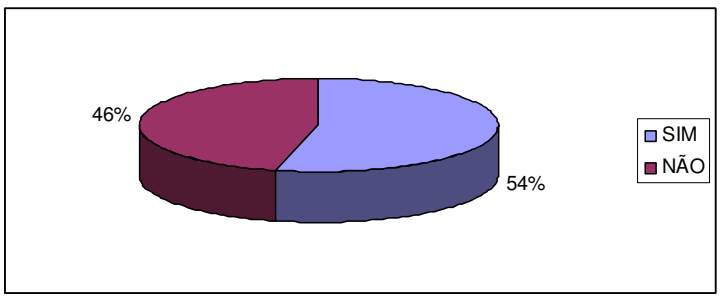
Média de Controle de Acesso	83,11%	Sim	16,89%	Não



8 - Desenvolvimento e manutenção de sistemas

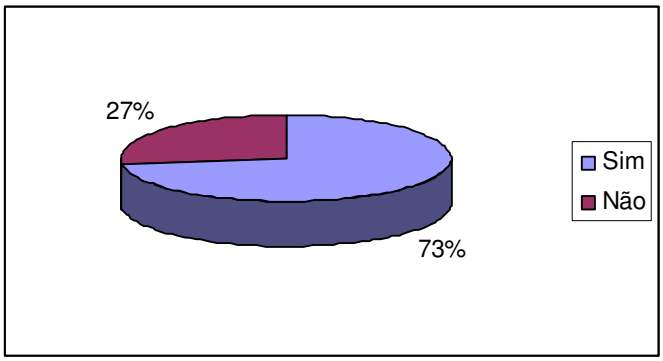
As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	8	72,72%	3	27,28%
Controle de criptografia	3	27,27%	8	72,73%
Mecanismo de segurança nos processos de desenv. e suporte	7	63,63%	4	36,37%

Média de Desenvolvimento e manutenção de sistemas	54,44%	Sim	45,56%	Não



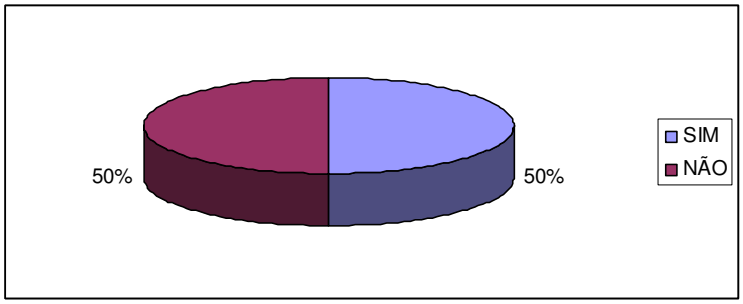
9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	8	72,72%	3	27,28%
Média de Gestão da continuidade do negócio	8	72,72%	3	27,28%



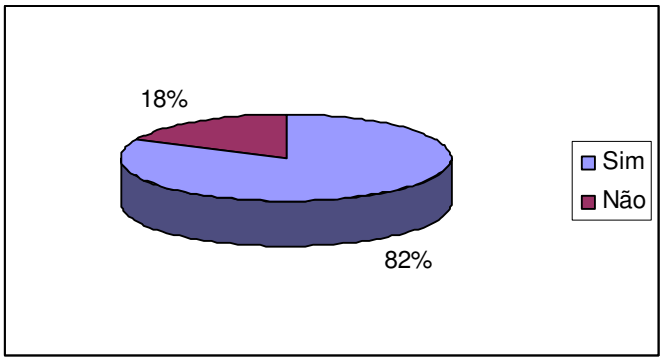
10 – Conformidade

As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	6	54,54%	5	45,56%
Recursos e critérios para auditoria de sistemas	5	45,45%	6	54,55%
Média de Conformidade	50%	Sim	50%	Não

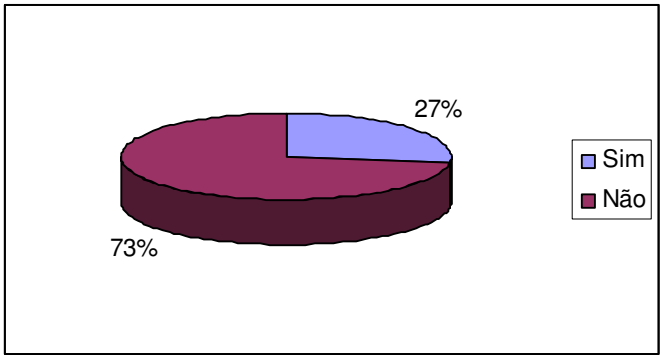


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	9	81,81%	2	18,19%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	3	27,27%	8	72,73%

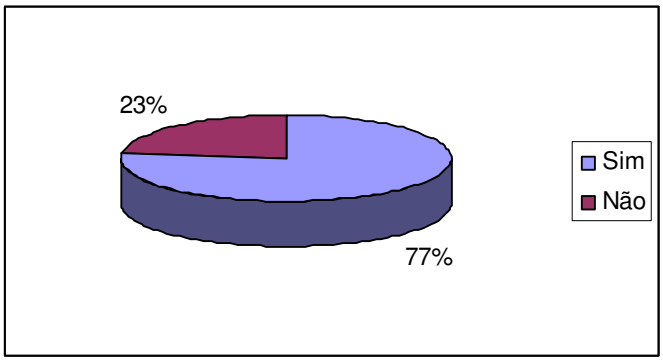


✓ **Comercio e Varejo**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	9	81,81	2	18,19%
Algum responsável pela Gestão da Política	8	72,72%	3	27,28%

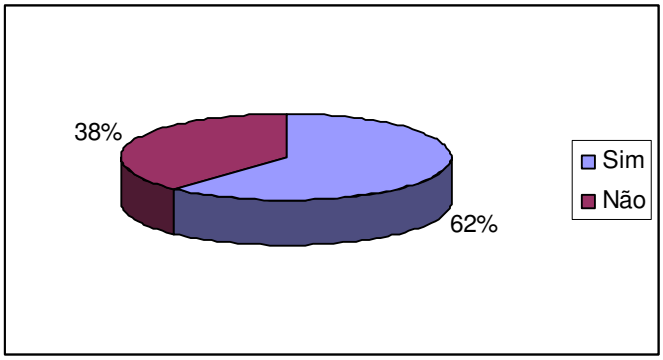
Média de Política de Segurança da Informação	77,26%	Sim	22,74%	Não



2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	9	81,81%	4	18,19%
Fórum de segurança formado pelo corpo diretor	5	45,45%	6	54,55%
Definição clara das atribuições associadas a segurança	7	63,63%	4	36,37%
Identificação dos riscos no acesso a prestadores de serviço	6	54,54%	5	45,56%
Controle de acesso específico para os prestadores de serviço	8	72,72%	3	27,28%
Requisitos de segurança dos contratos de terceirização	6	54,54%	5	45,56%

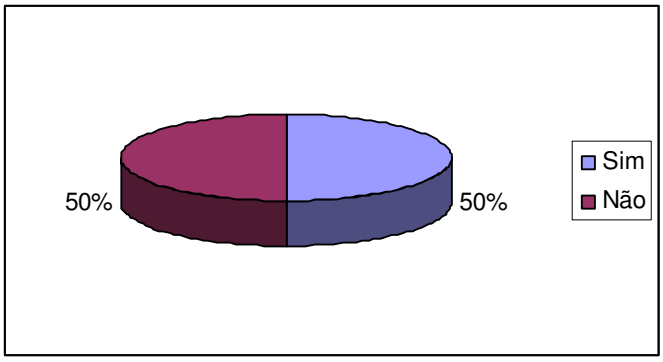
Média de Segurança Organizacional	62,11%	Sim	37,89%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	7	63,63%	4	36,37%
Critérios de classificação da informação	4	36,36%	7	63,67%

Média de Classificação e Controle dos ativos de Informação	50%	Sim	50%	Não

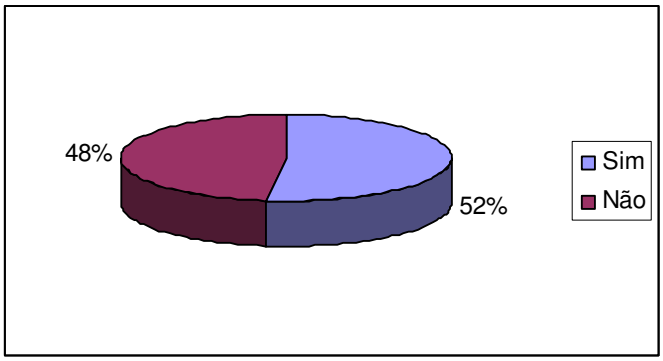


4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	6	54,54%	5	45,56%
Acordo de confidencialidade, termos e condições de trabalho	6	54,54%	5	45,56%
Processos para treinamento e capacitação de pessoas	7	63,63%	4	36,37%

Estrutura para notificar e responder aos incidentes de segurança	4	36,36%	7	63,67%

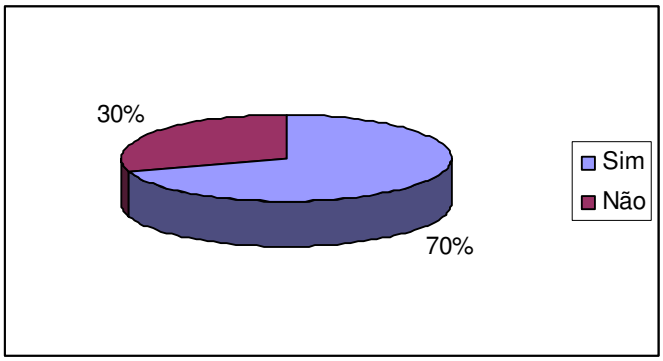
Média de Segurança em Pessoas	52,26%	Sim	47,78%	Não



5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	7	63,63%	4	36,37%
Recursos para segurança e manutenção dos equipamentos	7	63,63%	4	36,37%
Estrutura para fornecimento adequado de energia	8	72,72%	3	27,28%
Segurança de cabeamento de rede	9	81,81%	2	18,19%

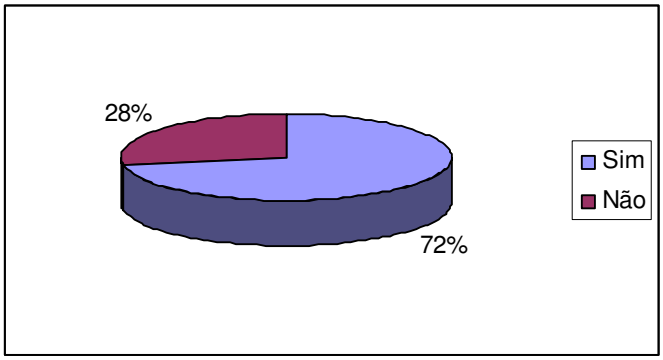
Média de Segurança Física e de Ambientes	70,44%	Sim	29,56%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	10	90,90%	1	9,10%
Controles de mudanças operacionais	6	54,54%	5	45,56%
Segregação de funções e ambientes	6	54,54%	5	45,56%
Planejamento de aceitação de sistemas	10	90,90%	1	9,10%
Procedimento para cópia de segurança	10	90,90%	1	9,10%
Controles de gerenciamento de rede	10	90,90%	1	9,10%
Mecanismos de segurança e tratamento de mídias	5	45,45%	6	54,55%
Procedimentos para documentação de sistemas	6	54,54%	5	45,56%
Mecanismo de segurança do correio eletrônico	9	81,81%	3	18,19%

Média de Gerenciamento da Operações e Comunicações	71,71%	Sim	28,29%	Não

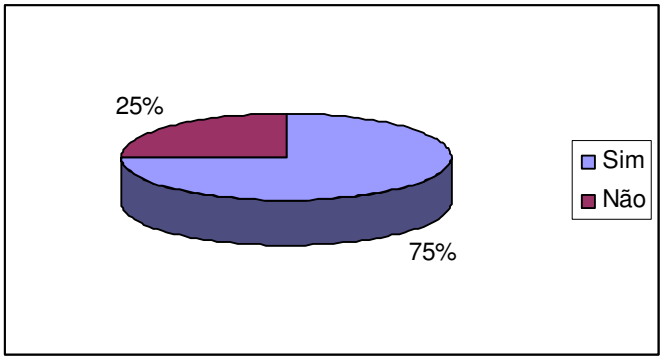


7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	7	63,63%	4	36,37%
Gerenciamento de acessos dos usuários	10	90,90%	1	9,10%
Controle de acesso a rede	10	90,90%	1	9,10%

Controle de acesso ao sistema operacional	11	100%	0	0%
Controles de acesso a aplicações	8	72,72%	3	27,28%
Monitoração de uso e acesso ao sistema	9	81,81%	2	18,19%
Critérios para computação móvel e trabalho remoto	4	36,36	7	63,64%%

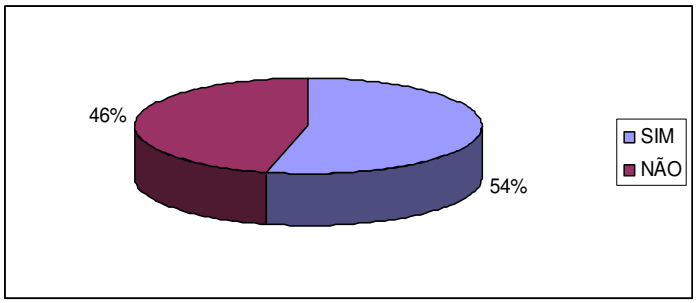
Média de Controle de Acesso	75,31%	Sim	34,69%	Não



8 - Desenvolvimento e manutenção de sistemas

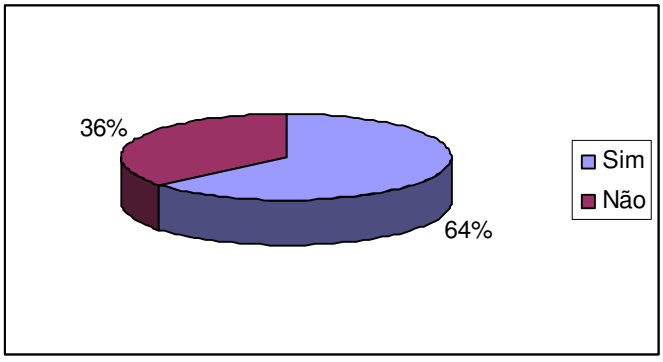
As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	9	81,81%	2	18,19%
Controle de criptografia	2	18,18	9	81,82%
Mecanismo de segurança nos processos de desenv. e suporte	7	63,63%	4	36,37%

Média de Desenvolvimento e manutenção de sistemas	54,44%	Sim	45,56%	Não



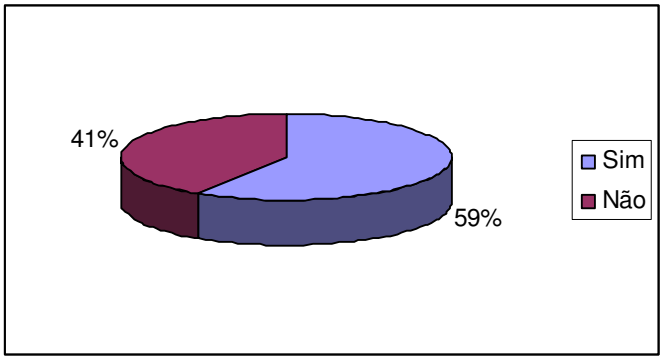
9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	7	63,63%	4	36,37%
Média de Gestão da continuidade do negócio	7	63,63%	4	36,37%



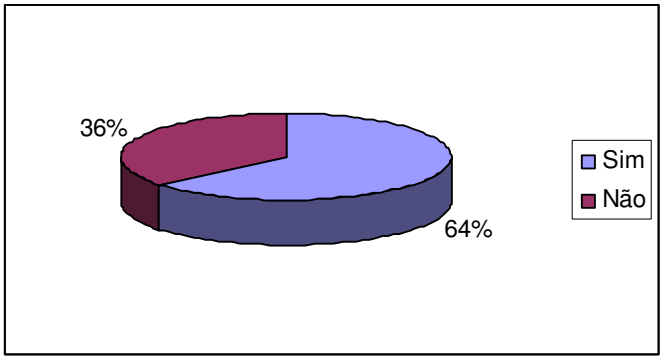
10 – Conformidade

As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	7	63,63%	4	36,37%
Recursos e critérios para auditoria de sistemas	6	54,54%	5	45,56%
Média de Conformidade	59%	Sim	41%	Não

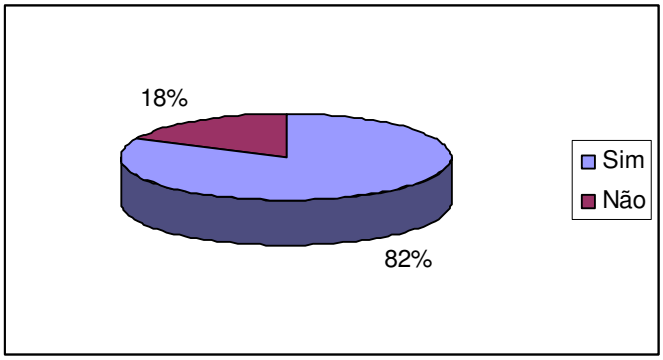


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	7	63,63%	4	36,37%



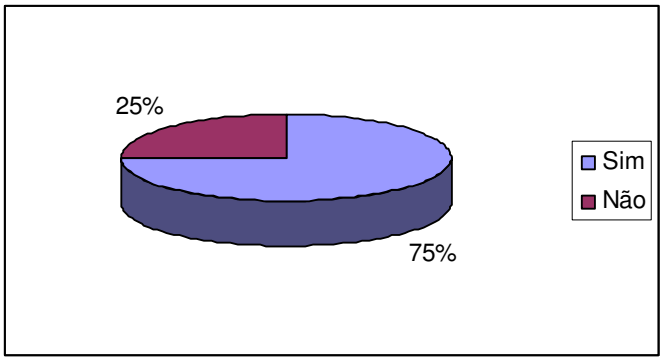
As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	2	18,18%	9	81,82%



✓ **Empresas com ramo de atividade Educacao**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	6	75%	2	25%
Algum responsável pela Gestão da Política	6	75%	2	25%
Média de Política de Segurança da Informação		75% Sim		25% Não

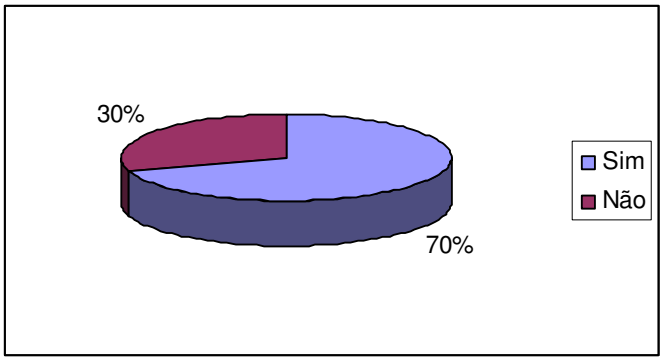


2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	5	62,5%	3	27,5%

Fórum de segurança formado pelo corpo diretor	3	37,5%	5	62,5%
Definição clara das atribuições associadas a segurança	5	62,5%	3	27,5%
Identificação dos riscos no acesso a prestadores de serviço	5	62,5%	3	27,5%
Controle de acesso específico para os prestadores de serviço	6	75%	2	25%
Requisitos de segurança dos contratos de terceirização	5	62,5%	3	27,5%

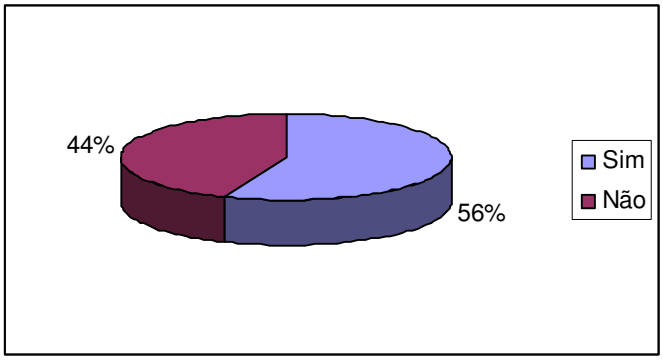
Média de Segurança Organizacional	70,08%	Sim	29,82%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	5	62,5%	3	27,5%
Critérios de classificação da informação	4	50%	4	50%

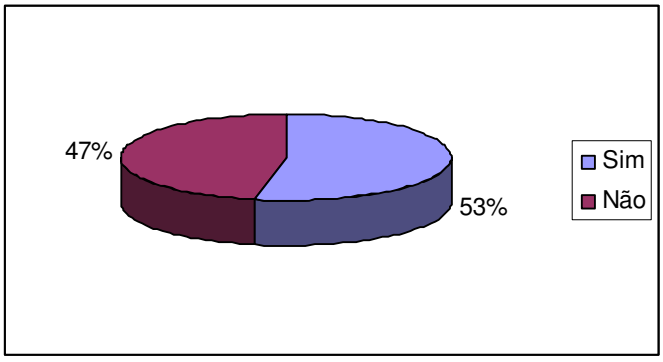
Média de Classificação e Controle dos ativos de Informação	56,25%	Sim	43,75%	Não



4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	5	62,5%	3	27,5%
Acordo de confidencialidade, termos e condições de trabalho	4	50%	4	50%
Processos para treinamento e capacitação de pessosas	5	62,5%	3	27,5%
Estrutura para notificar e responder aos incidentes de segurança	3	37,5%	5	62,5%

Média de Segurança em Pessoas	53,15% Sim	46,85%Não

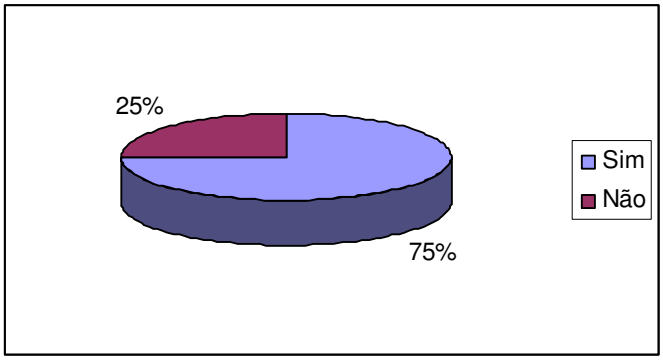


5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%

Controles de acesso físico aos ambientes	4	50%	4	50%
Recursos para segurança e manutenção dos equipamentos	7	87,5%	1	12,5%
Estrutura para fornecimento adequado de energia	7	87,5%	1	12,5%
Segurança de cabeamento de rede	6	75%	2	25%

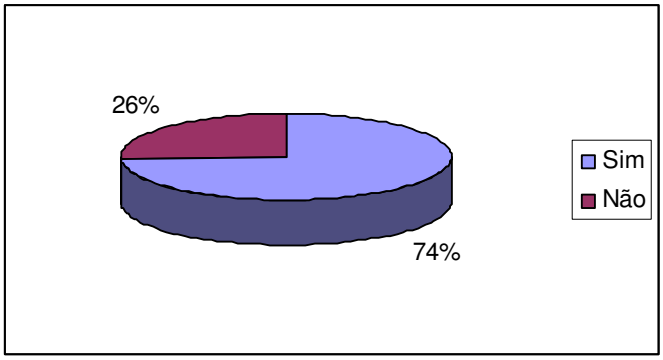
Média de Segurança Física e de Ambientes	75%	Sim	25%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	7	87,5%	1	12,5%
Controles de mudanças operacionais	5	62,5%	3	27,5%
Segregação de funções e ambientes	4	50%	4	50%
Planejamento de aceitação de sistemas	7	87,5%	1	12,5%
Procedimento para cópia de segurança	7	87,5%	1	12,5%
Controles de gerenciamento de rede	7	87,5%	1	12,5%
Mecanismos de segurança e tratamento de mídias	4	50%	4	50%
Procedimentos para documentação de sistemas	5	62,5%	3	27,5%
Mecanismo de segurança do correio eletrônico	7	87,5%	1	12,5%

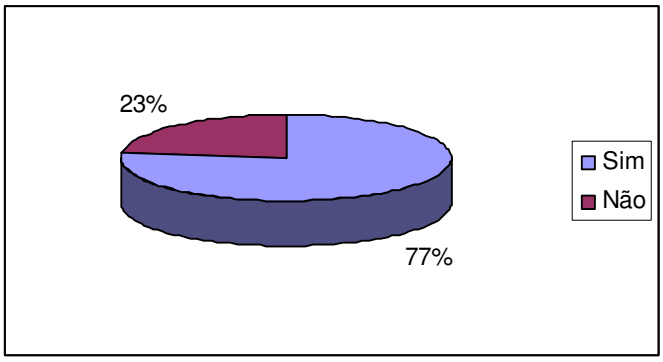
Média de Gerenciamento da Operações e Comunicações	73,6%	Sim	26,4%	Não



7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	5	62,5%	3	27,5%
Gerenciamento de acessos dos usuários	7	87,5%	1	12,5%
Controle de acesso a rede	7	87,5%	1	12,5%
Controle de acesso ao sistema operacional	8	100%	0	0%
Controles de acesso a aplicações	7	87,5%	1	12,5%
Monitoração de uso e acesso ao sistema	6	75%	2	25%
Critérios para computação móvel e trabalho remoto	4	50%	4	50%

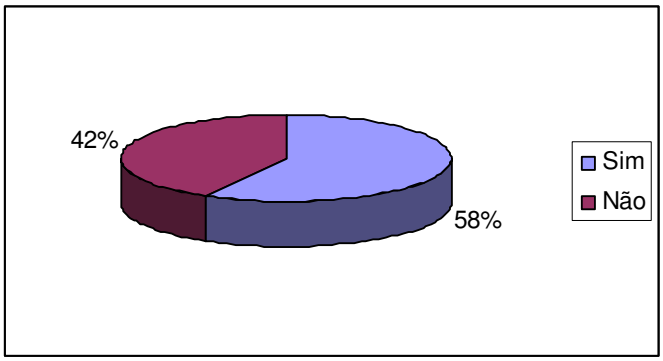
Média de Controle de Acesso	76,7%	Sim	23,3%	Não



8 - Desenvolvimento e manutenção de sistemas

As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	6	75%	2	25%
Controle de criptografia	3	37,5%	5	62,5%
Mecanismo de segurança nos processos de desenv. e suporte	5	62,5%	3	27,5%

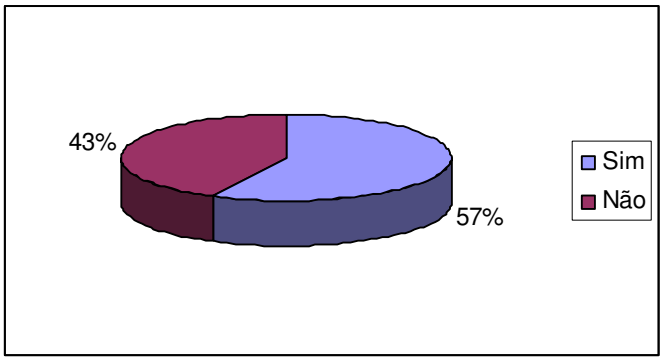
Média de Desenvolvimento e manutenção de sistemas	58,30%	Sim	41,7%	Não



9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	5	62,5%	3	27,5%

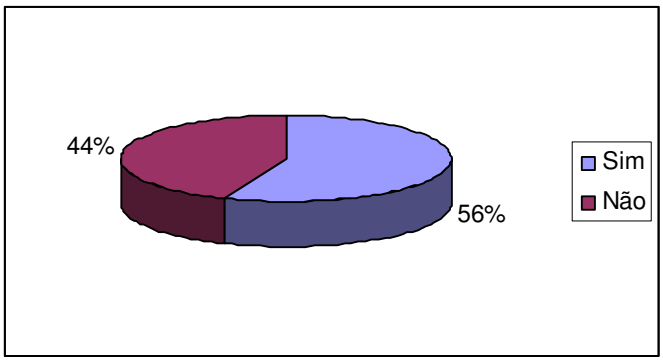
Média de Gestão da continuidade do negócio	62,5%	Sim	47,5%	Não



10 – Conformidade

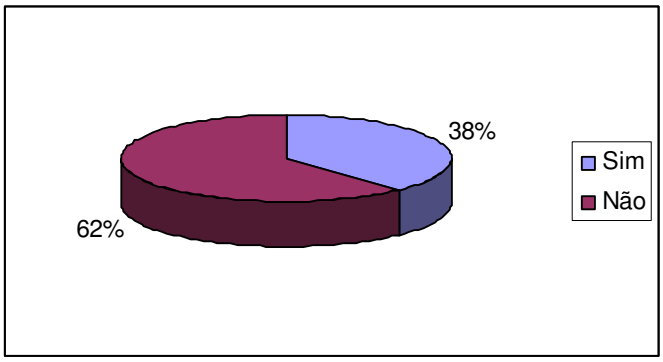
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	5	62,5%	3	27,5%
Recursos e critérios para auditoria de sistemas	4	50%	4	50%

Média de Conformidade	56,25%	Sim	43,75%	Não

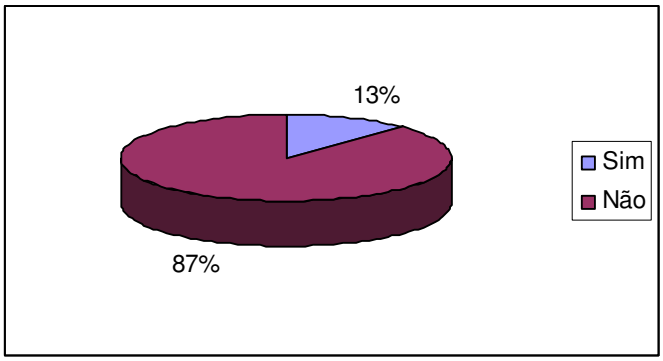


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	3	37,5%	5	62,5%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	1	12,5%	7	87,5%

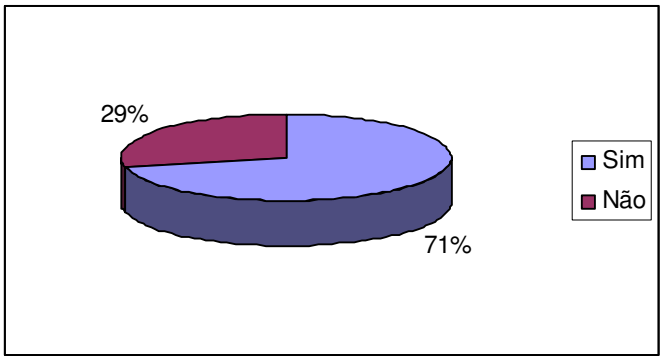


✓ **Empresas com ramo de atividade Saude**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	5	71,42%	2	28,58%
Algum responsável pela Gestão da Política	5	71,42%	2	28,58%

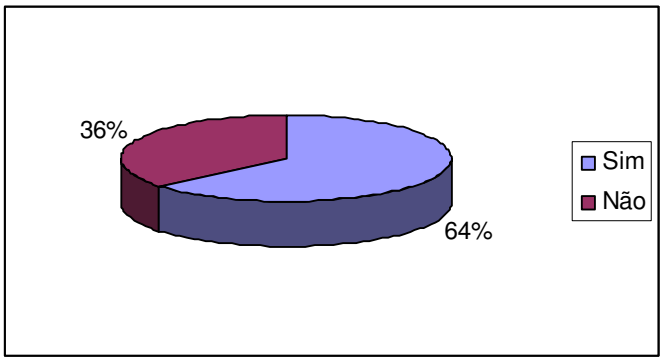
Média de Política de Segurança da Informação	71,42% Sim	28,48%Não



2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	4	57,14%	3	42,86%
Fórum de segurança formado pelo corpo diretor	3	42,85%	4	57,15%
Definição clara das atribuições associadas a segurança	5	71,42%	2	28,56%
Identificação dos riscos no acesso a prestadores de serviço	6	85,71%	1	14,29%
Controle de acesso específico para os prestadores de serviço	5	71,42%	2	28,56%
Requisitos de segurança dos contratos de terceirização	4	57,14%	3	42,86%

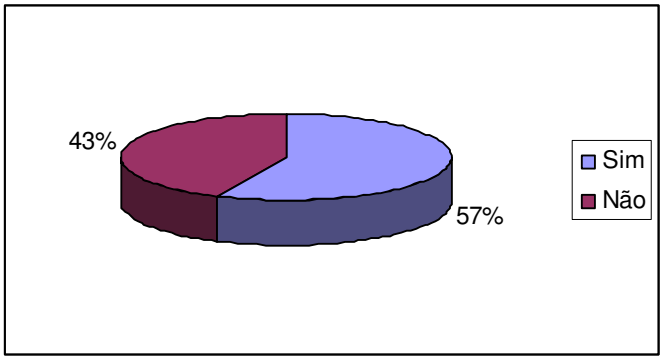
Média de Segurança Organizacional	64,28%	Sim	35,82%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	5	71,42%	2	28,56%
Critérios de classificação da informação	3	42,85%	4	57,14%

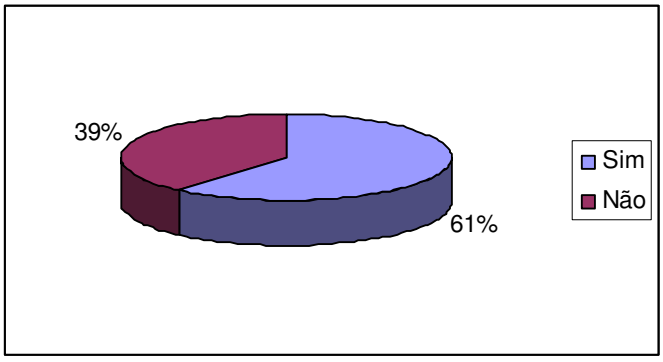
Média de Classificação e Controle dos ativos de Informação	57,13%	Sim	42,87%	Não



4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	6	85,71%	1	14,29%
Acordo de confidencialidade, termos e condições de trabalho	4	57,14%	3	42,86%
Processos para treinamento e capacitação de pessosas	4	57,14%	3	42,86%
Estrutura para notificar e responder aos incidentes de segurança	3	42,85%	4	57,14%

Média de Segurança em Pessoas	60,71%	Sim	39,29%	Não

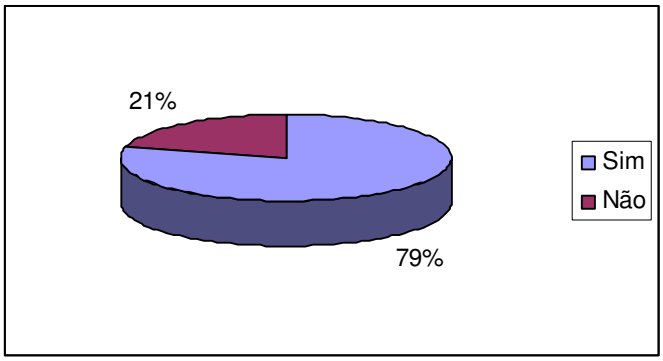


5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	4	57,14%	3	42,86%

Recursos para segurança e manutenção dos equipamentos	7	100%	0	0%
Estrutura para fornecimento adequado de energia	6	85,71%	1	14,29%
Segurança de cabeamento de rede	5	71,42%	2	28,56%

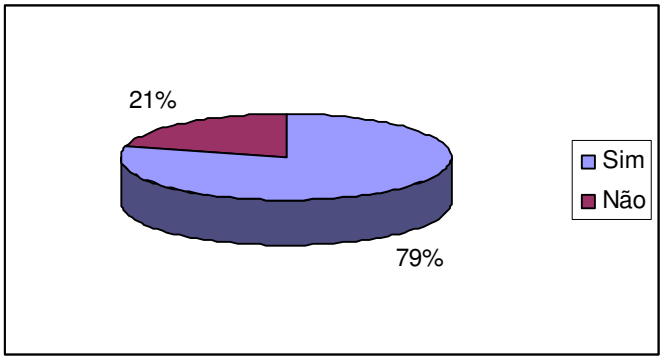
Média de Segurança Física e de Ambientes	78,56%	Sim	21,44%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	6	85,71%	1	14,29%
Controles de mudanças operacionais	6	85,71%	1	14,29%
Segregação de funções e ambientes	4	57,14%	3	42,86%
Planejamento de aceitação de sistemas	6	85,71%	1	14,29%
Procedimento para cópia de segurança	6	85,71%	1	14,29%
Controles de gerenciamento de rede	6	85,71%	1	14,29%
Mecanismos de segurança e tratamento de mídias	4	57,14%	3	42,86%
Procedimentos para documentação de sistemas	6	85,71%	1	14,29%
Mecanismo de segurança do correio eletrônico	6	85,71%	1	14,29%

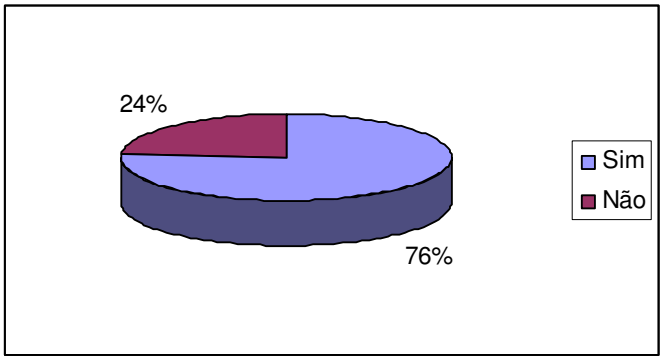
Média de Gerenciamento da Operações e Comunicações	79,36%	Sim	20,64%	Não



7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	4	57,14%	3	42,86%
Gerenciamento de acessos dos usuários	6	85,71%	1	14,29%
Controle de acesso a rede	6	85,71%	1	14,29%
Controle de acesso ao sistema operacional	7	100%	0	0%
Controles de acesso a aplicações	7	100%	0	0%
Monitoração de uso e acesso ao sistema	5	71,42%	2	28,56%
Critérios para computação móvel e trabalho remoto	2	28,57%	7	71,43%

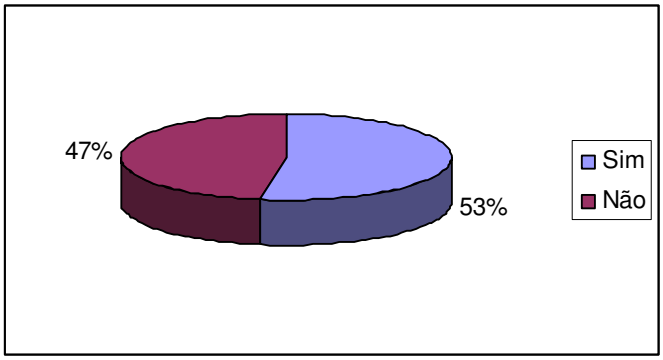
Média de Controle de Acesso	75,5%	Sim	24,5%	Não



8 - Desenvolvimento e manutenção de sistemas

As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	5	71,42%	2	28,56%
Controle de criptografia	2	28,57%	5	71,43%
Mecanismo de segurança nos processos de desenv. e suporte	4	57,14%	3	42,86%

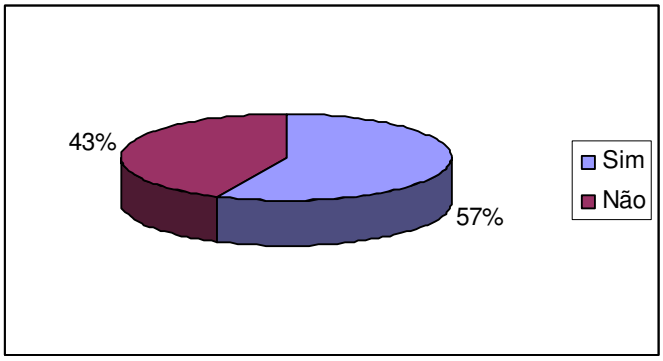
Média de Desenvolvimento e manutenção de sistemas	52,37%	Sim	47,63%	Não



9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	4	57,14%	3	42,86%

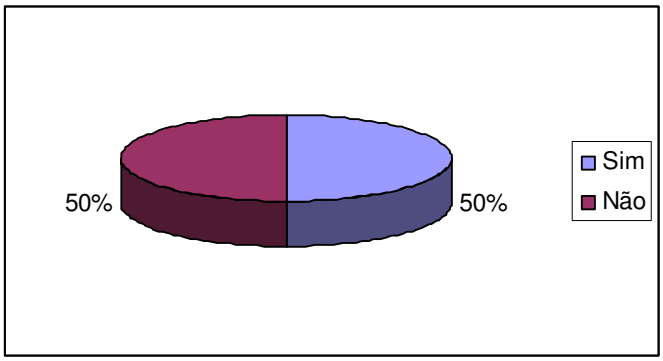
Média de Gestão da continuidade do negócio	57,14%	Sim	42,86%	Não



10 – Conformidade

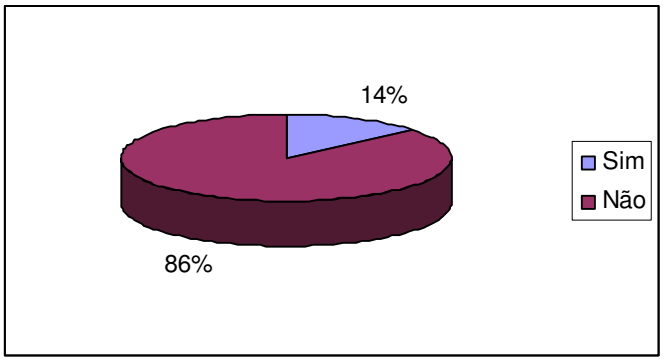
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	4	57,14%	3	42,86%
Recursos e critérios para auditoria de sistemas	3	42,85%	4	57,14%

Média de Conformidade	50%	Sim	50%	Não

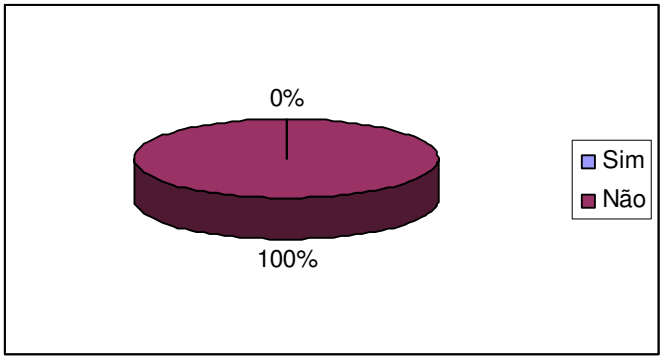


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	1	14,28%	6	85,72%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	0	0%	7	100%

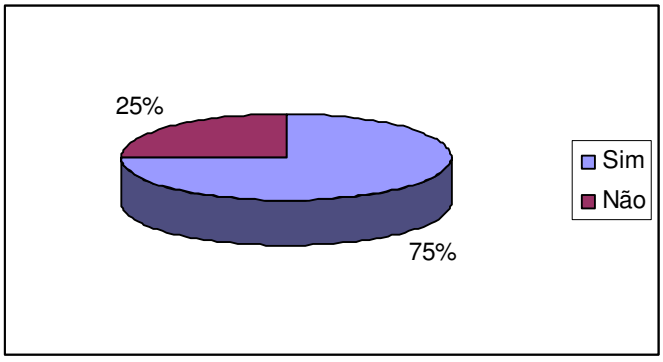


✓ **Empresas com ramo de atividade Governo**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	3	75%	1	25%
Algum responsável pela Gestão da Política	3	75%	1	25%

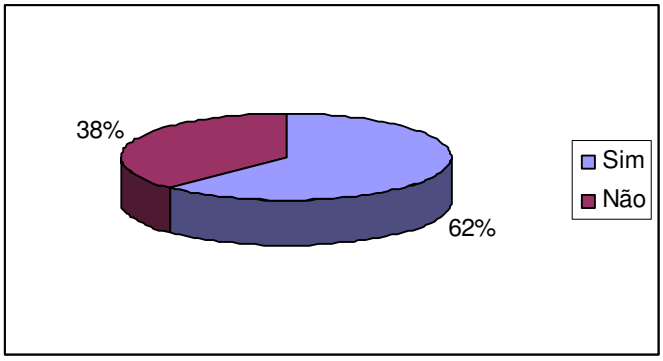
Média de Política de Segurança da Informação	75%	Sim	25%	Não



2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	3	75%	1	25%
Fórum de segurança formado pelo corpo diretor	2	50%	2	50%
Definição clara das atribuições associadas a segurança	3	75%	1	25%
Identificação dos riscos no acesso a prestadores de serviço	3	75%	1	25%
Controle de acesso específico para os prestadores de serviço	4	100%	0	0%
Requisitos de segurança dos contratos de terceirização	3	75%	1	25%

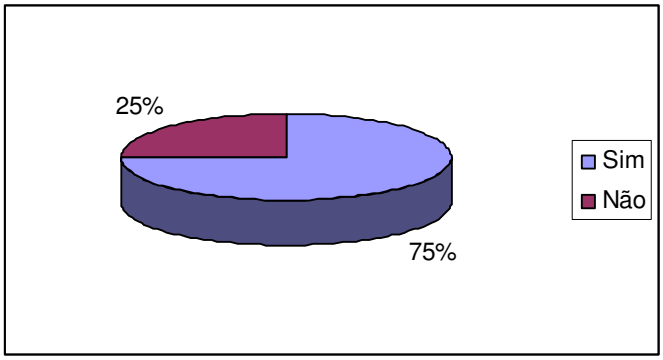
Média de Segurança Organizacional	62,5%	Sim	37,5%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	4	100%	0	0%
Critérios de classificação da informação	2	50%	2	50%

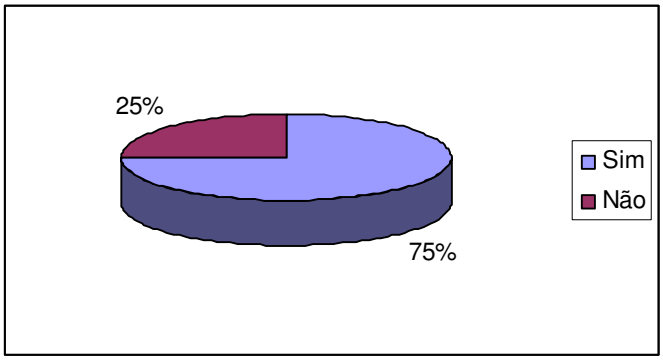
Média de Classificação e Controle dos ativos de Informação	75%	Sim	25%	Não



4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	4	100%	0	0%
Acordo de confidencialidade, termos e condições de trabalho	3	75%	1	25%
Processos para treinamento e capacitação de pessosas	2	50%	2	50%
Estrutura para notificar e responder aos incidentes de segurança	3	75%	1	25%

Média de Segurança em Pessoas	75%	Sim	25%	Não

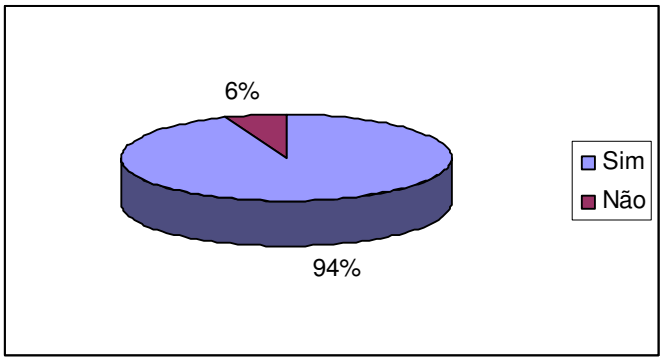


5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	3	75%	1	25%

Recursos para segurança e manutenção dos equipamentos	4	100%	0	0%
Estrutura para fornecimento adequado de energia	4	100%	0	0%
Segurança de cabeamento de rede	4	100%	0	0%

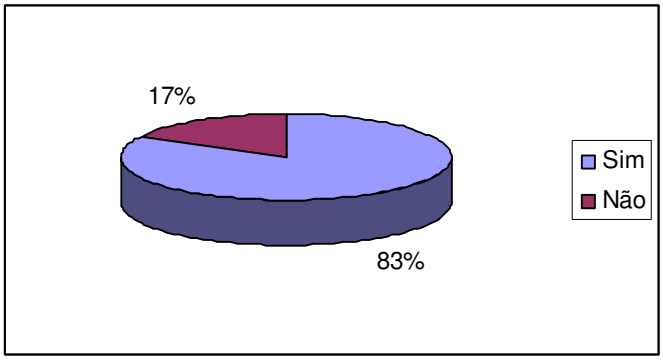
Média de Segurança Física e de Ambientes	93,75%	Sim	6,25%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	4	100%	0	0%
Controles de mudanças operacionais	3	75%	1	25%
Segregação de funções e ambientes	3	75%	1	25%
Planejamento de aceitação de sistemas	3	75%	1	25%
Procedimento para cópia de segurança	4	100%	0	0%
Controles de gerenciamento de rede	4	100%	0	0%
Mecanismos de segurança e tratamento de mídias	3	75%	1	25%
Procedimentos para documentação de sistemas	3	75%	1	25%
Mecanismo de segurança do correio eletrônico	4	100%	0	0%

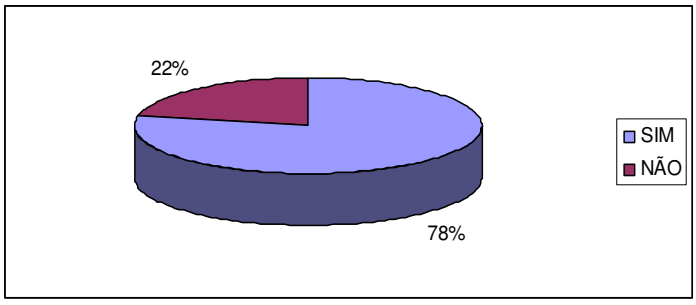
Média de Gerenciamento da Operações e Comunicações	83,33%	Sim	16,67%	Não



7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	3	75%	1	25%
Gerenciamento de acessos dos usuários	4	100%	0	0%
Controle de acesso a rede	4	100%	0	0%
Controle de acesso ao sistema operacional	4	100%	0	0%
Controles de acesso a aplicações	3	75%	1	25%
Monitoração de uso e acesso ao sistema	3	75%	1	25%
Critérios para computação móvel e trabalho remoto	1	25%	3	75%

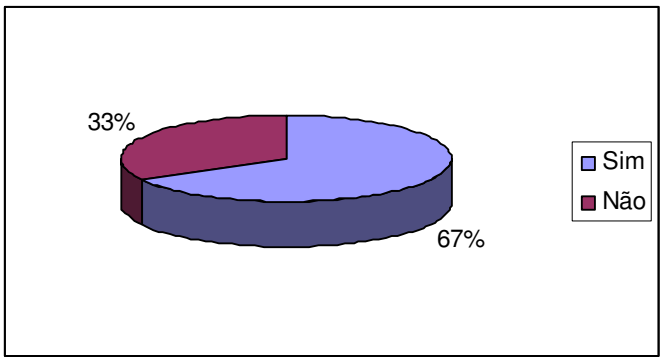
Média de Controle de Acesso	78%	Sim	22%	Não



8 - Desenvolvimento e manutenção de sistemas

As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	2	50%	2	50%
Controle de criptografia	3	75%	1	25%
Mecanismo de segurança nos processos de desenv. e suporte	3	75%	1	25%

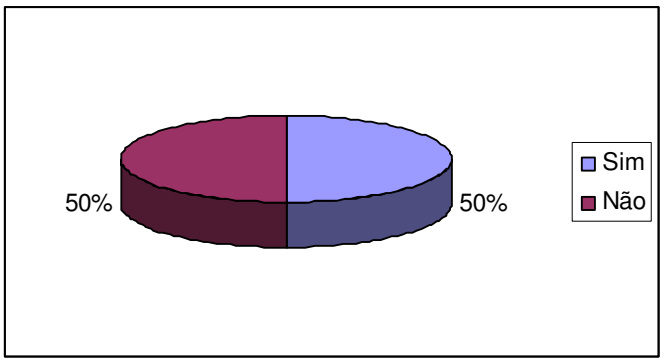
Média de Desenvolvimento e manutenção de sistemas	66,66%	Sim	43,34%	Não



9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	2	50%	2	50%

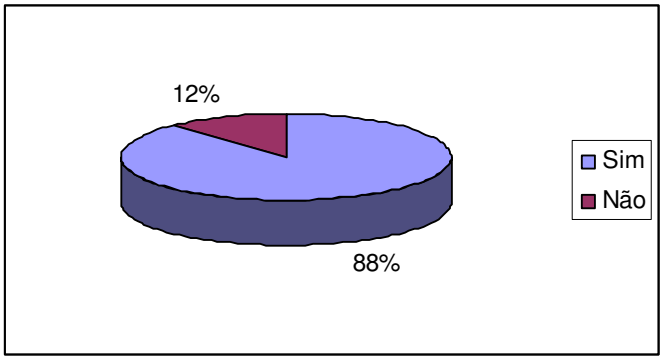
Média de Gestão da continuidade do negócio	50%	Sim	50%	Não



10 – Conformidade

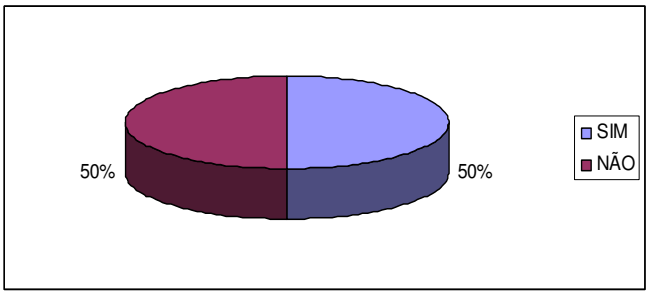
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	3	75%	1	25%
Recursos e critérios para auditoria de sistemas	4	100%	0	0%

Média de Conformidade	87,5%	Sim	22,5%	Não

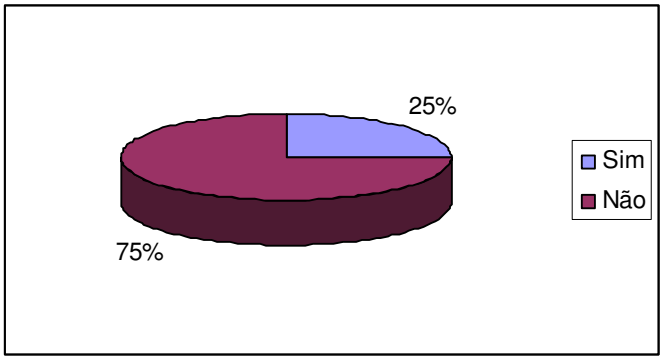


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	2	50%	2	50%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	1	25%	3	75%

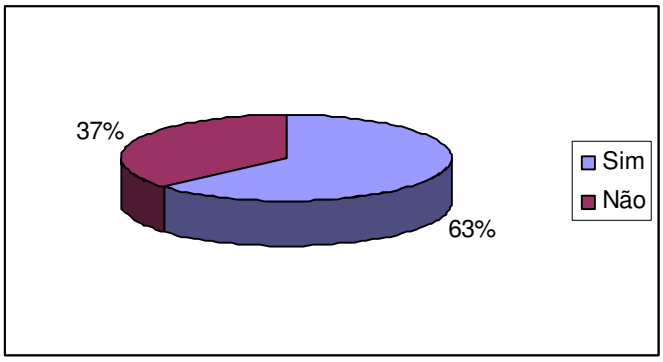


✓ **Prestação de Serviços**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	3	75%	1	25%
Algum responsável pela Gestão da Política	2	50%	2	50%

Média de Política de Segurança da Informação	62,5%	Sim	37,5%	Não

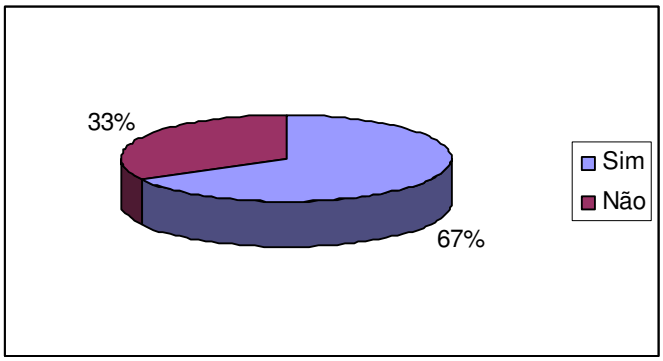


2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	3	75%	1	25%

Fórum de segurança formado pelo corpo diretor	1	25%	3	75%
Definição clara das atribuições associadas a segurança	3	75%	1	25%
Identificação dos riscos no acesso a prestadores de serviço	4	100%	0	0%
Controle de acesso específico para os prestadores de serviço	3	75%	1	25%
Requisitos de segurança dos contratos de terceirização	2	50%	2	50%

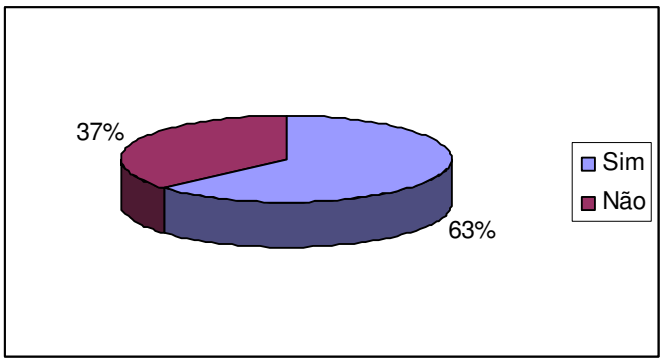
Média de Segurança Organizacional	66,66%	Sim	33,34%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	3	75%	1	25%
Critérios de classificação da informação	2	50%	2	50%

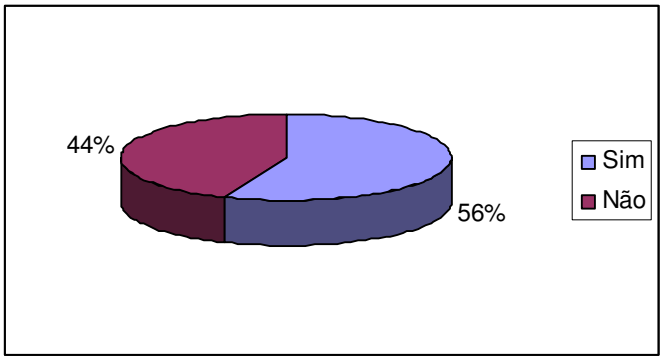
Média de Classificação e Controle dos ativos de Informação	62,5%	Sim	37,5%	Não



4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	3	75%	1	25%
Acordo de confidencialidade, termos e condições de trabalho	2	50%	2	50%
Processos para treinamento e capacitação de pessosas	2	50%	2	50%
Estrutura para notificar e responder aos incidentes de segurança	2	50%	2	50%

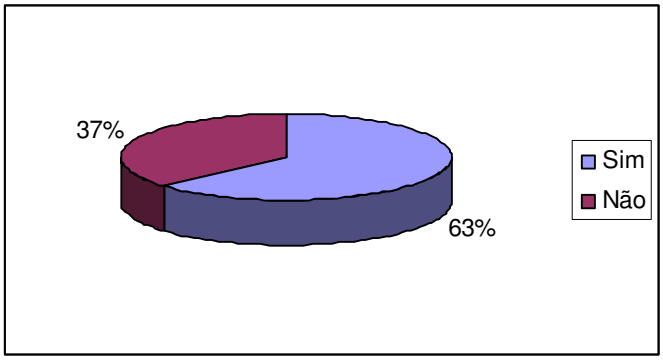
Média de Segurança em Pessoas	56,25%	Sim	43,75%	Não



5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	1	25%	3	75%
Recursos para segurança e manutenção dos equipamentos	3	75%	1	25%
Estrutura para fornecimento adequado de energia	4	100%	0	0%
Segurança de cabeamento de rede	2	50%	2	50%

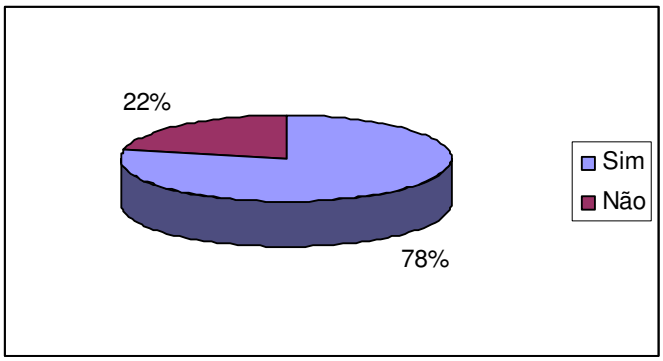
Média de Segurança Física e de Ambientes	62,5%	Sim	37,5%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	4	100%	0	0%
Controles de mudanças operacionais	4	100%	0	0%
Segregação de funções e ambientes	2	50%	2	50%
Planejamento de aceitação de sistemas	4	100%	0	0%
Procedimento para cópia de segurança	3	75%	1	25%
Controles de gerenciamento de rede	3	75%	1	25%
Mecanismos de segurança e tratamento de mídias	3	75%	1	25%
Procedimentos para documentação de sistemas	4	100%	0	0%
Mecanismo de segurança do correio eletrônico	3	75%	1	25%

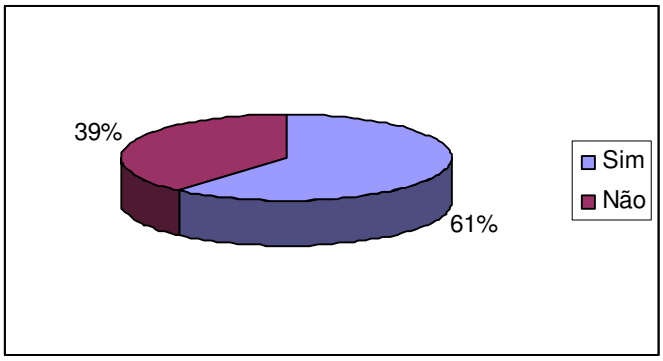
Média de Gerenciamento da Operações e Comunicações	77,77%	Sim	22,23%	Não



7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	2	50%	2	50%
Gerenciamento de acessos dos usuários	3	75%	1	25%
Controle de acesso a rede	3	75%	1	25%
Controle de acesso ao sistema operacional	3	75%	1	25%
Controles de acesso a aplicações	3	75%	1	25%
Monitoração de uso e acesso ao sistema	3	75%	1	25%
Critérios para computação móvel e trabalho remoto	0	0%	4	100%

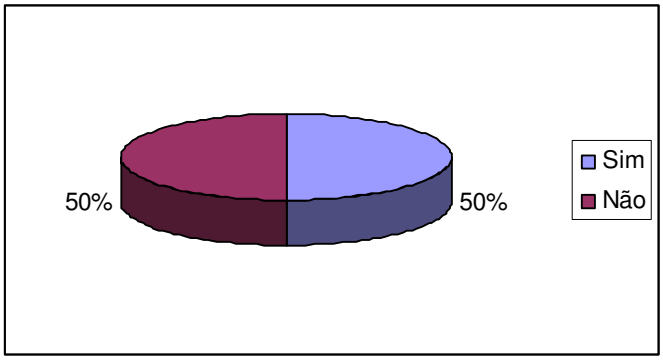
Média de Controle de Acesso	60,71%	Sim	39,28%	Não



8 - Desenvolvimento e manutenção de sistemas

As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	2	50%	2	50%
Controle de criptografia	2	50%	2	50%
Mecanismo de segurança nos processos de desenv. e suporte	2	50%	2	50%

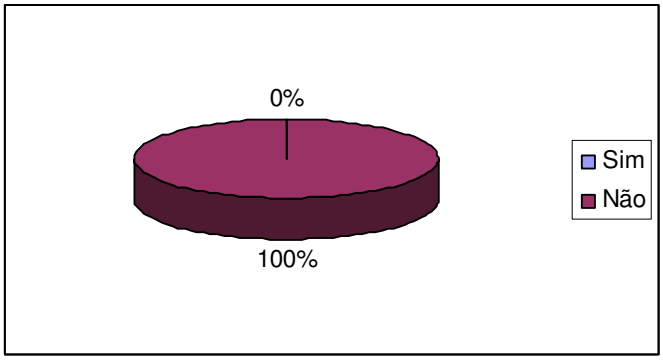
Média de Desenvolvimento e manutenção de sistemas	50 %	Sim	50%	Não



9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	0	0%	4	100%

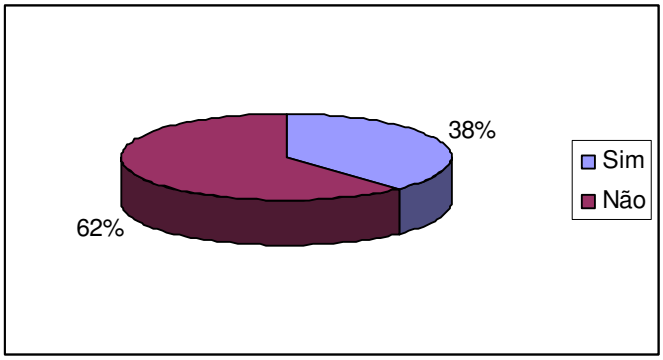
Média de Gestão da continuidade do negócio	0%	Sim	100%	Não



10 – Conformidade

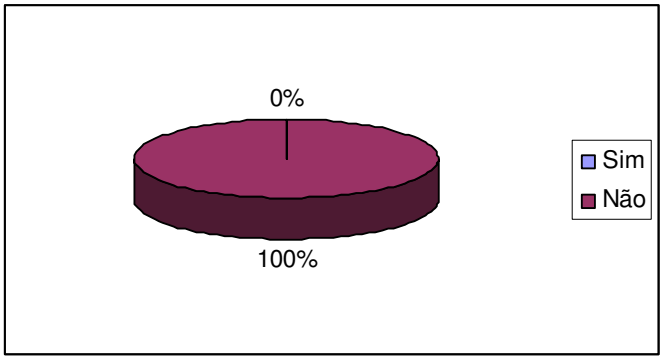
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	3	75%	1	25%
Recursos e critérios para auditoria de sistemas	0	0%	4	100%

Média de Conformidade	37,5%	Sim	62,5%	Não

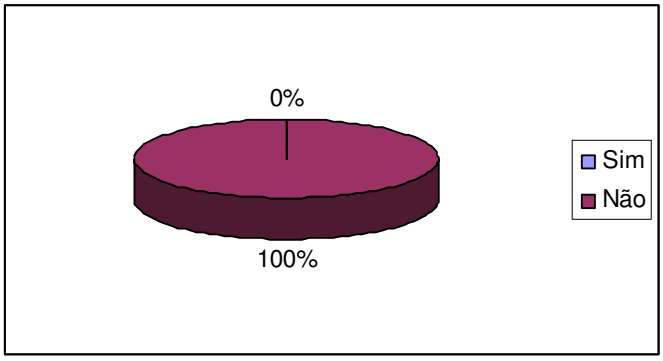


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	0	0%	4	100%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	0	0%	4	100%

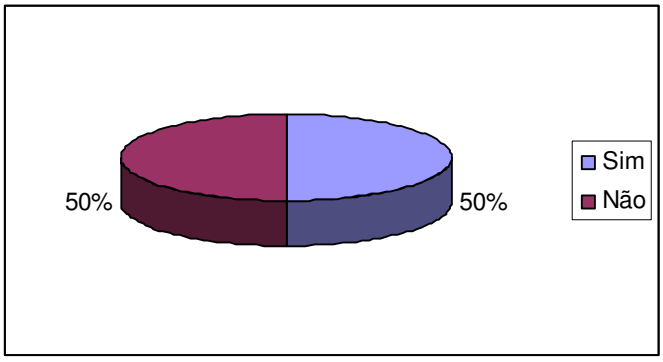


✓ **Outros**

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	2	66,66%	1	33,34%
Algum responsável pela Gestão da Política	1	33,33%	2	66,67%

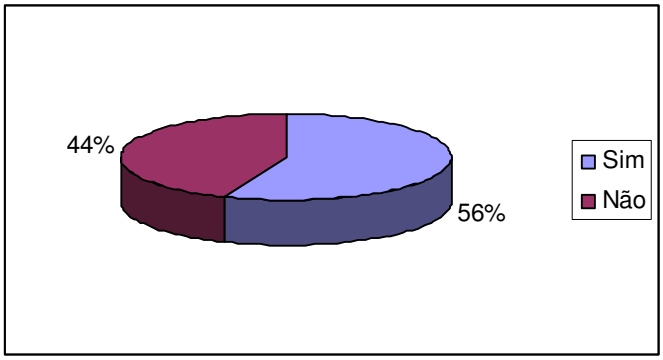
Média de Política de Segurança da Informação	50%	Sim	50%	Não



2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%
Infra-estrutura de SI para gerenciar as ações corporativas	2	66,66%	1	33,34%
Fórum de segurança formado pelo corpo diretor	1	33,33%	2	66,67%
Definição clara das atribuições associadas a segurança	2	66,66%	1	33,34%
Identificação dos riscos no acesso a prestadores de serviço	2	66,66%	1	33,34%
Controle de acesso específico para os prestadores de serviço	1	33,33%	2	66,67%
Requisitos de segurança dos contratos de terceirização	2	66,66%	1	33,34%

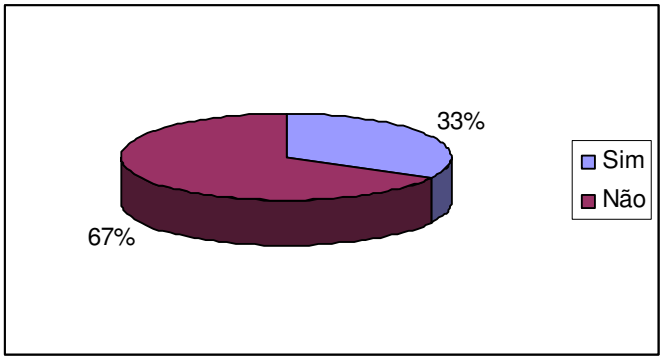
Média de Segurança Organizacional	55,55%	Sim	44,45%	Não



3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	1	33,33%	2	66,67%
Critérios de classificação da informação	1	33,33%	2	66,67%

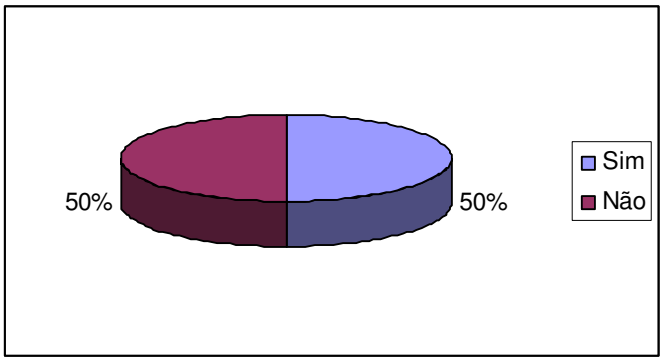
Média de Classificação e Controle dos ativos de Informação	33,33%	Sim	66,67%	Não



4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	2	66,66%	1	33,34%
Acordo de confidencialidade, termos e condições de trabalho	0	0%	3	100%
Processos para treinamento e capacitação de pessosas	1	33,33%	2	66,67%
Estrutura para notificar e responder aos incidentes de segurança	0	0%	3	100%

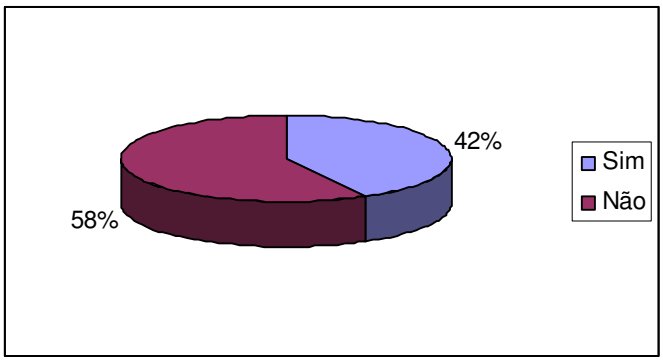
Média de Segurança em Pessoas	50%	Sim	50%	Não



5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	1	33,33%	2	66,67%
Recursos para segurança e manutenção dos equipamentos	2	66,66%	1	33,34%
Estrutura para fornecimento adequado de energia	1	33,33%	2	66,67%
Segurança de cabeamento de rede	1	33,33%	2	66,67%

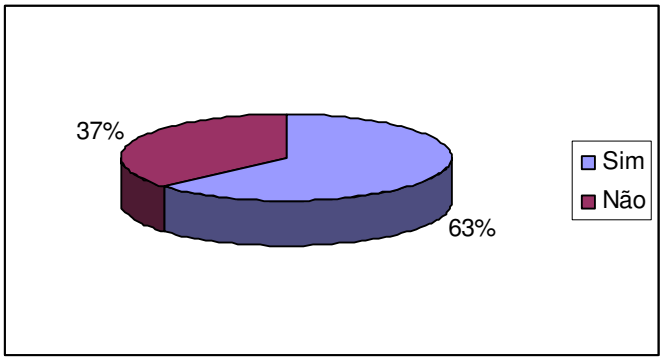
Média de Segurança Física e de Ambientes	41,66%	Sim	58,34%	Não



6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	2	66,66%	1	33,34%
Controles de mudanças operacionais	2	66,66%	1	33,34%
Segregação de funções e ambientes	1	33,33%	2	66,67%
Planejamento de aceitação de sistemas	2	66,66%	1	33,34%
Procedimento para cópia de segurança	2	66,66%	1	33,34%
Controles de gerenciamento de rede	2	66,66%	1	33,34%
Mecanismos de segurança e tratamento de mídias	2	66,66%	1	33,34%
Procedimentos para documentação de sistemas	2	66,66%	1	33,34%
Mecanismo de segurança do correio eletrônico	2	66,66%	1	33,34%

Média de Gerenciamento da Operações e Comunicações	62,95% Sim	37,05% Não

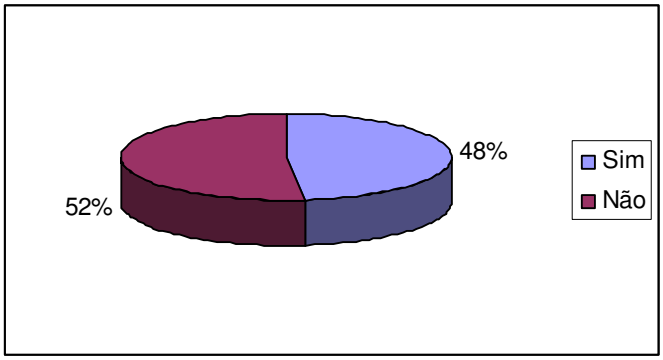


7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	1	33,33%	2	66,67%
Gerenciamento de acessos dos usuários	2	66,66%	1	33,34%
Controle de acesso a rede	1	33,33%	2	66,67%
Controle de acesso ao sistema operacional	2	66,66%	1	33,34%
Controles de acesso a aplicações	2	66,66%	1	33,34%

Monitoração de uso e acesso ao sistema	2	66,66%	1	33,34%
Critérios para computação móvel e trabalho remoto	0	0%	3	100%

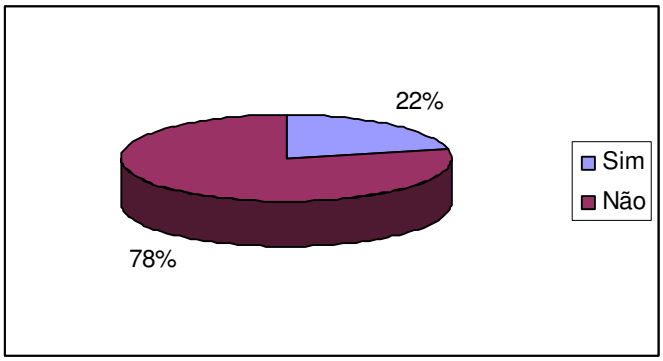
Média de Controle de Acesso	47,61%	Sim	52,38%	Não



8 - Desenvolvimento e manutenção de sistemas

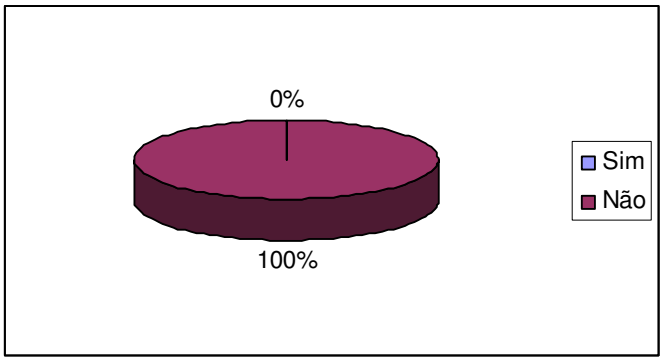
As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	1	33,33%	2	66,67%
Controle de criptografia	0	0%	3	100%
Mecanismo de segurança nos processos de desenv. e suporte	1	33,33%	2	66,67%

Média de Desenvolvimento e manutenção de sistemas	22,11 %	Sim	77,89%	Não



9 - Gestão da continuidade do negócio

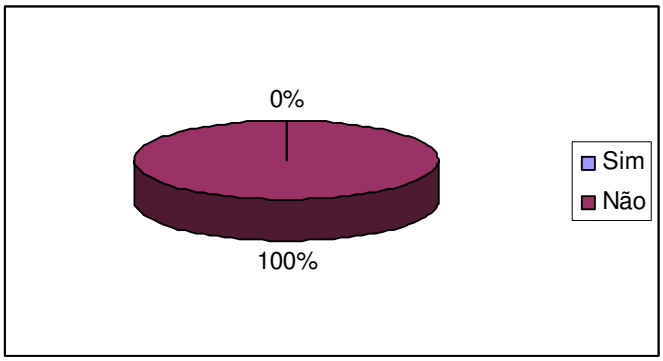
As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	0	0%	4	100%



10 – Conformidade

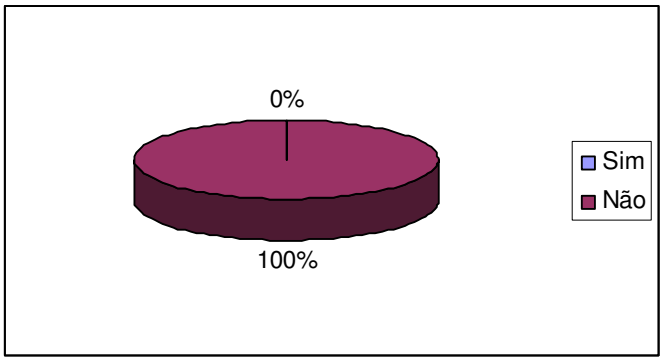
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	0	0%	4	100%
Recursos e critérios para auditoria de sistemas	0	0%	4	100%

Média de Conformidade	0%	Sim	100%	Não

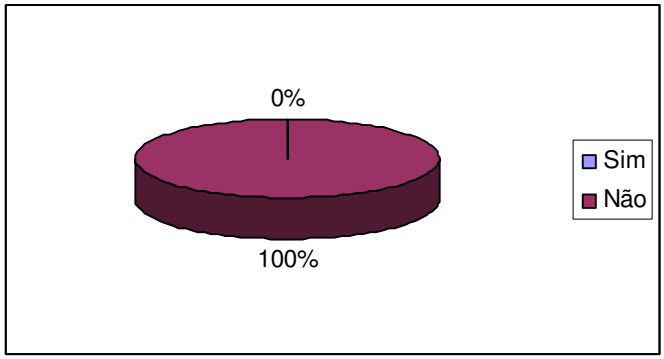


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	0	0%	4	100%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	0	0%	4	100%

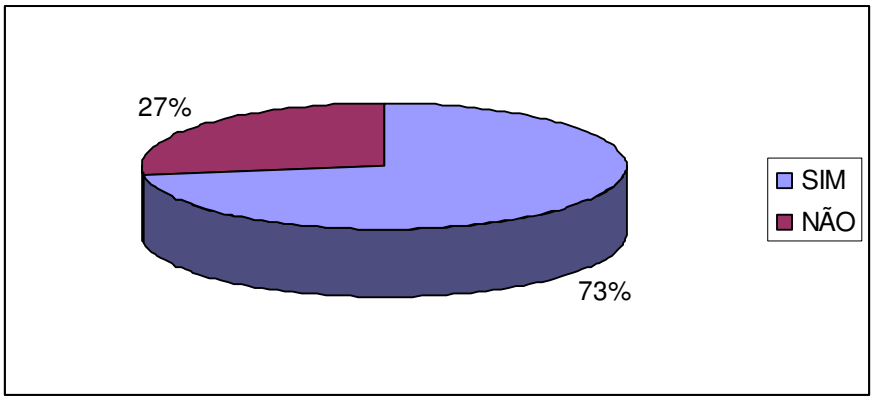


RESULTADO GERAL DA PESQUISA

1 - Política de Segurança da Informação:

As Organizações possuem:	Sim	%	Não	%
Política de Segurança	47	75,8%	15	24,20%
Algum responsável pela Gestão da Política	43	69,35%	19	30,65%

Média de Política de Segurança da Informação	72,57%	Sim	27,43%	Não



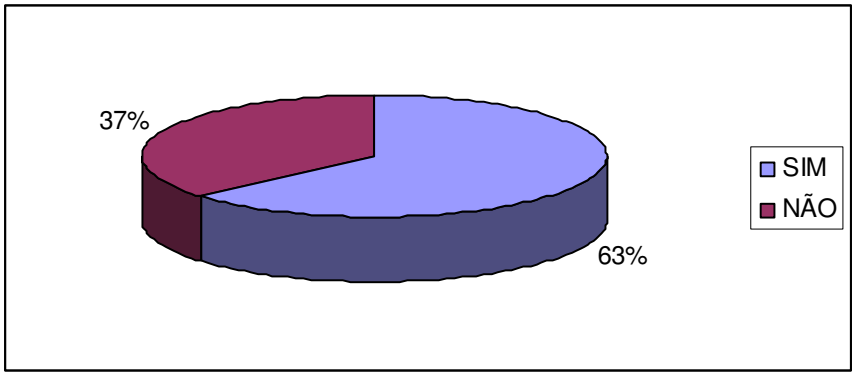
Conclui-se que o cenário é positivo com relação a Política de Segurança, em média 73% das organizações estão envolvidas com a política de segurança, o que mostra uma procupação com procedimentos de Segurança nas organizações. Um número grande de organizações, 43, possuem uma pessoa responsável pela gestão da política o que naturalmente aumenta o nível de exigência nas atualizações e uma maior aplicabilidade da política na organização.

2 - Segurança Organizacional:

As Organizações possuem:	Sim	%	Não	%

Infra-estrutura de SI para gerenciar as ações corporativas	47	75,8%	15	24,2%
Fórum de segurança formado pelo corpo diretor	24	38,7%	38	61,3%
Definição clara das atribuições associadas a segurança	41	66,12%	21	33,88%
Identificação dos riscos no acesso a prestadores de serviço	42	67,74%	20	32,26%
Controle de acesso específico para os prestadores de serviço	45	72,58%	17	27,42%
Requisitos de segurança dos contratos de terceirização	37	59,67%	25	40,33%

Média de Segurança Organizacional	63,44%	Sim	36,56%	Não

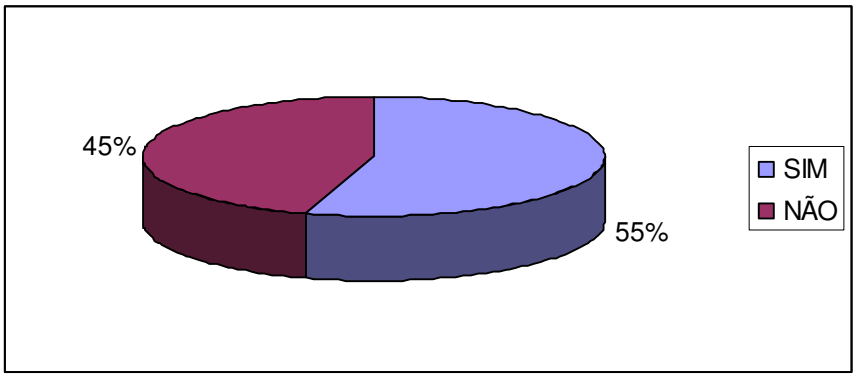


A conclusão é que a Segurança Organizacional em geral está com um índice de representatividade superior a 60% o que representa um bom resultado, porém o fato do envolvimento direto da diretoria estar baixo preocupa visto que o comprometimento da alta direção é fator fundamental para o sucesso da implantação de um Sistema de Gestão a Segurança da Informação.

3 - Classificação e Controle dos ativos de Informação

As Organizações possuem:	Sim	%	Não	%
Inventário dos ativos físicos, tecnológicos e humanos	41	66,12%	21	33,88%
Critérios de classificação da informação	27	43,54%	35	56,46%

Média de Classificação e Controle dos ativos de Informação	54,83%	Sim	45,17%	Não

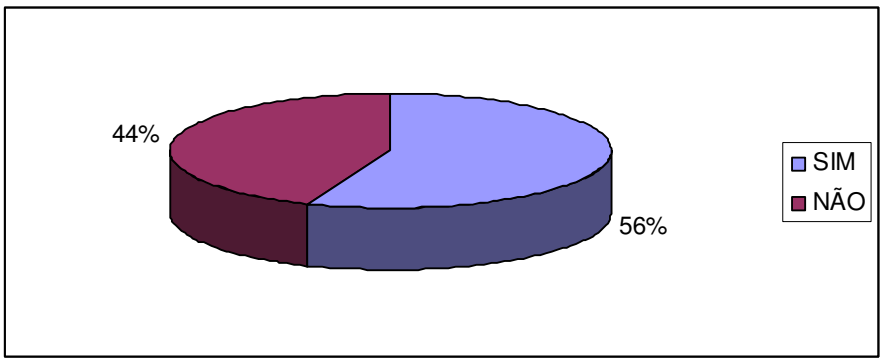


A média apresentada neste ítem foi representativa porém um fator importante como a critério de classificação da informação ainda não está sendo muito adotada nas organizações.

4 - Segurança em Pessoas

As Organizações possuem:	Sim	%	Não	%
Critério de seleção e política de pessoal	42	67,74%	20	32,26%
Acordo de confidencialidade, termos e condições de trabalho	32	51,61%	30	48,39%
Processos para treinamento e capacitação de pessosas	37	59,67%	25	40,33%
Estrutura para notificar e responder aos incidentes de segurança	27	43,54%	35	56,46%

Média de Segurança em Pessoas	55,64%	Sim	44,36%	Não

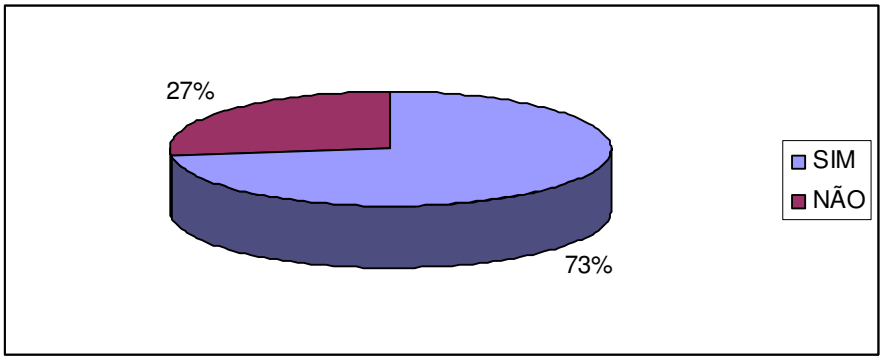


Conclui-se que, apesar dos 56% apresentados na média deste item, o fato de não haver uma estrutura para identificar de forma ordenada e documentada os incidentes de Segurança na maior parte da empresas, a avaliação da Segurança da Informação destas organizações fica comprometida.

5 - Segurança Física e de Ambientes

As Organizações possuem:	Sim	%	Não	%
Controles de acesso físico aos ambientes	34	54,83%	28	45,17%
Recursos para segurança e manutenção dos equipamentos	51	82,25%	11	17,75%
Estrutura para fornecimento adequado de energia	50	80,64%	12	19,34%
Segurança de cabeamento de rede	47	75,80%	15	24,20%

Média de Segurança Física e de Ambientes	73,38%	Sim	26,62%	Não

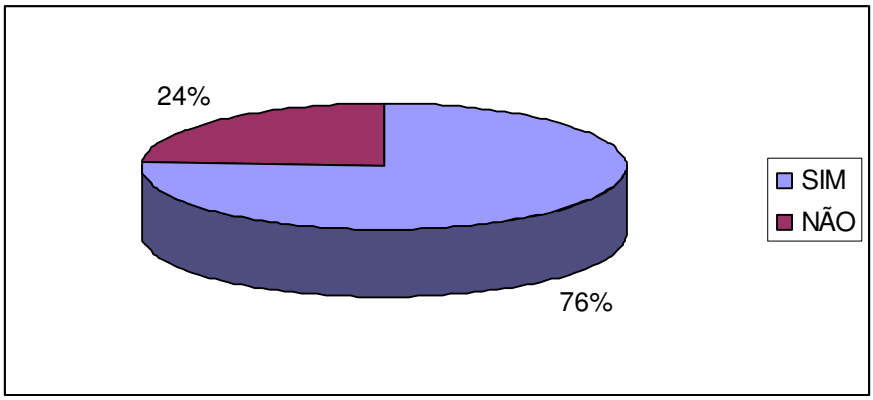


Este índice possui um percentual médio de 73%, alto e justificável, visto que a segurança física e dos ambientes é o mínimo de segurança esperada em organizações.

6 - Gerenciamento das operações e comunicações

As Organizações possuem:	Sim	%	Não	%
Procedimentos e responsabilidades operacionais	55	88,7%	7	11,3%
Controles de mudanças operacionais	42	67,74%	20	32,26%
Segregação de funções e ambientes	34	54,83%	28	45,17%
Planejamento de aceitação de sistemas	55	88,7%	7	11,3%
Procedimento para cópia de segurança	54	87,09%	8	12,91%
Controles de gerenciamento de rede	55	88,7%	7	11,3%
Mecanismos de segurança e tratamento de mídias	35	56,45%	27	43,55%
Procedimentos para documentação de sistemas	42	67,74%	20	32,26%
Mecanismo de segurança do correio eletrônico	52	83,87%	10	16,13%

Média de Gerenciamento da Operações e Comunicações	75,98%	Sim	24,02%	Não

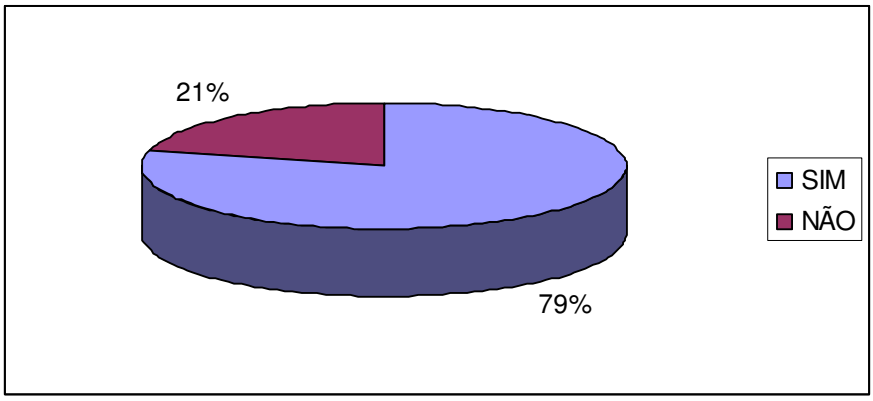


Encontra-se uma média alta de 76% neste tópico o que representa um altíssimo índice, muito positivo visto que este representa a segurança das operações no dia a dia das organizações. O que preocupa nesta sessão é que ainda existem organizações, mesmo que em minoria 16% que estão sem proteção no correio eletrônico, tornando a organização muito vulnerável às ameaças do mundo da Internet.

7 - Controle de Acesso

As Organizações possuem:	Sim	%	Não	%
Requisitos do negócio para controle de acesso	38	61,29%	24	39,71%
Gerenciamento de acessos dos usuários	56	90,32%	6	9,68%
Controle de acesso a rede	53	85,48%	9	14,52%
Controle de acesso ao sistema operacional	58	93,54%	4	6,46%
Controles de acesso a aplicações	55	88,70%	7	11,30%
Monitoração de uso e acesso ao sistema	47	75,80%	15	24,20%
Critérios para computação móvel e trabalho remoto	35	56,45%	27	43,55%

Média de Controle de Acesso	78,79%	Sim	21,21%	Não

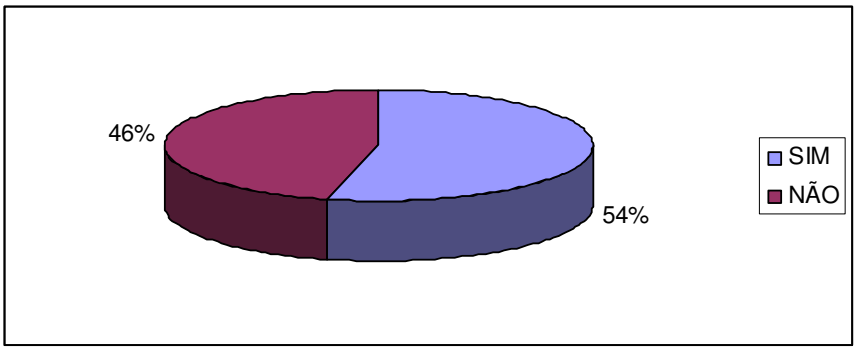


A média de Controle de Acesso deste ítem, 79%, representa um cenário positivo com relação a segurança de acessos das organizações, siginifica uma expressiva preocupação das organizações em proteger o acesso a seus sistemas.

8 - Desenvolvimento e manutenção de sistemas

As Organizações possuem:	Sim	%	Não	%
Requisitos de segurançade sistemas	43	69,35%	19	30,65%
Controle de criptografia	20	32,25%	42	67,75%
Mecanismo de segurança nos processos de desenv. e suporte	37	59,67%	25	40,33%

Média de Desenvolvimento e manutenção de sistemas	53,76%	Sim	46,24%	Não

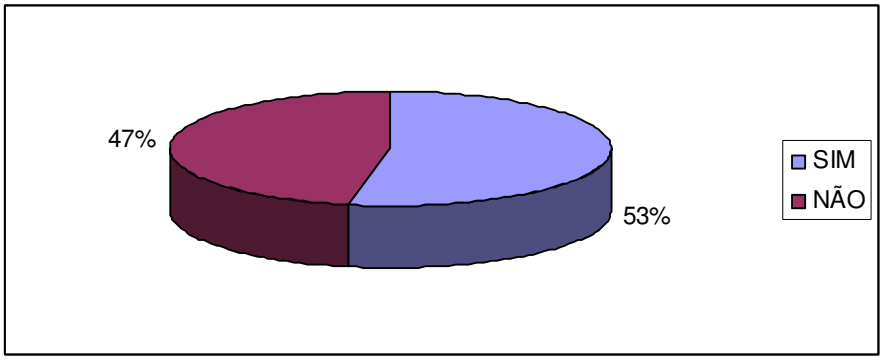


Apesar da média estar acima de 50% existe um ítem que é controle de criptografia, controle este que garante o sigilo de informações com apenas 32% de uso, o que preocupa visto que as vulnerabilidades dos sistemas podem ser exploradas e concretizadas caso os dados não estejam criptografados.

9 - Gestão da continuidade do negócio

As Organizações possuem:	Sim	%	Não	%
Gestão de continuidade do negócio	33	53,22%	29	46,88%

Média de Gestão da continuidade do negócio	53,22%	Sim	46,78%	Não

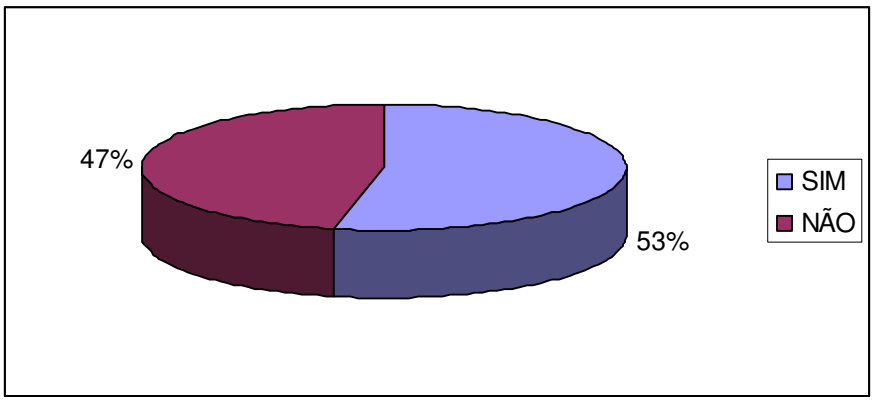


53% é um percentual pequeno porque significa que quase metade das organizações não possuem plano de contingência para sobreviver a ataques ou incidentes de segurança que impeçam a continuidade dos negócios.

10 – Conformidade

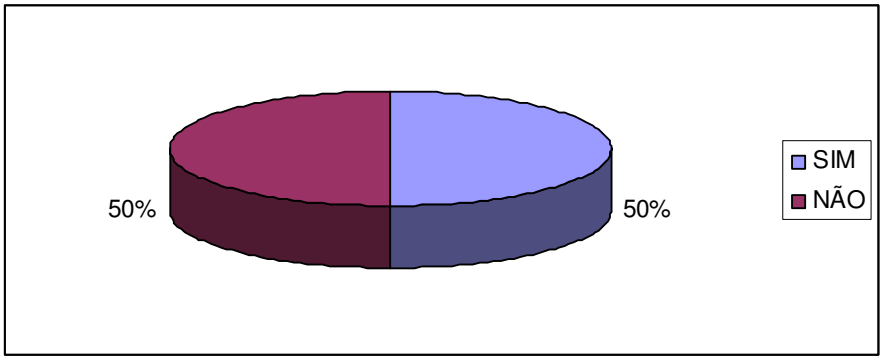
As Organizações possuem:	Sim	%	Não	%
Gestão de conformidades técnicas e legais	36	58,06%	26	41,94%
Recursos e critérios para auditoria de sistemas	30	48,38%	32	51,62%

Média de Conformidade	53,22%	Sim	46,78%	Não

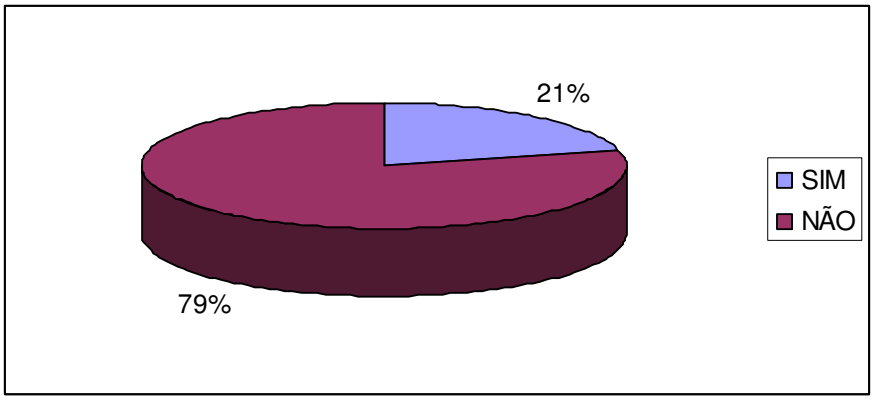


11 - Norma BS 7799 / ISO IEC 17799

As Organizações:	Sim	%	Não	%
Conhecem os controles da Norma	31	50%	31	50%



As Organizações:	Sim	%	Não	%
Utilizaram os controles de melhores práticas da Norma para implantar o Sistema de Gestão de Segurança da Informação	13	20,96%	49	79,04%



Apesar de um número significativo de organizações conhecerem a Norma e seus controles, apenas 21% utilizou seus controles para nortear a Gestão da Segurança da Informação na organização, o que mostra que mesmo sendo uma referência nacional e internacional de melhores práticas para a Segurança da Informação a Norma ainda não tem representação expressiva no mercado de Salvador.

Ao conhecer as respostas do questionário aplicado nas organizações, fica claro a amplitude dos assuntos abordados pela Norma e, obviamente, a complexidade em planejar, implementar e gerir todos os controles de segurança, a fim de proteger a confidencialidade, integridade e disponibilidade das informações. (Lista no Apêndice II)

Através dos índices obtidos, é possível ver que as organizações pesquisadas em Salvador consideram importante a Segurança da Informação nos seus ambientes, mas também, percebe-se como a organização está distante do que vem sendo considerado referência nacional e internacional de gestão de segurança da informação, visto que não estão trabalhando com rotinas baseadas na Norma, conforme comprova a questão 11.2 do questionário em anexo.

As organizações se sairam bem em um ou mais domínios e esta situação está presente na maioria delas, o que comprova a afirmação inicial com relação a considerar a Segurança da Informação importante nos seus ambientes. Quando se trabalha com Segurança da Informação é necessário um levantamento detalhado visando um diagnóstico abrangente e capaz de integrar o levantamento de ameaças, impactos, vulnerabilidades físicas, tecnológicas e humanas, associando-as às reais necessidades do negócio, para que se possa garantir a real situação da Segurnaça das Informação nas organizações.

As organizações podem ter adotado quase que a totalidade dos controles, mas deve-se levar em consideração que alguns requisitos podem estar defasados, desatualizados ou inativos, o que demonstra um bom nível de consciência, mas também pode apresentar deficiência na

estrutura de gestão ou a falta de fôlego financeiro para subsidiar os recursos de administração, caso esteja desatualizado. Pode, ainda, ter uma parcela representativa dos controles em ordem, deixando os demais inoperantes, ou mesmo inexistentes. Diante disto, é conveniente alertar para a grande possibilidade de evolução, bem como a possibilidade de estagnação e de redução tendenciosa do nível de segurança por falta de orientação.

Pode-se descartar a situação em que a segurança da informação não está sendo tratada como prioridade ou que indique ausência ou ineficácia de muitos dos controles recomendados pela Norma. É possível dizer que pode ocorrer ações isoladas – de um departamento ou de outro – apesar de louváveis, não distribuem com uniformidade a segurança e acabam por minimizar o aumento do nível de segurançado negócio.

O resultado obtido foi satisfatório no que diz respeito a relevância da Segurança da Informação nas organizações pesquisadas. O fato da média da maioria dos itens da pesquisa estar acima de 50 % significa uma preocupação com vários controles da Norma que norteiam a implantação de um Sistema de Gestão de Segurança da Informação, o que demonstra uma evolução considerável neste assunto.

Apesar da relevância das respostas da pesquisa com relação a Segurança da Informação e a aplicação dos controles da Norma, ainda é muito baixo o índice de organizações que estão utilizando, conscientemente, os requisitos da Norma para implantar o sistema de Gestão de Segurança da Informação. O índice de apenas 20% das organizações estarem utilizando a Norma como referência formal, confirma esta situação. O ponto positivo é que mesmo sem utilizar formalmente os controles da Norma para nortear o Sistema de Gestão de Segurança da Informação, as organizações estão trabalhando mesmo que parcialmente com estes controles e o resultado da pesquisa comprova esta constatação.

5.4 ODEPOIMENTO DOS RESPONDENTES

Os questionários aplicados nas organizações foram respondidos por profissionais envolvidos com as áreas de Tecnologia da Informação e Segurança da Informação, em sua maioria Gerentes e Analistas de Sistemas conforme apresentado anteriormente. O tema do questionário envolve diretamente o uso da Norma BS 7799 de Segurança da Informação e era necessário que as repostas viessem das pessoas envolvidas com este processo na organização para enriquecer a pesquisa.

A certificação na Norma britânica BS 7799 - Parte 2 vem sendo considerada por muitas empresas como uma ótima demonstração para o mercado do compromisso na Gestão da Segurança da Informação no ambiente corporativo. E para aprofundar o assunto referente a Norma BS 7799 e não querendo invadir a privacidade de algumas empresas que colaboraram com esta pesquisa, apresenta-se alguns aspectos e pontos de vista levantados por 3 dos entrevistados sobre o uso da Norma e o impacto da sua utilização na organização.

Por se tratar de um assunto muito delicado e importante, Segurança da Informação, encontra-se muita dificuldade e receio dos entrevistados em responder os questionamentos a respeito da Segurança e por este motivo o questionário foi fechado viabilizando assim a pesquisa. Por isso o direito de garantir o sigilo da identidade das Organizações nas quais apresentaremos alguns pontos conforme comentários de seus responsáveis pois esta foi uma condição exigida para a obtenção das informações que apresenta-se abaixo.

Um ponto comum na opinião de vários entrevistados é que os gerentes de segurança há muito tempo esperam por um conjunto razoável de padrões de Segurança da Informação, reconhecidos globalmente. Muitos acreditam que um código de prática ajuda a suportar os esforços dos gerentes de TI e também a influenciar decisões, aumentar a cooperação entre os vários departamentos em nome do interesse comum pela segurança e ajudar a tornar a Segurança uma das prioridades organizacionais.

A Norma é conhecida como um abrangente conjunto de controles formado pelas melhores práticas em segurança de informações e diante desta constatação questionou-se aos entrevistados porque as organizações onde trabalham resolveram utilizar a Norma BS7799-2; e eles responderam:

> “Inicialmente, o objetivo era garantir a segurança na área de Tecnologia da Informação, mas depois percebemos que o problema não era restrito a essa área. Então identificamos que a BS 7799 poderia nos ajudar e finalmente percebemos que poderíamos utilizá-la em várias áreas da Segurança, Tecnológica, de pessoas e dos processos.” (ENTREVISTADO A)

> “ Informação hoje é um ativo importante pois sustenta toda a estratégia e também as decisões do dia-a-dia da organização. Alcançar a certificação na BS 7799-2 é ter a certeza de possuir uma gestão sistêmica e estruturada das informações da empresa. Além disso, a organização acredita e valoriza modelos de gestão, prova disso é que possui o seu próprio Sistema Integrado de Gestão. A empresa possui também certificações nas áreas de Meio Ambiente (ISO 14.001), Saúde e Segurança do Trabalho (OHSAS 18.001) e Qualidade (IS0 9001:2000). Ocorreram, nos últimos meses, uma série de implementações que tornaram o ambiente de Tecnologia mais complexo e os seus negócios cada vez mais dependentes dos recursos de informação. “(ENTREVISTADO B)

E ainda complementa:

> “ Por outro lado, a área de TI já vinha desenvolvendo ações voltadas para a Segurança da Informação há alguns anos. Porém, era necessário algo mais estruturado, que consolidasse estas ações de controle de acesso e da disponibilidade das informações e, principalmente, que trabalhasse a cultura de todos os empregados e contratadas. Todos esses aspectos, somado ao fato de que a empresa, com a BS 7799-2, estaria alinhada com as melhores práticas de segurança da informação, tendo por base padrões internacionais.” (ENTREVISTADO B)

> **“** A área de Segurança de Sistemas e Tecnologia da empresa estava estudando as normas ISO/IEC 17799 e BS 7799-2 objetivando a implementação de um sistema de gestão da segurança das informações. A alta direção entendeu que a implementação de um sistema de gestão da Segurança da Informação certificado pela BS7799-2 seria uma forma de agregar maior garantia ao negócio pela redução de riscos e gerenciamento contínuo dos processos de segurança do mesmo.” (ENTREVISTADO C)

Sobre o uso da informação ele comenta:

> “Além disso, é uma empresa cujo negócio é "soluções em informação". A informação é nosso principal ativo, matéria-prima para nossos produtos e base para o nosso processo de Gestão. Buscar a certificação BS 7799-2 é um caminho natural e essencial para a empresa.” (ENTREVISTADO C)

Neste sentido acretida-se que existe em comum na resposta das três organizações é que todas iniciaram o interesse pela Segurança da Informação buscando Segurança da área de tecnologia e após conhecer o assunto todas perceberam que a Norma abrange todos os aspectos da Segurança da Informação, não apenas tecnológico mas também segurança em processos e pessoas.

Outro comentário importante dos entrevistados foi a frequencia de mudanças no ambiente corporativo após o processo de implantação da Norma. Segue abaixo alguns comentários referentes a estas mudanças.

> "Todos os funcionários sabem o que é Segurança da Informação e incorporaram essa preocupação em suas atividades diárias. Isso você não consegue somente com treinamento. As pessoas têm que incorporar o tema como um hábito saudável e praticá-lo." (ENTREVISTADO A)

Entretanto, o entrevistado B comenta:

> **"** Houve uma melhoria significativa dos controles na área de TI que após a sua implementação aumentaram, significativamente, a segurança dos dados e das informações da empresa. Outro aspecto está relacionado com a questão comportamental onde se observa uma maior conscientização dos empregados em relação à importância da Segurança da Informação para a empresa. "(ENTREVISTADO B)

O seguinte comentario revela:

> **"** Pelo fato de o ambiente ser monitorado constantemente por meio de indicadores de segurança, identificamos significativas melhorias nos controles sendo utilizados no processo. A conscientização de segurança dos funcionários também aumentou, o que trouxe novos ganhos para o próprio processo. A participação efetiva da alta direção no Sistema de Gestão da Segurança da Informação também contribui para que o processo esteja sempre em constante evolução." (ENTREVISTADO C)

Merece destaque os benefícios que a implantação da Norma trouxe para a organização:

> **"** Imagem externa de confiança e segurança. No âmbito interno, destaca-se a grande capacidade de realização de toda a equipe, a maturidade em gestão de projetos e, fundamentalmente, os ganhos financeiros decorrentes de maior disponibilidade e maior eficiência nos processos." (ENTREVISTADO A)

> **“** Com certeza a certificação será um diferencial competitivo junto aos seus clientes e demais partes interessadas, pois comprova o empenho da empresa em garantir a confidencialidade, integridade e disponibilidade das informações relativas às suas transações de negócio, através de um modelo de gestão que garante a adequação e eficácia de todos os controles implementados.” (ENTREVISTADO B)

Mais suscintamente o entrevistado C afirma:

> **“**Conforme comentei, a certificação BS 7799-2 é um diferencial de mercado. Além disso, podemos elencar, entre outros, os seguintes benefícios:
> - - Redução dos riscos de segurança do processo/negócio;
> - - Aumento da eficácia dos investimentos em controles frente aos riscos do processo/negócio;
> - - Aumento de confiança nas relações comerciais;
> - - Conformidade com requisitos legais e regulatórios;
> - - Imagem e Competitividade. “(ENTREVISTADO C)

Com base nas afirmativas dos entrevistados constata-se que o diferencial competitivo para os negócios e a imagem para os clientes são os benefícios mais visíveis e relevantes para os entrevistados que enxergam a implantação da Norma BS7799 com objetivos de marketing, fortalecimento da imagem ou criticidade do negócio e sua operação. Mas o principal benefício é diminuir o nível de exposição aos riscos em todos os ambientes para que a empresa possa estender a segurança aos seus produtos e serviços resultando em uma maior satisfação por parte de seus clientes.

Conversando com os responsáveis pelas as organizações que não utilizaram a Norma, como sintese de melhores praticas de Segurança da Informação, verifica-se que os motivos que justificaram a não utilização são surpreendentes. O maior ãondice de não utilização foi a falta de apoio da alta direção, fator este que compromete a implantação de um Sistema de Gestão de Segurança da Informação pois a cultura deve vir de cima para baixo como uma influência e não uma imposição, porque a segurança exige muita disciplina e envolvimento de todos dentro da organização.

O segundo maior problema foi o custo, porque para implantar um Sistema de Gestão de Segurança da Informação requer investimento, principalmente em consultoria. O fato de não ter sido tratado como prioridade no orçamento do ano fez com que muitas organizações não possuam verba disponível para investimento em Segurança da Informação, principalmente,

nos processos e nas pessoas. A verba disponível para segurança se encontra na maioria das organizações destinada a Segurança em Tecnologia e como a implantação da Norma envolve muito mais que a área de Informática, o uso da Norma foi descartado.

Uma questão foi a cultura organizacional. Esta na verdade em alguns casos inviabilizou a implantação por desistência dos responsáveis em educar os colaboradores da organização nos processos e procedimentos necessários para seguir os controles da Norma a ser implantada. O envolvimento e comprometimento de todos com a organização é condição fundamental para a implantação da Norma de Segurança; a falta de compromisso de alguns inviabilizou o uso da Norma.

Apesar de muitas organizações não utilizarem a Norma como balisador para a implantação de um Sistema de Gestão de Segurança da Informação, a maioria deixou bem claro que têm consciência dos beneficios do uso da Norma como balisador para adotar as melhores práticas de Segurança da Informação, apesar de não estarem adotando no momento por diversos motivos que já foram apresentados.

5.5 ANÁLISE DO USO DA NORMA ISO/IEC 17799/ BS 17799

O avanço tecnológico transformou a informação num dos ativos de maior importância para o ambiente corporativo. Assim, uma boa gestão em Segurança da Informação passou a ser fundamental para se garantir a continuidade dos negócios. Mas como fazê-la da melhor forma? Dois bons guias podem ser utilizados, as Normas BS 7799 e a ISO/IEC 17799, que proporcionam ao profissional de Segurança da Informação os subsídios necessários para o fortalecimento desse conceito dentro de uma organização.

Atualmente há um consenso mundial de que a nova versão da ISO/IEC 17799 é o melhor código de prática em gestão da Segurança da Informação que existe no mercado. Existem normas nessa área em vários países. Entretanto, essas normas não têm a abrangência da ISO 17799, que foi atualizada e melhorada por um grupo de mais de 50 especialistas de todas as partes do mundo. Foram cerca de três anos de trabalho, analisando mais de 1.000 comentários ao projeto da norma. A grande diferença, portanto, reside no fato de que a nova ISO/IEC

17799 é uma Norma global e que reflete os mais modernos conceitos sobre Gestão da Segurança da Informação.

Uma empresa que segue o padrão ISO 17799/BS 7799 pode fazer mais negócios do que aquelas que não seguem um padrão. Se um cliente em potencial estiver escolhendo entre dois serviços diferentes e a segurança for uma preocupação, eles, geralmente, selecionam àquela que seguir determinado padrão na área. Além disso, uma empresa que segue o padrão da Norma oferece:

- ✓ Segurança corporativa aprimorada
- ✓ Planejamento e Gerenciamento de segurança mais efetivo
- ✓ Parcerias e e-commerce mais seguros
- ✓ Confiança aprimorada do cliente
- ✓ Auditorias de segurança mais seguras e precisas
- ✓ Redução de responsabilidades legais

Se a empresa não possui um programa de proteção de informações, a Norma ISO 1779 /BS 7799 pode fornecer as diretrizes para sugerir a criação de um programa. Mesmo que não queira se tornar certificado, a Norma pode servir como um guia para a criação da postura de segurança da sua empresa. Pode-se pensar nesse padrão como uma boa diretriz de segurança a ser usada pela sua empresa.

Nesse sentido, a Norma ISO 17799/BS 7799 é uma compilação de recomendações para melhores práticas de segurança que podem ser aplicadas por empresas, independentemente do seu porte ou setor. Ela foi criada com a intenção de ser um padrão flexível, nunca guiando seus usuários a seguir uma solução de segurança específica em vez de outra. As recomendações da Norma continuam neutras com relação à tecnologia e não fornecem nenhuma ajuda na avaliação ou entendimento de medidas de segurança já existentes. Por exemplo, discute-se a necessidade de *firewall* mas não aprofunda nos tipos de *firewall* e como devem ser usados. Isso leva alguns opositores a dizer que a ISO 17799 é muito vaga e pouco estruturada como Norma para ter seu valor realmente reconhecido.

A flexibilidade e imprecisão da ISO 17799/BS 7799 são intencionais porque é muito difícil criar um padrão que funcione para todos os variados ambientes de tecnologia da informação e

que seja capaz de crescer com a mutante paisagem tecnológica atual. Ela simplesmente fornece um conjunto de regras em uma indústria onde elas não existiam.

Os benefícios da implantação da Norma de Segurança da Informação ISO/IEC 17799 / BS7799, são os benefícios internos, através da melhoria do gerenciamento de sua própria informação, garantindo assim para os sócios e parceiros da organização uma avaliação competente e imparcial sobre seu sistema de segurança da informação. Outra vantagem é possibilitar conformidade com a legislação nacional na área de segurança da informação de seu país, como por exemplo, ajudar as organizações a cumprirem as exigências de leis sobre privacidade de dados.

A Segurança da Informação pode ser usada pela maioria dos setores da economia, pois todas as organizações, independentemente do seu porte ou do ramo de atuação, sejam elas organizações privadas que visam lucro ou Ong's, organizações que disseminam informação, o importante é que todas precisam proteger as suas informações sensíveis e críticas.

Outros benefícios identificados são: a proteção das informações críticas e sensíveis da organização às ameaças e vulnerabilidades, assegurando a continuidade dos negócios; o aumento da competitividade; o atendimento aos requisitos legais e regulamentares, e, o que é muito importante, a imagem e reputação da organização. Existem vários exemplos que demonstram os benefícios de se adotar um modelo de gestão da Segurança da Informação.

Abaixo apresenta-se alguns casos de incidentes e como os controles da Norma poderiam evitar a ocorrencia dos mesmos:

Caso 1: Um Banco tinha dois escritórios funcionando no World Trade Center (WTC). No dia seguinte aos atentados terroristas de 11 de setembro, este Banco já operava os seus sistemas normalmente, assegurando assim a disponibilidade das suas informações.

O Banco tinha um site de backup remoto - instalado em local afastado da sede, com cópias de todos os arquivos importantes atualizados. Os itens 8.4.1 - Cópias de segurança e 11 -Gestão da continuidade do negócio - da NBR ISO/IEC 17799 definem regras para evitar a

interrupção do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.

Caso 2: Um *notebook* contendo segredos de segurança nacional, com informações sobre novos sistemas de armas foi deixado em um táxi, em Londres.

No caso em questão, a confidencialidade das informações não foi assegurada. O item 9.8.1 - Computação Móvel - da norma diz que "quando se utilizam recursos da computação móvel, como por exemplo, *notebooks, palmtops, laptops* e telefones celulares, cuidados especiais devem ser tomados para garantir que a informação não seja comprometida".

Neste caso o item recomenda que seja adotada uma política formal, levando em conta os riscos de se trabalhar com recursos de computação móvel, em ambientes desprotegidos. Estas políticas devem incluir requisitos para proteção física, controles de acesso, técnicas criptográficas, cópias de segurança e proteção contra vírus.
Caso 3: Um outro dado interessante é quanto às fitas de *backup*. Pesquisa realizada na Inglaterra revela que 50% das fitas de *backup* nunca funcionam. Ou seja, não basta apenas fazer cópias de segurança dos arquivos e dados importantes. É necessário proteger tais cópias contra danos ou deterioração.

O item 8.6 - Segurança e tratamento de mídias - da ISO/IEC 17799 recomenda que sejam estabelecidos procedimentos operacionais para proteger documentos, mídias magnéticas de computadores (fitas, discos, cartuchos), dados de entrada e saída e documentação dos sistemas da organização.

Caso 4: Um Senador da República teve o seu escritório invadido. Os criminosos levaram um computador, vários papéis importantes que estavam sobre a mesa, além de documentos recolhidos da lixeira.

Se o Senador tivesse adotado alguns dos controles da Norma, como o item 7.1 - Segurança Física e do Ambiente -, 7.3.1 - Política de mesa limpa e tela protegida - e 8.4.1 - Cópias de Segurança - este problema certamente não ocorreria. Neste caso, além da disponibilidade - pois vários documentos foram levados -, o principal componente da informação afetado foi a confidencialidade, pois o Senador participava de uma das CPIs do Congresso.

Caso 5: Um funcionário do Governo Federal brasileiro acessou o sistema de pagamento de aposentados e abriu várias contas de pessoas já falecidas em seu nome.

Neste caso, o componente da informação afetado foi a integridade. Se fossem adotados alguns dos controles da norma, como o item 8.1.4 - Segregação de funções -, 9.2.4 - Análise crítica dos direitos de acesso do usuário - e 9.7.2 - Monitoração do uso do sistema -, este problema certamente não aconteceria.

CONSIDERAÇÕES FINAIS.

No novo paradigma tecnológico da atual sociedade a informação é a matéria-prima e: "são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como nas revoluções tecnológicas anteriores." (CASTELLS, 1999).

Um traço fundamental do novo paradigma tecnológico informacional é que a informação passa a se constituir tanto em matéria-prima como em produto. Os principais efeitos das inovações recaem sobre os processos, muito mais que sobre os produtos. Os processos, diferentemente dos produtos, incorporam-se a todas as atividades humanas, produzindo transformações conduzidas por essas tecnologias. Os onipresentes fluxos de informação provocam modificações na organização social em seu conjunto: no modo de produzir, de consumir, de administrar, de morar, enfim, de viver.

A informação é tratada como um ativo pelas organizações. E, como qualquer outro ativo importante, ela precisa ser devidamente protegida para garantir a continuidade dos negócios. Mas isso não é tão simples como parece, pois o avanço tecnológico, que ao mesmo tempo agiliza e simplifica os trabalhos aumentando a produtividade, tem tornado as organizações mais vulneráveis às ameaças de segurança, o que dificulta cada vez mais a implementação de controles de acesso à informação realmente eficientes.

O mundo dos negócios percebe, nitidamente, a importância de se proteger as informações de uma organização em relação à sua confidencialidade, integridade e disponibilidade. Isto se torna especialmente importante pelo grande aumento da interconectividade no ambiente dos negócios onde a informação, cada vez mais, está exposta a um elevado número de ameaças e vulnerabilidades.

Segurança é responsabilidade e dever de toda organização e, como tal, deve ser de conhecimento de cada profissional o cumprimento e conscientização de medidas de proteção dos recursos da informação, para garantir os aspectos de disponibilidade, integridade e confidencialidade, pilares da Segurança da Informação.

Sêmola (2001) comenta que gerir informação nos heterogêneos e cada vez mais complexos ambientes corporativos é um grande desafio; sob a ótica da segurança, esse desafio tende a ser muito maior. De fato, é evidente que, quanto mais complexo é o ambiente computacional, mais recursos são disponibilizados aos usuários, mais informações são requeridas por estes usuários e assim mais difícil se torna garantir a confidencialidade, integridade e disponibilização das informações.

A Segurança da Informação deve ser um elemento chave dentro da organização envolvendo aspectos humanos e organizacionais, sendo fundamental a definição e existência de uma Política para efetiva proteção das informações. O objetivo da Segurança da Informação é proteger a empresa contra riscos, apoiada em um Plano de cultura de Segurança da Informação e uma estrutura de Planejamento de Segurança, onde se podem identificar as vulnerabilidades e ações pró-ativas para a proteção das informações.

É importante lembrar que para implementar e manter o Sistema de Segurança da Informação, o apoio da direção da organização e a participação de todos os funcionários é fundamental. Por isso, tornar as informações de uma organização seguras pode ser uma tarefa bastante complexa, requerendo gestão e procedimentos apropriados.

A implementação das principais práticas de Segurança da Informação em organizações, não é uma tarefa fácil, mesmo quando se trata de empresas de pequeno porte. Envolve fatores objetivos e subjetivos que, somados, representam um caso diferenciado, impossível de ser traduzido em uma fórmula. Todavia, o ato de conscientização da necessidade da adoção das práticas de segurança, já é um grande avanço da organização. Não esquecendo que a implantação compulsória não é o melhor caminho e sim a disseminação da cultura nos ambientes da empresa. Afinal, nem todos os colaboradores e funcionários entendem a necessidade de mecanismos de controle e de gerenciamento da Segurança da Informação.

Quando a empresa desperta para a importância de uma prática ativa de segurança em seus negócios, começa a estendê-la aos processos, informações, funcionários e seus produtos. E a importância e os benefícios passam a ser mais evidentes.

É essencial lembrar que um projeto termina com a implementação dos controles de segurança da informação, que podem ser baseados nos controle da Norma de Segurança BS 7799, mas não a segurança definitiva. Segurança requer um trabalho contínuo de acompanhamento e análise crítica periódica dos riscos, dos controles implementados, dos eventos, das mudanças nos requisitos de negócio e suas prioridades. Os controles aplicados devem ser sempre analisados e avaliados com relação a eficiência e adequação, além do constante estudo das novas tecnologias, de novas táticas de defesa e de novos ataques que poderiam comprometer a segurança da informação. Implantar um Sistema de Gestão da Segurança da Informação é uma vitória, porém, o desafio fundamental para as organizações é a manutenção deste sistema.

Busca-se apresentar o contexto atual das organizações e da sociedade da Informação com o impacto das mudanças e a apresentação dos conceitos básicos de Segurança da Informação e enfatizar que esta deve ser a mobilização de interesses comuns, coletivos e difusos em prol da defesa e fortalecimento do patrimônio intangível – a informação, um dos bens mais valiosos de qualquer organização. Para solidificar os conceitos, e auxiliar o amadurecimento no assunto foi apresentado as principais características da Norma BS7799 que norteiam a criação de um Sistema de Gestão de Segurança da Informação baseada em controles.

A pesquisa apresenta como as organizações de Salvador estão encarando a Segurança da Informação e se estão utilizando a Norma como balizador para a implementação da mesma. Os resultados obtidos na coleta de dados da pesquisa foram satisfatórios e positivos, no que diz respeito à sensibilização das organizações com relação à importância da implantação de um Sistema de Gestão da Segurança da Informação e reforço dos fatores de capacitação e conscientização como pontos fundamentais para proteção das informações corporativas, mas

não apresentou resultado positivo com relação ao uso da Norma como base para a implantação da Segurança nas Organizações.

A certificação na Norma BS 7799 traz uma grande melhoria na relação fornecedor/cliente. Assim, o cliente passa a ter maior confiança nos serviços prestados pelo fornecedor, pois a certificação é uma garantia que os dados e informações são protegidos adequadamente.

Após a pesquisa realizada em organizações de Salvador conclue-se que as Normas se adaptam melhor em organizações comerciais conforme constatação nas respostas da pesquisa por ramo de atividade. Instituições de ensino, instituições públicas e outras assemelhadas têem dificuldades em implantar certos controles da Norma devido a seus ambientes serem diferentes dos de uma empresa comercial. Apesar disso, qualquer organização pode aproveitar grande parte dos controles da Norma para implementar segurança da informação em suas instalações visto que a implantação de um modelo de gestão da Segurança da Informação, baseado na BS 7799-2, protege as informações das ameaças e vulnerabilidades, assegurando assim a continuidade dos negócios, minimizando os riscos e maximizando o retorno sobre o investimento (ROI).

Muitas dificuldades podem ser citadas para chegar a conclusão desta dissertação principalmente por se trartar de um tema novo e que não dispõe de farta bibliografia e de artigos, encontrou-se muita resistência para conseguir disponibilidade dos entrevistados que se inibem ao falar sobre o assunto de sua competência nas organizações, muitos se negaram a revelar informações e não emitiram nenhum comentário, apenas, responderam os questionários aplicados. Apesar das dificuldades, adquire-se muitos conhecimentos e foi possível verificar muitos pontos relativos ao uso da Norma BS 7799 e a consciência da necessidade de Segurança da Informação pesquisadas nas organizações de Salvador. Constata-se com esta pesquisa realizada em Salvador quais as tendências de Segurança da Informação no Brasil. Este é um cenário de uma sociedade que evolue permanentemente influenciada pelas Tecnologias da Informação.

Vale ressaltar que alguns temas foram mantidos em inglês porque são correntes no Brasil e se traduzidos podem dar um distorcimento dos conteudos.

7 BIBLIOGRAFIA:

ABELL, Angela. **Developing an information business-the HERTIS experience**. Bus. Inf. Review, v.6, n. 3, p.27-35, jan. 1990.

AGUDO GUEVARA, Álvaro. **Ética en la Sociedad de la Informacion: reflexiones desde América Latina**. In: Seminário Infoetica, 2000, Rio de Janeiro [2000]

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: Informação e documentação – Referências - Elaboração. Rio de Janeiro, 2000.

_____. **NBR 14724**: Informação e documentação – Trabalhos acadêmicos - Apresentação. Rio de Janeiro, 2001.

_____. **NBR 10520**: Informação e documentação - Apresentação de citações em documentos. Rio de Janeiro, 2001.

ARAÚJO V.M.R.H. DE. **Informação: instrumento de dominação e de submissão**. Ciência da Informação, V., n.1, 1991.

BARRETO, Aldo de Albuquerque. **A condição da informação**. São Paulo em Perspectiva, 16(3): 67-74, 2002.

_____. **A eficiência técnica e econômica e a viabilidade de produtos e serviços de informação**. Ci. Inf., Brasília, V.25, n.3, 1996. Disponível em: <http://www.ibict.br/cionline> Acesso em: 10 nov. 1999.

_____. **Perspectivas da Ciência da Informação.** Ci. Inf., Brasília, V.21, n.2, 1997. Disponível em: <http://www.ibict.br/cionline>

BATEMAN, T. S; SNELLL, S. S. **Administração. Construindo vantagem competitiva**. São Paulo: Atlas 1998.

BELKIN, N.J.,ROBERTSON,E.E. **Information science and teh phenomenon of information**. Jasis, v.27, n.4 1976.

BORGES, Mônica Erichsen Nassif. **A informação como recurso gerencial das organizações na sociedade do conhecimento**. C.i., vol. 24, n. 2, 1995.

BORGES, Mônica E.N., CAMPELLO, bernadete S. **A organização da informação para negócios no Brasil. Perspectivas em Ciencia da Informação**, v.2, n.2, jul/dez. 1997. p.149-162

BURKE, James & ORNSTEIN, Robert. **O presente do fazedor de machados**. Os dois gumes da história da cultura humana. Trad.: Pedro Jorgensen Jr. Rio de Janeiro: Bertrand do Brasil, 1998.

CALDAS, Miguel P e MOTTA, Fernando C. Prestes, **Cultura organizacional e cultura brasileira**. São Paulo: Atlas, 1997.

CARUSO, Carlos A A. **Segurança em informática e de informações**. São Paulo: SENAC,1999

CARVALHO, Kátia de. **Disseminação da informação e informação de inteligência organizacional**. Datagramazero revista da Ciência da Informação. V.2, n.3, jun/01.

_____. **O Profissional da Informação**: O Humano Multifacetado. Datagramazero revista da Ciência da Informação. V.3, n5, out/02.

CASTELLS, Manuel. **A sociedade em rede**. 4 ed. São Paulo: Paz e Terra, 1999.

CHIAVENATO, Idalberto. **Os novos paradigmas: como as mudanças estão mexendo com as empresas**. São Paulo: Atlas, 1996.

_____. **Recursos humanos**: Edição Compacta. São Paulo: Atlas, 1997.

_____. **Gestão de pessoas**: o novo papel dos recursos humanos nas organizações. Rio de Janeiro: Campus, 1999.

_____. **Introdução à teoria geral da administração**. 5 ed. São Paulo. Rio de Janeiro: Campus, 1999.

CHOO, Chun Wei. **A organização do conhecimento**. Como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. Trad.: Eliana Rocha. São Paulo: Editora Senac são Paulo, 2003.

COBRA Risk Consultant – http://www.securitypolicy.co.uk/risk.htm. Acessado em 20 de Outubro de 2004.

COUTINHO, L., FERRAZ,J. C. (Coords.) **Estudo das competitividade da indústria brasileira**. São Paulo: Papirus,1995.

CRASHAW, Sebastiam. **Competitive Intelligent**: developing value added information services. Infomediary, v.5, p.19-24, 1991

DAVENPORT, Thomas H. **Ecologia da informação**: por que só a tecnologia não basta na era da informação. Trad.: Bernadette S. Abrão. 4 ed. São Paulo: Futura, 1998.

DRAFT BS 7799-2:2002, Information **Security Management** - Part2: Specification for Information Security Management System. BSI, Novembro de 2001;

DRUCKER, P. F. **Administração em tempos de grandes turbulências**. São Paulo: Atlas, 1995

DRUCKER, Peter. **Sociedade pós-capitalista**. 7ª ed. São Paulo: Pioneira, 1999.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro. Axcel Books do Brasil Editora,2000.

FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário da Língua Portuguesa**. Rio de Janeiro, Editora Nova Fronteira, 1975.

FERREIRA, Rubens da Silva. **Gerencimento da informação no contexto empresarial**: uma abordagem sob o prisma da ecologia da informação. 2000. UFPa – Belém.

GAMMA. BS-7799. Disponível on-line na URL http:// www.gammassl.co.uk/ bs7799. 2000

GONÇALVES.M.A. **Os papéis do gerente e a qualidade da informação gerencial**. In: Encontro anual da associação nacional dos programas de pós-graduação em administraçào, 19.,1999, João pessoa. Rio de Janeiro, 1995. v.1, p.309-325.

GONÇALVES, Luís Rodrigo. **Pequeno histórico sobre o surgimento da Norma Nacional de Segurança de Informação** [NBR ISO/IEC-1779:2001]. 2003. Disponível em: <http://www.modulo.com.br>. Acesso em: 20 de Novembro. 2004.

HAICAL Cristiane. BS 7799 – **O Novo Paradigma da Segurança**. Modulo Security Solutions. Disponível on-line na URL, http://www.modulo.com. br. 12 set 2000, 1p.

IANNI, Octavianio. **A sociedade global**. 6 ed. Rio de Janeiro: Civilização Brasileira, 1998.

ISO 17799. Nascimento, Neide Landim Teixeirense do Nascimento, UNEB - COPEX, Setembro de 2001.

ISO 17799 World - http://www.iso-17799-security-world.co.uk/. Acesso em 15 de Janeiro de 2005

KUMAR, K. Da **sociedade pós-industrial à pós-moderna**. Rio de Janeiro: Jorge Zahar Editora Ltda, 1997.

LASTRES, Helena M.M.; ABAGLI, Sarita. **Informação e globalização na era do conhecimento**. S/ed, 2ª tiragem. Rio de Janeiro: Editora Campus Ltda, 1999.

LE COADIC, Yves F.**A ciência da informação**. Brasília Bruinquet de Lemos, 1996

LUZ, Ricardo. **Clima organizacional**. Rio de Janeiro: Qualitymark, 1995.

LUSSATO, B. **La théorie de l'empreinte**. Paris: ESF, 1991.
MALHOTRA, Y. **What is knowledge mangement?** Disponível em : <http:// www.brint.com.papers/copint.htm>.1993.

MARTINS, José Carlos Cordeiro. **Gestão de Projetos de Segurança da Informação**. Rio de Janeiro. Brasport, 2003.

MARTTELART, Armand. **História da sociedade da informação**. São Paulo: Edições Loyola, 2002.

MASUDA, Yoneji. **A sociedade da informação como sociedade pós industrial**. Rio:Ed. Rio 1982.

MAXIMINIANO, A. C. A. **Introdução à administração**. São Paulo: Atlas 1995

_____**Teoria geral da administração**. São Paulo: Atlas, 1997

McGARRY, Kevin. **O contexto dinâmico da informação:** uma analise introdutória. Trad.: Helena Vilar de Lemos. Brasília: Briquet de Lemos/Livros, 1999.

MENDES, Antônio. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistemas de Informações. Disponível em http://www.espacoacademico.com.br. Acesso em Julho de 2005.

MODULO Security, 9ª Pesquisa Nacional de Segurança da Informação. http://www.modulo.com.br. Acesso em fevereiro de 2005

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

MOTTA, Fernando C. Prestes. **Teoria Geral da administração: uma introdução,** 11a ed. São Paulo: Pioneira 1984.

_____**Teoria das organizações**: Evolução crítica, 2a ed. São Paulo: Pioneira Thompson Learning, 2001

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício de. **Segurançade Redes em Ambientes Cooperativos** . São Paulo. Editora Futura, 2002

NASSAR, Paulo. **História e cultura organizacional**. In: Revista Comunicação Empresarial – Nº 36, 2000.

NBR ISO/IEC 17799 – " **Tecnologia da Informação** – Código de prática para gestão da segurança da informação"

NIMER, Fernando. **Segurança da Informação em Ambientes Distribuídos**. Developers Magazine, vol 24 , pag 22-24, 1998

OLIVEIRA, Jayr Figueiredo de. **TIC - Tecnologias da informação e da comunicação**. São Paulo: Érica, 2003.

PARK, Kil H., DE BONIS, Daniel e ABUD, Marcelo R. **Introdução ao Estudo da Administração**. São Paulo, Pioneira, 1997.

Portal ISO 17799 - http://www.iso17799.hpg.ig.com.br/. Acesso em 20 de fevereiro de 2003.

PINHEIRO, Lena Vania R.,LOUREIRO José Mauro M. **Traçados e limites da ciência da informação**. Ci. Inf., Brasília, V.24, n.1 1995 Disponível em: <http://www.ibict.br/cionline>

RAMOS, Anderson. **O mercado econômico e a Segurança da Informação**. Disponível em: <http://www.modulo.com.br>. Acesso em: 23 de Fevereiro. 2005.

RAMOS, F. F. **Qualidade na Segurança da Informação Digital**. ESecurity Solutions. Axur Communications Inc. Disponível on-line na URL http://www.axur.org/bs7799/ bs7799.pdf. Jul. 2000, 19p.

SAGAN, C. **The dragons of Eden; especulations on the evolution of humam intelligence**. New York: Ballantine Books, 1977

SÊMOLA, Marcos. **Gestão da Segurança da Informação**, Ed. Campus, 2003.

SARACEVIC, Tefko. **Interdisciplinary nature of information science**. Ci. Inf., Brasília, v.24, n.1, p. 36-41, jan./abr 1995.

SOARES, Vanessa Pires. **A cultura organizacional e seus componentes**. Disponível em: <http://www.nead.unama.br/charles/cultura.htm>. Acesso em: 29 abr. 2002.

SOUZA, Edela Lanzer Pereira de. **Clima e cultura organizacionais**: como se manifestam e como se manejam. Porto Alegre: Edgar Blücher, 1978.

SROUR, Robert Henry. **Poder, Cultura e Ética nas Organizações**. São Paulo, Editora Campus, 1998.

SPÍNOLA, S.B., PESSOA. **Tecnologia de informação e estratégia empresarial**. In: MARCOVITCH, J. Administração de operações. São Paulo: Futura, 1997.

SVEIBY, K.E. **A nova riqueza das organizações**. Rio de Janeiro: Campus, 1998.

TARAPANOFF, Kira; ARAÚJO Jr, Rogério Henrique de; CORMIER, Patricia Marie Jeanne. **Sociedade da informação e inteligência de informação**. Ci. Inf., Brasília, v.29, n.3, p.91-100, set./dez. 2000.

TARAPANOFF, Kira; Organizadora. **Inteligência Organizacional e Competitiva**. Brasília : Editora Universidade de Brasília, 2001.

TURBAN, Efrain; RAINER JR, R. Kelly & POTTER, Richard E. **Administração de tecnologia da informação**. Teoria e prática.Trad: Teresa Cristina Felix de Souza. Rio de Janeiro: Campus, 2003.

VERGASTA, Patrícia Dantas. **Cultura e aprendizagem organizacional**. 2001. Disponível em: <http://www.terravista.pt/enseada/5831/trabalho/t200310.html>. Acesso em: 7 abr. 2002.

WEIL, Pierre. **Organizações e tecnologias para o terceiro milênio**: a nova cultura organizacional holística. Rio de Janeiro: Rosa dos Tempos, 1995.

WETHERBE, Alan. **A volta do capitalismo**. São Paulo: EDUSC, 1999

WIENER, Norbert. **Cibernética e sociedade**. São Paulo: Editora Cultrix Ltda, 1954.

APÊNDICE I

Questionário para identificar o grau de aderência da sua empresa em relação às recomendações de Segurança da Informação da Norma internacional BS 7799 ou de sua versão brasileira ISO/IEC 17799. Um diagnóstico simples e rápido, baseado em perguntas objetivas. Escolha apenas uma resposta para cada pergunta.

SUA EMPRESA POSSUI:

1 POLÍTICA DE SEGURANÇA

1.1 Política de Segurança?

( ) SIM
( ) NÃO

1.2 Algum responsável pela gestão da política de segurança?

( ) SIM
( ) NÃO

2 SEGURANÇA ORGANIZACIONAL

2.1 Infra-estrutura de segurança da informação para gerenciar as ações corporativas?

( ) SIM
( ) NÃO

2.2 Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?

( ) SIM
( ) NÃO

2.3 Definição clara das atribuições de responsabilidade associadas à segurança da informação?

( ) SIM
( ) NÃO

2.4 Identificação dos riscos no acesso de prestadores de serviço?

( ) SIM
( ) NÃO

2.5 Controle de acesso específico para os prestadores de serviço?

( ) SIM
( ) NÃO

2.6 Requisitos de Segurança dos contratos de terceirização?

( ) SIM
( ) NÃO

3 CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO

3.1 Inventário dos ativos físicos, tecnológicos e humanos?

( ) SIM
( ) NÃO

3.2. Critérios de Classificação da Informação?

( ) SIM
( ) NÃO

4 SEGURANÇA EM PESSOAS

4.1. Critério de seleção e política de pessoal?

( ) SIM
( ) NÃO

4.2. Acordo de confidencialidade, termos e condições de trabalho?

( ) SIM
( ) NÃO

4.3. Processos para capacitação e treinamento de usuários?

( ) SIM
( ) NÃO

4.4. Estrutura para notificar e responder aos incidentes e falhas de segurança?

( ) SIM
( ) NÃO

5 SEGURANÇA FÍSICA E DE AMBIENTE

5.1 Definição de perímetros e controles de acesso físico aos ambientes?

( ) SIM
( ) NÃO

5.2. Recursos para segurança e manutenção dos equipamentos??

( ) SIM
( ) NÃO

5.3. Estrutura para fornecimento adequado de energia?

( ) SIM
( ) NÃO

5.4. Segurança do cabeamento de rede?

( ) SIM
( ) NÃO

6 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

6.1 Procediemntos e responsabilidades operacionais?

( ) SIM
( ) NÃO

6.2 Controle de mudanças operacionais?

( ) SIM
( ) NÃO

6.3 Segregação de funções e ambientes?

( ) SIM
( ) NÃO

6.4 Planejamento e aceitação de sistemas?

( ) SIM
( ) NÃO

6.5. Procedimentos para cópias de segurança ?

( ) SIM
( ) NÃO

6.6. Controles e gerenciamento de Rede?

( ) SIM
( ) NÃO

6.7 Mecanismos de segurança e tratamento de mídias?

( ) SIM
( ) NÃO

6.8 Procedimentos para documentação de sistemas?

( ) SIM
( ) NÃO

6.9 Mecanismos de segurança do correio eletrônico?

( ) SIM
( ) NÃO

7 CONTROLE DE ACESSO

7.1. Requisitos do negócio para contorle de acesso?

( ) SIM
( ) NÃO

7.2 Gerenciamento de acessos do usuário?

( ) SIM
( ) NÃO

7.3 Controle de acesso à rede?

( ) SIM
( ) NÃO

7.4. Controle de acesso ao sistema operacional?

( ) SIM
( ) NÃO

7.5 Controle de acesso à aplicações?

( ) SIM
( ) NÃO

7.6 Monitoração de uso e acesso ao sistema?

( ) SIM
( ) NÃO

7.7 Critérios para computação móvel e trabalho remoto?

( ) SIM
( ) NÃO

8 DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

8.1 Requisitos de segurança de sistemas?

( ) SIM
( ) NÃO

8.2 Controles de Criptografia?

( ) SIM
( ) NÃO

8.3 Mecanismo de segurança nos processos de desenvolvimento e suporte?

( ) SIM
( ) NÃO

9 GESTÃO DA CONTINUIDADE DO NEGÓCIO

9.1 Processo de gestão da continuidade do negócio?

( ) SIM
( ) NÃO

10 CONFORMIDADE

10.1 Gestão de conformidade técnicas e legais?

( ) SIM
( ) NÃO

10.2. Rcursos e critérios para auditoria de sistemas?

( ) SIM
( ) NÃO

11 NORMA BS 7799 / ISO IEC 17799

11.1 Conhece os controles da Norma de Segurança da Informação BS7799/ISO IEC 17799?

( ) SIM
( ) NÃO

11.2 Utilizou os controles de melhores práticas da Norma BS 7799/ISO IEC 17799 para implantar o Sistema de Gestão de Segurança da informação?

( ) SIM
( ) NÃO

APÊNDICE II

Lista das Organizações pesquisadas:

1 – Hospital Jorge Valente
2 – Ministério Público da Bahia
3 – Construtora BCL
4 - Hospital da Cidade
5 – Valia Corretora de Seguros
6 – Scar Alimentos Congelados
7 – BA Empreendimentos
8 – Sol Bahia Atlântico
9 – Sisthemica
10 – Cidade Companhia Incorporações e Desenvolvimento
11 – Centro de Medicina Laboratorial
12 – Laboratório Dirceu Ferreira
13 – Laboratório Qualitech
14 – Canal Jeans
15 – Pro-Experts
16 – Boa Viagem Transportes
17 – Dupont S/A
18 – Sasil Distribuidora de Produtos Químicos
19 – Aliança Navegação
20 – Instituto Superior de Candeias
21 – Sian Produtos Automotivos
22 – TRM Resinas Termoplásticas
23 – Supricel Logística e Transportes
24 – Sol Embalagens
25 – Danelon Informática
26 – Haltecnologia
27 – Help Informática
28 – Prodasal
29 – IPQ Tecnologia
30 – Desembahia
31 – Lebre Informática
32 – Oftalmoclin – Clínica Oftalmológica
33 – Saveiro Veículos

34 –R2M Postos e Serviços
35 – Fiber Line Telecomunicações
36 – Associação Bahiana de Educação e Proficiência – ABEP
37 – Digita Informática
38 – Iguatemi Pneus
39 – Passe Livre
40 – Unibahia
41 – Perbrás
42 - Bahema
43 – Contasso
44 – Banda Larga Telecomunicações
45 – Cosbat Engenharia
46 – Clínica Santa Helena
47 – SGS do Brasil
48 – Mills Rental
49 – TW Espumas
50 –Entel
51 – Praia Grande Transpostes
52 – VCI Viação Cidade Industrial
53 – ECR Postos
54 – Axé Transportes
55 – Sol Nordeste
56 –Iguatemi Autopeças
57 – Frios e Congelamentos Souza Carvalho
58 – Posto Bahia Marina
59 – Scar Hotel Turismo
60 – Instituto Sol
61 – Realce Transporte
62 – Sol Reciclagem