UNIVERSIDADE CATÓLICA DE BRASÍLIA

PRÓ-REITORIA DE PÓS-GRADUAÇÃO
STRICTO SENSU EM GESTÃO DO CONHECIMENTO
E DA TECNOLOGIA DA INFORMAÇÃO

Mestrado

A PERCEPÇÃO GERENCIAL SOBRE O MODELO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA PÚBLICA DE TIC: Perspectiva de evolução para um modelo de governança

Autora: Maria do Carmo Soares de Mendonça
Orientadora: Luiza Beth Nunes Alonso
Co-orientador: Rildo Ribeiro dos Santos

Brasília 2007

MARIA DO CARMO SORES DE MENDONÇA

A PERCEPÇÃO GERENCIAL SOBRE O MODELO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA PÚBLICA DE TIC: Perspectiva da evolução para um modelo de governança

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu da Universidade Católica de Brasília, como requisito parcial para obtenção do título Mestre em Gestão do Conhecimento e da Tecnologia da Informação.

Orientadora: Profª Dra. Luiza Beth Nunes Alonso
Co-orientador: Prof. Dr.Rildo Ribeiro dos Santos

Brasília
2007

M539p Mendonça, Maria do Carmo Soares de.
A percepção gerencial sobre o modelo de gestão da segurança da informação de uma empresa pública de TIC : perspectiva de evolução para um modelo de governança / Maria do Carmo Soares de Mendonça. – 2007.
171 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade Católica de Brasília, 2007.
Orientação: Luiza Beth Nunes Alonso.
Co-orientação: Rildo Ribeiro dos Santos.

1. Gestão do conhecimento – Sistemas de segurança. 2. Tecnologia da informação. I. Alonso, Luiza Beth Nunes, orient. II. Santos, Rildo Ribeiro dos, co-orient. III. Título.

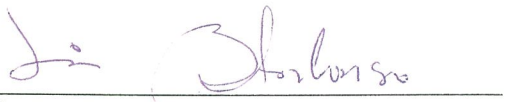
CDU 004:658

Ficha elaborada pela Coordenação de Processamento do Acervo do SIBI – UCB.

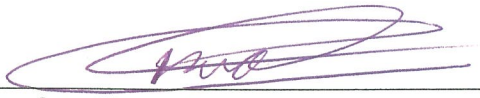
TERMO DE APROVAÇÃO

A PERCEPÇÃO GERENCIAL SOBRE O MODELO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA PÚBLICA DE TIC:
PERSPECTIVA DE EVOLUÇÃO PARA UM MODELO DE GOVERNANÇA

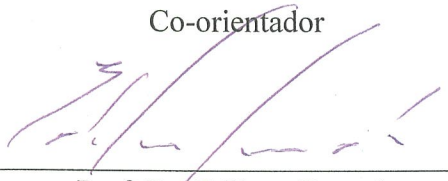
Dissertação defendida e aprovada como requisito parcial para obtenção do grau de Mestre no Programa de Gestão do Conhecimento e da Tecnologia da Informação, defendida e aprovada, em 14 de setembro de 2007, pela banca examinadora constituída por:



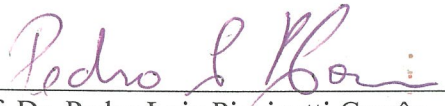
Profª. Drª. Luiza Beth Nunes Alonso
Orientadora



Prof. Dr. Rildo Ribeiro dos Santos
Co-orientador



Prof. Dr. Edilson Ferneda



Prof. Dr. Pedro Luiz Pizzigatti Corrêa

Brasília
UCB

À memória de meu sobrinho Everaldo de Carvalho Nascimento Filho.
Meu "Everaldinho de Bonito", que de tão lindo e puro, autêntico
semeador do amor, cedo foi para o Céu, a morada do Pai.

AGRADECIMENTOS

A meu Deus agradeço Sua eterna misericórdia, o dom da vida, a esperança, a diversidade dos carismas – *Por ora subsistem a fé, a esperança e a caridade – as três. Porém, a maior delas é a caridade*. Coríntios I -13. E Ele nos ensina em Eclesiastes 2.3, que "... para tudo há um tempo, para cada coisa há um momento debaixo dos céus: Tempo para nascer... Tempo para ser feliz..."

É o momento de lembrar com carinho de todos que me ajudaram e compartilharam comigo esta caminhada tão especial, realização de um sonho.

Agradeço ...

... à Professora Luiza Beth Nunes Alonso e ao Professor Rildo Ribeiro dos Santos, meus orientadores e amigos, sua compreensão, atenção, dedicação e competência, orientando-me durante este estudo, incentivando-me a explorar novos conhecimentos.

... ao Professor Ivan Rocha Neto que orientou meus primeiros passos neste estudo.

... às Professoras Germana Menezes da Nóbrega, Kátia Marçal de Oliveira e Rejane Maria da Costa Figueiredo e aos Professores Eduardo Amadeu Dutra Moresi, Gentil José de Lucena Filho e Paulo Sergio Vilches Fresneda;

... aos Professores que participaram da banca de qualificação, seu apoio, abrindo minha mente para novas possibilidades: Edilson Ferneda, Ivan Rocha Neto, Luiza Beth Nunes Alonso e Paulo Sergio Vilches Fresneda.

Agradeço à assessoria do mestrado. À Georgiane Pessoa Alcoforado Jordão, com sua amizade, compartilhando de meus momentos de fraqueza, sempre trazendo conforto e apoio. À Janine dos Santos Silva, a incansável ajuda. À Elisângela Aguiar Fernandes, o grande carinho.

Aos amigos anônimos da Católica: da secretaria, da limpeza, da biblioteca, da lanchonete, da segurança a alegria, o sorriso, a gentileza, o bom-dia, enfim, tudo.

Agradeço aos amigos e amigas do Serpro ...

... Marcos Allemand Lopes, pela aprovação de minha participação no Mestrado, incentivando-me em todas as etapas e contribuindo com sua competência na validação do questionário da pesquisa e conteúdo da dissertação.

... Paulo Afonso Almeida da Silva, pelas leituras e estudo, no sentido de verificar a compreensão do texto.

... Pedro André de Faria Freire e Paulo Ricardo Lima Hidaka, pela contribuição na validação do instrumento de pesquisa e os comentários importantes ao questionário.

... Gilberto de Oliveira Netto, pela compreensão em meus afastamentos periódicos para dedicação ao estudo.

... Vera Lúcia de Moraes e Maisa Pieroni de Lima, da Universidade Corporativa do Serpro, pelo apoio para tornar possível a aplicação da pesquisa aos superintendentes da Empresa.

... aos líderes executivos, superintendentes dos segmentos UPS, URC, UGE, UAE e Órgãos de Consultoria e Apoio que contribuíram respondendo à pesquisa: Ângelo José Bezerra, André de Cesero, Aluysio Marques, Bell Simões, Carlos Roberto Magalhães,

Cátia Gontijo, Edson Geraldo Ferreira, Eunides Chaves, Fernando Bento, Gilberto Netto, Heloisa Helena de Rezende Silva, Ivo Torres, Iran Martins Porto Junior, João Carlos dos Santos, Lucio Lage, Luiz Cláudio Turbay, Luis Gustavo Loyola, Marco Sobrosa, Marcus Vinicius da Costa, Miyuki Abe, Mauricio Vasconcelos Saraiva, Roberval Lopes Ádamo, Roberto da Silva Plá, Robinson Margato, Viviane Santos Cohen e Vitor Propato.

... Liana Selma de Souza, pela disponibilidade e principalmente o apoio durante a fase de recepção do questionário da pesquisa.

... Ney Fernandes Marinho e a sua filha Raíssa, pelas contribuições com seus conhecimentos estatísticos na consolidação da pesquisa, e a colaboração do colega José Antonio Carletti na finalização da pesquisa.

... Isamir Machado de Carvalho, pelo apoio e incentivo, compartilhando sua experiência de vida acadêmica.

... Janaína Alves Catúlio, por sua presteza e atenção em atender no fornecimento de material bibliográfico.

Enfim, agradeço a meus amigos, a minha família, a meu grupo de oração a amizade, o apoio incondicional e, sobretudo, as orações.

Mas eu confiei em ti, Senhor e disse:
Tu és o meu Deus.
Salmo 31
O Senhor é o meu pastor, nada me faltará.
Salmo 23

RESUMO

No mundo globalizado da tecnologia da informação e comunicação, as ameaças a sistemas de informação e redes de computadores qualificam a segurança da informação como elemento de diferencial competitivo, para garantir o sucesso de uma organização, pública ou privada. Neste contexto, a gestão da segurança assume um papel de protagonista na estratégia de conhecer riscos e definir controles adequados para garantir a perenidade institucional, aliando-se à responsabilidade da alta administração, gerentes executivos, clientes e interessados (*stakeholders*) na definição e no apoio aos planos que possam suportar o objetivo do negócio. Com este direcionamento, na atualidade, percebe-se a tendência de adotar-se uma estrutura de governança da segurança da informação, buscando garantir que a segurança seja substancialmente atrelada ao objetivo estratégico de crescimento sustentável da empresa. Diante disto, esse estudo se propôs a investigar a percepção dos gerentes executivos de uma empresa pública de TIC sobre a segurança da informação no âmbito de seus segmentos de atuação. A pesquisa discutiu as questões sobre governança e gestão, segurança em recursos humanos, planejamento, gestão de incidentes, continuidade do negócio e conformidade com requisitos legais. O resultado da pesquisa indicou que, apesar de existir uma política de gestão de segurança da informação, fatores como pouca visibilidade estratégica da segurança pela alta administração, apoio parcialmente suficiente da alta direção e integração parcial entre as áreas para melhorar o nível de segurança têm sido determinantes para que as ações de segurança sejam isoladas, sinalizando a necessidade de controles mais efetivos sobre o investimento em segurança e seu resultado sobre o negócio.

Palavras-chave: Tecnologia da Informação; Governança e Gestão; Segurança da Informação.

ABSTRACT

In the globalized world of information and communication technology (ICT), the threats to information systems and computer networks make information security a key element to competitive advantage in order to guarantee the success of both private and public organizations. In this context, security management takes on a key role in the strategy of risk recognition and definition of adequate controls in order to guarantee institutional longevity, joining the responsibility of upper management, management executives, clients and stakeholders in the definition and the aid of plans that can support the objectives of the business. Nowadays, one can note a tendency to adopt a structure of governance for information security, in an effort to guarantee a substantial link to the strategic objective of sustainable growth of the enterprise. Accordingly, this study proposes to investigate the perception of senior management of a public ICT enterprise related to information security in their line of business. This research discusses the issues of governance and management, security in the area of human resources, planning, incident management, business continuity and conformity with regard to legal requisites. The results of this research indicate that, in spite of the existence of an information security management policy, factors such as poor strategic visibility of security by top management, partially sufficient support from upper management and partial integration between the areas to improve the level of security have been determining factors in order for the security actions to be isolated, indicating a necessity for more effective controls regarding investment in security and its result with respect to the business.

Keywords: Information Technology; Governance and Management, Information security.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SIGLAS

AICPA (American Institute of Certified Public Accountants)

BASEL II (second of the Basel Accords – Health Insurance Portability and Accountability Act)

CERT (Computer Emergency Response Team)

CERT-br (Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil)

CIAO (Critical Infrastructure Assurance Office)

CIO (Chief Information Officer)

CISO (Chief Information Security Officer)

CSO (Chief Security Officer)

CNASI (Congresso de Auditoria de Sistemas e Segurança da informação)

COBIT (Control Objectives for Information and Related Technology)

FISMA (Federal Information Security Management Act of 2002 – United States federal law)

GLBA (Gramm-Leach-Bliley Act)

GMI (Governance Metrics International)

HIPAA (Health Insurance Portability and Accountability Act)

IIA (Institute of Internal Auditors)

ISACA (Information System Audit and Control Association)

ISSA (Information Systems Security Associations)

ITGI (IT Governance Institute)

ITIL (Information Technology Infrastructure Library)

NACD (National Association of Corporate Directors)

NIST (National Institute of Standards and Technology)

OCTAVE – (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OECD (Organization for Economic Co-operation and Development)

ROI (Return On Investment)

Serpro (Serviço Federal de Processamento de Dados)

SUMÁRIO

1. INTRODUÇÃO

No mundo globalizado da tecnologia da informação e comunicação, as ameaças a sistemas de informação e redes de computadores qualificam a segurança da informação como elemento de diferencial competitivo, para garantir o sucesso de uma organização, pública ou privada. Neste contexto, a gestão da segurança assume um papel de protagonista na estratégia de conhecer riscos e definir controles adequados para garantir a perenidade institucional, aliando-se à responsabilidade da alta administração, gerentes executivos, clientes e interessados (stakeholders) na definição e no apoio aos planos que possam suportar o objetivo do negócio.

A realidade das ameaças à segurança da informação tem sido reportada aos Centros de Estudos, Respostas e Tratamento de Incidentes de Segurança (CERT) de vários países. No Brasil, o Cert-br é a organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. Em 2005 foram reportados ao Cert-br 68 mil incidentes de segurança. Em 2006, mais de 137 mil.

As ameaças à segurança da informação e comunicações atingem o mundo globalizado. A título de exemplo, cita-se pesquisa realizada em 2006, pelo Computer Security Institute do Federal Bureau of Investigation – CSI/FBI em parceria com a Australian Computer Crime and Security Survey, que apresentaram os seguintes dados: em 2004 foram reportados 51% de incidentes de segurança considerados graves, em 2005 o índice foi de 63% e em 2006 o índice foi de 76%.

Diante da crescente ameaça à segurança da informação, alguns institutos como o Information Security Governance Institute (ITGI), Instituto Brasileiro de Governança Corporativa (IBGC), National Institute of Standards and Technology (NIST), Software Engineering Institute, da Carnegie Mellon University, têm recomendado a migração do modelo tradicional de gestão da segurança para uma estrutura de governança, por entender que segurança, controles e transparência são fatores fundamentais para a sustentação do negócio.

A estrutura de governança, a partir do modelo da governança corporativa, consiste

de um conjunto de políticas e controles internos pelos quais as organizações, independentemente do escopo - privada, pública ou outros tipos são dirigidas. Inclui nesse contexto o relacionamento entre a alta direção, executivos seniores, patrocinadores, empregados e interessados (stakeholders) para garantir a responsabilidade administrativa de cada um dos envolvidos com os resultados da organização (VON SOLMS, 2004, p.1).

O que sugerem os institutos é um modelo de segurança da informação baseado nessas premissas. Adicionalmente, segundo Chairman (2001, p.1), a governança da segurança da informação é uma evolução dos modelos de gestão porque, além do envolvimento da alta administração e dos lideres seniores, os líderes da segurança compartilham da mesma responsabilidade, da conformidade com leis, regulamentos e política. Todos, de acordo com suas responsabilidades, respondem e fornecem o nível de segurança adequado ao negócio e ao interesse das partes.

A segurança da informação é a busca da proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio. (ASSOCIAÇAO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005, p.ix).

No formato do cenário de ameaças à segurança da informação e diante da tendência de convergência para um modelo de gestão da segurança que melhor responda às premissas de que a “segurança é uma questão do negócio e não uma questão técnica” (VON SOLMS, 2004, p. 1) e que “nem sempre é fácil para os gestores alinharem a política de segurança da informação às estratégias do negócio da empresa” (HÖNE e ELOFF, 2002, p.403), este estudo pesquisou junto aos gerentes executivos de uma empresa pública de TIC para conhecer a percepção desses gerentes sobre a segurança da informação no âmbito de seu segmento de atuação, com o objetivo de verificar estatisticamente quanto a gestão da segurança da informação, numa empresa pública de tecnologia, está convergindo para um modelo de governança de segurança da informação.

O resultado da pesquisa indicou que, apesar de existir uma política de gestão de segurança que contempla a gestão de riscos como fundamento para definir os controles de segurança, fatores como pouca visibilidade estratégica da segurança pela alta administração, apoio parcialmente suficiente da alta direção e integração parcial entre as

áreas para melhorar o nível de segurança têm sido determinantes para que as ações de segurança sejam isoladas, sinalizando a necessidade de controles mais efetivos sobre o investimento em segurança e seu resultado sobre o negócio.

A discussão do estudo foi estruturada em capítulos. A introdução aborda o problema, objetivos, relevância do tema, contexto e delimitação do estudo. O segundo capítulo é o referencial teórico em que são discutidos os temas governança: explorando os significados, objetivos e modelos de governança corporativa, de tecnologia da informação e da segurança da informação. Apresenta ainda a gestão da segurança da informação, gestão de riscos e gestão da continuidade do negócio. O terceiro discute a metodologia da pesquisa. O capítulo quarto descreve o resultado da pesquisa, discutindo a interpretação e análise dos dados. O quinto apresenta a conclusão para cada um dos temas da pesquisa e recomendações para trabalhos futuros. Ao final, estão as referências que embasaram o estudo, listas de diagramas, figuras, tabelas, siglas e abreviaturas.

1.1 Formulação do problema da pesquisa

A evolução tecnológica trouxe uma nova realidade: velocidade para tornar disponíveis as funcionalidades do negócio numa disponibilidade de infra-estrutura de 24 horas por dia, todos os dias do ano. Paralelamente a essa evolução estão ameaças, vulnerabilidades, ou seja, riscos ao negócio. Para minimizar o quadro de riscos surge a segurança da informação, que busca a preservação da confidencialidade, da integridade e da disponibilidade da informação por meio do uso adequado de controles.

Esse cenário exige a responsabilidade de todos: do conselho de diretoria, alta gerência, empregados, clientes, fornecedores para a proteção dos ativos de informação, garantindo a conformidade com os requisitos legais, sob pena de responder pessoalmente pelas falhas de segurança, se comprovada a falha de gestão. Além disso, os gerentes executivos têm a responsabilidade de perceber que a segurança da informação é uma "disciplina multidimensional" e que todas as dimensões devem ser levadas em conta (governança, estrutura organizacional, política, boas práticas, ética, certificações, legalidade, pessoa humana, consciência, técnica, métricas e auditoria) e disseminar boas práticas no âmbito da organização. Um plano de segurança com todas essas dimensões deve ser suportado por um modelo de governança da segurança da informação. (VON SOLMS, 2004, 2-3).

Diante desse contexto pode-se afirmar que:

- A segurança da informação é uma área de importância estratégica para a organização, pois é um elemento que potencializa sua competitividade e agrega valor aos serviços e produtos da organização;
- Os gerentes executivos são responsáveis diretos para que a política e procedimentos de segurança da informação ocorram de forma efetiva na organização.

Considerando essas premissas, pode-se formular o seguinte problema: qual é a real percepção dos gerentes executivos sobre a segurança da informação no âmbito de seu segmento de atuação?

1.2 Objetivos

A pesquisa pretende verificar como os gerentes executivos percebem a segurança da informação no âmbito de sua área de atuação. Diante disso, foram considerados os seguintes objetivos específicos:

- Identificar os elementos que caracterizam a gestão de segurança da informação;
- Definir um instrumento e método para identificar a percepção dos gerentes executivos quanto à gestão de segurança da informação;
- Verificar o quanto a gestão atual da segurança da informação numa empresa pública de TIC está convergindo para uma governança de segurança da informação;
- Detectar pontos de ação de melhoria no modelo atual de gestão da segurança da informação.

1.3 Relevância do tema

Na atualidade, diante das ameaças e riscos a que estão expostas as organizações, principalmente aquelas que prestam serviços especializados em tecnologia de informação e comunicações e cujos produtos são considerados de missão crítica para a administração pública direta, necessitam adotar um comportamento gerencial conciliável com essa realidade. Na prática, significa dispor de políticas de segurança compatíveis com o tipo de risco do negócio, que reflitam as necessidades internas e externas de proteção. Há estudos indicando que em torno de 80% das falhas de segurança podem ser resultantes não de fracas soluções de segurança, mas de fracos comportamentos de segurança da alta liderança: daí, um bem focado programa de segurança com metas de melhorias e um "comportamento de segurança" eficiente poderia trazer significativas reduções dos altos índices de falhas de segurança (LEACH, 2003, p. 685).

Segundo Leach, (2003, p. 689), a liderança é ponto fundamental da cultura de segurança, sugerindo que muitos fatores influenciam o comportamento de segurança da organização. Alguns estão relacionados a atitudes adotadas pela liderança quanto a definir e seguir as políticas e padrões de segurança, coibindo ações personalizadas de tomada de decisão movidas por crenças, a sustentar o controle realístico das ameaças internas, seguindo as regras, a fim de manter a confiança da organização. No entanto, acredita Leach (2003, p. 692), que três fatores influenciam fortemente a formação da cultura de segurança. São eles:

- A certeza de que o comportamento da alta liderança não é contraditório com o conhecimento sobre segurança da organização;
- A habilidade da alta direção para reconhecer, fortalecer e treinar os usuários sobre as regras comuns de segurança;
- A convicção de que a alta administração vê seriamente as questões de segurança porque demonstra um bom comportamento para operar a organização.

No contexto da importância do conhecimento e envolvimento da alta liderança nas questões de segurança da informação na organização, Chairman (2001, p. 36) afirma que as ameaças a sistemas de informação, interna e externa, que emanam - entre outras - de

condições tecnológicas, desastre natural, condições ambientais, fatores humanos, acesso não-autorizado ou vírus, podem resultar potencialmente em menor controle e realisticamente em riscos ao negócio. Diante disto, nos últimos anos, o trabalho de diretor tem mudado drasticamente, sendo exigidos da alta liderança conhecimentos sobre segurança da informação, visto que se forma no mercado o entendimento de que segurança é responsabilidade da alta direção. Para o autor, de acordo com as boas práticas, o conhecimento da alta liderança deve abranger principalmente:

- Disponibilidade: os sistemas de segurança devem estar disponíveis sempre que requeridos;
- Confidencialidade: os dados e informações devem ser revelados somente a quem precisa conhecer;
- Integridade: os dados e informações devem ser protegidos de acessos indevidos e modificações não-autorizadas.

Segundo o NIST para que a segurança da informação tenha uma estrutura de governança, é necessário que a organização adote uma estrutura em que a alta administração, gerentes executivos, clientes e interessados (*stakeholders*) tenham claramente definidos sua missão e as necessidades do negócio e reconheçam sua respon-sabilidade diante das leis, políticas e regulamentos para garantir a segurança do negócio. (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 800-100, 2006, p.8),

Caralli (2004, p.2-3) argumenta que observações e pesquisas indicam que um dos problemas de falha de segurança está relacionado à gerência sênior e patrocinadores que não reconhecem o valor da segurança para o negócio. Por outro lado, existem organizações que destinaram ao CSO (CHIEF SECURITY OFFICER), subordinado à alta direção, a responsabilidade de gerir a segurança, no âmbito de governança.

As organizações estão cada dia mais dependentes de tecnologia e mais vulneráveis aos riscos e ameaças. Para mudar esse cenário, mantendo níveis aceitáveis de riscos, as empresas precisam investir no conhecimento de segurança empresarial, que não é uma disciplina isolada, mas alinhada ao negócio, à missão e aos objetivos da empresa (CARALLI, 2004, p. vi).

Segundo Allen (2005, p. 8), é responsabilidade da alta direção, dos gerentes executivos e CSO (chefes de segurança) manter as ações necessárias à segurança, sabendo que seus comportamentos e ações sobre a segurança influenciam toda a organização. A influência da liderança não se restringe à questão de conformidade, mas de perda de credibilidade quando quebram a confiança por adotar condutas diferentes daquelas definidas em políticas e procedimentos, controles e supervisão, monitoramento, treinamento e conscientização. Enfim, coerência, ética e transparência no direcionamento e controle são essenciais para estabelecer e sustentar a cultura de consciência de segurança, numa boa governança.

Adicionalmente, de acordo com Allen (2005, p. 8), é responsabilidade da alta direção revisar as políticas e programas de segurança, enquanto cabe aos gerentes a responsabilidade de garantir a conformidade com as leis e regulamentos, mantendo controle e métricas de verificação do nível de segurança.

Para o ITGI (INFORMATION SECURITY GOVERNANCE INSTITUTE, 2004, p. 8), a segurança da informação não é somente uma questão de tecnologia, mas um negócio e como tal requer governança que envolva uma adequada gestão de riscos. Efetivamente, a segurança abrange a gerência executiva para avaliar as ameaças emergentes e as respostas da organização para mitigar esses riscos.

O ITGI (2004, p. 8-9) entende que a dependência de sistemas de informação e a vulnerabilidade desses sistemas representam riscos que ameaçam a continuidade do negócio da organização. Diante disto, no modelo de governança - orientado pelo Instituto - cabe ao conselho de administração a responsabilidade de entender as questões de segurança e recomendar o fornecimento de estratégias concernentes a:

- Entender a criticidade das informações e a segurança da informação para a organização;
- Revisar os investimentos para alinhar a segurança da informação com a organização e os perfis dos riscos;
- Endossar o desenvolvimento e implantação de um programa de segurança da informação;

- Definir a regularidade de relatórios sobre a eficiência e efetividade do programa de segurança.

Adicionalmente, recomenda o ITGI (2004, p. 9) que a alta direção e a gerência executiva devem revisar a implementação do programa de segurança corrente, identificar as tendências e buscar investimento em soluções que garantam a otimização do processo e minimizem custos, criando novas oportunidades do negócio.

1.4 Contextualização do estudo

Este estudo tomou como base o Serviço Federal de Processamento de Dados (Serpro) por se tratar de uma empresa pública que presta serviço de tecnologia da informação e comunicação à Administração Pública Federal e dispõe de um modelo de gestão de segurança, cuja estrutura está sedimentada como apoiadora dos processos de segurança com abrangência em todos os segmentos organizacionais.

1.4.1 Histórico do Serpro

O Serviço Federal de Processamento de Dados (Serpro), empresa pública vinculada ao Ministério da Fazenda, criado pela Lei nº. 4.516, de 1° de dezembro de 1964, regido pela Lei nº. 5.615, de 13 de outubro de 1970, pelo Estatuto Social, criado pelo Decreto nº. 3.972, de 16 de outubro de 2001, e pelas normas legais que lhe forem aplicáveis, tem por objeto a execução de serviços de tratamento de informações e processamento de dados, incluindo as atividades de teleprocessamento e comunicação de dados, voz e imagens, que sejam requeridas, em caráter limitado e especializado, para a realização dos referidos serviços e a prestação de assessoramento e assistência técnica no campo de sua especialidade.

O Serpro foi criado para modernizar e dar agilidade a setores estratégicos da

administração pública. Atualmente é a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil. Cresceu desenvolvendo programas e serviços que permitiram maior controle e transparência sobre a receita e os gastos públicos. Consolidou-se ao longo desses anos, aprimorando tecnologias que foram adotadas por diversos órgãos públicos federais, estaduais e municipais e incorporadas à vida do cidadão brasileiro. Diante disto, tem se consolidado como uma empresa de missão crítica para o Governo Federal.

Situa-se fisicamente em uma sede central, localizada em Brasília, e em dez regionais distribuídas em dez regiões fiscais – Brasília, Belém, Fortaleza, Recife, Salvador, Belo Horizonte, Rio de Janeiro, São Paulo, Curitiba e Porto Alegre. São quase 8 mil empregados prestando serviços e desenvolvendo soluções de tecnologia, gestão empresarial e relacionamento com clientes em mais de 330 municípios brasileiros.

1.4.2 Mercado do Serpro

O mercado de atuação do Serpro, no âmbito da tecnologia da informação e comunicações, está no segmento das finanças públicas, constituído pelo Ministério da Fazenda, suas secretarias e demais órgãos, correspondendo a 85,2% do volume do negócio da Empresa.

Atua, também, no segmento das ações estruturadoras e integradoras da Administração Pública Federal, que é constituído pelo Ministério do Planejamento, Orçamento e Gestão; estende-se a outros órgãos governamentais que venham a constituir ações nesse segmento e que demandem serviços característicos da Empresa.

O Serpro presta serviços em rede que abrange todo o território nacional, tendo a seguinte estrutura de rede, como mostrado na Figura 1.

Figura 1: Estrutura de rede do Serpro
Fonte: www.serpro.gov.br

O Serpro é credenciado como Autoridade Certificadora (AC) da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil. Como AC, está habilitado para representar uma entidade responsável pela emissão, gerenciamento, renovação e revogação de certificação digital e apta a prover serviços de certificação digital para seus atuais clientes.

Com esse perfil e buscando maior credibilidade e competitividade, cercou seu Centro de Certificação Digital de segurança e conquistou, em dezembro de 2006, a certificação British Standart 7799, conhecida como BS7799, referência internacional no campo da segurança da informação, tornando-se a primeira empresa pública brasileira com tal certificação. Em fevereiro de 2007, obteve a certificação ISO 27001, a nova norma de segurança da

informação.

1.4.3 Estrutura institucional

A estrutura institucional do Serpro é orientada pelo Conselho Diretor, integrado por quatro membros indicados e designados pelo Ministro de Estado da Fazenda, entre eles o Presidente do Conselho, e um membro indicado pelo Ministro de Estado do Planejamento, Orçamento e Gestão. O Diretor-Presidente do Serpro substitui o Presidente do Conselho, em suas faltas e impedimentos eventuais.

Seguindo a hierarquia, há uma Diretoria composta por um Diretor-Presidente, um Diretor-Superintendente e quatro Diretores. Os membros da Diretoria são nomeados pelo Presidente da República, por indicação do Ministro de Estado da Fazenda, todos com mandato de quatro anos, permitida a recondução, por igual período. Pelo menos dois membros da Diretoria são escolhidos entre os empregados do Serpro.

Subordinadas à Diretoria estão as Unidades de Alinhamento Estratégico (UAE), a Consultoria Jurídica (COJUR), o Gabinete do Diretor-Presidente (GABDP) e as Superintendências. Os titulares dessas unidades compõem a diretoria colegiada. As UAE têm a responsabilidade de formular e controlar o cumprimento de políticas e apoiar a ação da diretoria. Os processos corporativos estratégicos, por unidades, são Planejamento, Orçamento e Controle, Projetos, Pessoas, Tecnologia da Informação, Mercados e Marketing, e Segurança da Informação.

Como o Serpro foi criado para atender prioritariamente ao Ministério da Fazenda, foram criadas unidades regionais nas dez regiões fiscais do País. Cada unidade tem atividades subordinadas aos segmentos da sede, relacionados a cliente, produtos e serviços e gestão empresarial.

A fim de retratar visualmente a estrutura institucional e hierárquica do Serpro, será apresentado o Diagrama Estrutural, contido na Norma: (Estrutura Orgânica do Serpro, 2006, Anexo 11, p.1) conforme a Figura 2.

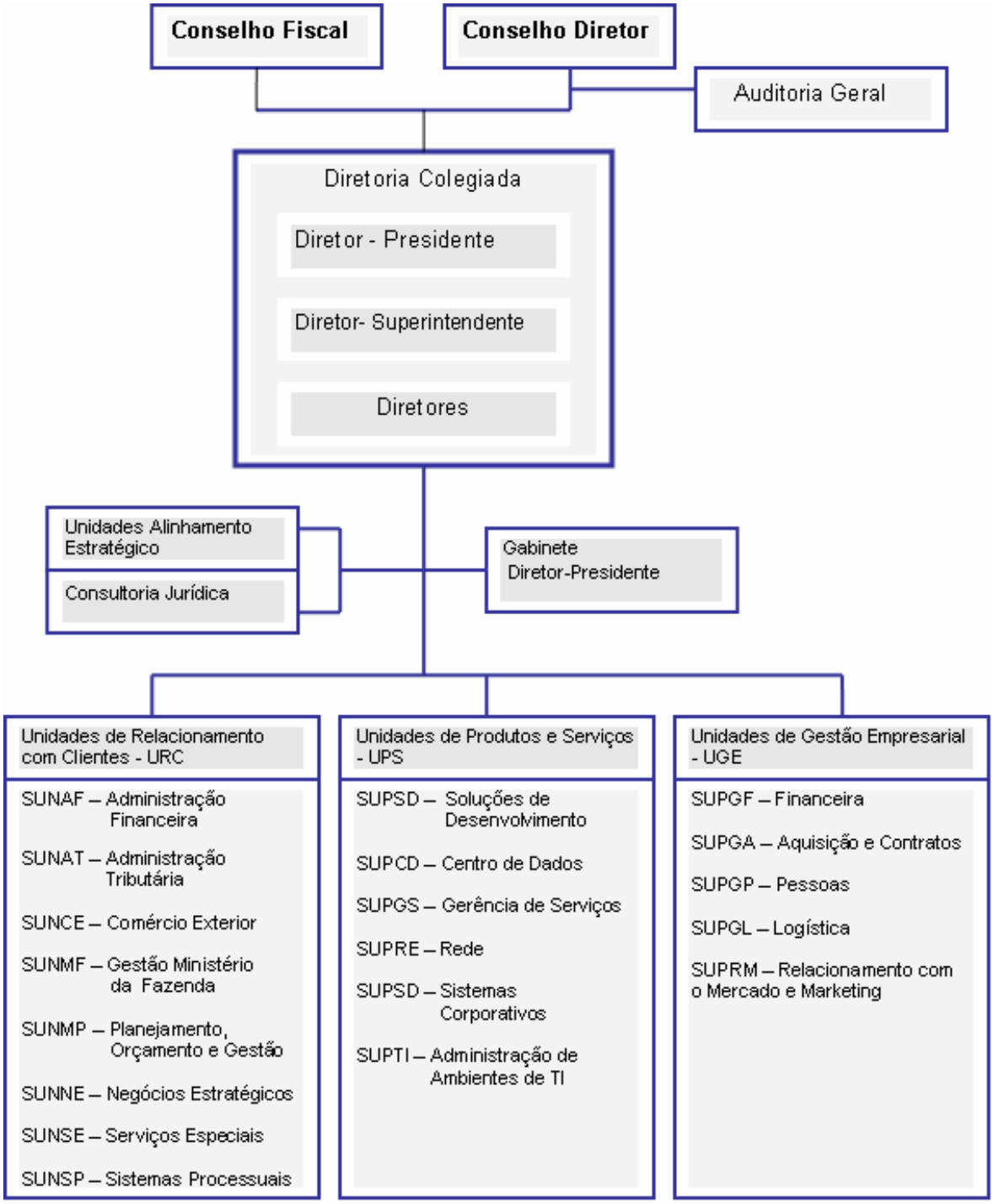


Figura 2 – Diagrama da estrutura do Serpro
Fonte: www.serpro.gov.br

1.4.4 Componentes estratégicos

Os componentes estratégicos do Serpro estão direcionados para atender à administração pública, como determina a lei de criação. Dessa forma, atualmente estão determinadas as seguintes declarações:

- Visão – ser líder em soluções de Tecnologia da Informação e Comunicações (TIC) para a realização das políticas públicas.
- Missão – prover e integrar soluções em Tecnologia da Informação e Comunicações para o êxito da gestão das finanças públicas e da governança do Estado, em benefício da sociedade.
- Premissas:
  - Conquistar o reconhecimento de clientes, Estado e sociedade;
  - Prestar serviços com pontualidade, inovação, qualidade e segurança;
  - Manter os empregados comprometidos e motivados;
  - Orientar a gestão para resultados, lucratividade e competitividade;
  - Empregar soluções inovadoras com tecnologia adequada;
  - Praticar gestão integrada e participativa;
  - Atuar com ética e responsabilidade social.
- Negócio – tecnologia da informação e comunicações;
- Produtos e serviços – Sistemas de Informação, Serviços de Tecnologia da Informação e Comunicações, Integração de Soluções, Consultoria e Informações;
- Força Motriz – capacidade de inovar e realizar;
- Fatores críticos – disponibilidade e utilidade, competitividade e domínio tecnológico;
- Valores – respeito às pessoas, responsabilidade social e cidadania, integridade profissional e pessoal, orgulho de trabalhar no Serpro, gosto por desafios, compromisso com resultados, confidencialidade das informações.

1.4.5 Principais linhas do negócio

- Desenvolvimento de Soluções – desenvolvimento de aplicações, desenvolvimento de plataforma livre, fábrica de *sites*; desenvolvimento web, metodologia de desenvolvimento de soluções;
- Serviços de centro de dados (Datacenter) – hospedagem de aplicações; hospedagem de servidores, armazenamento de dados, espelhamento de bases de dados, publicações Internet, gerenciamento e administração de aplicações, gerenciamento e administração de serviços;
- Rede multiserviços – redes virtuais privadas (VPN), redes corporativas, provimento de acesso corporativo Internet, interconexões de redes, convergência de dados, voz e vídeo, redes locais, gerenciamento integrado de redes, acesso remoto discado;
- Segurança – consultoria em gestão de segurança, definição de políticas de segurança, certificação digital, análise de vulnerabilidades, política de antivírus, pesquisa e investigação (análise forense computacional), grupo de resposta e ataques, auditoria de segurança;
- Integração / interoperabilidade - barramento de integração, Data Warehousing, sistemas de apoio à decisão, integração de processos, sistemas e dados, padrões para interoperabilidade, integração de diretórios, plataforma de pagamentos;
- Serviços ao cidadão - central de atendimento, caixa postal eletrônica do cidadão, ouvidoria, espaço Serpro Cidadão, ensino a distância.

1.5 Delimitação do estudo

Este estudo tomou como base de referência o modelo de gestão de segurança do Serpro, pelo fato de ser uma estrutura sedimentada como apoiadora dos processos de segurança com abrangência em todos os segmentos organizacionais.

1.5.1 Breve histórico sobre a institucionalização da segurança da informação

O modelo de segurança adotado pelo Serpro foi instituído em 1997. É composto por uma Política Corporativa de Segurança da Informação (PCSI) e pelo Programa de Segurança do Serpro (PSS). São revisados anualmente ou em situações especiais, diante de novos cenários de ameaças, leis, alterações contratuais, entre outros fatores condicionantes.

Em 2000, por meio do Decreto nº. 3.505, foi instituída a Política de Segurança da Informação para ser implantada em todos os órgãos da Administração Pública Federal. O decreto determina a criação de um Comitê Gestor da Segurança da Informação, com a responsabilidade de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.

O comitê é subordinado ao Chefe do Gabinete de Segurança Institucional da Presidência da República. Os membros, representantes de cada um dos ministérios, são indicados pelos respectivos ministros e designados pelo citado Chefe.

A partir do Decreto nº. 3.505, todos os órgãos vinculados à Administração Pública devem criar e implantar sua política de segurança. Destaca-se que o Serpro já havia instituído e implementado seu programa de segurança, com a obrigatoriedade de revisá-lo a cada dois anos, como recomenda a ABNT NBR ISO/IEC 17799:2005.

1.5.2 Modelo de segurança do Serpro

Foi delineado com base na ABNT NBR ISO/IEC 17799:2005 – Código de práticas para a gestão da segurança da informação e a BS 7799-2, norma que orienta a especificação para o sistema de gestão de segurança da informação, além de outras práticas de segurança assimiladas por meio de parcerias, investimento em conhecimentos especializados dos técnicos, contratação de consultoria e adaptação de práticas internacionais à realidade da Empresa.

A Política Corporativa de Segurança da Informação (PCSI) é o instrumento direcionador das ações de segurança que devem ser adotadas em cada uma das Unidades do Serpro, observando as peculiaridades de cada área de conhecimento. O documento abrange a definição de segurança, metas, missão, escopo, princípios de segurança, objetivos e controles sobre avaliação e gerenciamento de riscos, campanhas de conscientização, gestão de continuidade do negócio e definição de responsabilidades.
O documento que institui a Política é assinado pelo Diretor-Presidente (DP) e disseminado, por meio de campanhas, no âmbito da Empresa. O gestor do processo é a Unidade de Alinhamento Estratégico Segurança da Informação, subordinado ao Diretor-presidente.

1.5.2.1 O Programa de Segurança do Serpro (PSS)

O PSS visa atender à Política Corporativa de Segurança da Informação. Fornece subsídios e orientações de segurança aos demais processos e programas corporativos, de forma a buscar permanentemente o alinhamento desses processos às necessidades de segurança do negócio da Empresa. Incorporam os fundamentos do PSS os seguintes processos corporativos:

- Programa Serpro de Melhoria do Processo de Desenvolvimento de Soluções (PSMPDS);
- Programa Serpro de Gerenciamento de Projetos (PSGP);
- Programa Serpro de Gerenciamento de Serviços de Tecnologia da Informação e Comunicação (PSGTI).

O PSS é um instrumento formal e disseminado no âmbito da Empresa. Para atender às necessidades de segurança, aborda as questões de processo, tecnologia e pessoas, tendo como objetivos:

- definir e estruturar o relacionamento entre as diversas unidades, visando ao gerenciamento de segurança no Serpro.

- assegurar o negócio da Empresa nos aspectos da integridade, disponibilidade e confidencialidade da informação, por meio de um conjunto estruturado de diretrizes e controles de segurança.

É orientador das ações de segurança, cabendo a cada uma das unidades da Empresa a responsabilidade pela segurança em sua área de atuação. As principais atividades do PSS que agregam valores à organização e a seu negócio são abordadas nos seguintes temas de segurança, conforme Quadro 1.

Quadro 1 – Temas de segurança abordados no PSS

Cultura de segurança	Considera o elemento humano o mais importante fator de segurança. O modelo busca tornar a segurança um valor e o meio de viabilizá-lo é criar as condições, englobando os temas conscientização, treinamento, educação e certificação
Classificação da informação	Tem o objetivo de assegurar que a informação receba um nível adequado de proteção. O tema foi institucionalizado em 2004, por meio de uma norma específica, baseada no Decreto nº. 4.553, de 27 de dezembro de 2002
Controle de acesso	Considera-se o primeiro nível de proteção da informação. A orientação institucional baseia-se em requisitos do negócio e de segurança, observando regras de autorização, identificação e autenticação, mantendo controle para fins de contabilização e auditoria
Gestão de incidentes	Trata da resposta rápida para incidentes de segurança, permitindo ações corretivas em tempo hábil, visando minimizar o impacto no negócio
Segurança física	Abrange a proteção física e controle dos locais onde residem os ativos, áreas, prédios e instalações, buscando coibir perdas e danos, furto ou comprometimento dos ativos, interrupção dos serviços e acessos físicos não- autorizados
Gestão de riscos	Processo sistematizado de análise e tratamento de risco por meio de controles adequados à complexidade e necessidade do risco, considerando as ameaças, vulnerabilidades e impacto no negócio
Gestão de continuidade do negócio	Visa assegurar que os processos e serviços de missão crítica possam ser mantidos após falha ou interrupção significativa, em processo normal, antes que as perdas se tornem inaceitáveis
Gestão da forense computacional	Orienta sobre as regras e procedimentos que devem ser adotados para a preservação, restauração e análise das evidências em ambiente de tecnologia da informação e comunicação, a fim de fundamentar legalmente a investigação, por meio de provas digitais, se o incidente foi ou não delito
Acompanhamento da segurança	Visa manter as unidades organizacionais sobre a segurança em seu âmbito de atuação, quanto à qualidade da segurança, indicadores e auditoria

Fonte: Programa de Segurança do Serpro (PSS) v. 5 /2005

1.5.3 Modelo de funcionamento da segurança do Serpro

O modelo de funcionamento da segurança da informação no Serpro estabelece um relacionamento com todos os segmentos organizacionais, formalizado por meio de representante no comitê de segurança (um titular e outro suplente) devidamente designado pelo período de um ano, podendo ser renovado. O papel de cada representante é gerir as ações de segurança no âmbito de atuação, inclusive interagindo com as representações regionais.

O comitê atua como grupo consultivo, apoiando as decisões e as ações de segurança, tanto no nível estratégico quanto no tático-operacional. Existem ainda os grupos de segurança regional, vinculados ao comitê de segurança. Sua responsabilidade é interagir, orientar e apoiar internamente as questões de segurança, repassando as boas práticas e solicitando apoio para as dificuldades. Neste mesmo segmento, existem os grupos de continuidade e contingência em unidades que possuem centro de dados.

O modelo de relacionamento, de acordo com o PSS (2005, p.9) apresenta uma estrutura simplificada, conforme mostrado na Figura 3.

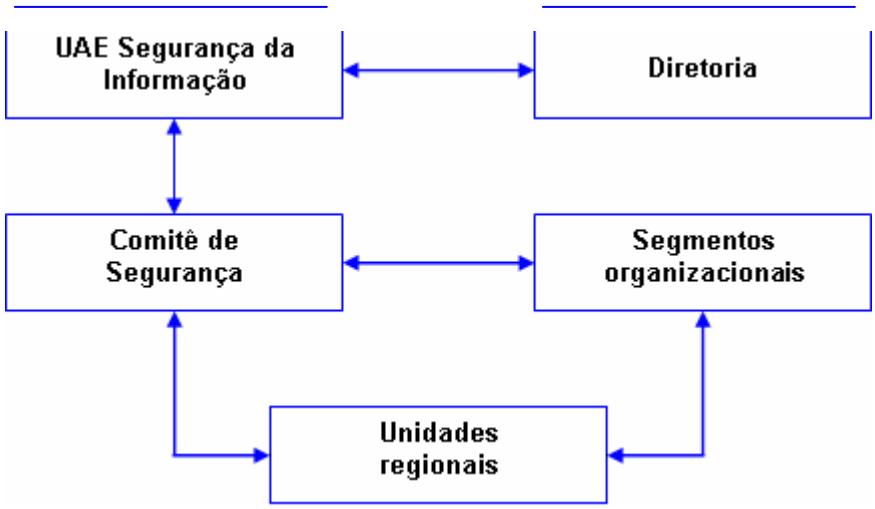


Figura 3 – Relacionamento interáreas da segurança da informação no Serpro
Fonte: Programa de Segurança do Serpro (2005, p. 9)

1.5.4 Modelo de gestão de riscos da segurança do Serpro

A política de segurança do Serpro também abrange a Gestão de Riscos. Trata-se de um processo sistematizado de análise e tratamento dos riscos de segurança, por meio da adoção de controles que, de acordo com o risco, são implementados para proteger a informação de danos que possam ser causados por falhas de segurança.

Nesse processo são consideradas as ameaças, as vulnerabilidades e impactos que podem afetar os recursos, a probabilidade dessas ocorrências, a viabilidade da adoção dos controles necessários à aceitação dos riscos.

De acordo com a ABNT NBR ISO/IEC 17799:2005, o conceito de risco é "combinação da probabilidade de um evento e sua conseqüência". O PSS conceitua o risco numa dimensão mais abrangente, como a probabilidade de que ameaças explorem vulnerabilidades dos ativos, gerando impacto e perdas nos negócios. Representa o risco com a seguinte expressão:

Risco = Ameaça x Vulnerabilidade x Impacto

Onde:

- Ameaça é o que tem potencial para causar perda ou dano;
- Vulnerabilidade é uma fraqueza que pode ser explorada;
- Impacto é o resultado negativo da exploração de uma vulnerabilidade.

A Empresa considera que a gestão de riscos apresenta benefícios à organização pois aumenta a conscientização, à medida que os riscos são discutidos em vários segmentos; permite a identificação dos recursos envolvidos, ameaças e medidas existentes; estabelece uma base de referência para auxiliar nas decisões de controle; justifica o investimento em segurança.

O modelo implementado no Serpro inclui as seguintes etapas:

- Avaliação de riscos: inclui a análise e a valoração dos riscos. Nessa fase há a identificação dos ativos e dos riscos e sua significância em relação ao negócio;

- Tratamento dos riscos: refere-se a riscos não-aceitáveis, define a seleção e a implementação das medidas de controle;
- Aceitação dos riscos: identifica os riscos que não podem ser tratados, riscos residuais e riscos assumidos como baixos para o negócio da empresa;
- Comunicação dos riscos: é feita às partes envolvidas e interessadas.

1.5.5 Modelo de gestão de continuidade do negócio do Serpro

Na seqüência das boas práticas recomendadas para empresas complexas, de alta tecnologia e que trata de sistemas sensíveis, o item Gestão de Continuidade do Negócio (GCN) é considerado outro pilar da gestão da segurança da informação, no âmbito da Empresa.

A GCN, no Serpro, está incorporada à estrutura de segurança e alinhada aos procedimentos de tratamento de riscos, controles para limitar os danos e garantir a recuperação tempestiva dos serviços críticos.

A recomendação principal é de que os planos de contingência devem ser atualizados, documentados, testados e conhecidos pelos envolvidos. Com estas características de gestão, a continuidade do negócio foca nas seguintes especialidades:

- plano de continuidade operacional: busca manter em operação os processos e serviços fundamentais;
- plano de recuperação de desastre: objetiva recuperar os ativos;
- plano de contenção de incidente: visa responder em tempo hábil a um determinado incidente;
- plano de retorno a normalidade: atende ao retorno à operação normal, após operação alternativa;
- plano de gerenciamento da continuidade: consiste em gerenciar as ações de continuidade a fim de evitar falhas no processo.

Os processos de gestão de riscos e de continuidade do negócio são estruturados e orientados por meio de instrumentos normativos corporativos. A disseminação do conhecimento e da cultura das práticas é feita mediante treinamento, cabendo aos membros do Comitê de Segurança o exercício do uso continuado.

2. REFERENCIAL TEÓRICO

Este capítulo trata dos tipos de governança: corporativa, de tecnologia da informação e de segurança da informação, temas que têm sido desenvolvidos no âmbito global, como um sistema para dirigir as organizações a fim de que os resultados obtidos sejam responsabilidade de todos os interessados. Adicionalmente, é feita uma abordagem sobre a segurança da informação, visando dar mais subsídio ao tema governança da segurança da informação, referencial desta pesquisa.

2.1 A governança corporativa

2.1.1 Conceitos

Segundo Háfez (2005, p.1), a expressão governança corporativa vem do inglês corporate governance. “É definida como um feixe de princípios, um sistema que viabiliza o monitoramento da gestão de empresas. Esses princípios dizem respeito à transparência, à equidade, à accountability, aqui traduzido como responsabilidade, e à compliance – obediência à lei”.

Para o IBGC (2003, p.6) a “Governança Corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas/quotistas, conselho de administração, diretoria, auditoria independente e conselho fiscal”. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para sua perenidade (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2003, p. 6).

O Governo brasileiro instituiu a Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, por meio do Decreto nº. 6.021, em 22 de janeiro de 2007, com a finalidade de tratar de matérias

relacionadas com a governança corporativa nas empresas estatais federais e da administração de participações societárias da União.

O referido decreto conceitua Governança Corporativa como o “conjunto de práticas de gestão, envolvendo, entre outros, os relacionamentos entre acionistas ou quotistas, conselhos de administração e fiscal, ou órgãos com funções equivalentes, diretoria e auditoria independente, com a finalidade de otimizar o desempenho da empresa e proteger os direitos de todas as partes interessadas, com transparência e eqüidade, com vistas a maximizar os resultados econômico-sociais da atuação das empresas estatais federais”.

De acordo com a ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, o conceito de governança foi desenvolvido em 1998 e teve a colaboração dos governos dos países-membros, outros organismos internacionais e o setor privado. Aborda o tema como sendo um conjunto de relações entre a administração de uma empresa, seu conselho de administração, seus acionistas e outras partes interessadas, proporcionando a estrutura que define os objetivos da empresa, como atingi-los e a fiscalização do desempenho. (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD, 2004, p.11-17).

2.1.2 Objetivo da governança corporativa

Segundo a OECD, o objetivo da governança corporativa é o desenvolvimento de uma estrutura para suportar os padrões que facultem a transparência e eficiência no mercado, seja consistente com seu papel e com as leis e claramente articulado na divisão de responsabilidades entre os diferentes níveis (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2004, p. 11-17).

Para Rabelo e Silveira (1999, p. 2), a governança corporativa é o sistema por meio do qual se exerce e se monitora o controle nas corporações. Está claro, desde logo, que esse sistema está intimamente vinculado à estrutura de propriedade, às características do sistema financeiro, à densidade e profundidade dos mercados de capitais e ao arcabouço legal de cada economia.

De acordo com Steinberg (2003, p. 28) a governança corporativa tem o "objetivo de dar bases para as decisões de investimentos dos administradores de recursos". Sugere Steinberg (2003, p.29-33) que a governança corporativa teve evolução maior a partir de 2002, motivada pelos casos das empresas americanas Enron Corporation, empresa de energia elétrica, e WorldCom, empresa de telefonia, no Brasil controladora da Embratel, "que apresentavam balanços fraudados para elevar a cotação das ações". Na trajetória dos fatos, na edição do Fórum Econômico Mundial, no mesmo ano, em Nova York, foi lançada uma declaração "cidadania corporativa global: o desafio de liderança para CEO (CHIEF EXECUTIVE OFFICER) e conselhos" com o objetivo de mostrar que a responsabilidade social e o desenvolvimento sustentável não apenas agregam valor, mas são essenciais ao cerne do negócio.

2.1.3 O futuro da governança corporativa

Heskett (2001, p.1-3) apresenta um questionamento sobre o futuro da Governança Corporativa: "no futuro poderá refletir um crescimento na ênfase a satisfação do cliente como um meio de medir a adaptabilidade da organização o tempo todo". Observa-se que, atualmente, a GC foca fortemente nos recursos financeiros, no comitê de auditoria, esquecendo-se de privilegiar de fato os recursos humanos que são os mais importantes componentes do fator de sucesso.

Shann Turnbull (*apud* HESKETT 2001, p. 1-3) sugere que o mundo da Governança Corporativa irá beneficiar-se do estabelecimento de "novos tipos de informações empresariais e arquitetura de controles". De fato, estão indo além do propósito de uma rede de grupos de administradores mais especializados e conselhos consultivos de patrocinadores constituídos de empregados. Outras ofertas de soluções úteis surgem para preencher o vácuo que existe na maioria das organizações de hoje.

Pesquisa realizada pela consultoria especialista em soluções para grandes empresas ou corporações, *Mckinsey & Company*, (*apud* WILL e ROSS 2004, p. 4-5) constatou que investidores profissionais se dispõem a pagar um ágio para investir em empresas que tenham altos padrões de governança. De certa forma, a pesquisa corrobora a percepção de

Shann Turnbull (*apud* HESKETT 2001, p.1-3), quanto ao beneficio de informações empresariais confiáveis e controles eficientes.

De acordo com as orientações da ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD, 2004, p.19-25), a governança corporativa é parte de um longo contexto econômico, no qual as firmas operam e incluem políticas macroeconômicas, aprofundam a competição de produtos e fator de mercado, e dependem de lei, regulamentação e ambiente institucional. Adicionalmente, fatores como ética do negócio, comportamento corporativo do ambiente e interesses sociais das comunidades nas quais a companhia opera também têm impacto na reputação e sucesso a longo prazo. Os princípios da governança corporativa, segundo a OECD, são os seguintes:

- garantir as bases para uma efetiva estrutura de GC;
- proteger e facilitar o exercício dos colaboradores certos (proprietários, clientes, fornecedores, empregados, entre outros);
- tratar com eqüidade os colaboradores e a sociedade em geral;
- estabelecer regras para colaboradores;
- apresentar publicidade e transparência organizacional.

No Brasil, o Código de Modelos e Práticas de Governança Corporativa do IBGC, adequado à legislação brasileira em 2001 e 2003, fundamenta-se nos seguintes princípios básicos:

- Transparência: obrigação de informar;
- Eqüidade: tratamento justo e igualitário entre todas as partes interessadas;
- Prestação de contas: os agentes devem prestar contas de seus atos, respondendo integralmente por eles;
- Responsabilidade Corporativa: destinada aos conselheiros e executivos que se comprometem a zelar pela perenidade das organizações, pela visão de longo prazo e pela sustentabilidade.

Ainda no contexto do futuro da governança corporativa, uma pesquisa conduzida pela Economist Intelligence Unit, da revista inglesa The Economist, em 2002, com 150

empresários no mundo inteiro, por meio da Internet, indicou que a GC está entre as três principais preocupações para 46% dos entrevistados e prioridade absoluta para 14% das organizações. Outros 36% alegaram que o poder de tomar decisões rápidas e eficientes fica comprometido (STEINBERG, 2003, p.32).

O INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA inseriu, em 2007, um Guia de Orientação para Gerenciamento de Riscos Corporativos (versão preliminar), cumprindo recomendação do Código de Modelos e Práticas de Governança Corporativa, em 2003, que orientava: "o conselho de administração deve assegurar-se de que a diretoria identifique preventivamente, por meio de sistema de informações adequado, e liste os principais riscos aos quais a sociedade está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização".

É importante refletir que a governança é uma prática que se amplia em segmentos da economia como o da tecnologia da informação (TI). Segundo Weill e Ross (2006, p. 8-9), a cultura de governança corporativa e uma boa governança financeira ajudam na especificação dos direitos decisórios e da estrutura de responsabilidades para estimular comportamentos desejáveis na utilização de TI.

A tendência indica que o modelo de governança que determina os objetivos organizacionais, que monitora o desempenho para assegurar a concretização dos objetivos, que agrega os valores das crenças e da cultura da organização para garantir comportamentos desejáveis e que protege os interesses dos patrocinadores, empregados e clientes para manter a sustentabilidade é uma prática a ser adaptada a outros segmentos (WEILL e ROSS, 2006, p. 4).

Heskett (2001, p.1-3) acredita que a governança corporativa promete ser mais efetiva que outros modelos de gestão e seu diferencial é a ênfase na satisfação do cliente e a rápida adaptação a outros times, focando fortemente no retorno financeiro e principalmente na satisfação do empregado, que são os responsáveis pelo sucesso da companhia.

2.2 A convergência para a governança da tecnologia da informação

As aplicações das tecnologias da informação e de comunicação têm um papel fundamental na convergência das diversas tecnologias. Além das tecnologias de rede de longa distância, como a Internet, existem as emergentes, como as redes ubíquas, que permitem acompanhar as pessoas e os objetos e proceder a um rastreamento, armazenamento e processamento em tempo real da informação. Há as tecnologias de prevenção e aviso de catástrofe (avisam ou prevêem tsunâmis, por exemplo). Também há aplicação da tecnologia na área da saúde, da educação, da biotecnologia. Essa convergência tem fornecido mais oportunidades e impactos econômico-sociais e tem fomentado o questionamento sobre a necessidade de melhoria das políticas de gestão, tanto em nível de Estado quanto das organizações. (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD, 2006, p.5-6).

Nas empresas é cada vez mais premente o uso da tecnologia para dar velocidade a novas funcionalidades do negócio, ter disponibilidade de infra-estrutura 24 horas do dia, todos os dias do ano, com mais benefícios para os clientes, menor risco e maior retorno. Essa caminhada requer alinhamento estratégico e gestão competente dos recursos de TI, considerando seu valor estratégico para os resultados da organização (CARR, 2003, p. 1).

Para o INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2003, p.7), a tecnologia da informação tem-se tornado essencial para sustentar a economia e as atividades sociais, é parte integrante dos negócios e é fundamental para suportar, manter e participar do crescimento das organizações. Contudo, segundo o Instituto, sem conhecer os riscos não poderá haver direcionamento estratégico. Assim, a alta direção deve conhecer a importância estratégica de TI, avaliar os riscos e definir um modelo de gestão adequado a seu negócio.

O pressuposto é que o uso da tecnologia não é suficiente para garantir o sucesso do negócio. Existe a necessidade de adotar controles e promover a gestão do uso de Tecnologia da Informação (TI) no negócio. Então, qual modelo deve ser adotado? A gestão é focada no efetivo suprimento, nos serviços, operações e produtos de TI, enquanto a governança é estratégica, concentrada no desempenho e transformação de TI, conhecendo

o presente e as demandas do negócio futuro e do negócio do cliente (INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE, 2003, p. 14-15). Enfim, como sugere o ITGI, o modelo a ser implementado na organização deve ser coerente com a estratégia de TI para o negócio, crescimento e inovação e principalmente o risco do negócio.

2.2.1 Conceitos de governança da tecnologia da informação

De acordo com o INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2003, p. 10) a "Governança de Tecnologia da Informação é responsabilidade da alta administração e da gerência executiva. É parte integrante da governança da empresa e consiste em que a liderança, a estrutura organizacional e os processos garantam que a organização de TIC sustente e aumente as estratégias e objetivos da organização".

Adicionalmente, o ITGI (2003, p.11) recomenda que a Governança de TI disponha de uma estrutura alinhada ao cenário estratégico da empresa, à importância da entrega de produto, à gestão de risco, à gestão de recursos financeiros e à medição do desempenho.

Fernandes e Abreu (2006, p. 7-12) formulam o conceito de Governança de TI a partir dos conceitos do INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2003, p.10) e de Weill e Ross (2006, p.4), concluindo que a "Governança de TI busca o compartilhamento de TI com os demais dirigentes da organização, assim como estabelece as regras, a organização e os processos que nortearão o uso da tecnologia da informação pelos usuários, departamentos, divisões, negócios da organização, fornecedores e clientes, e também determinarão como TI deverá prover os serviços da empresa". No entanto, adverte: a "Governança de TI não é somente a implantação de modelos de melhores práticas ou estruturas de COBIT, ITIL, CMMI". A implementação de um modelo de governança é motivada por fatores que interferem no desenho a deve ser adotado, conforme mostrado na Figura 4.

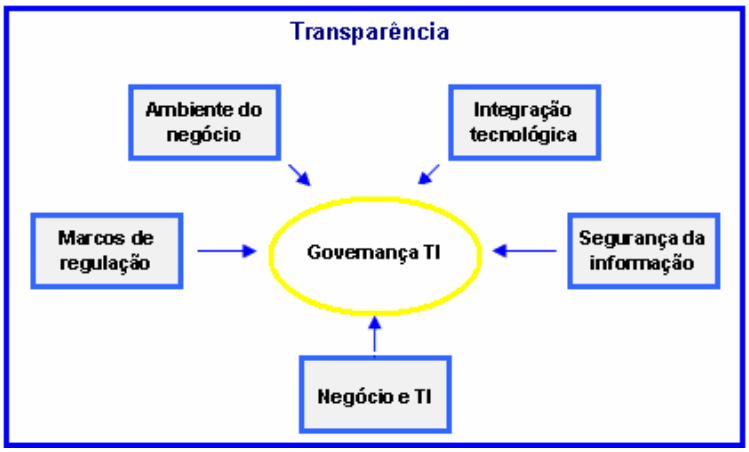


Figura 4: Fatores motivadores da governança da Tecnologia da Informação
Fonte: adaptado de Fernandes e Abreu (2006, p.7)

Cada fator tem a seguinte significância para a governança de tecnologia da informação:

- Transparência da administração: exigência de maior transparência nos negócios;
- Ambiente do negócio: ciclo de vida cada vez mais curto para os produtos e serviços, novos concorrentes globais e de baixo custo;
- Integração tecnológica: integração de redes de distribuição de aplicativos e de infra-estrutura de comunicação de dados;
- Segurança da informação: diante uso global da Internet, a gestão da tecnologia da informação (TI) ficou mais complexa e os riscos diários de intrusão e ataques de códigos maliciosos afetam o desempenho da infra-estrutura de TI;
- Dependência do negócio em relação a TI: as operações diárias e as estratégias chaves dependem cada vez mais de tecnologia, significando que essa equação põe TI em posição estratégica para o negócio;
- Marcos da regulação (conformidade): representam restrições ao negócio; entretanto, devem ser seguidos uma vez que consideram a capacidade de atração de capital de risco e geração de lucro.

Na mesma linha de percepção, Haes e Grembergen (2005, p.1) entendem que a Governança de TI é a capacidade organizacional exercida pela direção, gestores executivos e gestores de TI para controlar, formular e implementar estratégias de TI a fim de garantir a fusão do negócio à TI. E complementa – “a governança de tecnologia da informação deve ser integrada à governança da empresa e deve permitir que a liderança, a estrutura organizacional e os processos que garantem à organização a sustentação de TI sejam

estendidos aos objetivos estratégicos da organização".

Ribbeers, Peterson e Parker (2002, p.1-2) partem da premissa de que a governança de TI é um recurso para garantir o desenvolvimento de estratégias flexíveis para sustentar vantagens estratégicas da organização. Complementam, dizendo que existe uma necessidade de gerir com mais assertiva e menos desperdício de recursos de Tecnologia da Informação e Comunicação. Neste caso, a orientação é que a infra-estrutura de TI seja integrada à estrutura do negócio da organização, pois as falhas, quando ocorrem, têm impacto sobre todos os setores. Argumentam que o modelo tradicional de tomada de decisão sustenta-se no processo do ciclo interativo de "identificação de problema e solução de problema", o que não atende mais às exigências dos patrocinadores, clientes, emprega-dos e mercado.

De acordo com Weill e Woodham (2002, p.1-2), a governança de TI especifica a decisão certa sobre a responsabilidade de uma estrutura para encorajar o comportamento desejável da firma para o uso de TI. Significa, ainda, que outros recursos são inseridos para a completeza do modelo, citando os recursos financeiros, recursos humanos e também a necessidade de focar os investimentos direcionados para os objetivos da firma.

2.2.2 Objetivos e importância da governança da tecnologia da informação

A governança de TI tem o objetivo de direcionar TI na organização, estabelecendo os controles e indicadores num ciclo contínuo a fim de medir o desempenho, comparando os objetivos e redirecionando as atividades quando necessário para atender aos objetivos ou mudanças de objetivos (INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE, 2003, p. 11).

A governança de TI responde por quatro objetivos importantes para o negócio da organização, segundo Weill e Ross (2004, p. 2):

- custo efetivo do uso de TI;
- efetiva vantagem na utilização de TI;

- participação de TI no crescimento da organização;
- flexibilização dos negócios pelo uso de TI.

Esses objetivos devem ser controlados e os resultados devem ser avaliados, considerando inclusive comparações com o resultado de outras empresas.

Para Weill e Woodham (2002, p.2-3), a importância da governança de TI na empresa está associada ao fomento da cuidadosa análise sobre como tomar decisão em quatro áreas de domínio, que são interligadas; portanto, não podem ser tratadas isoladamente. As áreas são as seguintes:

- Princípios: estabelecer como TI será utilizada e o direcionamento da empresa para o futuro;
- Infra-estrutura: estabelecer as orientações sobre o compartilhamento e padrões de TI quanto a rede, capacitação da infra-estrutura, estação de trabalho, gestão de relacionamento com o cliente, compartilhamento dos dados de clientes, entre outros;
- Arquitetura: prover a integração dos vários níveis de escolha de tecnologia para guiar a organização nas necessidades de seus negócios;
- Priorização: disponibilizar informações que orientem todo o processo da tomada de decisão sobre o processo de investimento em TI.

Na mesma linha de percepção posicionam-se Fernandes e Abreu (2006, p.13) – o "principal objetivo da Governança de TI é alinhar TI aos requisitos do negócio. Esse alinhamento tem como base de sustentação a continuidade do negócio, o atendimento as estratégias do negócio e as tendências externas".

Observa-se que há uma tendência em manter a mesma percepção sobre conceitos e objetivos da governança de TI: ITGI (2003, p.14-15), Weill e Ross (2006, p.15- 19), Weill e Woodham (2002, p.2-3), Fernandes e Abreu, (2006, p.4-5), Haes e Grembergen (2005, p.1), corroboram a recomendação de que os investimentos em tecnologia da informação sejam direcionados aos objetivos dos negócios essenciais e que gerem benefícios, considerando que as empresas que têm governança como modelo de gestão são mais valorizadas no mercado. A governança de TI que for alinhada continuamente a comportamentos que permitam transformar TI de um passivo estratégico para uma

vantagem estratégica irá consolidar processos que garantam decisões eficazes na área de TI e no fortalecimento da tomada de decisão, com maior vantagem competitiva.

2.2.3 Modelos de governança da tecnologia da informação

Pesquisa realizada por Peterson, Van Grembergen, De Haes e Guldentops, Weill e Wooddham (Haes e Van Grembergen, 2005, p.2) sobre como pragmaticamente as organizações poderiam implementar um modelo de governança de TI apresentou o resultado de que esse modelo pode ser desenvolvido, usando um *mix* de estruturas, processos e mecanismos de relacionamento, de acordo com:

- Estrutura – regras e responsabilidades, estrutura organizacional, comitê estratégico de TI e comitê operacional;
- Processo – plano estratégico de sistemas de informação, Balanced Scorecards; aprofundamento de nível de serviço, COBIT e ITIL; TI alinhado ao modelo de maturidade de governança;
- Mecanismos de relacionamento – participação ativa e colaboração entre os principais patrocinadores, clientes para decidir sobre recompensas e incentivos, novos negócios e TI, treinamento e rotação.

Segundo Weill e Woodham (2002, p.2-3), cada empresa deve ter um modelo de governança de TI que melhor atenda a sua necessidade. Para ilustrar, cita o exemplo do serviço bancário que oferece acesso à Internet Banking 24 horas por sete, e isto cria muita brecha eletrônica. Para esse caso, a tecnologia deve promover a segurança requerida pelo cliente. E acrescenta: o princípio da governança de TI é dispor de:

- infra-estrutura estratégica de TI: para garantir uma estrutura de TI alinhada à especificidade do negócio;
- arquitetura de TI: para fornecer a integração, em vários níveis, de forma a permitir o processo de gestão compatível com o negócio e a alta tecnologia;
- priorização nos investimentos de TI: para justificar a necessidade e prioridade de investimento e o desejo de retorno do investimento.

Segundo o INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2005, p. 6), o eixo global gira em torno de questões de governança com vários níveis de relacionamento. O gestor necessita saber se TI é capaz de garantir os objetivos; é suficientemente flexível para aprender e adaptar; existe prudente gestão de risco; há apropriado reconhecimento das oportunidades e ações tomadas. Adicionalmente, as empresas bem sucedidas entendem o risco e exploração de benefícios de TI como um meio para:

- alinhar TI às estratégias da empresa;
- promover uma estrutura organizacional que facilite a implementação de estratégias e regras;
- criar um relacionamento e uma comunicação efetiva entre o negócio e TI, e com os padrões externos;
- insistir que a estrutura de controle de TI seja adotada e implementada;
- medir a *performance* de TI.

Seguindo recomendações da INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2003, p.11-12), a definição de um framework para garantir um processo de Governança de TI deve começar pelos objetivos da empresa em relação a TI e a partir daí estabelecer uma freqüência de revisão a fim de medir a *performance*, comparando com os objetivos e o resultado. De acordo com o resultado, recomenda redirecionar as atividades onde for necessário e alterar os objetivos onde for apropriado. Seguindo a recomendação, o ITGI sugere a estrutura apresentada na Figura 5.

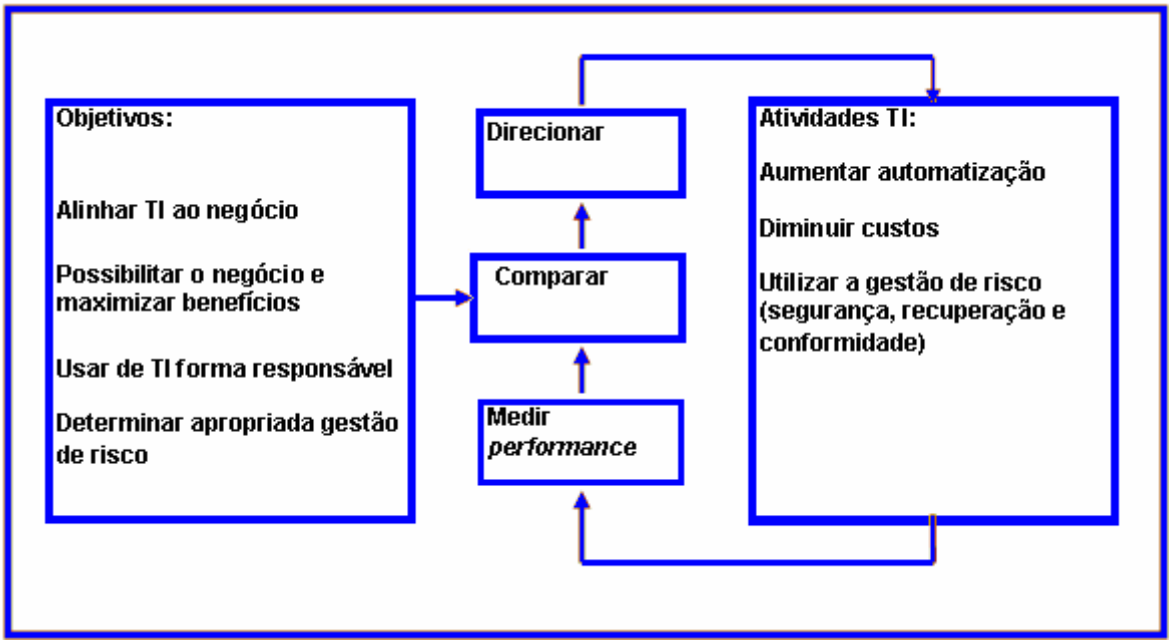


Figura 5 – Estrutura de Governança da Tecnologia da Informação
Fonte: INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE, 2003, p.12.

Ainda no contexto das recomendações do INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2003, p.19-20), a governança de TI deve ser concentrada em dois pontos: entrega do valor do negócio e mitigação de riscos de TI. O primeiro é orientado por uma estratégia de alinhamento de TI como o negócio; o segundo é direcionado à responsabilidade da empresa. Ambos necessitam ser suportados por recursos adequados e ciclos de medição para garantir os resultados a serem obtidos. Cada empresa opera num ambiente em que é influenciado por:

- Valores dos colaboradores;
- Missão, visão e valores da empresa;
- Aplicabilidade das leis, regulamentos e políticas;
- Práticas industriais.

Na percepção de Weill e Ross (2006, p. 5-6) sobre a escolha de uma estrutura, esta deve associar as governanças corporativas e de TI, verificando ou identificando a clientela-alvo, as ofertas de produtos e serviços, a posição almejada pela empresa e os processos centrais que incorporam a posição de mercado única na empresa. Adicionalmente, explicita que os comportamentos desejáveis incorporam as crenças e a cultura da organização, definidas e praticadas não somente mediante estratégias, mas também por meio de declaração de valor corporativo, missões institucionais, princípios do negócio, rituais e estruturas. “São os comportamentos desejáveis que geram valor”.

Segundo Fernandes e Abreu (2006, p. 168-170), tem surgido uma série de modelos de me-

lhores práticas para a gestão de TI. Alguns modelos são originais e outros são derivados ou evoluídos de outros modelos. Os principais modelos são os apresentados no Quadro 2.

Quadro 2 – Modelos de Melhores Práticas de TI

Modelos de Melhores Práticas de TI	Escopo do modelo
COBIT – *Control Objectives for Information and Related Technology*	Aplicável para a auditoria e controle de processos de TI.
CMMI – *Capability Maturity Model Integration*	Aplicável em desenvolvimento de produtos e sistemas
ITIL – *Information Technology Infrastructure Library*	Aplicável em serviços de TI, segurança, gerenciamento da infra-estrutura, gestão de ativos e aplicativos
ISO 27001:2006,ISO 17799:2005, Códigos de prática para a gestão da segurança da informação	Aplicável à segurança da informação
Modelos ISO – *International organization for Standardization*	Sistemas de qualidade, ciclo de vida de sistema e testes de sistemas
SCM-SP – *Service Provider Capability Maturity Model*	*Outsourcing* em serviços que usam TI de forma intensa
PRINCE2 – *Project in Controlled Environment*	Metodologia de gerenciamento de projeto
PMBOK – *Project Management Body of Knowledge*	Base de conhecimento em gestão de projeto
BSC – *Balanced Scorecard*	Metodologia de planejamento e gestão da estratégia
Seis Sigma (Six Sigma)	Metodologia para melhoria de qualidade de processos
SAS 70 – *Statement on Auditing Standards for Services Organizations*	Regras de auditoria para empresas de serviços

Fonte: Fernandes e Abreu (2006, p.168-169)

Enfim, a implementação de modelos de melhores práticas tem a finalidade de auxiliar na implantação da governança de TI, devendo ser observado que não é um modelo fechado à estrutura e cultura da organização. Há necessidade de ser adaptado e, como sugerem Peterson, Van Grembergen, De Haes e Guldentops, Weill e Wooddham (HAES E VAN GREMBERGEN, 2005, p.2), as organizações poderiam implementar um modelo de governança de TI, usando um *mix* de estruturas, processos e mecanismos de relacionamento.

2.3 A convergência para a governança da segurança da informação

De acordo com o Gartner (G00136867, 2006, p.1), as grandes empresas estão percebendo a segurança da informação como um segmento estratégico e faz a seguinte previsão: até 2008, 80% das empresas terão implementado um processo de segurança da informação e até 2011, 30% dessas empresas terão migrado para um modelo onde a arquitetura tenha uma estrutura que enxergue a organização de forma integrada em sua necessidade de segurança, envolvendo a alta direção.

Para Eloff e Solms (2000, p.243), as empresas dependem de tecnologia da informação para serem competitivas, cumprirem sua missão, mas também necessitam de uma estrutura de segurança para garantir sua competitividade no mundo de ameaças globalizadas. Sugerem algumas práticas internacionais, adaptadas à organização, controles e pessoal treinado como sendo o caminho para uma governança da segurança da informação.

O INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI, 2006, p. 36) recomenda a governança da segurança da informação para as empresas de tecnologia porque é um modelo que estabelece procedimentos para analisar o risco, definir os controles necessários no contexto da segurança da informação com o apoio e envolvimento da alta direção e gestão da alta gerência.

O NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-53, 2006, p. 2) recomenda a governança da segurança da informação, considerando sua finalidade de estabelecer e manter uma estrutura de segurança para garantir que a segurança da informação esteja alinhada com os objetivos estratégicos da organização, em conformidade com a aplicação da lei e regulamentos, atribuindo responsabilidades à resposta aos riscos.

2.3.1 Conceitos de governança da segurança da informação

De acordo com o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 2006, p.11), a governança da segurança da informação é um modelo de gestão da segurança da informação, onde as regras têm direcionamento estratégico para garantir os objetivos da organização. Os riscos devem ser conhecidos e geridos adequadamente uma vez que nesse modelo a responsabilidade pelos resultados é da alta direção e dos gerentes seniores.

Bitterli (2005, p.1) entende que a governança da segurança da informação é uma evolução da Segurança da Tecnologia da Informação, fundamentando-se nos critérios de confidencialidade, integridade e disponibilidade para aumentar a confiança dos patrocinadores no negócio por trazer novos conhecimentos para garantir a segurança.

A governança é uma clara expectativa para gerir comportamentos e ações. A governança é direcionamento, controle e deve influenciar fortemente a organização para alcançar as expectativas. A governança inclui especificamente um framework de tomada de decisão, de forma que as decisões sejam assertivas e responsáveis. A governança é mais efetiva porque é sistematizada, atinge a cultura organizacional de comportamentos e ações, criando conexões sustentáveis entre as principais políticas, processos, produtos, pessoas e *performance* (ALLEN, 2005, p.5-6).

Para o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY a governança da segurança da informação é uma política de Estado, regida por meios legais, que estabelecem as políticas, as responsabilidades e o direcionamento a fim de garantir a segurança dos serviços de missão crítica. As atividades-chaves estão relacionadas para facilitar a integração dos planos estratégicos, do desenho da organização, desenvolvimento, estabelecimento de regras e responsabilidades, de forma que atendam aos objetivos de segurança da organização (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST, 800-100, 2006, p.3-5).

Analisando os conceitos abordados, percebe-se que a governança da segurança da informação é componente estratégico, e a alta direção deve conhecer os riscos e seu impacto no resultado do negócio. Diante disto, deve ser a governança, como elemento

estratégico, direcionadora das políticas de segurança para a proteção do negócio, tendo na alta direção a responsabilidade do resultado do negócio com os patrocinadores, clientes, empregados e a sociedade.

2.3.2 Objetivo e importância da governança da segurança da informação

Enfrentar as ameaças requer mudança cultural. A mudança cultural, sugerida por Caralli (2004, p.12-13), pressupõe um modelo de segurança direcionado para os riscos do negócio, creditando ao Chief Security Office (CSO) a responsabilidade de incluir o elemento estratégico no contexto da segurança. A flexibilidade administrativa e a segurança transparente também se inserem nessa concepção e envolvem os recursos humanos, financeiros, estratégias e processos do negócio, e a tecnologia da informação como elementos essenciais para a realização da missão.

Segundo o ITGI (, 2006, p.7), atualmente as organizações, diante da revolução da globalização, também buscam nas práticas de governança a melhoria da gestão da segurança da informação, apresentando claramente a necessidade de focar na total proteção da informação para cumprir o prometido, em termos de serviços.

Para atender à criação da governança da segurança da informação, o ITGI (2006, p. 6) recomenda a criação de um grupo estratégico, formado por um conselho consultivo de segurança da informação, com membros da alta administração, tendo a responsabilidade de:

- direcionar e prover as bases para garantir o alinhamento do programa de segurança com os objetivos da organização;
- fomentar a formação de uma cultura de segurança, promovida pelas boas práticas de segurança e por uma política de conformidade;
- ser o canal de comunicação com os representantes de cada uma das áreas da organização.

O INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (ITGI) sugere ainda

um Chief Information Security Officer (CISO) com a responsabilidade de identificar os riscos associados a TI que impactam o negócio e relacioná-los ao programa de segurança da informação, como também conscientizar a alta direção sobre os riscos de segurança de TI. Observando que antes havia o entendimento de que a segurança era problema de TI, atualmente existe o reconhecimento de que os riscos de segurança atingem a imagem da firma, sua reputação, as pessoas e a sociedade com as quais a empresa se relaciona. (INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE, ITGI, 2006, p.7-12).

Para o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-53, 2005, p.1), o modelo de segurança da informação fundamenta-se em controles adequados para proteger os sistemas de informação. A organização deve conhecer suas necessidades e a partir daí definir o modelo que mitigue os riscos. Dessa forma, o modelo deve incluir periodicidades para verificar riscos, no âmbito de acesso não-autorizado, no uso indevido da informação, na destruição. A definição de políticas e procedimentos deve ser baseada nos riscos identificados.

Em 2006, o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST 800-100, 2006, p. 2) recomendou uma estrutura de governança da segurança da informação para gerir a segurança, para garantir que as estratégias da segurança da informação estejam alinhadas com os objetivos do negócio, em conformidade com as leis e regulamentos e que os controles internos estejam inerentes com as políticas e com a responsabilidade pela missão de gerir o risco.

A percepção de Conner (2003, p.3) relaciona-se ao cenário de ameaças para sugerir a Governança da Segurança da Informação, como um subgrupo da Governança Corporativa, para tratar os sistemas de segurança da informação, acrescentando que a segurança da informação é uma questão associada ao uso de tecnologias e que talvez as empresas devessem torná-la parte integral das operações do negócio para garantir a confidencialidade das informações do negócio, a disponibilidade e a integridade das transações. E acrescenta: “o melhor caminho a seguir é incluir os controles e as políticas de segurança na governança corporativa”.

Adicionalmente, Conner (2003, p.3) admite que essa nova realidade do negócio requer constantes ações de equilíbrio com a lei, com regulamentos sobre a privacidade das informações, com o desempenho financeiro, com as expectativas dos investidores, dos

clientes, dos empregados e sugere um modelo de governança da segurança da informação, no qual o equilíbrio deve ocorrer quando as medidas da balança apresentam o mesmo peso, ou seja, os processos da organização são estruturados dentro da legalidade, conforme a figura 6.

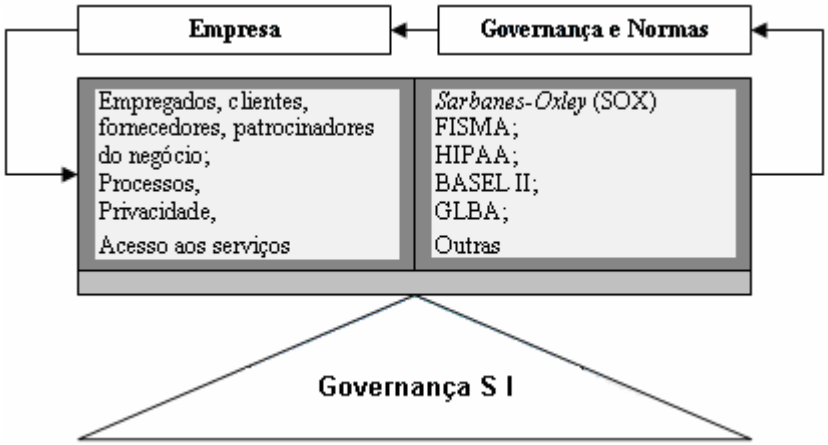


Figura 6 – Escopo da governança da segurança da informação
Fonte: Conner (2003, p.3)

Conner (2003, p.2-3) admite que os escândalos relacionados a negócios financeiros tornaram urgente a questão da Governança Corporativa, com várias políticas e controles internos direcionados ao negócio da empresa. No entanto, não é suficiente porque, segundo o autor, o crescimento tecnológico e a sustentabilidade da vantagem competitiva contribuem para o investimento em processos de acesso em tempo real à informação e serviços, usando a velocidade Web.

De acordo com Bitterli (2005, p.1-3), as companhias, no mundo inteiro, começaram a expandir a percepção sobre a importância da segurança da informação entre 1999 e 2003. Os requerimentos de confidencialidade, integridade e disponibilidade da informação foram fundamentais para identificar que segurança não era uma questão isolada. A rede sem critérios de segurança em TI trazia problemas e emergência na solução, carecendo de novos conhecimentos em segurança. A estratégia aprovada foi a formulação de procedimentos de análise de risco para conhecer as ameaças e mantê-las sobre controle. O autor sugere que, para tomar as rédeas do equilíbrio da segurança da informação, o modelo a ser adotado deve sustentar-se em quatro iniciativas, conforme Figura 7.

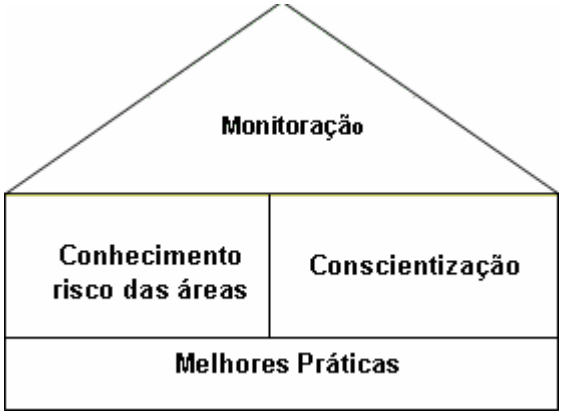


Figura 7 – Quatro iniciativas de Segurança da Informação
Fonte: Bitterli (2005, p.3)

A abordagem de Pironti (2006, p.1-3) é sobre a motivação, benefícios e resultados da adoção de modelo de governança da Segurança da Informação (SI). A percepção fundamenta-se em pesquisa aplicada entre executivos, gestores de segurança da informação e gestores de TI. O resultado da pesquisa evidenciou que os fatores que mais influenciam a iniciativa de adotar um modelo de governança da segurança da informação são: responsabilidade da legalidade, proteção da organização quanto aos aspectos da reputação e conformidade com a lei.

Quanto aos resultados obtidos pela implantação de um modelo de governança da SI, a pesquisa apontou que, de acordo com o pesquisado, houve uma variação: os executivos consideraram respectivamente mais importantes – a gestão de risco, o alinhamento à estratégia da organização e a conformidade com a lei. Para os executivos de SI e de TI o item mais relevante foi a conformidade com a lei; a variação ocorreu quanto à gestão de risco que foi considerado o segundo mais importante para o gestor de SI, enquanto o de TI considerou o alinhamento como o negócio mais relevante. Entretanto, os três itens (responsabilidade da legalidade, proteção da organização quanto aos aspectos da reputação e conformidade com a lei) foram considerados importantes por todos.

Os benefícios da governança da SI, segundo a pesquisa apresentada por Pironti (2006, p.3), foram verificados, entre outros meios, por aferição de métricas, constatando-se que houve um efetivo controle de riscos e um estágio de corrente evolução no desempenho da efetividade do programa de governança.

2.3.3 O novo cenário da segurança em relação ao negócio

Segundo Booz, Allen e Hamilton (2005, p.6), a convergência para a segurança nas empresas está fortemente ligada a cinco questões:

- rápida expansão do ecossistema da empresa, tornando-se esta mais complexa na economia global, onde os parceiros estão aumentando;
- migração do valor físico da informação para ativos intangíveis;
- surgimento de novas proteções tecnológicas, criando uma sobreposição entre o físico e as funções da segurança da informação;
- novas conformidades e regimes regulatórios desenvolvidos para responder a novas ameaças e à interação com o negócio;
- contínua pressão para reduzir os custos, as empresas tentando constantemente eficiência na mitigação de riscos.

Essas questões estão provocando alteração na moldura da segurança e forçando a mudança nas regras de segurança em relação aos patrocinadores e o valor corrente do negócio. A discussão sobre o risco tem-se tornado mais integrada ao negócio, atravessando todos os setores da organização a fim de melhorar o valor do negócio.

Atualmente a economia depende mais do fluxo de informação, dentro e fora da organização. Neste particular, a segurança da informação é envolvida como uma questão de vital importância, considerando que segurança e confiança nos ambientes de armazenagem e distribuição/compartilhamento de informação requerem melhorias constantes, visando ao benefício do desempenho e produtividade do negócio. (CONNER, NOONAN, HOLLEYMAN, 2004, p.1). Segundo esses autores (2004, p.1-3), o Estado, atento a essas questões, tem aprovado mais leis e regulamentos sobre a segurança da informação no sentido de serem aplicados tanto no setor público quanto no privado, visando garantir que a informação não seja apenas uma questão técnica, mas uma gestão de estrutura, de melhores práticas de governança.

De acordo com Caralli (2004, p.1-2), a segurança tem-se tornado uma das mais urgentes questões para muitas organizações. É um requerimento essencial para quem utiliza a rede global da economia para seu negócio, uma vez que o ambiente tecnológico é

complexo e os riscos aumentam e se modificam a cada dia. Os incidentes de segurança atingem números recordes e tem atingido os clientes com roubo de identidade, alta escala de infecção por vírus e outros tipos de ataques que comprometem a confidencialidade, a integridade e a disponibilidade da informação. Esses incidentes têm afetado a estabilidade econômica das organizações, porque impactam diretamente na consolidação dos objetivos, suscitando a necessidade da gestão da segurança empresarial como uma forma de minimizar o problema.

2.3.4 A gestão da segurança, um passo para a governança da segurança da informação

Para tratar da gestão da segurança da informação (GSI), é importante observar a norma ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27001: 2006 (p.v) sobre o Sistema de Gestão em Segurança da Informação (SGSI). Segundo a norma, a adoção de um modelo de SGSI deve ser uma decisão estratégica para a organização, no contexto de suas necessidades, objetivos, requisitos de segurança e tamanho da instituição.

Ainda de acordo com as orientações da ISO 27001, o sistema de gestão de segurança deve embasar-se num ciclo de melhoria contínua, de PDCA (planejar - *Plan*, fazer - *Do*, monitorar - *Check e* promover - *Act*), visando a que o impacto de um incidente possa ser minimizado pelo uso adequado das ações de:

- planejar, definir como deve ser o modelo de gestão (políticas, objetivos, gestão de riscos) de acordo com a organização;
- fazer, implementar e operar as políticas , os controles e os processos definidos;
- monitorar, analisar e medir o desempenho e verificar os resultados obtidos;
- promover ações de melhoria.

Com o mesmo direcionamento, afirma Caralli (2004, p.14-20) que a gestão da segurança empresarial significa envolver ações de planejamento, de controle e de coordenação das atividades, que atravessam a empresa com a profundidade que as regras de segurança necessitam alcançar. Em síntese, para atender aos clientes, patrocinadores, empregados, clientes e fornecedores, a gestão da segurança empresarial deve alinhar as estratégias de segurança com as estratégias organizacionais para garantir, melhorar e

sustentar a flexibilidade da organização, observando que existe um ciclo de vida de ameaças, de vulnerabilidades, um plano de continuidade do negócio e que o modelo deve prever a fim de preparar-se para agir e reagir, de acordo com a situação do incidente de segurança.

A necessidade de segurança é reconhecida pela maioria, senão por todas as organizações sejam de economia, de política ou sociais, públicas ou privadas, grandes ou pequenas. Os clientes apresentam suas preocupações quanto à privacidade e ao aumento do roubo de identidade. Diante disto, Allen (2005, p.5-11) entende que as organizações necessitam adotar ações que garantam um processo de prevenção, proteção e continuidade do negócio, com base nos riscos a que estão expostas.

Adicionalmente, Allen (2005, p. 11) propõe que essas ações devem estar alinhadas ao processo de tecnologia da informação e devem ser direcionadas aos objetivos estratégicos e táticos da organização. Os líderes das organizações precisam tratar a segurança como uma questão do negócio, entendendo o que são risco de segurança e estratégias de segurança. Essa abrangência sinaliza para um programa de segurança que coloque a gestão de risco como uma ação de responsabilidade da alta direção, dentro de uma perspectiva onde a efetiva gestão de risco seja a base de sustentação de uma ampla governança da segurança.

Enfim, a gestão da segurança da informação pressupõe um modelo de gestão que combine tecnologia, processo e pessoas em uma estrutura que promova a confidencialidade, integridade e disponibilidade da informação, baseado nos requerimentos do negócio e na análise de riscos. Depende fortemente de um processo que estabeleça as metas e busque os resultados, direcionando esforços para uma efetiva governança da segurança da informação (SETHURAMAN, 2006, p.1).

2.4 A gestão da segurança da informação

2.4.1 Conceito de segurança da informação

“Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o

retorno sobre os investimentos e as oportunidades do negócio" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799, 2005, p. ix).

A segurança da informação não é apenas uma questão de tecnologia, mas uma questão do negócio e envolve uma apropriada gestão de riscos para proteger adequadamente a informação em todos os níveis da organização (INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE, 2006, p. 8).

A segurança da informação busca proteger a informação dos riscos a que está exposta para garantir a confidencialidade, a integridade e a disponibilidade (PFLEEGER, 1997, p. 17).

Krutz e Vines (2001, p.3) argumentam que a segurança da informação se sustenta em três objetivos de controle: confidencialidade, integridade e disponibilidade para reduzir o impacto de ameaças e a probabilidade da ocorrência de incidentes.

Allen (2005, p.7) entende a segurança num âmbito da empresa, defendendo a segurança empresarial como sendo ações para proteger a informação em todas as formas de riscos: eletrônica e física, sistemas de rede, considerando área de armazenagem, acesso, processamento e transmissão. Adicionalmente diz que a empresa deve ter o nível de segurança adequado a suas necessidades de proteção estratégica e tática.

A segurança da informação é o meio de utilizar leis, normas e regulamentos para garantir que os controles sejam adequados para assegurar a efetividade dos requerimentos de segurança diante dos riscos a que a informação está exposta (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 800-100, 2006, p.1). O fato é que os riscos a que as empresas estão sujeitas em seus diversos ambientes operacionais são os fatores que suscitam a necessidade de que cada empresa tenha um apropriado modelo de segurança da informação que permita conhecer inicialmente os riscos e, a partir daí, definir a política e procedimentos a serem adotados.

2.4.2 Evolução da segurança da informação

De acordo com Pfleeger (1997, p. xv-xvi), no final dos anos oitenta começou a ser fomentada a questão sobre a “segurança em computador”. Essa preocupação coincide com a cadeia de valor que a informação começa a integrar sob o rótulo de “economia da informação”. Foi a época em que a Internet era usada principalmente por profissionais da área computacional, academias e empresas de sistemas. Os códigos maliciosos e vírus não eram comuns, os crimes cibernéticos raramente eram notícia de jornal e as pessoas não tinham noção das ameaças por meio de computador.

No final dos anos noventa, a Internet passou a ser meio de comunicação de massa. As pessoas começaram a acessar sua conta bancária por computador, fazer pagamentos e o *e-commerce* cresceu em quantidade de empresas e volume de dinheiro. O novo cenário, segundo Pfleeger (1997, p. 4), evidenciou que a “segurança de computador” coexistiria se mantivesse três características fundamentais:

- confidencialidade: consiste em manter o acesso ao computador por pessoas autorizadas;
- integridade: consiste em assegurar que o dados não sejam modificados por pessoa não-autorizada;
- disponibilidade: consiste em garantir que o acesso seja legítimo, por meio da pessoa autorizada, no momento em que deseja acessar o objeto. O autor entende que existe um relacionamento entre os três atributos de segurança, conforme exposto na Figura 8.

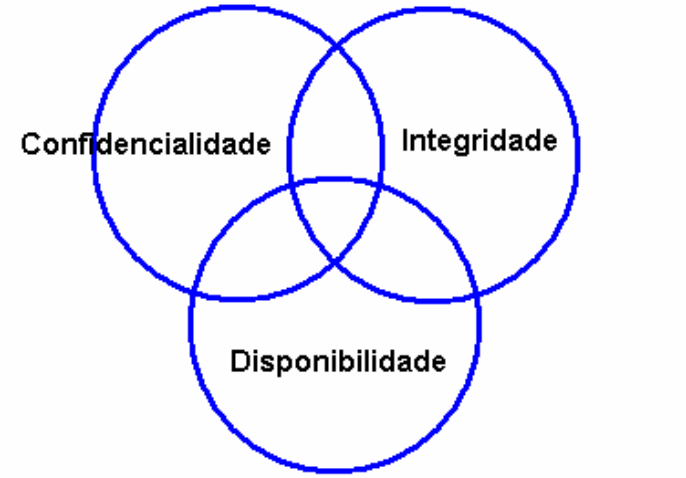


Figura 8 - Relacionamento entre confidencialidade, integridade e disponibilidade
Fonte: Pfleeger (1997, p. 5)

2.4.3 Melhores práticas

Em 1995 o British Standard Institute (BSI) publicou a primeira versão da norma internacional BRITISH STANDARD (BS 7799), logo considerada padrão para o gerenciamento da segurança da informação. A norma tornou possível a implementação de um sistema de gestão de segurança baseado em controles e práticas.

Em 2000, a parte 1 da BRITISH STANDARD (BS 7799) passou a ser ISO/IEC 17799. Em 2001, o Brasil adotou essa norma como padrão, por meio da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. A versão mais atual é a ABNT NBR ISO/IEC 17799:2006.

Registra-se que no estágio atual de padronização das normas está sendo criada a família das normas de segurança, como padrão internacional, sob o código 27000, iniciando-se pela norma da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27001:2006 que irá abranger, além da ISO/IEC 17799:2005, outras como a ISO Guide 73:2002, que trata da análise de risco; ISO/IEC TR 18044:2004, trata do incidente de segurança; ABNT ISO/IEC Guia 2:1998, sobre terceirizados; ISO/IEC 13335-1:2004, sobre ameaças.

De acordo com a norma da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ABNT NBR ISO/IEC 17799:2005 (p.ix), a informação é um ativo essencial aos negócios de uma organização e por isso necessita de proteção adequada, significando conhecer o valor da informação para a continuidade do negócio e os tipos de ameaças que a circundam, buscando assim os controles que possam garantir sua sustentabilidade.

Os controles de segurança da informação são estabelecidos visando à tríade confidencialidade, integridade e disponibilidade da informação. Adicionalmente, poderão ser agregadas outras propriedades como autenticidade, responsabilidade, não-repúdio e confiabilidade. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005, p. 1).

A ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 orienta que a gestão de segurança da informação deva ser iniciada com a análise, avaliação e tratamento de risco, e define 11 (onze) seções de controle com finalidades específicas, que devem ser adotadas de acordo com os riscos identificados. Neste contexto, o gestor da organização poderá medir a dosagem de investimento no controle que seja mais significativo a seu objeto de gestão sobre o risco de maior significância a seu negócio, observando o nível de risco aceitável.

De acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC 17799:2006 (p.6), a análise de risco é o uso sistemático de informações para identificar fontes e estimar riscos. Na aplicação da análise de risco em segurança da informação, o escopo deve ser previamente definido para que a amplitude e a complexidade da análise sejam dimensionadas. Devem ser consideradas as seguintes premissas:

- identificação, quantificação e priorização de riscos;
- critérios para aceitação dos riscos em relação ao tipo de organização;
- determinação das ações de gestão de riscos, visando à adoção de controles adequados;
- determinação da periodicidade de avaliação de riscos a fim de conhecer mudanças nos requisitos de riscos e na situação de risco, gerando resultados comparáveis e reproduzíveis.

Os controles de segurança e respectivas finalidades, sugeridos pela norma ABNT NBR ISO/IEC 17799:2005, são mostrados no Quadro 3.

Quadro 3. 11 (onze) seções de controle com finalidades específicas

Controles	Finalidades
Política de SI	Prover uma orientação e apoio da direção para SI, de acordo com o tipo do negócio e a legislação.
Organização de SI	Gerenciar SI dentro da organização
Gestão de ativos	Alcançar e manter a proteção adequada dos ativos da organização
Segurança em recursos humanos	Assegurar que empregados, fornecedores e terceiros entendam suas responsabilidades com o negócio da organização
Segurança física e do ambiente	Prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações
Gerenciamento das operações e comunicações	Garantir a operação segura dos recursos de processamento da informação
Controle de acesso	Controlar o acesso à informação
Aquisição, desenvolvimento e manutenção de SI	Garantir que a segurança é parte integrante de sistemas de informação
Gestão de incidentes de SI	Assegurar que fragilidades e eventos de SI sejam comunicados, permitindo ações corretivas em tempo hábil
Gestão de continuidade do negócio	Não permitir a interrupção das atividades do negócio e proteger os processos críticos
Conformidade	Evitar a violação de qualquer lei criminal, estatuto, obrigações contratuais e de quaisquer requisitos de SI

Fonte: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005

2.4.4 Formas de implementar um modelo de segurança da informação

Diante da complexidade de cada seção que trata de um segmento da segurança da informação, as organizações optam por contratar profissionais especializados nessa área. O CISO (CHIEF INFORMATION SECURITY OFFICER) tem sido referência como aquele que tem conhecimento e visão estratégica de segurança para gerenciar os riscos que cercam o negócio e identificar os níveis de habilidades necessários a uma gestão eficiente. Trata-se de profissional que, ao atingir níveis de maturidade de conhecimento na área de segurança, entende a questão de segurança com mais profundidade e maturidade, atualmente, evoluindo para uma visão mais abrangente, que emerge sob o rótulo de “governança da segurança da informação” (GARTNER, 2006, p.2).

Para o Gartner (2006, p. 3-12), a empresa que deseja tornar-se mais efetiva e coordenar suas práticas de segurança deve investir num modelo de segurança da informação no contexto de sua necessidade, observando que conter as ameaças à segurança é um processo contínuo. Entende ainda ser obrigação das organizações implementar um processo de segurança para manter mecanismos que sejam capazes de traduzir os requerimentos de segurança necessários ao negócio da organização. Com esse direcionamento, sugere o modelo EISA (ENTERPRISE INFORMATION SECURITY ARQUITECTURE).

Sob o ponto de vista da arquitetura de segurança EISA, a segurança da informação pode ser definida em três dimensões (GARTNER, 2006, p. 3):

- Negócio: reflete a segurança para o negócio, significando a decisão sobre a prática de segurança que deve ser tomada pela organização, identificando o relacionamento com as outras áreas da organização, processo, papéis, regras, responsabilidades e estrutura organizacional;
- Informação: representa o modelo de informação que é utilizado pelo time de segurança e os requerimentos de segurança necessários para garantir a segurança da informação da empresa;
- Tecnologia: representa a arquitetura de infra-estrutura, sistemas e equipamentos de segurança para garantir a segurança da empresa.

A arquitetura de segurança EISA tem o objetivo de fornecer os mecanismos necessários à construção de soluções para a segurança do negócio. Baseia-se em três níveis hierárquicos:

- camada conceitual: identifica a estratégia da organização, a forma como o negócio tem a confidencialidade, a integridade e a disponibilidade e como poderá ser gerida;
- camada lógica: entre outros procedimentos, detalha os requerimentos, os princípios e modelos que podem ser utilizados para a solução das regras conceituais, define o modelo de segurança da informação alinhado à necessidade do negócio da empresa;
- camada implementação: define os recursos humanos necessários a cada processo e como serão envolvidos relacionamentos, responsabilidades, fluxo de informações e controles.

De acordo com o Gartner, o EISA teria a seguinte arquitetura: adaptado do modelo apresentado na p.10, Figure 3 Example of Technical Security Architecture Structure, apresentado na Figura 9.

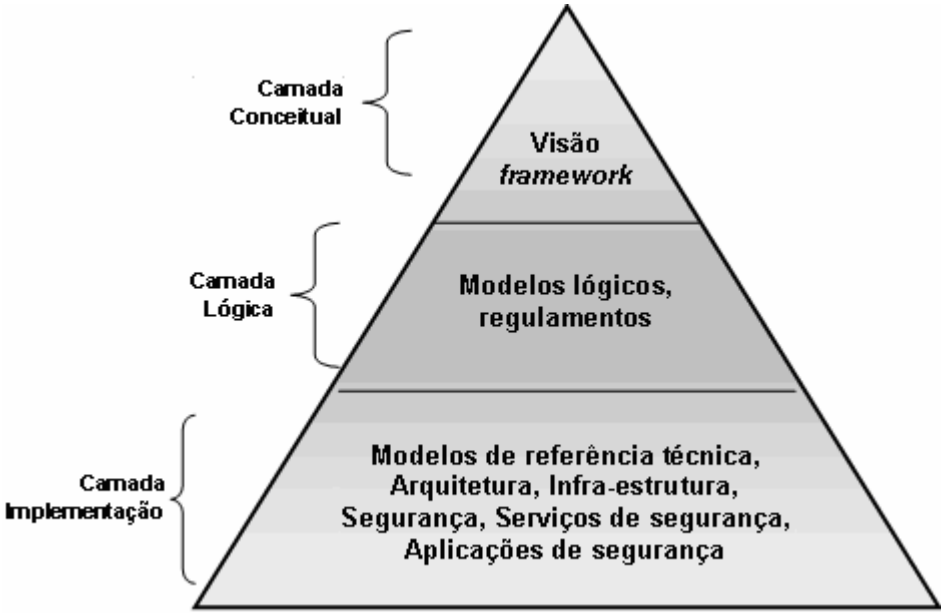


Figura 9 – Exemplo de Arquitetura Técnica de Segurança
Fonte: Gartner, (2006, p. 10)

O fato é que, à medida que aumentam as ameaças e riscos ao negócio, mais se especializam as organizações a fim de manter a competitividade. Em qualquer modelo de segurança há que ser observados os segmentos de confidencialidade, integridade e disponibilidade, voltados para a proteção de três elementos que são os maiores objetos de ataque: sistemas, equipamentos e dados. Adicionalmente, o fator humano também é considerado como vítima e como responsável pelos problemas de segurança, dependendo do contexto em que esteja inserido. Diante disto, de acordo com a política adotada, o investimento em segurança baseia-se em três segmentos da segurança da informação: pessoas, tecnologia e processos (PFLEEGER, 1997, p. 16-17).

Observa-se que para cada um dos segmentos há um objetivo específico dentro da organização. Investe-se em pessoas com o objetivo de reduzir os erros humanos, fraude, uso indevido, acesso malicioso. Quanto à tecnologia, é fundamental em segurança; tem sido o item de maior investimento das organizações, setor público, privado e academias, em razão do avanço da própria tecnologia de informação e comunicação, e em detrimento de vários fatores, desde a questão das ameaças, riscos, até a busca de melhores resultados empresariais e de competitividade. A tecnologia tem sido tratada, sob a ótica de governan-

ça de TI, em *framework* consolidado como CONTROL OBJECTIVES FOR INFORMATION (COBIT), IT INFRASTRUCTURE LIBRARY (ITIL**)**, BALANCE SCORECARD (BSC), de acordo com Weill e Ross (2004, p.177).

O modelo de segurança da informação a ser adotado pela organização deve fundamentar-se na necessidade de segurança do negócio. Inicia-se pela análise de risco, que significa identificar, quantificar e priorizar os riscos com base em critérios de aceitação dos riscos e dos objetivos organizacionais. A seguir, a definição dos controles, avaliação e gestão a serem implementados devem considerar os ativos que serão protegidos e em que criticidade. Conhecer os serviços críticos significa segurança e retorno financeiro (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS T NBR ISO/IEC 17799:2005, p. 6).

O NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-53, 2005, p.1) recomenda que, ao definir o modelo de segurança, algumas perguntas devem ser respondidas, tais como:

- Quais controles de segurança são adequados para proteger os sistemas de informação e garantir a operacionalização da organização?
- O plano de implementação dos controles está adequado à realidade?
- Quais níveis de segurança são requeridos para garantir a confidencialidade das informações?

Para o NIST (800-53, 2005, p.4-5), a segurança da informação está associada à gestão de riscos, pois a avaliação de riscos recomenda os controles mínimos, os documentos e o plano de segurança para os sistemas de informação. Trata-se de um processo que requer muitas competências para gerir os sistemas de informação. As competências podem ser financiadas pela organização enquanto durar o ciclo de vida do sistema. Realisticamente, avaliar os riscos operacionais da organização e manter a continuidade das operações da organização com o nível tolerável de riscos é extremamente importante e requer custos e cronogramas associados à operação de sistemas.

Os controles da segurança da informação, segundo o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-53, 2005, p.6), estão divididos em classes associadas a famílias. As classes são relacionadas à gestão, operação e proteção

tecnológica, enquanto as famílias alocam a suas respectivas classes os domínios de controles necessários, observando-se que um controle pode ser associado a mais de uma classe. Para demonstrar, é apresentada no Quadro 4 uma adaptação do modelo sugerido pelo NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) na Table 1: Security Control Classes, Families and Identitifiers:

Quadro 4: Classes de controle e respectivas famílias

Gestão	Avaliação de riscos Planejamento Aquisição de sistemas e serviços Certificação, credibilidade, avaliação da segurança
Operacional	Segurança pessoal Segurança física e ambiental Plano de contingência Gestão de configuração Manutenção Integridade dos sistemas de informação Medidas de proteção Resposta a incidente Conscientização e treinamento
Técnico	Identificação e autenticação Controle de acessos Auditoria e conformidade Proteção a sistemas e comunicações

Fonte: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, (NIST, 800-53, 2005, p.6)

Observa-se que há semelhança entre os requisitos de controles sugeridos pelo NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-53, 2005, p.34-35) e os controles da ABNT NBR ISO/IEC 17799:2005, ambos descrevem as onze seções de controle e respectivas finalidades. Todos os itens do NIST estão contidos nos controles da ISO como subitens de seções. A análise sugerida é de que os itens requeridos para a segurança da informação são semelhantes em qualquer modelo que se pretenda inserir. A diferença seria quanto ao tipo do negócio, os riscos associados e tolerados, e o alinhamento do modelo de segurança da informação ao negócio.

A ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) percebe a questão da segurança da informação num contexto social mais amplo,

considerando a integração dos setores público, privado e cidadãos, enfim, a sociedade em geral que, por ser a grande massa dependente dos sistemas de informação e de sistemas de missão crítica (energia, água, transporte, setor financeiro, telecomunicações, seguro de serviços de saúde), precisa evitar os transtornos operacionais dessas infra-estruturas.

Diante dessa perspectiva, a ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT propõe que o Estado seja o fomentador, patrocinador e incentivador de práticas em segurança a partir do direcionamento de políticas sobre tecnologias, processos e educação, sustentados por um programa como o The Culture of Security for Informations Systems que visa prioritariamente às seguintes necessidades (OECD, 2005, p.11-25):

- Direcionamento da cultura de segurança;
- Implementação de políticas nacionais para uma cultura de segurança;
- Estabelecimento de cooperação internacional;
- Criação de áreas voltadas para o combate ao crime cibernético; criação de área de respostas a ataques; conscientização e fomento à educação;
- Evolução e avaliação das ações.

Observa-se que na abordagem da ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT a segurança da informação ganha uma abrangência estratégica, requerendo ações efetivas do Estado, interagindo com o setor privado e a sociedade. Esses pilares, defende a OECD, devem integrar-se, cada um com sua responsabilidade específica, e construir uma cultura de segurança da informação (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2005, p. 6-7).

A cultura de segurança da informação pressupõe primeiramente políticas nacionais para sistema de informações e compartilhamento de redes, enfatizando que uma cultura de segurança não pode depender somente de soluções técnicas, mas considerar as questões socioeconômicas e legais e daí a dimensão multidisciplinar. Ressalte-se ainda que o Governo sozinho não poderá solucionar os problemas de segurança da informação (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2005, p. 6).

Enfim, na prática, a definição de um modelo de segurança da informação tem o objetivo de assegurar o negócio da empresa, alicerçado nos aspectos da confidencialidade, integridade e disponibilidade, conforme observado por Pfleeger (1997, p.4), e utilizando um conjunto de controles que permitam conhecer e gerir riscos, orientar as ações de continuidade do negócio, níveis de responsabilidade e conformidade com diretrizes, legislações e acordos contratuais, como recomenda o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-53, 2005, p.1).

A ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27001:2006 propõe o Sistema de Gestão da Segurança da Informação (SGSI), que utiliza o modelo de PDCA (*Plan*- planejar, *Do*- implementar, *Check*- verificar, *Act*- revisar) visando prover um modelo de gestão, dentro de uma perspectiva estratégica da organização, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar os controles de segurança e garantir que os controles sejam adequados para proteger os ativos de informação.

Na dinâmica das atividades das organizações, onde, segundo Weill e Woodham (2002, p. 2-3), a empresa funciona 24 horas por sete, todos os dias do ano, o ativo de informação está sujeito a riscos que podem gerar um incidente de segurança e comprometer a segurança da informação e do negócio. Diante disso, uma organização precisa identificar e gerenciar muitas atividades para funcionar efetivamente, identificando as atividades como processos que interagem para dar sustentação a organização.

A adoção de um modelo de sistema de gestão da segurança da informação visa assegurar a implementação de processos que garantam as operações para proteger informações estratégicas aos negócios e evitar incidentes de segurança. A medida de proteção deve ser proporcional à necessidade do negócio em relação a seus riscos, considerando os critérios de confidencialidade, integridade e disponibilidade.

A implementação da ISO 27001:2006 requer inicialmente que a organização formule o plano de tratamento de risco e identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades. Identifique os controles para atender os objetivos de controle, definindo como medir a eficácia desses controles de modo a produzir resultados compatíveis e reproduzíveis. Outra requisição fundamental é o apoio da alta direção que deve apresentar evidências do seu comprometimento com o estabelecimento,

implementação, operação, monitoramento, análise crítica, manutenção e melhorias do sistema, mediante o estabelecimento da Política de Gestão da Segurança da Informação (SGSI), garantia de que serão estabelecidos os planos e objetivos da política de gestão, estabelecimento de papéis e responsabilidades, comunicação à organização sobre a importância em atender aos objetivos e a conformidade com a política, provisão dos recursos para implantar e manter a melhoria da gestão, definir critérios para manter a aceitação de riscos e dos níveis aceitáveis, garantia de realização de auditorias internas, e condução da análise crítica do SGSI pela diretoria. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS NBR ISO/IEC 27001:2006, p.9-10).

De acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27001:2006 a adoção do modelo de PDCA (PLAN, DO, CHECK, ACT) refletirá os princípios para a governança da segurança de sistemas de informação e redes. A Figura 10 ilustra como um Sistema de Gestão da Segurança da Informação (SGSI) considera as entradas de requisitos de segurança da informação, expectativas das partes interessadas e as ações necessárias e processos resultam no atendimento. A figura é adaptada do modelo apresentado na p.vi, Figure 1 – Modelo PDCA aplicado aos processos SGSI:

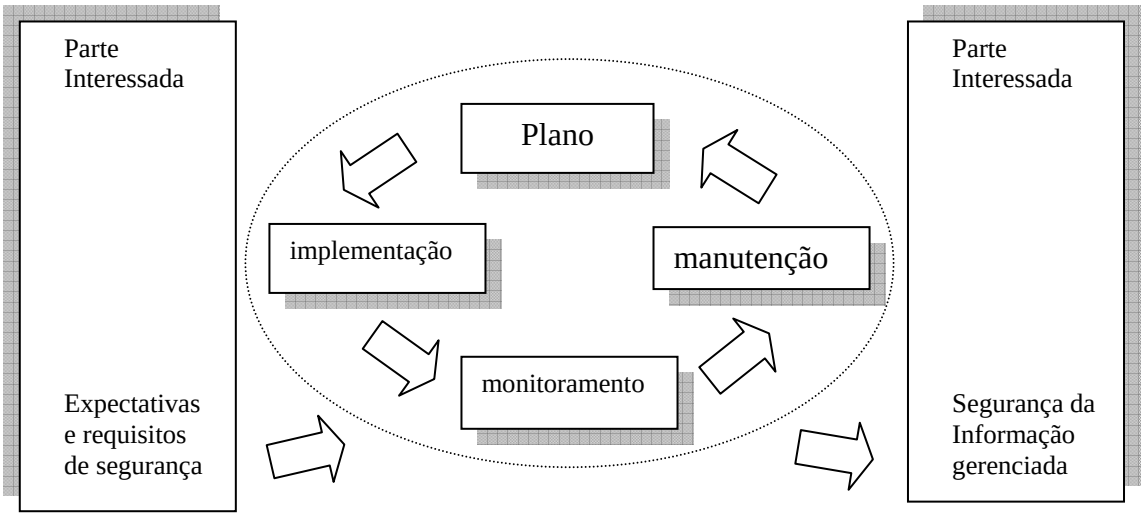


Figura 10: Modelo PDCA (PLAN, DO, CHECK, ACT
Fonte: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISSO/IEC 27001: 2006, p.vi

2.5 Os riscos da segurança da informação

"O risco é a probabilidade da ocorrência de um evento e de suas conseqüências". (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC Guia 73:2005, p. 2). A necessidade da gestão de riscos é unanimidade em todos os segmentos. Os institutos que tratam da governança recomendam em seus códigos de melhores práticas o gerenciamento de riscos. O fato é que a organização, independentemente do setor (público, privado ou 3º setor), deve investir no negócio a partir da análise e avaliação de riscos, contribuindo para a perenidade do empreendimento. Nesse contexto, o Instituto Brasileiro de Governança Corporativa (IBGC) está lançando um "Guia de Orientação para o Gerenciamento de Riscos Corporativos", contendo recomendações sobre o Gerenciamento de Riscos Corporativos. (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2007, p. 6).

2.5.1 Conceitos de riscos

De acordo com Krutz e Vines (2001, p. 15), é importante que a empresa entenda que o risco será mitigado, nunca totalmente eliminado. Mitigar riscos significa encontrar um nível aceitável de risco e continuar efetivamente as funções.

Para a estimativa do risco, o processo de análise deve atribuir valores à probabilidade e às conseqüências do risco e, então, definir o tratamento (seleção e implementação de medidas para modificar um risco). Para melhor compreensão, a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC Guia 73:2005, p.2 oferece os conceitos complementares ao risco: Risco é a combinação da probabilidade de um evento e suas conseqüências, onde:

- Probabilidade é o grau de possibilidade de que um evento ocorra;
- Evento é a ocorrência de um conjunto especifico de circunstâncias;
- Conseqüências são o resultado de um evento.

Segundo o IBGC, o “conceito atual de risco envolve a quantificação e qualificação da incerteza, tanto no que diz respeito à perdas como aos ganhos, com relação ao rumo dos acontecimentos planejados, seja por indivíduos ou por organizações” (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2007, p.7).

Para Schumacher et al. (2006, p.137), risco é o resultado final de um processo de avaliação de riscos, através do qual, após a avaliação da ameaça e de vulnerabilidade, o resultado é incorporado para priorizar o risco e a vantagem dessa priorização para o negócio.

Segundo Allen (2005, p. 10), risco é a possibilidade de que um evento poderá ocorrer e afetar de forma adversa os objetivos do negócio.

Segundo o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-100, 2006, p. 85), risco é a probabilidade de que uma fonte de ameaça e uma potencial vulnerabilidade resultem em um evento que cause um impacto adverso à organização. Ou seja, se houver o cruzamento de uma ameaça com uma vulnerabilidade, o risco estará presente. A Figura 11 apresenta um processo de análise de risco.

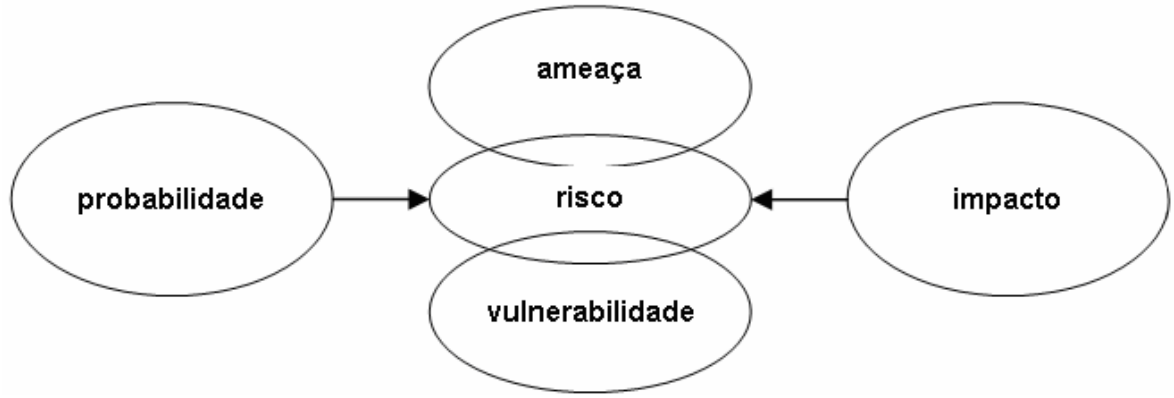


Figura 11 – Processo de risco
Fonte: NIST, 800-100, 2006, p. 85

2.5.2 Análise, avaliação e tratamento de riscos

A análise de riscos é o uso sistemático de informações para identificar elemento ou atividade que possuem potencial para causar um incidente de segurança e estimar o risco.

Após essa etapa, o risco deve ser avaliado e se traduz num processo de comparação de riscos, por meio de critérios que estabelecem a importância do risco. O tratamento de risco é modalidade de seleção e implementação de ações para modificar um risco de acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC Guia 73:2005 (2005, p.3-4).

A ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 (p.6) sugere que a análise de risco deve ser a primeira ação que a organização precisa empreender antes da tomada de decisão sobre investimento em qualquer segmento do negócio.

A análise e avaliação de riscos devem ser realizadas sempre, periodicamente, a fim de contemplar as mudanças nos requisitos de segurança e na situação do risco. Importante salientar que, antes de tratar o risco, a organização deve definir quais riscos poderão ser ou não aceitos, e esse tipo de decisão faz parte da política e deve ser devidamente registrado. Diante disto, para cada risco a ser tratado deve-se verificar, de acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 (p. 6-7), os seguintes pontos:

- considerar os requisitos e restrições da legislação;
- conhecer claramente a política da empresa de aceitação de riscos;
- evitar riscos, orientando sobre ações que podem causar a ocorrência de riscos;
- transferir os riscos associados para outras partes, como seguradoras e fornecedores.

Adicionalmente, a norma ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27001:2006 reporta no Anexo1 (p.15) que a organização deve identificar os riscos relacionados com as partes externas, oriundos de processos do negócio que envolvem partes externas, e controlar com controles apropriados antes de conceder o acesso. Esse requisito vale para tratamento com clientes e terceiros.

Segundo o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800.100, 2006, p. 85-87), a análise e avaliação de riscos devem ser usadas como uma boa prática para suportar a missão e objetivos do negócio da organização. Também devem ser direcionadas para definir os sistemas de missão crítica e delinear os controles necessários para o tratamento do risco. Para iniciar a análise de riscos, a organização deve verificar:

- O escopo da análise: consiste inicialmente em autorização da alta gerência, definição das fronteiras, recursos e informações;
- A identificação das ameaças: existem três tipos de ameaças mais comuns – ameaças naturais (relacionadas com aspectos da natureza), ameaças humanas (podem ser intencionais e não-intencionais), e ameaças do ambiente (falhas de segurança);
- A identificação das vulnerabilidades: trata-se de detectar falhas, brechas ou violação de uma política de sistema de informação. As vulnerabilidades podem ocorrer acidentalmente ou intencionalmente.

O tratamento do risco é uma etapa posterior à definição dos riscos aceitos, que são os que causam menos impacto ou cujo custo do tratamento não é economicamente viável para a organização. O tratamento é destinado ao risco não-aceito. Para cada risco identificado mediante a análise e avaliação de riscos, segundo a ABNT NBR ISO/IEC 17799:2005 (p. 6), uma decisão sobre como tratar o risco deve ser tomada, considerando opções como:

- Estabelecer controles que podem ser aplicados;
- Documentar claramente os riscos aceitos e não-aceitos, de acordo com a política e orientações da alta direção;
- Identificar ações que podem causar riscos e definir os controles para evitar;
- Transferir riscos associados a situações não-controláveis para seguradoras, fornecedores ou outros segmentos.

Enfim, é importante observar que, de acordo com o que a ABNT NBR ISO/IEC 17799:2005 (p.6-7) o tratamento de riscos deve prever mecanismos de controle apropriados para verificar se o risco está em nível aceitável e para definir sistemas de monitoração e coleta de evidências e periodicidade para revisão da análise de risco.

2.5.3 Importância da gestão de riscos

A gestão de risco é um processo utilizado em todos os tipos de empreendimentos com a finalidade de identificar oportunidades e ameaças ao negócio. No contexto da

segurança da informação, a gestão do risco é focada na prevenção e mitigação dos danos, e as ações dependem do tipo do negócio e das ameaças às quais estão submetidas. (NORMA BRASILEIRA ISO/IEC Guia 73:2005, p. 1).

O processo de gestão de riscos é um importante componente para o sucesso de um programa de segurança da informação e deve ser integrado ao ciclo de vida do sistema de informação. Outro ponto a ser considerado, ainda de acordo com o NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-100, 2006, p. 84), a gestão de risco deve focar essencialmente os sistemas críticos, aqueles que são essenciais para o negócio da organização, considerando que a principal função da gestão de riscos é proteger a organização e tornar viável a capacidade de cumprir sua missão.

A determinação do nível de risco é verificada mediante a probabilidade de sua ocorrência e do impacto no negócio, nos sistemas críticos. Diante disto, a organização deve definir em suas políticas o nível de risco aceitável, os riscos que devem ser mitigados e os que serão controlados. O NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST, 800-100, 2006, p.89-91) propõe uma matriz para identificar, dentro de uma escala de riscos, o que significa baixa, moderada e alta ameaça. A partir da definição, na hipótese de opção pela mitigação do risco, recomenda que sejam adotadas as seguintes ações:

- Priorizar as ações;
- Avaliar as opções de controles recomendadas;
- Analisar o custo – benefício da ação a ser executada;
- Selecionar os controles;
- Designar responsabilidades;
- Desenvolver e implantar o plano de proteção;
- Implementar os controles selecionados.

A gestão de riscos, de acordo com a norma AUSTRALIAN STANDARD FOR RISK MANAGEMENT (AS/NZS 4360:2004), é um processo importante para o negócio do setor público e privado, em qualquer lugar do mundo. A gestão de risco deve ser entendida como um processo holístico de gestão que se aplica a todos os tipos de organização em todos os níveis e também aos indivíduos. Apresenta alguns benefícios,

como:

- Redução de surpresas: o controle de eventos adversos é tomado por meio da identificação e ações para minimizar sua probabilidade e reduzir os efeitos;
- Aproveitamento de oportunidades: a confiança no entendimento dos riscos e a capacidade de gerir fomentam a busca de oportunidades;
- Melhoria do planejamento, desempenho e eficácia: o acesso a informações estratégicas torna o planejamento mais adequado e eficaz;
- Melhoria das relações com as partes envolvidas: a gestão de riscos motiva as partes envolvidas a desenvolverem um canal de comunicação para compartilhamento de informações e melhoria para a tomada de decisão;
- Melhoria da reputação: investidores, fornecedores, credores, seguradoras e clientes são mais atraídos para organizações que têm processo satisfatório de gestão de riscos;
- Responsabilidade: garantia e governança, demonstração por evidências da abordagem de gestão adotada, com foco na conformidade com os requisitos e na melhoria organizacional.

A norma AUSTRALIAN STANDARD FOR RISK MANAGEMENT (AS/NZS 4360:2004) argumenta que a gestão de riscos contribui para a boa governança corporativa, dando garantias à alta liderança de que os objetivos organizacionais serão atingidos dentro de um nível aceitável de risco residual. Também contribui para proteger diretores e gerentes que poderão, diante de resultados adversos, demonstrar que agiram com o devido zelo.

A norma AS/NZS 4360:2004 apresenta o seguinte panorama genérico de um processo de gestão de riscos, constante na página 12, adaptada na Figura 12.

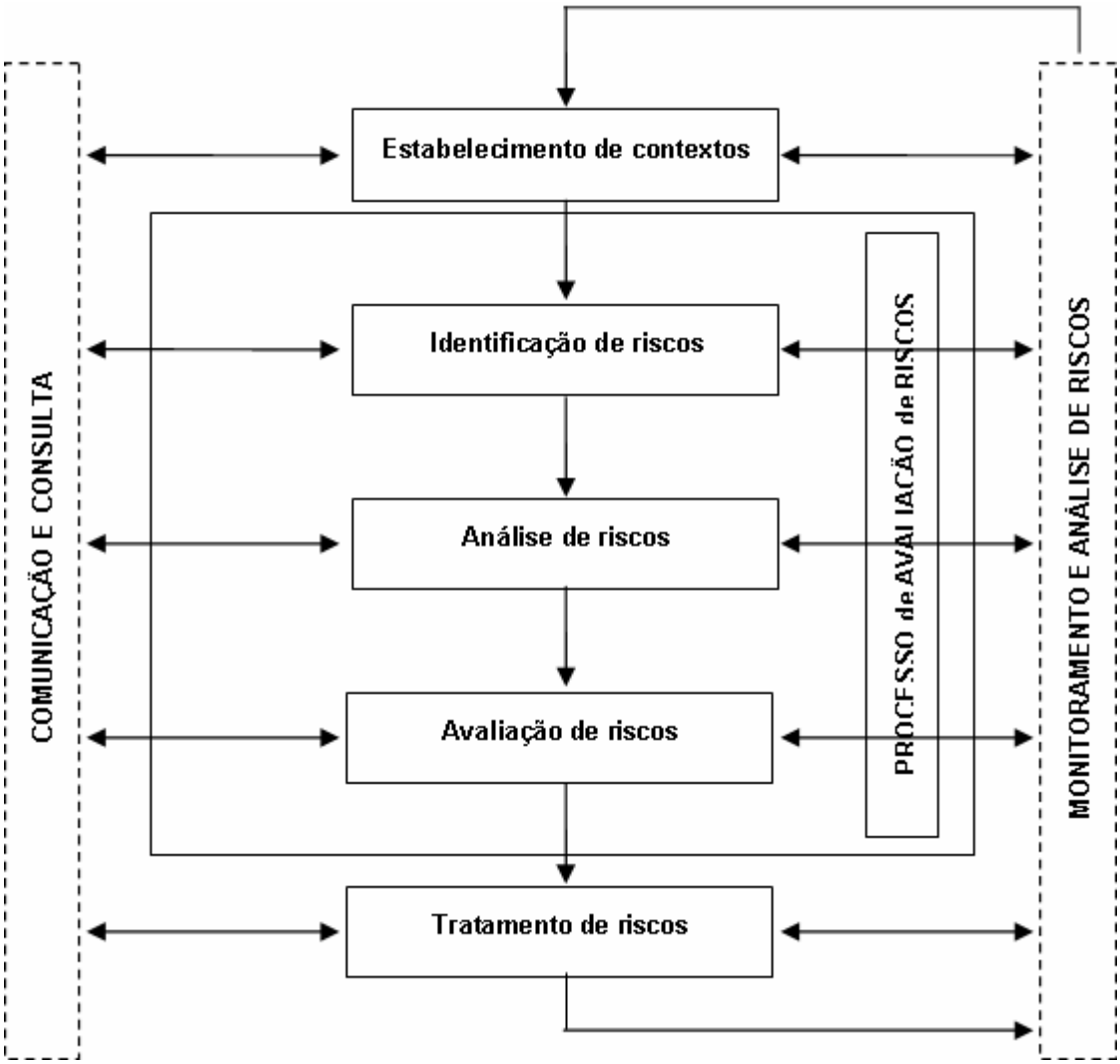


Figura 12 – Processo de Gestão de Risco
Fonte: Australian Standard for Risk Management (AS/NZS 4360:2004, p.12)

O estabelecimento de contexto consiste em identificar os riscos da organização, considerando o histórico de riscos. Neste ponto define-se o escopo da avaliação de riscos que será realizada, devendo observar os objetivos da organização, o ambiente, os critérios segundo os quais os riscos serão mensurados e a estruturação do processo de avaliação de riscos. (AUSTRALIAN STANDARD FOR RISK MANAGEMENT AS/NZS 4360:2004, p.21).

A identificação tem a finalidade de identificar os riscos e desenvolver uma lista abrangente de fontes de riscos e eventos que podem ter um impacto na consecução de cada um dos objetivos, devendo considerar, entre outros, fonte, evento, conseqüência, causa, controles, quando e onde pode ocorrer o risco. (AUSTRALIAN STANDARD FOR RISK MANAGEMENT AS/NZS 4360:2004, p.29).

De acordo com a norma NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (AS/NZS 4360:2004, p.32), a análise de risco visa promover o entendimento do nível de risco e de sua natureza. Deve ajudar a definir as prioridades e opções de tratamento do risco, ressaltando que essa análise permite expressar a combinação de dois componentes, conseqüência e probabilidade, que são os fatores que definem o risco.

A avaliação de riscos depende da compreensão que se tem dos riscos por meio da análise. Na avaliação deve ser decidido qual risco terá tratamento, qual atividade deve ser realizada e, principalmente, a prioridade do tratamento. Há que ser considerado ainda o impacto no risco, os efeitos cumulativos. Os critérios que subsidiam a avaliação de riscos devem ser definidos previamente pela alta direção e podem ser expressos quantitativa ou qualitativamente. Outro requisito é o risco tolerável. (AUSTRALIAN STANDARD FOR RISK MANAGEMENT AS/NZS 4360:2004, p.49-50).

O tratamento de risco considera a definição das prioridades e classificação estabelecidas. Nesse segmento, devem-se considerar as opções e planejamento de ações para tratar o risco, observando a legislação e normas específicas sobre o risco a ser tratado, verificando também as causas do surgimento do risco, tomando como base a causa-raiz, fatores que poderão influenciar na eficácia da medida de mitigação de risco e as conseqüências. (AUSTRALIAN STANDARD FOR RISK MANAGEMENT AS/NZS 4360:2004, p. 54).

O fato é que o risco é inerente a qualquer atividade, pode envolver perdas e oportunidades. Na questão da governança, o risco está associado a vários setores, mas o importante é conhecer e ter a capacidade de administrá-lo. A implantação de um modelo de Gestão de Risco Corporativo (GRC), segundo o Instituto Brasileiro de Governança Corporativa (IBGC, 2007, p. 8), traz alguns benefícios para a organização:

- Preserva e aumenta o valor da organização, mediante a redução da probabilidade de impacto de eventos de perdas no mercado;
- Promove maior transparência ao informar aos investidores e ao público em geral os riscos aos quais a organização está sujeita e as ações adotadas para mitigar;
- Melhora o padrão de governança mediante a explicitação dos riscos em consonância com o posicionamento com os acionistas e a cultura da organização.

2.6 Gestão da continuidade do negócio

A Gestão da Continuidade do Negócio (GCN) é complementar à análise de riscos. Busca entender os riscos às operações e aos negócios e suas conseqüências para evitar a interrupção da entrega dos serviços e produtos (NORMA BRASILEIRA NBR 25999-1:2007, p. 6).

Para melhor significar a GCN, a norma britânica BRITISH STANDARD (BS 25999-1:2006), Business Continuity Management (BCM), Part 1: Code of Practice, (p. 5), publicada pelo BRITISH STANDARD INSTITUTE (BSI), conceitua como "Apetite a Riscos", a "quantidade total de riscos que uma organização está preparada para aceitar, tolerar ou ser exposta a qualquer tempo". O foco da GCN é o serviço ou produto de que depende a organização para sobreviver, diante de um incidente que pode provocar dano à organização. Orienta sobre o que deve ser feito para proteger as pessoas, instalações, tecnologias, informações, cadeia de fornecimento, partes interessadas e reputação da organização (NORMA BRASILEIRA NBR 25999-1:2007, p. 6-7).

2.6.1 Abordagem geral da gestão da continuidade do negócio

A Gestão da Continuidade do Negócio, de acordo com a NBR 25999-1:2007 (p.6), é um processo da organização, movido por uma estrutura estratégica e operacional adequada para:

- Melhorar proativamente a resiliência da empresa contra possíveis interrupções de sua capacidade em atingir seus principais objetivos;
- Prover uma prática para restabelecer a capacidade da empresa em fornecer seus principais produtos e serviços, em níveis previamente acordados;
- Obter capacidade para gerenciar uma interrupção no negócio e proteger a imagem da empresa.

Para a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC

17799:2005, (p.103-104), a continuidade do negócio deve ser tratada como um processo de gestão que agrega as informações compatíveis com a gestão de riscos, no contexto dos riscos a que a organização está exposta, incluindo a identificação e priorização dos processos críticos do negócio, devendo dispor também de controles para identificar e reduzir riscos. Observa-se que a continuidade do negócio está alinhada à gestão de riscos para não pôr em risco o próprio processo de continuidade do negócio.

O INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC) entende que a Gestão da Continuidade do Negócio está associada à prevenção e redução de riscos de diversas origens e fontes, mas principalmente de riscos operacionais, residuais ou externos, identificados com base na análise de riscos e avaliação dos impactos. Para o Instituto, a gestão de riscos, no contexto da governança, deve estar sob a responsabilidade do conselho de administração que, por meio de um "Comitê de Riscos", deve institucionalizar o processo, cabendo ao comitê a discussão e a clara definição do "apetite a riscos" da organização e a orientação adequada a ser sugerida, emanada da alta administração (INSTITUTO BRASILEIRO DE GOVERNAÇA CORPORATIVA, 2007, p. 36-37).

É necessário ressaltar que a implementação da GCN está condicionada ao apoio e envolvimento da alta direção e partes interessadas, porque requer responsabilidades por meio de uma cadeia de comando (NORMA BRASILEIRA NBR 25999-1:2007, p. 5).

2.6.2 Conceitos de gestão da continuidade do negócio

A NORMA BRASILEIRA NBR 25999-1:2007 (p.1-3), que trata sobre a gestão da continuidade do negócio, parte 1: código de práticas, define alguns termos básicos aplicáveis ao escopo da Gestão da Continuidade do Negócio (GCN). Aqui serão citados os que contribuem para melhor explicitar a prática, conforme a seguir:

- continuidade do negócio: "capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções do negócio para conseguir continuar suas operações em um nível aceitável, previamente definido";

- gestão da continuidade do negócio (GCN): “processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos as operações do negócio caso essas ameaças se concretizem”;
- impacto: “conseqüência avaliada de um evento em particular”.

Para a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 (p.103), a GCN é um processo que visa minimizar um impacto sobre a organização e recuperar perdas de ativos da informação, que podem ser resultantes de desastres naturais, acidentes, falhas de equipamentos e ações intencionais.

O objetivo da continuidade do negócio é evitar a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, garantindo a retomada das atividades em tempo hábil (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - NBR ISO/IEC 17799:2005, p.103). Recomenda a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 (p.103) que um processo de Gestão de Continuidade do Negócio (GCN) contemple os requisitos de segurança necessários ao tipo de impacto.

2.6.3 Estrutura da gestão da continuidade do negócio

A adoção de um modelo de Plano de Continuidade do Negócio (PCN) deve partir de uma política que tenha abrangência apropriada à natureza, escala, complexidade, geografia e criticidade das atividades do negócio da empresa, devendo refletir sua cultura. Nesse contexto, a função governança também é um atributo, pois depende da alta direção a designação de responsabilidade, a partir de seu apoio. De acordo com a NORMA BRASILEIRA NBR 25999-1:2007 (p. 11-15), um PCN deve dispor de documentação que inclua as seguintes etapas:

- política, contendo a declaração do escopo e termos de referência;
- análise de impacto nos negócios;
- avaliação de riscos e ameaças;
- estratégias do Plano de Continuidade do Negócio;

- programa de conscientização;
- programa de treinamento;
- plano de gerenciamento de incidentes;
- plano de continuidade do negócio;
- plano de recuperação do negócio;
- agenda de testes e relatórios;
- contratos e acordos de níveis de serviço.

A ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 (p.103-104) recomenda que um processo de gestão da continuidade do negócio deve adotar, entre outras, as seguintes premissas:

- Entender os riscos a que a organização está exposta, considerando a probabilidade de ocorrência e o impacto no negócio;
- Determinar todos os ativos envolvidos em processos críticos do negócio;
- Identificar e implementar controles preventivos e de mitigação;
- Garantir a segurança das pessoas e a proteção dos recursos de processamento das informações e bens;
- Definir a documentação dos planos de continuidade, contendo os requisitos de segurança e o pessoal envolvido treinado, de acordo com a especialização;
- Assegurar que a gestão de continuidade do negócio seja incorporada aos processos da organização.

O processo de Business Continuity Management (BCM), de acordo com a norma BRITISH STANDARD (BS 25999-1:2006, p.6), tem o propósito de estabelecer uma estrutura estratégica e operacional adequada para:

- Melhorar proativamente a resiliência da organização contra possíveis interrupções de sua capacidade em atingir seus objetivos;
- Prover uma prática para restabelecer a capacidade de uma organização fornecer seus principais produtos e serviços, em um nível previamente acordado, dentro de um tempo previamente determinado após a interrupção;
- Obter reconhecida capacidade de gerenciar uma interrupção no negócio de forma a proteger a marca e a reputação da organização.

A BRITISH STANDARD (BS 25999-1:2006, p. 9) estabelece o ciclo de vida de um processo de BCM (THE BUSINESS CONTINUITY MANAGEMENT LIFECYCLO, FIGURE 1, p. 9) que pode ser implementado em qualquer setor organizacional, seja público ou privado, empresa pequena, média ou de grande porte. O que varia é o escopo e a estrutura, dependendo da organização; entretanto, os elementos identificados na Figura 13 são fundamentais e, portanto, obrigatórios. Cada um dos elementos, de acordo com a BS 25999-1:2006 (p.8-10), tem o seguinte valor:

- A gestão do Business Continuity Management (BCM) possibilita manter a continuidade do negócio de forma apropriada a seu tamanho e a sua complexidade;
- Entender a organização significa obter as informações que propiciam a priorização dos produtos e serviços e a urgência das atividades que são necessárias para mantê-los;
- Determinar a estratégia permite que uma resposta apropriada seja escolhida para cada produto ou serviço, de forma que haja continuidade dos serviços em nível e quantidade operacional aceitáveis, durante uma interrupção;
- Desenvolver e implementar uma resposta resulta em uma estrutura de gestão e de resposta a incidentes, continuidade do negócio e planos de recuperação, com detalhamento de todos os passos a serem tomados durante e depois de um incidente;
- Testar, manter, revisar e auditar demonstra a capacidade da organização quanto à maturidade de suas estratégias e planos a fim de identificar oportunidades de melhoria;

O BUSINESS CONTINUITY MANAGEMENT (BCM), na cultura da organização, permite que a gestão da continuidade se torne parte do valor da organização, dando confiança às partes interessadas quanto à capacidade de sobreviver a interrupções. A figura 13 apresenta o fluxo do ciclo de vida da gestão de continuidade do negócio.

Figura 13 – Ciclo de vida da gestão da continuidade do negócio
Fonte: BRITISH STANDARD (BS 25999-1:2006, p. 9)

Adicionalmente, a norma AUSTRALIAN STANDARD FOR RISK MANAGEMENT (AS/NZS 4360:2004, p. 58-60) considera que a gestão da continuidade do negócio proporciona à organização a capacidade de continuar a operar, de forma sustentável, diante das interrupções adversas.

O desenvolvimento e implantação de um modelo de gestão da continuidade do negócio, adequado e ajustado aos objetivos e missão da empresa, é importante porque desenvolve, segundo a NORMA BRASILEIRA (NBR 25999-1:2007, p. 7), a capacidade de identificar e agir proativamente sobre os impactos de uma interrupção, de gerenciar os riscos que não podem ser segurados e de se apresentar com vantagem competitiva por ter a capacidade de manter a entrega dos serviços diante de adversidades.

3. METODOLOGIA DA PESQUISA

Este capítulo apresenta a caracterização, o delineamento da pesquisa, da amostra, a construção dos questionários, a aplicação e o método estatístico para consolidar os dados e a análise dos dados.

3.1 Caracterização da pesquisa

De acordo com Marconi e Lakatos (2006, p. 43), a pesquisa é um procedimento formal com método de pensamento e constitui o caminho para se conhecer a realidade ou para descobrir verdades parciais.

O método de investigar respalda-se em técnicas para a obtenção dos propósitos. Com esse direcionamento, a coleta de dados foi realizada por meio de questionário, constituído de uma série de afirmações que foram mantidas, negadas ou complementadas pelos respondentes, correspondendo à observação direta extensiva. A fim de auxiliar na análise, interpretação e explicitação da coleta de dados, foi utilizado o método de procedimento estatístico (MARCONI e LAKATOS, 2006, p.106-107).

Para tratar o problema da pesquisa: **Qual é a real percepção dos gerentes executivos sobre a segurança da informação no âmbito de seu segmento de atuação?** no contexto de uma organização de alta tecnologia de informação e comunicações, que dispõe de um processo de segurança da informação, política de segurança e controles baseados em análise das ameaças, vulnerabilidades, impactos e requisitos legais, a opção foi adotar o método da pesquisa qualitativa, com uso de questionário como meio de auxiliar na identificação do conhecimento e da percepção dos líderes da organização sobre uma área de vital importância para o negócio da Empresa, que é a segurança da informação.

A pesquisa qualitativa revela nos padrões de resposta as áreas de consenso tanto

positivo quanto negativo, proporcionando ainda ao pesquisador a oportunidade da imersão no contexto e perspectiva interpretativa de condução da pesquisa, segundo Kaplan & Duchon, 1988, apud Moresi, 2004, p. 71-73.

3.2 A amostra

A amostra da pesquisa foi restrita a 29 (vinte e nove) empregados da Empresa, que representam o universo dos principais líderes da linha de comando da estrutura organizacional. Na prática, são ocupantes de cargos de superintendência que, adicionados à diretoria, formam a diretoria ampliada. São profissionais de carreira, que dispõem de conhecimentos estratégicos e táticos sobre o negócio da organização, especialmente do segmento sob sua responsabilidade. Dessa forma, contribuem com sua experiência em áreas especializadas e necessárias à cultura da organização e, por conseguinte, à cultura de segurança. Os cargos gerenciais da principal linha de comando da estrutura organizacional são os seguintes:

- Auditor Geral, subordinado ao Conselho Diretor, o segundo nível na hierarquia organizacional da Empresa;
- Consultor Jurídico e Gabinete do Diretor-Presidente, subordinados ao Diretor-Presidente, ocupantes do quarto nível na hierarquia organizacional, ocupantes de cargo de Consultoria e Apoio. São responsáveis pela assessoria direta ao Diretor-Presidente e à diretoria;
- Unidades de Alinhamento Estratégico, subordinadas diretamente ao Diretor–Presidente, ocupantes do quarto nível na hierarquia organizacional, com a responsabilidade de formular os procedimentos necessários à implementação do modelo conceitual de organização e de gestão. Compõem a Unidade os seguintes segmentos de conhecimento: segurança da informação, tecnologia de informação, planejamento, orçamento, pessoas, marketing e projetos;
- Unidades de Relacionamento com Clientes, subordinadas a uma diretoria especifica, ocupantes do quinto nível na hierarquia organizacional, responsáveis pelo

relacionamento com os clientes e comercialização dos produtos e serviços da Empresa. Compõem a Unidade os seguintes segmentos de clientes: administração financeira, administração tributária, comércio exterior, gestão do Ministério da Fazenda, Planejamento, Orçamento e Gestão, Negócios estratégicos, serviços especiais, sistemas processuais;

- Unidades de Produtos e Serviços, subordinadas a uma diretoria especifica, ocupantes do quinto nível na hierarquia organizacional, responsáveis pela gestão do ciclo produtivo dos produtos e serviços comuns à Empresa. Compõem a Unidade os seguintes segmentos: Soluções de desenvolvimento, centro de dados, gerência de serviços, rede, sistemas corporativos e administração de ambientes de tecnologia da informação;
- Unidades de Gestão empresarial, subordinadas a uma diretoria especifica, ocupantes do quinto nível na hierarquia organizacional, responsáveis pelas atividades de apoio à gestão empresarial. Compõem a Unidade os seguintes segmentos: gestão financeira, aquisição e contratos, pessoas, logísticas.

O delineamento da pesquisa qualitativa, de acordo com a própria metodologia, visou identificar por meio de respostas das lideranças por segmentos do negócio o nível de aderência da gestão da segurança da informação, considerando, sobretudo, processos que são de subsistência para o negócio da empresa, assim como para a continuidade do negócio.

3.3 A construção do questionário da pesquisa

A fim de coletar os dados, de acordo com o problema da pesquisa, foi construído um questionário com temas específicos sobre a governança da segurança da informação e a segurança da informação. O critério de construção das questões da pesquisa foi documental, com base nos autores citados no Referencial Teórico e a norma ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005, tendo ocorrido em quatro etapas:

- Primeira etapa - foram selecionadas questões sobre o que os diretores e gerentes de alto nível deviam entender a respeito da segurança da informação, como a organização tratava as questões de segurança em relação à segurança do negócio, se a segurança estava alinhada às metas e objetivos da organização, se havia cultura de segurança, se existia direcionamento estratégico de segurança e quanto estava alinhado ao negócio, se o processo de gestão de risco estava consolidado ao negócio, se existia processo de gestão de continuidade do negócio, integração da gestão dos recursos com as prioridades de segurança, retorno dos investimentos em segurança, pessoas preparadas para atuar no segmento de segurança e outras afirmações afins;
- Segunda etapa - as observações e recomendações sobre cada um dos itens acima enumerados foram transformadas em afirmativas, com o objetivo de que o pesquisado, identificando-se ou não com a situação, se posicionasse de acordo com a situação real de sua linha do negócio. Ainda nessa etapa, houve a seleção dos assuntos por item de controle de segurança, de acordo com a norma ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005 e o tema governança da segurança da informação. Os conceitos sobre os temas foram extraídos da referida norma;
- Terceira etapa - consistiu em validar os itens da pesquisa. Foram convidadas pessoas da área de segurança da informação e certificados como auditor líder, conforme a norma BRITISH STANDARD (BS 7799-2) para fazer a análise de conteúdo, identificação das inconsistências, clareza, simplicidade e objetividade das questões e também para medir o tempo de resposta da pesquisa, que foi avaliado em 30 (trinta) minutos, em média;
- Quarta etapa - foi a consolidação das críticas e sugestões, revisão do texto e impressão dos formulários. Foram no total 40 (quarenta) questões, de múltipla escolha ou única escolha, permitidos comentários que de alguma forma pudessem contribuir com as respostas, de modo a motivar resposta para todas as questões. As 40 questões foram distribuídas em 6 seções: governança e gestão, segurança em recursos humanos, planejamento, gestão de incidentes, continuidade do negócio e conformidade. A primeira página da pesquisa foi construída com os seguintes itens:

- Apresentação, explicitando o objetivo da pesquisa, universo pesquisado e o porquê, a importância da colaboração em responder e o compromisso de não-revelação da identidade dos pesquisados;
- Instruções de preenchimento, contendo informações básicas sobre o preenchimento, explicitação de que não haveria respostas certas ou erradas, mas as que melhor expressassem a realidade da área do pesquisado, tempo de preenchimento e prazo de resposta. Foi estabelecido o prazo de 5 dias úteis para que os pesquisados respondessem a pesquisa.

A distribuição da pesquisa foi precedida de uma correspondência formal pelo segmento Gestão de Pessoas, Universidade Corporativa do Serpro – UniSerpro, responsável pelo processo de treinamento, correspondência dirigida a todas as pessoas que faziam parte do universo a ser pesquisado. Os questionários da pesquisa foram entregues pessoalmente pela pesquisadora a cada uma das pessoas, com uma breve explanação sobre o tema da pesquisa, sua relevância, conteúdo e importância da cooperação e agradecimento prévio pela atenção e colaboração. Ressalte-se que a receptividade foi muito positiva, inclusive a manifestação do desejo em conhecer o resultado final do trabalho.

3.4 A coleta de dados

A coleta de dados, após a distribuição dos questionários da pesquisa, ocorreu formalmente durante o período de 23 a 27 de abril. Entretanto, em virtude de solicitações verbais, o prazo foi estendido até 04 de maio de 2007. As justificativas alegadas foram compromissos assumidos com clientes e viagens a serviço. O fato ocorreu com 5 pesquisados, dos quais dois não entregaram a pesquisa.

Dos 29 questionários distribuídos, dois não foram devolvidos, resultando que a amostra tivesse 27 respondentes. Após o recebimento das pesquisas, a pesquisadora enviou formalmente, por meio do correio corporativo da Empresa, uma nota de agradecimento a todos que responderam ao questionário. O resultado da avaliação sobre a aceitação dos

pesquisados considerou que a receptividade foi muito boa.

As críticas apresentadas pelos pesquisados sobre a formulação das questões foram relativas aos itens de múltipla escolha pois, em alguns casos, segundo alguns, as melhores opções seriam quanto à aplicabilidade – “aplico, não aplico” - pois melhor explicitariam a realidade.

Para garantir a segurança dos dados coletados, foram copiados os 27 questionários da pesquisa, uma vez que os dados foram digitados em banco de dados preparado para a coleta e tratamento desses dados.

3.5 O modelo estatístico da pesquisa

Uma vez determinada a amostra, esta foi direcionada e se constituiu de 27 respondentes, empregados da empresa, conforme citado acima. Embora tenha havido abstração da teoria probabilística para determinação dos parâmetros amostrais, não houve comprometimento teórico do modelo, tendo em vista que, em função do tema abordado e a necessidade de não ocorrer um deslocamento das respostas com a visão estratégica da Empresa, foi definido que os respondentes deveriam ser pessoas ocupantes de cargos de relevância dentro do processo decisório, a fim de dar credibilidade aos resultados.

Diante disto, é importante explicitar a posição da amostra diante dos conceitos formulados para a pesquisa:

- População: conjunto de indivíduos que participam da gestão estratégica da empresa e podem interferir no processo decisório por meio de decisões que possam tomar, no uso de suas atribuições como líderes;
- Grupo: conjunto de indivíduos ligados ao processo de amostragem e que foi selecionado na população da empresa, portanto, são os respondentes.

Assim, o ponto central da análise está direcionado para o grupo de pessoas que pode influenciar o direcionamento estratégico da empresa no que concerne ao tema –

Segurança da Informação, no âmbito da gestão e governança.

Utilizou-se o modelo de estatística descritiva, de acordo com Marconi e Lakatos (2006, p.109), que consistiu na tabulação dos dados por meio de freqüência e percentagens das respostas obtidas e apresentação dos dados por meio de uma série de quadros e gráficos. Assim, as variáveis estudadas foram consideradas como discretas, categóricas e não-paramétricas, observando-se os seguintes critérios:

- A representação numérica de cada questão está representada por meio de uma matriz, sendo as linhas os itens de cada questão e as colunas os 5 segmentos de atuação da Empresa e sua visão;
- O preenchimento da matriz foi feito por meio da totalização de cada item dentro de cada segmento, conforme a Tabela 1, onde a Matriz de Resposta é formada pela freqüência de resposta em cada item de uma determinada questão e de um determinado segmento. Assim, x_{ij} representa a freqüência das respostas do segmento *j*, referente à questão Q_i. A fórmula observada foi a seguinte:

$$t_i = \sum_{j=1}^{5} x_{ij}$$

Nesse contexto, a pesquisa objetivou identificar a percepção de cada um dos pesquisados, no âmbito de cada segmento, considerando os seguintes temas: governança e gestão, segurança em recursos humanos, planejamento, gestão de incidentes, continuidade do negócio e conformidade.

Tabela 1 – Matriz de Resposta

Questão	**URC**	**UPS**	**UGE**	**UAE**	**Apoio**	**Serpro**
Q_1	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	t_1
Q_2	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	t_2
Q_3	x_{31}	x_{32}	x_{33}	x_{34}	x_{35}	t_3
Q_n	x_{n1}	x_{n2}	x_{n3}	x_{n4}	x_{n5}	t_n
					Total Geral	*total*

4. RESULTADOS DA PESQUISA: INTERPRETAÇÃO E ANÁLISE DOS DADOS

Neste capítulo será mostrado o resultado da pesquisa oriundo da interpretação e da análise dos dados coletados. A interpretação consiste em apresentar os dados coletados, e a análise é complementar à interpretação dos dados, estabelecendo o relacionamento com o referencial teórico no que couber, sob a perspectiva da governança da segurança da informação.

4.1 Interpretação dos dados

4.1.1 Visão geral da alta liderança

A amostra da pesquisa foi direcionada a ocupantes de cargo de gerência nível estratégico. Trata-se de grupo gerencial localizado hierarquicamente entre o nível de diretoria e o nível gerencial tático, conforme descrito anteriormente.

Atualmente a gerência de nível estratégico no Serpro é composta por 29 cargos, e os questionários foram entregues pessoalmente a cada um dos respondentes. Destes, 27 responderam, apresentando um percentual de participação de 93%, conforme a Tabela 2.

Tabela 2 – Gerentes que responderam à pesquisa

Gerentes estratégicos	Nº. de empregados	Nº. de respondentes	% de respostas
Nível superintendente	29	27	93%

Fonte: Pesquisa acadêmica da autora

Relativamente ao tempo de serviço dessas pessoas na Empresa, dados internos da área de Gestão de Pessoas indicam que a média de tempo de serviço dos empregados que ocupam função de liderança estratégica é 24 anos, sendo no mínimo 10 e no máximo 34

anos.

Para complementar a análise dos dados funcionais, foram lançados nessa seção sobre a visão geral da alta liderança os resultados das questões 15 e 22, pertencentes ao segmento Segurança em Recursos Humanos.

A **Questão 15** buscou identificar a quantidade de pessoas lotadas em cada segmento organizacional, obtendo os seguintes resultados: as áreas de maior contingente de pessoas internas, lotadas nas dependências da Empresa, são respectivamente, a Unidade de Produto e Serviço (UPS), com 3.180 empregados (46%), a Unidade de Relacionamento com Cliente (URC), com 2427 (36%), a Unidade de Gestão Empresarial (UGE), com 1.011 (15%), a Consultoria e Apoio (APOIO), com 124 (2%) e a Unidade de Alinhamento Estratégico (UAE), com 39 (1%), perfazendo um total de 6.781 empregados, conforme mostrado no Gráfico 1.

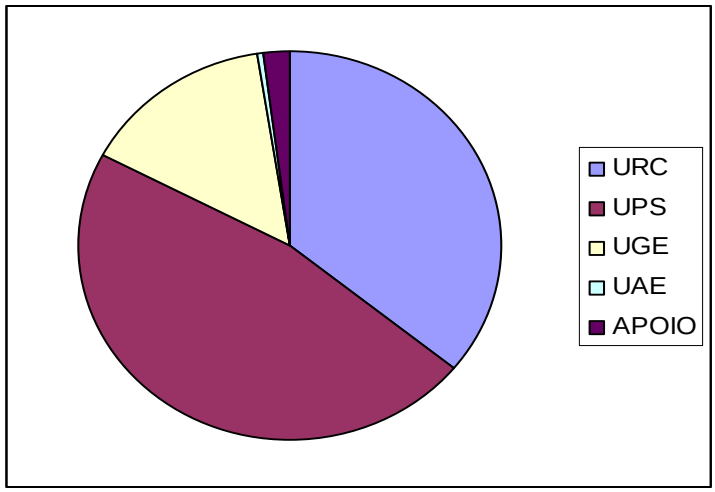


Gráfico 1: Percentagem de Recursos Humanos, por segmento
Fonte: Demonstrativo da área de gestão de pessoas do Serpro

Ressalta-se que nos segmentos de maior contingente de recursos humanos apresentam-se as seguintes características:

- Unidades de Produtos e Serviços (UPS): concentram-se as atividades responsáveis pela operacionalização e efetivação dos itens de segurança relacionados à rede Internet e intranet para atendimento a clientes e internos, centro de dados, análise e homologação de ferramentas para operacionalização de produtos e serviços, principalmente no que se refere a teste de invasão em códigos, visando ao código

seguro nos produtos e aplicativos.

- Unidades de Relacionamento com Cliente (URC): responsáveis pela negociação, desenvolvimento e entrega de serviços e produtos a clientes. São das mais populosas em Recursos Humanos. Neste segmento organizacional a segurança deve ser elemento intrínseco ao negócio, pois a partir da análise de requisitos, o serviço contratado, a entrega e uso devem ser revestidos de requisitos de segurança, acordados em níveis de serviços contratados.
- Unidades de Gestão Empresarial (UGE): são responsáveis pelas atividades de apoio empresarial. Neste segmento encontram-se as funções que são fundamentais para o negócio como a gestão dos recursos elétricos, considerado um dos itens de criticidade no contexto da segurança e da continuidade do negócio. Há também as atividades relacionadas com o disciplinamento do acesso a locais sensíveis e críticos. Ainda compõem esse segmento a gestão financeira, a gestão dos contratos, a gestão das pessoas e o relacionamento com mercado e promoção dos negócios.
- Unidades que apresentaram menor contingente de recursos humanos, UAE e Apoio: são áreas de segmento estratégico, direcionador das estratégias do negócio, lançando diretrizes e variáveis de controle do negócio, onde se insere a gestão da segurança da informação.

A **Questão 22** teve como objetivo identificar se nos últimos 12 meses houve participação desse grupo de gerentes em algum programa de treinamento, visando ao conhecimento voltado para sua Unidade, sobre a segurança da informação. O resultado encontrado foi: 7 gerentes estratégicos da URC (26%) participaram, 6 da UPS (22%), 4 da UGE (15%), 7 da UAE (26%) e 3 do Apoio (11%), conforme o Gráfico 2.

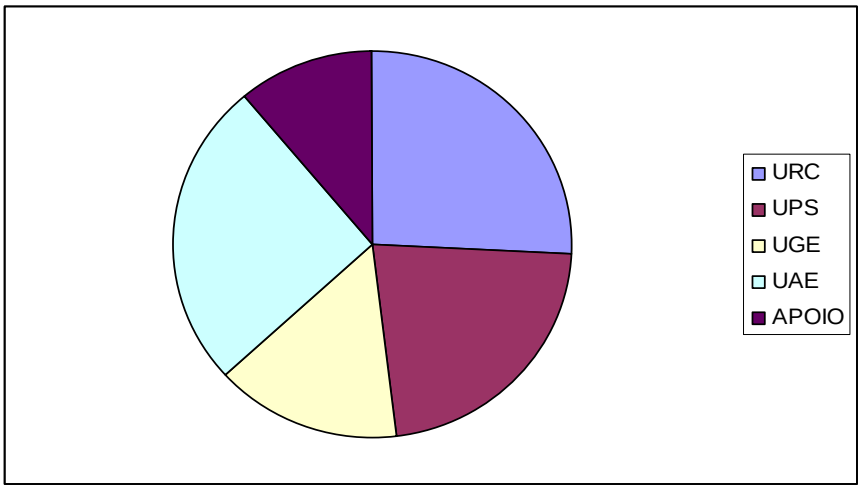


Gráfico 2: Participação dos gerentes em treinamento em segurança
Fonte: Dados da pesquisa acadêmica da autora

O resultado indicou que nos últimos doze meses nenhum segmento teve participação expressiva em treinamento sobre a segurança da informação no contexto de sua área de atuação, suscitando a necessidade de a empresa investir mais em treinamento dos gerentes estratégicos.

4.1.2 Governança e gestão

A seção Governança e Gestão buscou identificar, por meio da pesquisa, quais as funções de segurança existentes em cada um dos segmentos pesquisados, considerando os itens explicitados no questionário e outros não contemplados, mas relatados pelos respondentes, compõem cada um dos segmentos organizacionais. Também verificou o nível em que se encontram itens fundamentais num processo de governança ou de gestão da segurança da informação, sob a ótica dos líderes principais da linha de comando da estrutura organizacional, tais como:

- Qual o apoio ou comprometimento da alta direção com a segurança;
- A segurança adotada na organização tem sido ou não suficiente para proteger patrocinadores, clientes, empregados e fornecedores de acordo com as expectativas da Unidade;
- Qual o nível de importância de cada unidade pesquisada em relação à segurança da

informação para o sucesso do negócio;

- Quanto a segurança adotada nos processos sob a responsabilidade de cada unidade pesquisada contribui para que a organização garanta e sustente um nível previsível, aceitável e adequado de segurança compatível com a missão do negócio.
- Quanto os contratos que determinam responsabilidade das partes (empresa, clientes, empregados e fornecedores) garantem a confidencialidade, integridade e disponibilidade do negócio contratado;
- Quanto o processo de gestão de riscos do negócio favorece ações proativas para manter o risco em níveis aceitáveis;
- Quanto a revisão periódica dos processos de segurança por meio da gestão de risco é fundamental para garantir a sustentação da continuidade do negócio, adequabilidade e efetividade da segurança;
- Quanto os controles de segurança utilizados são adequados e incluem os documentos de política, a atribuição de responsabilidade, o processamento correto nas aplicações, a gestão de vulnerabilidade técnica, a gestão da continuidade do negócio e a gestão de incidentes de segurança da informação e melhorias;
- Quanto a segurança da informação faz parte da cultura da organização; se existe respeito às regras e ações de segurança em todos os processos do negócio, nos níveis gerenciais estratégico, tático e operacional.
- Quanto a gestão da continuidade do negócio é institucionalizada, faz parte da cultura da organização e inclui controles para identificar e reduzir riscos, protegendo os processos críticos contra falhas ou desastres significativos;
- Quanto os processos críticos estão protegidos contra ameaças que interferem na confidencialidade, integridade e disponibilidade dos serviços.
- Quanto o processo de recuperação de desastre para atendimento em níveis de serviço contratados pelo cliente está institucionalizado ou garantido.
- Qual o nível de certeza de que a segurança aplicada ao negócio tem sido suficiente para detectar e prevenir incidentes de segurança.

A primeira questão da pesquisa buscou identificar as funções de governança da segurança da informação que ocorrem no âmbito de cada segmento pesquisado e aquelas que apresentaram maior freqüência no cômputo geral. O resultado geral é apresentado na Tabela 3.

O resultado da pesquisa mostrou que a maioria das atividades inerentes à governança da segurança da informação ocorre na maior parte dos segmentos pesquisados, excetuando-se a UPS e Apoio. No primeiro não existem as atividades "Proteção de propriedade intelectual" e "Desenvolvimento e manutenção de sistemas de informação". Na segunda, não existem as atividades de "Gestão de incidentes", "Segurança de rede" e "Desenvolvimento e manutenção de sistemas de informação".

Observou-se, entretanto, que, de acordo com as características e objetivos de determinados segmentos, ocorre uma variação das atividades que são inerentes ou não. A observação torna-se clara ao analisar cada quadro, a seguir apresentado, que pontua as atividades no formato de sua importância dentro de seu segmento.

Tabela 3 – Ocorrência de funções de governança da segurança da informação, por segmento

Questão 1: Escopo da Governança - Quais das funções abaixo existem em sua Unidade? Marque todas as aplicáveis.

Itens	URC	UPS	UGE	UAE	Apoio
Planejamento e estratégia de segurança para serviços de Cliente	42%	25%	8%	17%	8%
Gestão da segurança em ambiente de TI	21%	36%	14%	21%	7%
Implementação de segurança em serviços de clientes	33%	33%	13%	13%	7%
Gestão da segurança para proteção de dados e informação	16%	32%	21%	21%	11%
Gestão de segurança física e do ambiente	8%	23%	23%	31%	15%
Controle de acesso	26%	26%	16%	16%	16%
Gestão da continuidade do negócio	29%	29%	7%	29%	7%
Gestão de Recursos Humanos	32%	18%	18%	18%	14%
Gestão de incidentes	25%	42%	17%	17%	0%
Proteção de propriedade intelectual	13%	0%	25%	50%	13%
Segurança de rede	11%	33%	11%	44%	0%
Desenvolvimento e manutenção de sistemas de informação	100%	14%	21%	14%	0%
Gestão de contratos de serviços	37%	26%	21%	5%	11%
Gestão financeira	23%	8%	31%	31%	8%
Nenhum dos itens	0%	0%	0%	0%	0%
Outros	0%	0%	0%	0%	0%
Total	27%	25%	18%	21%	9%

Fonte: Dados da pesquisa acadêmica da autora

Registra-se ainda que existem atividades que foram relacionadas por determinados segmentos, mas que não fazem parte de seu elenco de atribuições. Citam-se, como exemplo, neste contexto, as atividades de gestão de rede, desenvolvimento e manutenção

de sistemas de informação e gestão da segurança em ambiente de TI. Por outro lado, a atividade “Proteção de propriedade intelectual” deveria aparecer em todos os segmentos, com maior ou menor pontuação, de acordo com o envolvimento e classificação dos dados sob a responsabilidade do segmento.

A seguir, será apresentado o Quadro 5 contendo o resultado das ocorrências da função governança nas diversas áreas pesquisadas. O objetivo foi verificar se no cotidiano das atividades de gestão da segurança da informação, conhecidas e exercitadas pela alta gerência, há aderência com as atividades de governança. Foram oferecidos 14 (quatorze) itens sobre o tema governança e cada gerente, no âmbito de seus segmentos, assinalou as funções que observam ocorrer.

Quadro 5: Resultado funções de governança da segurança da informação, por segmento

Funções	**URC**	**UPS**	**UGE**	**UAE**	**Apoio**
Planejamento e estratégia de segurança para serviços de Cliente	•	•	•	•	•
Gestão da segurança em ambiente de TI	•	•	•	•	•
Implementação de segurança em serviços de clientes	•	•	•	•	•
Gestão da segurança para proteção de dados e informação	•	•	•	•	•
Gestão de segurança física e do ambiente	•	•	•	•	•
Controle de acesso	•	•	•	•	•
Gestão da continuidade do negócio	•	•	•	•	•
Gestão de Recursos Humanos	•	•	•	•	•
Gestão de incidentes	•	•	•	•	-
Proteção de propriedade intelectual	•	-	•	•	•
Segurança de rede	•	•	•	•	-
Desenvolvimento e manutenção de sistemas de informação	•	•	•	•	-
Gestão de contratos de serviços	•	•	•	•	•
Gestão financeira	•	•	•	•	•

Fonte: Dados da pesquisa acadêmica da autora

Na seqüência do resultado da pesquisa, serão apresentados em cinco tabelas, por segmento, os valores percentuais sobre como percebem os gerentes o exercício de cada item ou função inerente a governança. Observa-se que a Tabela 4, Unidade de Relacionamento com Cliente, foi unânime (100%) quanto à função Desenvolvimento e Manutenção de Sistemas de Informação. Os demais itens apresentam valores menos significativos.

Tabela 4: Unidade de Relacionamento com Clientes (URC)

Desenvolvimento e manutenção de sistemas de informação	100%
Planejamento e estratégia de segurança para serviços de Cliente	42%
Gestão de contratos de serviços	37%
Implementação de segurança em serviços de clientes	33%
Gestão de recursos humanos	32%
Gestão da continuidade do negócio	29%
Controle de acesso	26%
Gestão de incidentes	25%
Gestão financeira	23%
Gestão da segurança em ambiente de TI	21%
Gestão da segurança para proteção de dados e informação	16%
Proteção de propriedade intelectual	13%
Gestão de segurança física e do ambiente	8%

Fonte: Dados da pesquisa acadêmica da autora

A Tabela 5, Unidade de Produto e Serviço apresentou o item Gestão de Incidentes com 42% de ocorrência, significando que a função seria de maior relevância no contexto do segmento UPS. Os demais itens apresentam valores menos significativos

Tabela 5: Unidade de Produto e Serviço (UPS)

Gestão de incidentes	42%
Gestão da segurança em ambiente de TI	36%
Implementação de segurança em serviços de clientes	33%
Segurança de rede	33%
Gestão da segurança para proteção de dados e informação.	32%
Gestão da continuidade do negócio	29%
Gestão de contratos de serviços	26%
Controle de acesso	26%
Planejamento e estratégia de segurança para serviços de Cliente	25%
Gestão de segurança física e do ambiente	23%
Gestão de recursos humanos	18%
Desenvolvimento e manutenção de sistemas de informação	14%
Gestão financeira	8%
Proteção de propriedade intelectual	0%

Fonte: Dados da pesquisa acadêmica da autora

A Tabela 6, Unidade de Gestão Empresarial apresentou o item Gestão Financeira com 31% de ocorrência, significando que a função seria de maior relevância no contexto do segmento UGE. Os demais itens apresentam valores menos significativos.

Tabela 6: Unidade de Gestão Empresarial (UGE)

Gestão financeira	31%
Proteção de propriedade intelectual	25%
Gestão de segurança física e do ambiente	23%
Desenvolvimento e manutenção de sistemas de informação	21%
Gestão de contratos de serviços	21%
Gestão da segurança para proteção de dados e informação	21%
Gestão de Recursos Humanos	18%
Gestão de incidentes	17%
Controle de acesso	16%
Gestão da segurança em ambiente de TI	14%
Implementação de segurança em serviços de clientes	13%
Segurança de rede	11%
Planejamento e estratégia de segurança para serviços de Cliente	8%
Gestão da continuidade do negócio	7%

A Tabela 7, Unidade de Alinhamento Estratégico apresentou o item proteção de propriedade intelectual com 50% de ocorrência. Os demais itens apresentam valores menos significativos.

Tabela 7: Unidade de Alinhamento Estratégico (UAE)

Proteção de propriedade intelectual.	50%
Segurança de rede	44%
Gestão de segurança física e do ambiente.	31%
Gestão financeira	31%
Gestão da continuidade do negócio	29%
Gestão da segurança em ambiente de TI	21%
Gestão da segurança para proteção de dados e informação	21%
Gestão de Recursos Humanos	18%
Planejamento e estratégia de segurança para serviços de Cliente	17%
Gestão de incidentes	17%
Controle de acesso	16%
Desenvolvimento e manutenção de sistemas de informação	14%
Implementação de segurança em serviços de clientes	13%
Gestão de contratos de serviços	5%

Fonte: Dados da pesquisa acadêmica da autora

A Tabela 8, Consultoria e Apoio, apresentou valores menos significativos sobre o exercício de atividades relacionadas a governança.

Tabela 8: Consultoria e Apoio

Controle de acesso	16%
Gestão de segurança física e do ambiente	15%
Gestão de Recursos Humanos	14%
Proteção de propriedade intelectual	13%
Gestão da segurança para proteção de dados e informação	11%
Gestão de contratos de serviços	11%
Planejamento e estratégia de segurança para serviços de Cliente	8%
Gestão financeira	8%
Gestão da segurança em ambiente de TI.	7%
Implementação de segurança em serviços de clientes.	7%
Gestão da continuidade do negócio	7%
Gestão de incidentes	0%
Segurança de rede	0%
Desenvolvimento e manutenção de sistemas de informação	0%

Fonte: Dados da pesquisa acadêmica da autora

A **Questão 2** buscou verificar como os gerentes estratégicos percebem o apoio da alta direção – diretores, diretor-presidente, diretor-superintendente, conselho diretor e conselho fiscal, nos negócios de segurança. O resultado foi: 55% consideraram médio o apoio da alta direção nos negócios de segurança, 41% consideraram suficiente e 4% consideraram insuficiente o apoio, conforme mostrado no Gráfico 3.

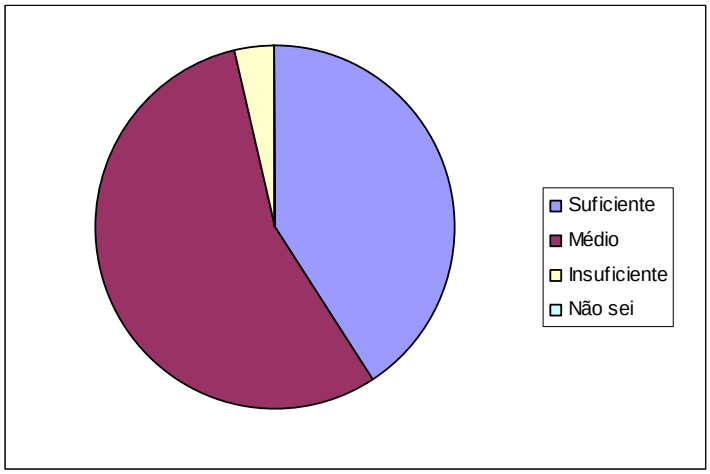


Gráfico 3: Apoio da alta direção ao processo segurança da empresa
Fonte: Dados da pesquisa acadêmica da autora

Dois pontos devem ser observados: primeiro é que a maioria, 15 líderes estratégicos, representando 55% que consideraram médio ou parcialmente suficiente o apoio da alta direção sobre as questões de segurança; o outro é conhecer quais fatores motivaram os 4%, uma gerência considerar insuficiente o apoio da alta direção.

A **Questão 3** buscou verificar se a segurança adotada na organização tem sido suficiente para proteger patrocinadores, investidores, clientes, empregados e fornecedores, de acordo com as expectativas da Unidade. O resultado foi: 14 gerentes estratégicos, (52%) consideraram ser suficiente ou adequada a segurança adotada pelos segmentos para proteger o negócio dos interessados; 12 gerentes, (44%) consideram médio o apoio de suas áreas para o requisito analisado e um gerente, (4%), considerou insuficiente esse apoio, conforme Gráfico 4.

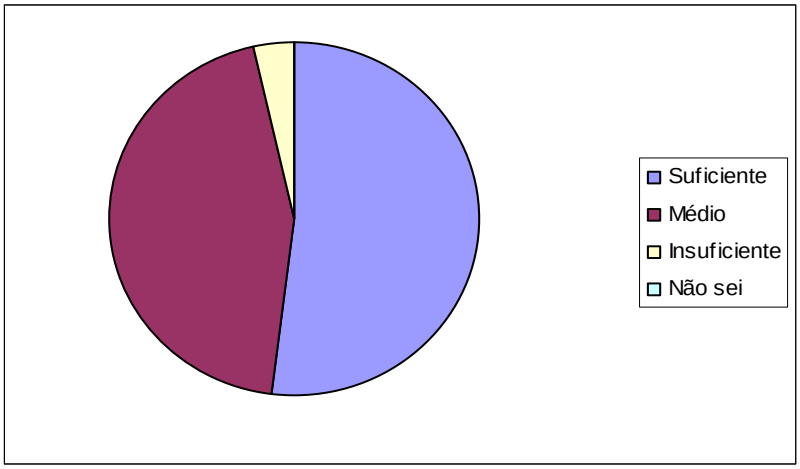


Gráfico 4: Segurança para proteger o negócio, visão geral
Fonte: Dados da pesquisa acadêmica da autora

O resultado sugere que a segurança adotada é suficiente para proteger o negócio. Entretanto, na composição dos 44% que disseram que a segurança estaria num patamar mediano, destacam-se as Unidades de Relacionamento com Clientes (URC) e Unidades de Produção e Serviços (UPS), que apresentaram índices de 25%. Ressalta-se a importância do segmento pois é voltado especialmente para atendimento e desenvolvimento de produtos de clientes.

A Unidade de Alinhamento Estratégico (UAE) que controla a segurança a nível estratégico também apresentou o resultado de 25%. Os demais segmentos, as áreas de

Consultoria e Apoio e a Unidade de Gestão Empresarial (UGE) apresentaram respectivamente 17% e 8%, destacando-se que a UGE é gestora de infra-estrutura de áreas de missão crítica para a segurança do negócio. O resultado por segmento está apresentado no Gráfico 5.

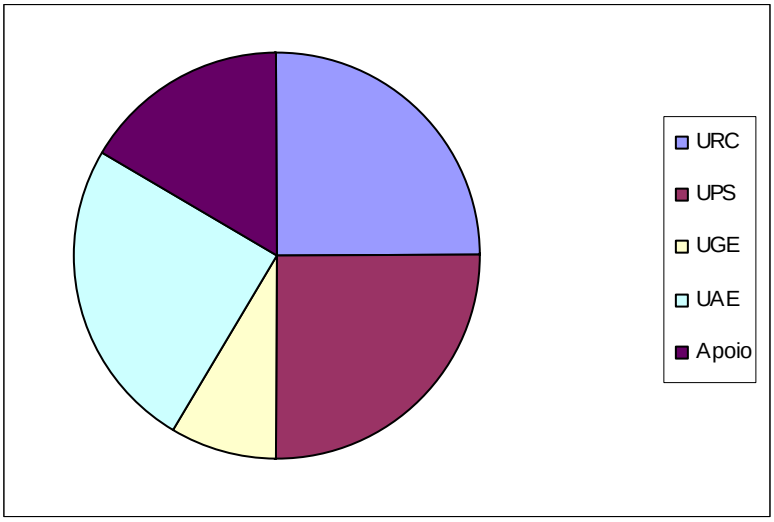


Gráfico 5: Segurança para proteger o negócio, por segmento
Fonte: Dados da pesquisa acadêmica da autora

Questão 4: buscou identificar qual o nível de importância do segmento em relação à segurança da informação para o sucesso do negócio da organização. O resultado foi: 14 gerentes estratégicos, representando 52% dos segmentos consideraram que dispõem de serviços de alta relevância para o sucesso do negócio; 12 gerentes, representando 44%, disseram que seus serviços são de relevância média e um gerente estratégico considerou seus serviço de relevância baixa para contribuir com o sucesso do negócio, conforme Gráfico 6.

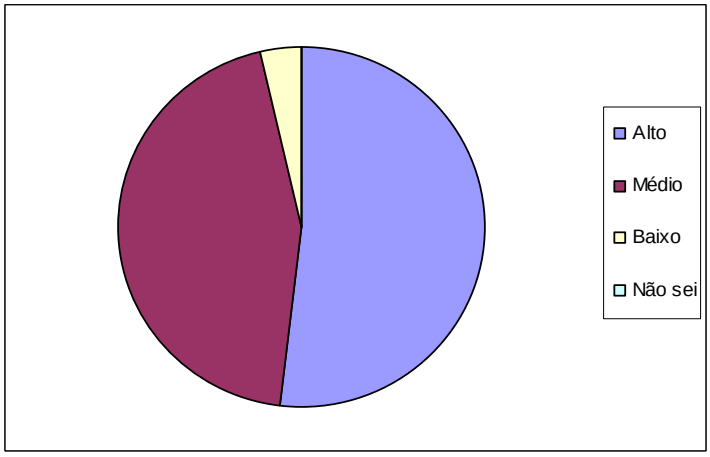


Gráfico 6: Importância dos segmentos para a segurança do negócio
Fonte: Dados da pesquisa acadêmica da autora

Diante da importância do item pesquisado, optou-se por verificar qual a percepção por segmento sobre a sua relevância para a segurança do negócio. O resultado mostrou que 29% dos serviços das unidades que compõem as URC têm alta relevância para a segurança do negócio da empresa; 21% dos serviços das unidades que compõem as UPS foram considerados de alta relevância da segurança para o negócio. Ressalta-se que existem nessas áreas serviços essenciais, de missão crítica, como rede, centro de dados e outros serviços de tecnologia da informação e comunicação; 14% dos serviços realizados pelas unidades da UGE têm alto nível de importância.

Importante destacar que existem serviços essenciais, como energia elétrica, ar condicionado, entre outros sob a responsabilidade desse segmento; os segmentos Apoio e UAE, unidades direcionadoras de políticas, apresentaram respectivamente 21% e 14% que dispõem de serviços relevantes para o sucesso do negócio. O Gráfico 7 apresenta o resultado.

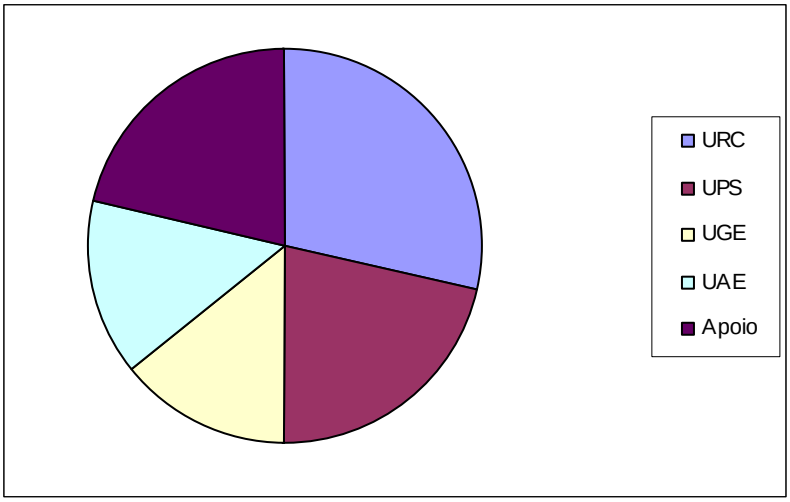


Gráfico 7: Serviços de alta relevância para a segurança do negócio sob a óticas dos diversos segmentos
Fonte: Dados da pesquisa acadêmica da autora

Questão 5: buscou identificar se a segurança adotada nos processos sob a responsabilidade de cada segmento contribui para que a organização garanta e sustente um nível previsível, aceitável e adequado de segurança compatível com a missão do negócio. O resultado apresentou que 63% dos segmentos disseram que seus processos contribuem

parcialmente para o nível adequado da segurança ao negócio e 37% disseram contribuir plenamente, conforme apresenta o Gráfico 8.

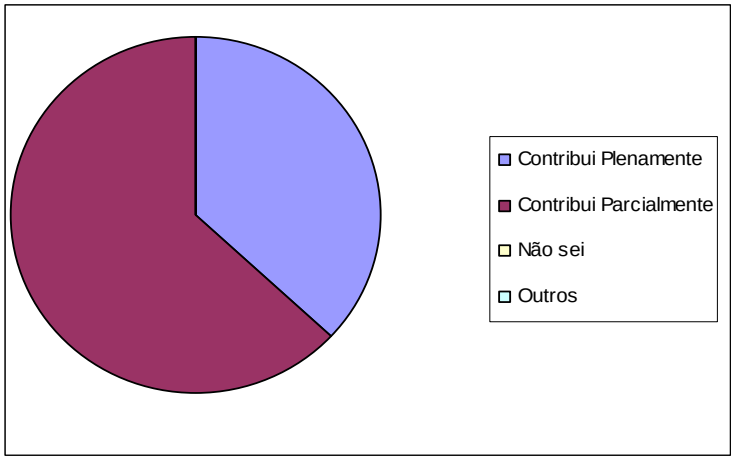


Gráfico 8: Níveis aceitáveis de segurança dos processos
Fonte: Dados da pesquisa acadêmica da autora

Focando os resultados das URC e UPS, por serem segmentos fundamentais para o negócio, os resultados foram respectivamente 35% e 29%, suscitando a importância de identificar os processos e importância para que a organização garanta e sustente um nível previsível, aceitável e adequado de segurança compatível com a missão do negócio.

Adicionalmente, é importante também verificar os resultados das UAE e Apoio. Entretanto, considerando que há no segmento UGE atividades críticas, suscita-se a necessidade de aprofundar a análise. O Gráfico 9 apresenta o resultado.

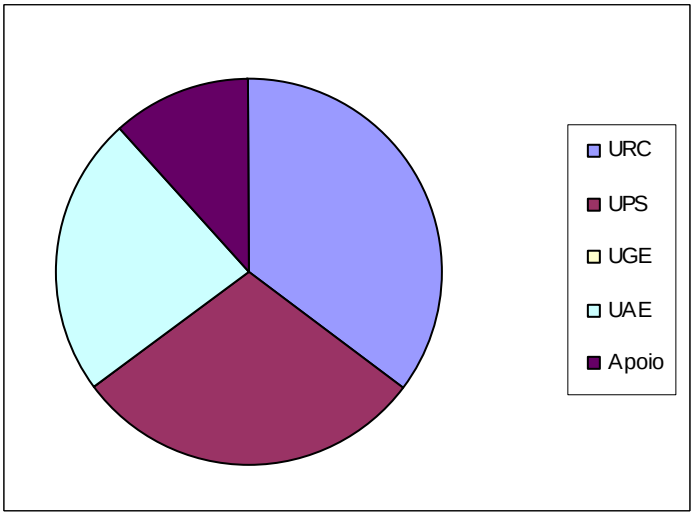


Gráfico 9: Níveis aceitáveis de segurança por segmento
Fonte: Dados da pesquisa acadêmica da autora

Questão 6: buscou identificar se os contratos que determinam responsabilidade das partes (empresa, clientes, empregados e fornecedores) garantem a confidencialidade, integridade e disponibilidade do negócio contratado. O resultado apresentado indicou que 67% dos segmentos entendem que seus contratos garantem parcialmente e 33%, que seus contratos garantem plenamente. Há necessidade de identificar os contratos que estão alinhados com as responsabilidades e direitos das partes e utilizá-los como modelo de melhoria para os demais. O Gráfico 10 apresenta o resultado.

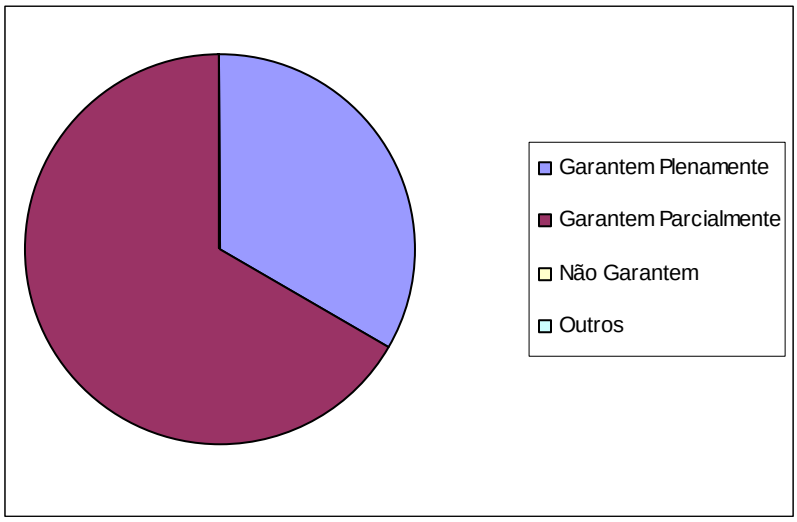


Gráfico 10: Contratos garantem responsabilidade das partes
Fonte: Dados da pesquisa acadêmica da autora

Questão 7: buscou identificar se o processo de gestão de risco do negócio favorece ações proativas para manter o risco em níveis aceitáveis. O resultado da pesquisa apresentou que: 66% dos segmentos disseram que favorece parcialmente; 30% disseram que favorece plenamente as ações de mitigação de riscos; 4% optaram por outros, mas não fizeram observações. Diante desse resultado, a pergunta a se fazer é: quais os serviços que estão dentro da faixa dos 30% favorecidos plenamente pelo processo de gestão de riscos? se forem os serviços de missão crítica, o cenário é favorável ao negócio da Empresa e clientes. O Gráfico 11 apresenta o resultado.

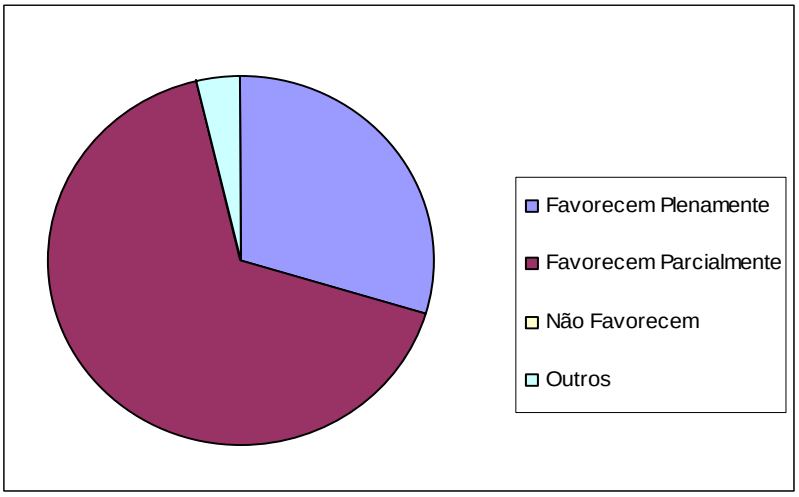


Gráfico 11: Processo de gestão de riscos em níveis aceitáveis
Fonte: Dados da pesquisa acadêmica da autora

No geral, o resultado da variável indicou que o processo de gestão de riscos - em prática na Empresa - não tem sido eficaz, carecendo de ações de melhoria, de forma que a maioria dos processos seja favorecida na análise, conhecimento e controle dos riscos e ameaças.

Questão 8: buscou verificar se a revisão periódica dos processos de segurança, por meio da gestão de riscos é fundamental para garantir a sustentação da continuidade do negócio, adequabilidade e efetividade da segurança. De acordo com o resultado 70% concordaram que a revisão periódica dos processos de segurança, por meio da gestão de riscos é fundamental para garantir a sustentação da continuidade do negócio, adequabilidade e efetividade da segurança; 22% disseram concordar parcialmente com a afirmativa; 4% não consideraram suficiente o processo para garantir a continuidade do negócio e outros 4% disseram não saber informar.

A atenção deve voltar-se para as áreas que representam os 22% que concordaram parcialmente e identificar quais os serviços que não são atendidos e ainda verificar porquê 4% que não concordaram com a afirmativa. O Gráfico 12 apresenta o resultado.

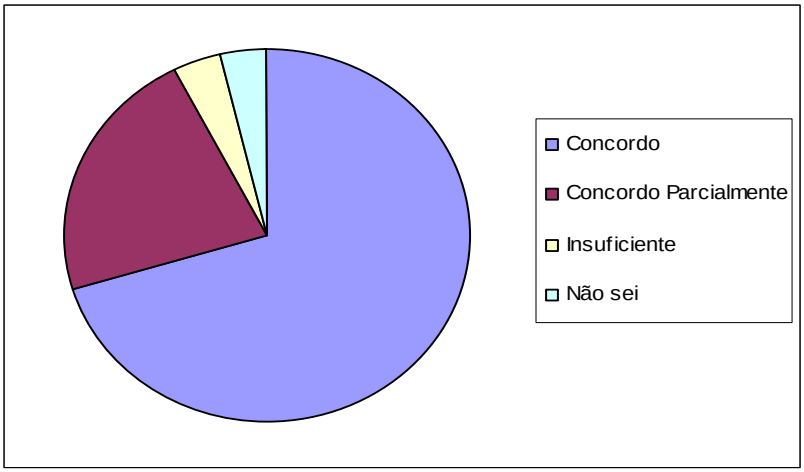


Gráfico 12: Revisão por meio de gestão de riscos garante a continuidade do negócio
Fonte: Dados da pesquisa acadêmica da autora

Questão 9: buscou identificar se os controles de segurança utilizados são adequados e incluem os documentos de política, a atribuição de responsabilidade, o processamento correto nas aplicações, a gestão de vulnerabilidade técnica, a gestão da continuidade do negócio e a gestão de incidentes de segurança da informação e melhorias. O resultado indicou que 50% dos gerentes consideraram que os controles de segurança são parcialmente suficientes; 28% disseram ser suficientes os controles de segurança utilizados; 15% disseram ser insuficientes os controles; 7% disseram não saber informar. A avaliação sugerida é que os controles existentes são parcialmente adequados, evidenciando a necessidade de revisão e adequação, principalmente dos serviços críticos. O Gráfico 13 apresenta o resultado.

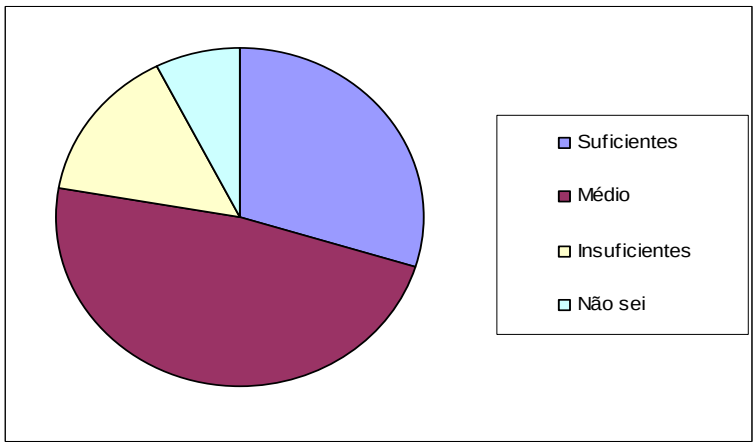


Gráfico 13: Controles de segurança adequados e baseados em políticas
Fonte: Dados da pesquisa acadêmica da autora

Questão 10: buscou identificar se a segurança da informação faz parte da cultura da organização, se existe respeito às regras e ações de segurança em todos os processos do negócio, nos níveis gerenciais estratégico, tático e operacional. O resultado apresentado foi que 74% concordaram parcialmente com a questão; 19% acreditam que a segurança da informação faz parte da cultura da organização; 7% optaram por outros, alegando que a "segurança ainda não é integrada à organização, existindo segmentos mais fortes em segurança e outros menos". No geral a segurança não faz parte da cultura organizacional. O Gráfico 14 apresenta o resultado.

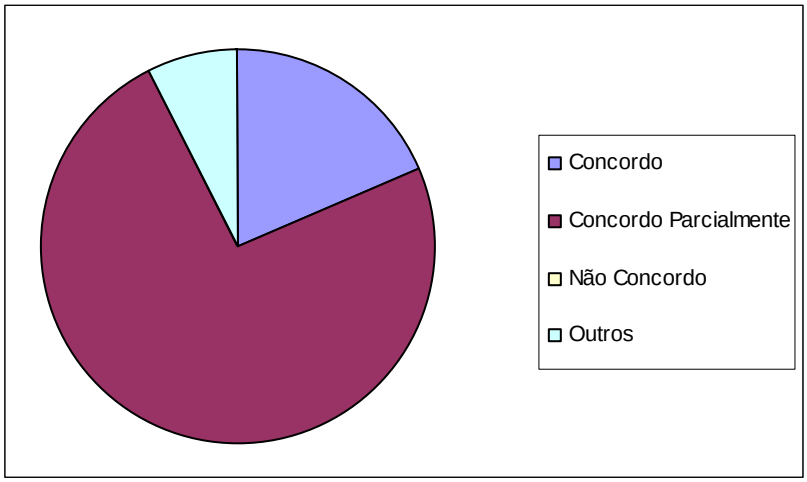


Gráfico 14: Segurança faz parte da cultura organizacional
Fonte: Dados da pesquisa acadêmica da autora

Questão 11: buscou identificar se a gestão da continuidade do negócio é institucionalizada, faz parte da cultura da organização e inclui controles para identificar e reduzir riscos, protegendo os processos críticos contra falhas ou desastres significativos. O resultado da pesquisa indicou que 56% dos segmentos concordam parcialmente com a afirmativa; 22% não concordam com a afirmativa; 18% dos gerentes concordam e 4% disseram não saber informar. Há indícios de que a gestão de continuidade do negócio é institucionalizada mas com há necessidade de melhorias. Ressalta-se ainda a importância de aprofundar as razões que motivaram 22% dos gerentes a discordarem da questão. O Gráfico 15 apresenta o resultado.

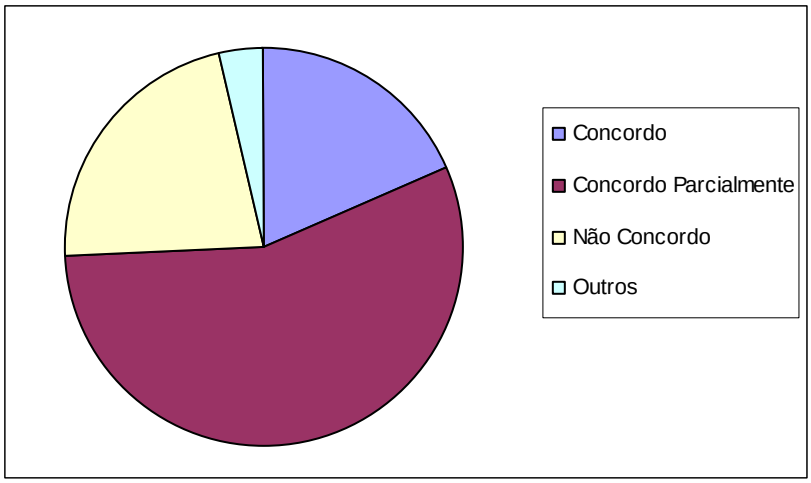


Gráfico 15: Gestão da continuidade do negócio institucionalizada
Fonte: Dados da pesquisa acadêmica da autora

Questão 12: buscou identificar se os processos críticos estão protegidos contra ameaças que interferem na confidencialidade, integridade e disponibilidade dos serviços. O resultado indicou que 56% dos gerentes concordam parcialmente que os processos críticos estão protegidos contra ameaças que interferem na confidencialidade, integridade e disponibilidade dos serviços; 40% concordam com a afirmativa e 4% optaram por "outros", sem apresentar justificativas. Diante desse resultado, suscita-se a necessidade de reavaliação e adequação visando manter os processos críticos em níveis de proteção que permitam a continuidade do negócio. O Gráfico 16 apresenta o resultado.

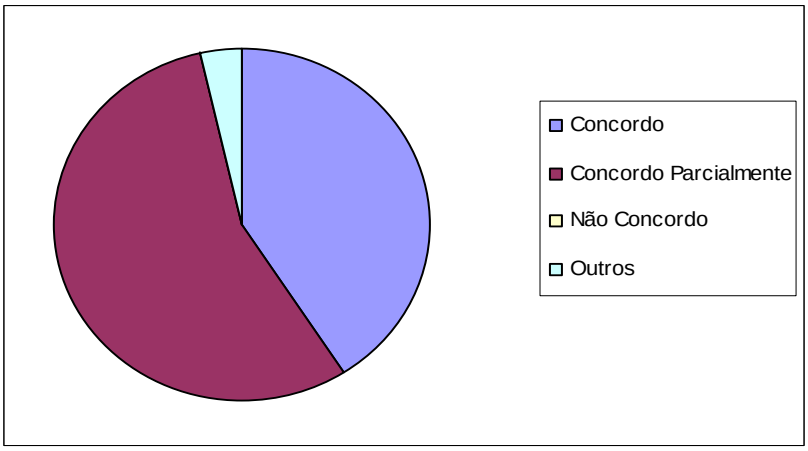


Gráfico 16: Processos críticos protegidos
Fonte: Dados da pesquisa acadêmica da autora

Questão 13: buscou identificar se o processo de recuperação de desastre, para atendimento aos níveis de serviço contratados pelo cliente, está institucionalizado ou garantido. 56% dos gerentes concordam parcialmente com a afirmativa; 33% concordam que o processo de recuperação de desastre está institucionalizado e atende aos níveis de serviços contratados; 7% optaram por "outros", sem apresentar justificativas e 4% não concordam com a afirmativa. Considerando que 56% dos gerentes concordaram parcialmente e 11% não concordaram, torna-se importante a revisão do processo a fim de detectar ações de melhoria. Se for necessário, institucionalizar o processo. O Gráfico 17 apresenta o resultado.

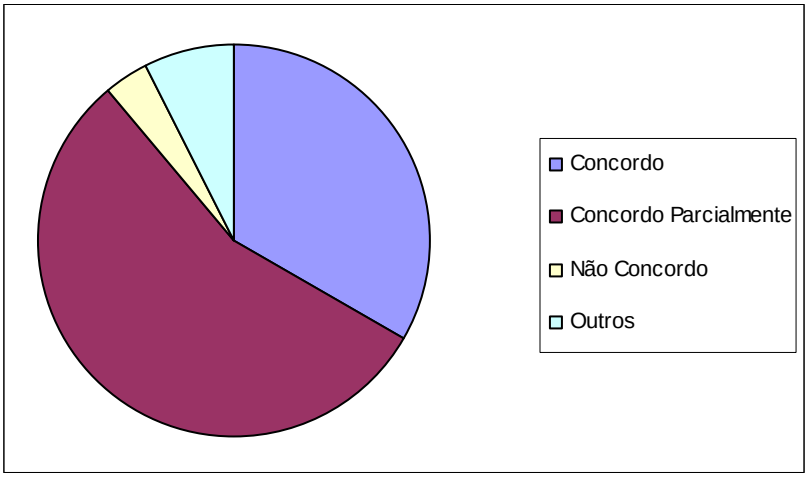


Gráfico 17: Processo de recuperação de desastre institucionalizado
Fonte: Dados da pesquisa acadêmica da autora

Questão 14: buscou identificar se a certeza de que a segurança aplicada ao negócio tem sido suficiente para detectar e prevenir incidentes de segurança respalda-se no fato de que não houve registro de infecção de vírus nos últimos doze meses, que comprometesse o negócio. 52% dos líderes concordaram com a afirmativa; 32% disseram concordar parcialmente e 16% não concordam. Importante observar que 32% disseram concordar parcialmente suscitando a necessidade de identificar os processos que se inserem nessa avaliação, e, caso se trate de processos críticos, adotar medidas de melhoria. O Gráfico 18 apresenta o resultado.

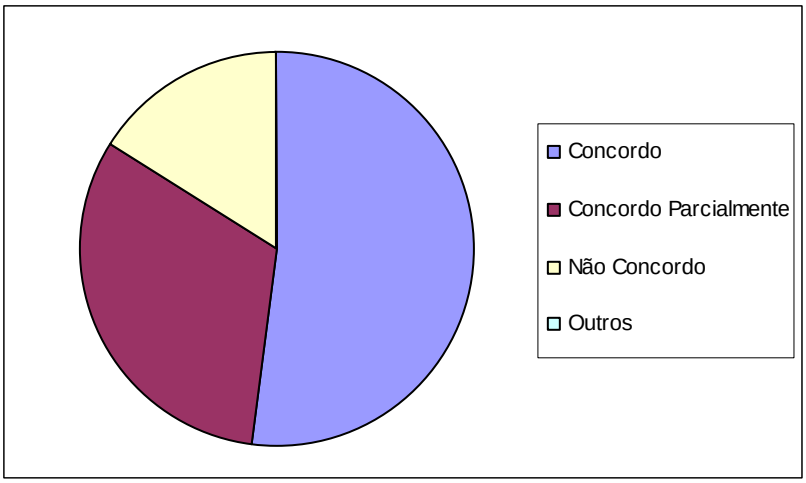


Gráfico 18: Segurança preparada para detectar e prevenir incidentes
Fonte: Dados da pesquisa acadêmica da autora

4.1.3 Segurança de Recursos Humanos

A seção tem o objetivo de verificar se existem, por segmento organizacional, pessoas qualificadas e dedicadas ao exercício das atividades de segurança no âmbito de suas áreas, considerando a complexidade das atividades desenvolvidas para atendimento ao negócio.

Questão 15: verificou a quantidade de pessoas por segmento e foi extraído das bases disponíveis no portal de recursos humanos, no ambiente de intranet da Empresa. Será utilizada para ilustrar a análise ou interpretação dos dados, quando necessário. O quantitativo por segmento está apresentado na Quadro 6.

Quadro 6: RH por segmento

URC	2.427
UPS	3.180
UGE	1.011
UAE	39
APOIO	124
TOTAL	6.781

Fonte: Dados da pesquisa acadêmica da autora

Questão 16: procurou identificar por segmento organizacional a quantidade de pessoas com atividades específicas em segurança da informação. O resultado, conforme Tabela 15, demonstrou que todos os segmentos dispõem de pessoas voltadas para atividade de segurança, observando-se que 62% dos segmentos dispõem de 1 a 5 empregados com atividades em segurança; 15% dos segmentos dispõem de 6 a 10 pessoas e outros 15% disseram dispor de até 50 empregados em atividades de segurança. O resultado está apresentado na Quadro 7.

Quadro 7: Demonstrativo de pessoas com atividade em segurança

Itens	URC	UPS	UGE	UAE	Apoio	Serpro
1 a 5 pessoas	57%	17%	100%	71%	100%	62%
6 a 10 pessoas	29%	33%	0%	0%	0%	15%
até 50 pessoas	14%	50%	0%	0%	0%	15%
Outros	0%	0%	0%	29%	0%	8%

Fonte: Dados da pesquisa acadêmica da autora

Registra-se que exceto os segmentos UAE e Apoio que se concentram na sede da empresas, os demais têm extensão em todos os Estados, esse cenário colaborou para a obtenção dos seguintes resultados:

a) Unidade de Relacionamento com Clientes (URC) – existem em torno de 2.400 empregados lotados nas diversas áreas que compõem esse segmento. A pesquisa indicou que 57% das áreas dispõem de 1 a 5 pessoas com atividades em segurança; 29% dispõem de 6 a 10 pessoas e 14% dispõem de até 50 pessoas com atividades em segurança;

b) Unidade de Produto e Serviço (UPS) – existem em torno de 3.100 empregados lotados nas diversas áreas que compõem esse segmento. A pesquisa indicou a seguinte situação por área: 17% das áreas dispõem de 1 a 5 pessoas com atividades em segurança; 33% das áreas dispõem de 6 a 10 pessoas e 50% das áreas dispõem de até 50 pessoas com atividades em segurança;

c) Unidade de Gestão Empresarial (UGE) – existem em torno de 1.000 empregados lotados nas diversas áreas que compõem esse segmento. A pesquisa indicou a seguinte situação por área: 100% das áreas dispõem de 1 a 5 pessoas com atividades em segurança;

d) Unidade de Alinhamento Estratégico (UAE) – existem em torno de 40 empregados lotados na sede. A pesquisa indicou a seguinte situação por área: 71% das áreas dispõem de 1 a 5 pessoas com atividades em segurança e que 29% das áreas não dispõem de pessoas com essa atividade; e

e) Apoio (Consultoria e Apoio) – existem em torno de 130 empregados lotados na sede. A pesquisa indicou que 100% das áreas dispõem de 1 a 5 pessoas com atividades em segurança;

Questão 17: buscou identificar, por segmento organizacional, se o investimento em treinamento sobre a segurança da informação é adequado às necessidades do negócio. O resultado indicou que 48% dos segmentos organizacionais concordam que o investimento em treinamento é adequado ao negócio; 33% disseram que eventualmente investem em treinamento de segurança; 19% optaram por "outros", e apresentaram os seguintes comentários: "O investimento não é simplesmente eventual, mas ainda não pode ser considerado totalmente adequado"; "Os treinamentos que existem são definidos em plano corporativo e não são suficientes"; "A liberação de pessoas da área para treinamento em segurança é abaixo da oferta, há mais oferta. Motivo: falta de pessoal para atender à demanda"; e que "Os eventos de segurança não são bem difundidos". O Gráfico 19 apresenta o resultado.

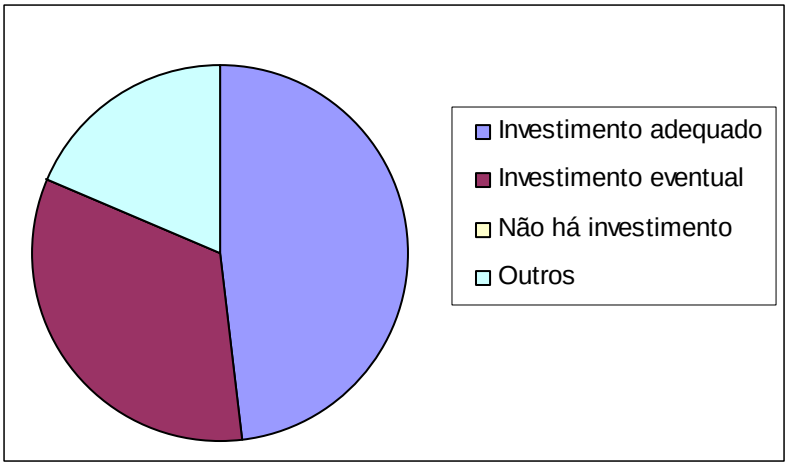


Gráfico 19: Treinamento adequado às necessidades de segurança
Fonte: Dados da pesquisa acadêmica da autora

Questão 18: buscou identificar se o acompanhamento dos resultados dos treinamentos aplicados demonstra que as pessoas ficam mais motivadas, contribuem mais com a Área, compartilham o conhecimento e apresentam melhores níveis de assertiva. 52% concordaram parcialmente que as pessoas treinadas são mais motivadas; 44% concordaram e 4% optaram pelo item outros e apresentaram as seguintes observações: “O treinamento não tem conseqüência direta na motivação”; “É necessário haver mudanças de atitudes, a motivação carece de trabalho mais eficiente e está associada a outros elementos”; “Há necessidade de trabalho de conscientização”. O Gráfico 20 apresenta o resultado.

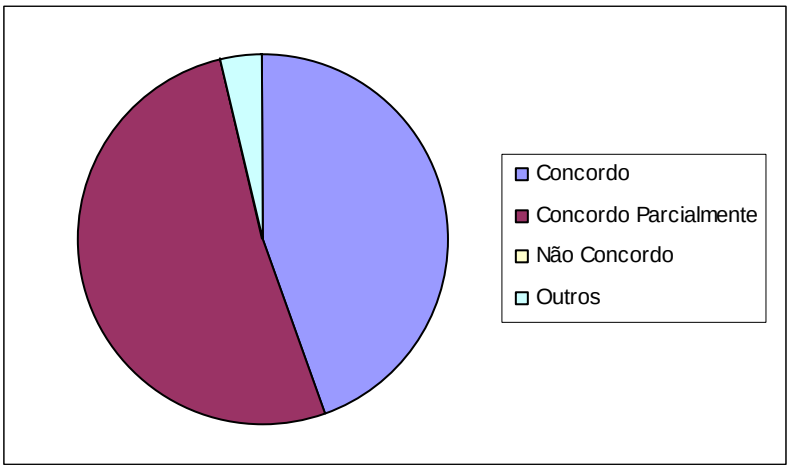


Gráfico 20: Pessoas treinadas são mais motivadas
Fonte: Dados da pesquisa acadêmica da autora

Questões 19 e 20: são complementares. A primeira identifica os tipos de certificações existentes nos segmentos organizacionais e a outra a quantidade de pessoas certificadas e por tipo. Existem as certificações CISSP (Certified Information System Security Professional); MCSO (Modulo Certified Security Officer); Auditor Líder ISO 27001 ou BS 7799-2; ACPCF (Axur Certified Professional Computer Forensics, CERT/CC (Computer Security Incident Response Team). O Gráfico 21 apresenta o resultado.

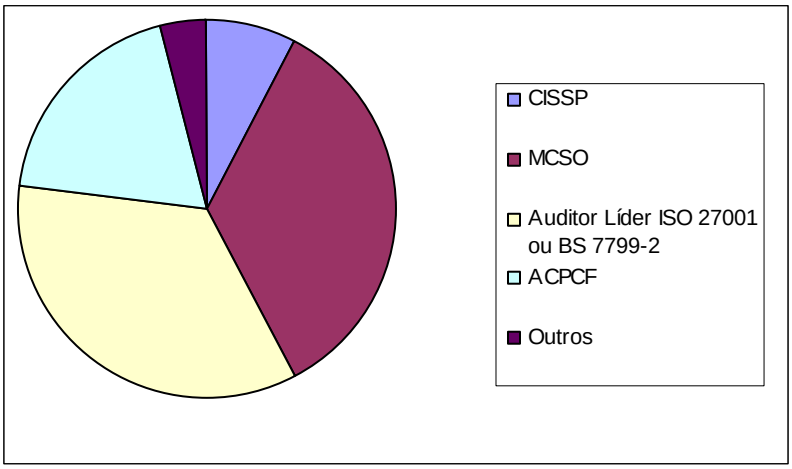


Gráfico 21: Tipos de certificações em segurança
Fonte: Dados da pesquisa acadêmica da autora

O item 20 apresentou os índices de certificações existentes por segmento. De acordo com a pesquisa dentro das certificações indicadas são 25 empregados com certificação em Auditor Líder ISO 27001 ou BS 7799-2, total de 35%; 20 pessoas em MCSO, total de 34%; 19 têm certificação em ACPCF, em torno de 19%; 2 em CISSP, 8% e 1 empregado, 4%, em CERT. O Gráfico 22 apresenta o resultado.

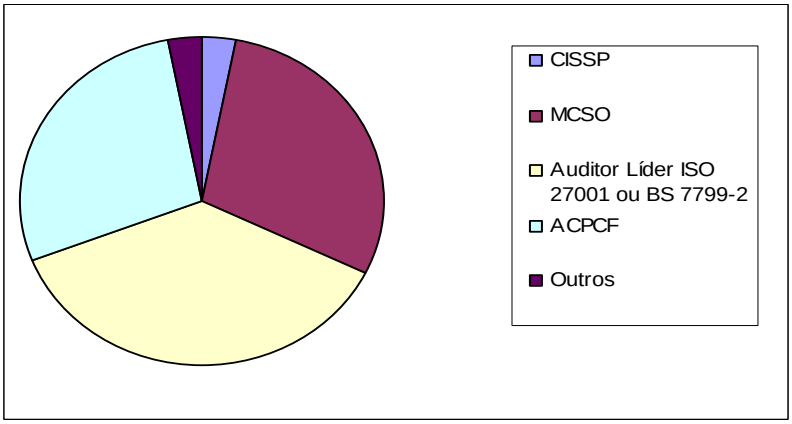


Gráfico 22: Percentual de certificação em segurança
Fonte: Dados da pesquisa acadêmica da autora

Questão 21: buscou identificar se "há melhor resposta das pessoas certificadas nas questões de segurança em relação aos demais". O resultado indicou que 55% dos gerentes confirmaram que as pessoas certificadas dão melhores respostas às questões de segurança; 41% disseram não saber informar e 4% disseram que não. Importante ressaltar que 41% dos gerentes não percebem se a contribuição das pessoas certificadas, em seus respectivos

segmentos, tem sido efetiva. Outro ponto a ser considerado refere-se aos 4% que disseram que não há contribuição. O Gráfico 23 apresenta o resultado.

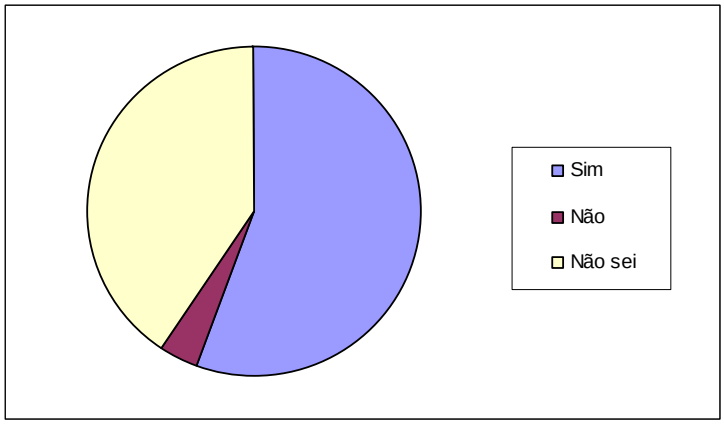


Gráfico 23: Pessoas certificadas contribuem mais
Fonte: Dados da pesquisa acadêmica da autora

Questão 22: buscou identificar se "nos últimos 12 meses o gerente participou de algum programa de treinamento, visando ao conhecimento voltado para sua Unidade sobre a segurança da informação".

O resultado da pesquisa indicou dos 27 gerentes que responderam a pesquisa 13 disseram ter participado de algum treinamento, são 48%; 8 gerentes disseram que não houve treinamento em segurança em assuntos específicos de suas áreas, correspondendo a 29%; 4 optaram por "outros" (15%) e apresentaram os comentários: "Os cursos de segurança da informação são muito técnicos e as necessidades gerenciais são mais voltadas para a gestão da segurança, visão holística da segurança"; "Não houve treinamento com abordagem estratégica, mais voltada para a alta liderança"; "Não houve motivação para participar"; 8% disseram que não houve tempo para participar de treinamento. O Gráfico 24 apresenta o resultado.

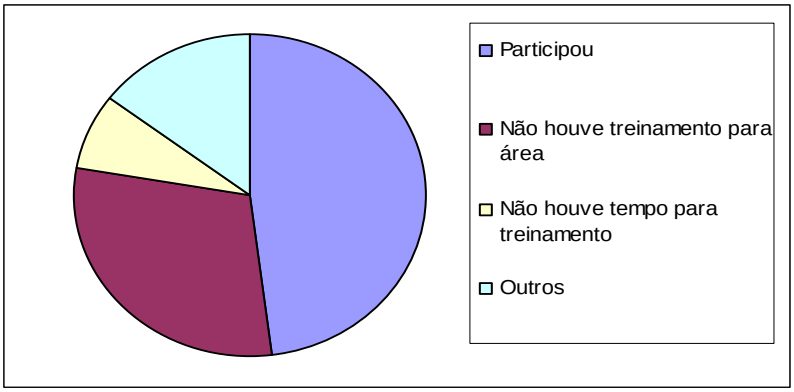


Gráfico 24: Participação de gerentes em treinamento de segurança
Fonte: Dados da pesquisa acadêmica da autora

Questão 23: buscou identificar "que ações estão sendo adotadas pelos gerentes para garantir o uso ético das informações críticas da empresa". O resultado indicou que 85% dos gerentes utilizam processos de conscientização; 7% disseram não saber qual medida é utilizada; 4% disseram que foram aplicadas ações disciplinares administrativas diante de situações de reincidência e 4% responderam ao item "outros", com o comentário de que "nenhuma ação é realizada nesse sentido". O Gráfico 25 apresenta o resultado.

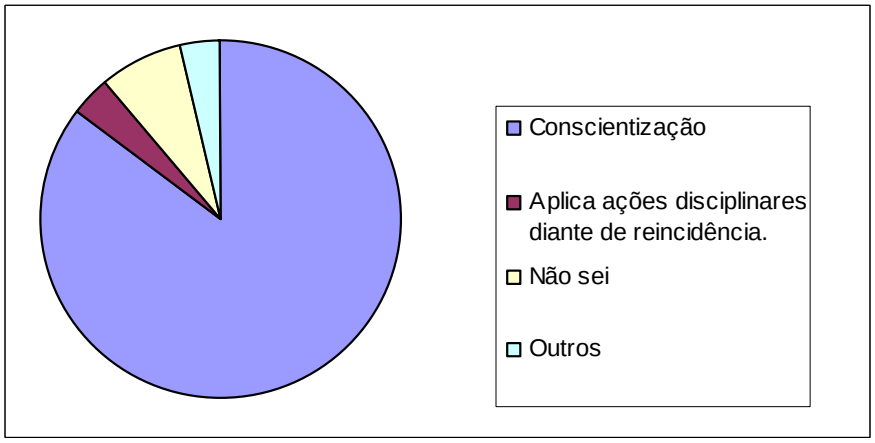


Gráfico 25: Orientação para uso ético das informações
Fonte: Dados da pesquisa acadêmica da autora

4.1.4 Planejamento

A seção tem o objetivo de verificar se o planejamento em segurança está alinhado ao negócio, considerando as políticas estabelecidas, os objetivos, processos e procedimentos para a gestão de riscos e melhoria da segurança da informação.

Questão 24: buscou verificar se o orçamento destinado à segurança, com prioridade para os processos críticos e de infra-estrutura, está alinhado ao planejamento estratégico da Empresa. Para 34% dos gerentes o orçamento está alinhado aos processos críticos; 33% disseram concordar parcialmente com a afirmativa; 22% disseram não concordar e 11% optaram por "outros" e fizeram as seguintes observações: "Não há orçamento específico na unidade para a segurança da informação"; "Orçamentos para a segurança são corporativos e não atendem às necessidades". O Gráfico 26 apresenta o resultado.

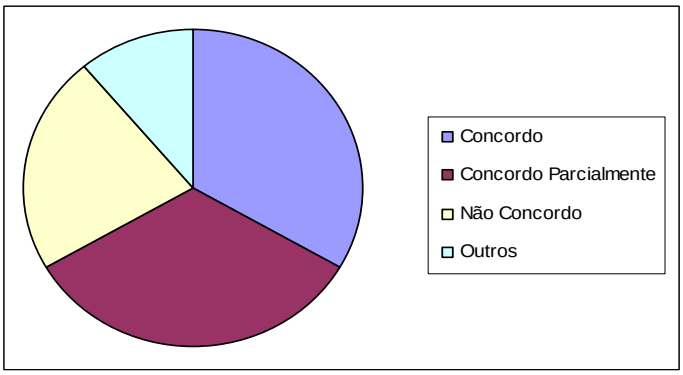


Gráfico 26: Orçamento para segurança alinhado ao planejamento
Fonte: Dados da pesquisa acadêmica da autora

Diante dos resultados bastante difusos quanto à concordância, suscita-se a necessidade de que o orçamento destinado à segurança priorizando serviços críticos carece de revisão e ações de melhoria.

Questão 25: buscou verificar se "um dos critérios para priorizar os investimentos em segurança da informação direciona para os processos críticos". Para 56% dos gerentes os critérios para priorizar os investimentos em segurança da informação direcionam para os processos críticos; 37% concordaram parcialmente e 7% fizeram a seguinte

observação: “A unidade não tem orçamento para atender a essa necessidade”. Diante do resultado da questão 24 sugerindo que o orçamento para segurança não é uma prática, surge a necessidade de revisão da política de planejamento estratégico de forma a implementar as ações de alinhamento com a política de segurança. O Gráfico 27 apresenta o resultado.

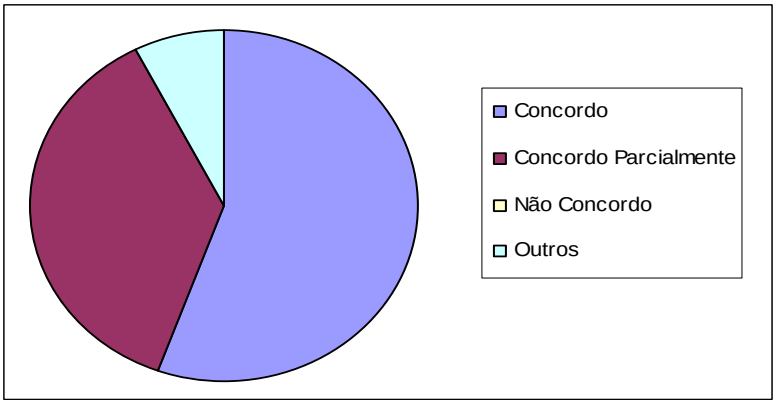


Gráfico 27: Investimento em segurança direciona para processos críticos
Fonte: Dados da pesquisa acadêmica da autora

Questão 26: buscou verificar se um dos critérios considerados para priorizar os investimentos em tecnologia da informação direciona para os processos críticos em infra-estrutura. A pesquisa indicou que 55% dos gerentes concordaram com a afirmativa; 37% dos segmentos concordaram parcialmente; 4% não concordaram e 4% optaram por “outros” e fizeram a seguinte observação: “A unidade não tem orçamento para atender a essa necessidade”. O resultado confirma o que se obteve nas questões 24 e 25, onde há indicação de uma revisão e melhoria da política estratégica de planejamento, tornando-a alinhada com as políticas de segurança e seus reflexos. O Gráfico 28 apresenta o resultado.

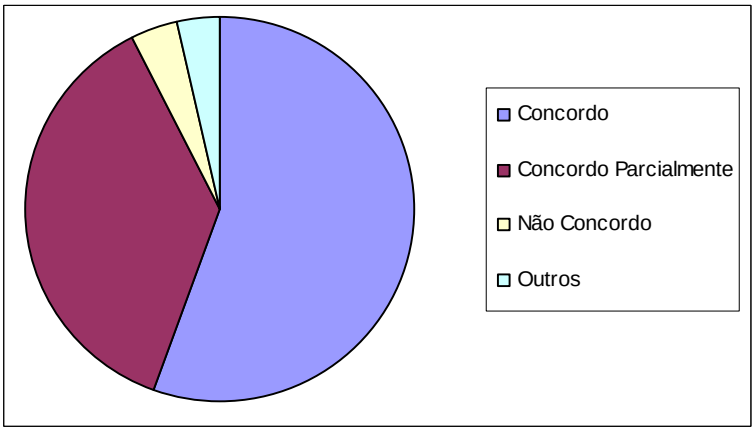


Gráfico 28: Investimento em TI direciona para processos críticos em infra-estrutura
Fonte: Dados da pesquisa acadêmica da autora

Questão 27: buscou verificar se a adoção dos controles de segurança respalda-se prioritariamente nos resultados das auditorias internas e externas, registros de incidentes e análise e gestão de risco. 52% dos gerentes concordaram parcialmente com a afirmativa; 44% concordaram com a afirmativa; 4% optaram por "outros" e fizeram a seguinte observação: "Esta ainda não é uma prática disseminada, mas há iniciativas nessa direção"; "Há clientes que definem os controles de segurança para seus serviços". O Gráfico 29 apresenta o resultado.

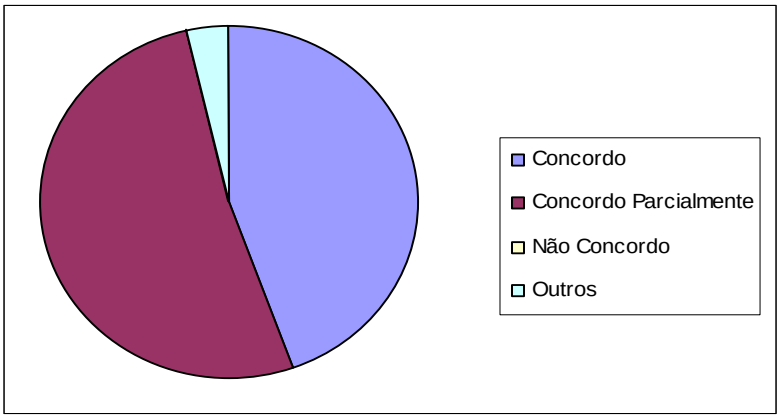


Gráfico 29: Controles de segurança baseados em auditoria
Fonte: Dados da pesquisa acadêmica da autora

Questão 28: buscou verificar se "o controle existente sobre o investimento de segurança em tecnologia da informação é aferido pela relação do custo do investimento e do resultado no negócio". 47% dos gerentes concordaram parcialmente com a afirmativa; 19% concordaram com a afirmativa; 19% disseram não concordar com a afirmativa e 15% optaram por "outros", apresentando as seguintes observações: "A unidade não tem este direcionamento"; "Não há esse relacionamento com custo do investimento e resultado do negócio". O Gráfico 30 apresenta o resultado.

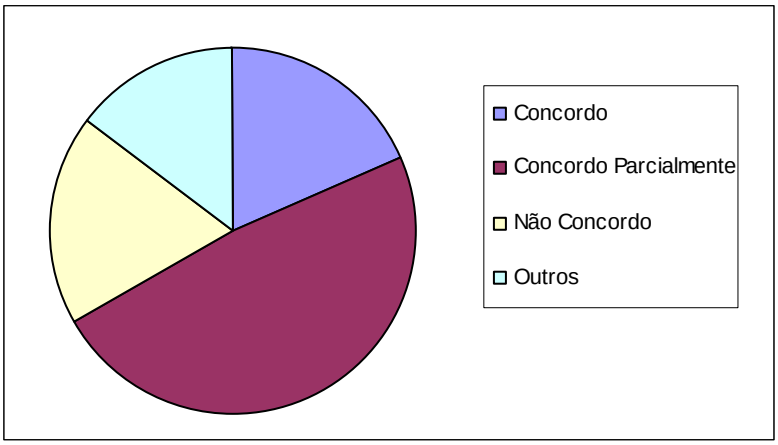


Gráfico 30: Controle do investimento em segurança de TI sobre resultado
Fonte: Dados da pesquisa acadêmica da autora

Questão 29: vinculada à 28, portanto, deveria ser respondida em consonância à anterior, uma vez que buscou verificar a freqüência com que ocorre o controle do investimento em segurança de TI, aferido pela relação do custo do investimento e resultado do negócio. A resposta foi 37% dos gerentes não souberam informar; 26% optaram por "outros", mas não fizeram comentários; 22% disseram ser sem prazo determinado e 15% disseram ser anual. O resultado evidencia que não existe prática desse quesito ou se trata de atividade não- institucionalizada. Considerando os resultados dos itens 24, 25 26 e 28, o item 29 seria mais um a ser adicionado a uma política de planejamento estratégico. O Gráfico 31 apresenta o resultado.

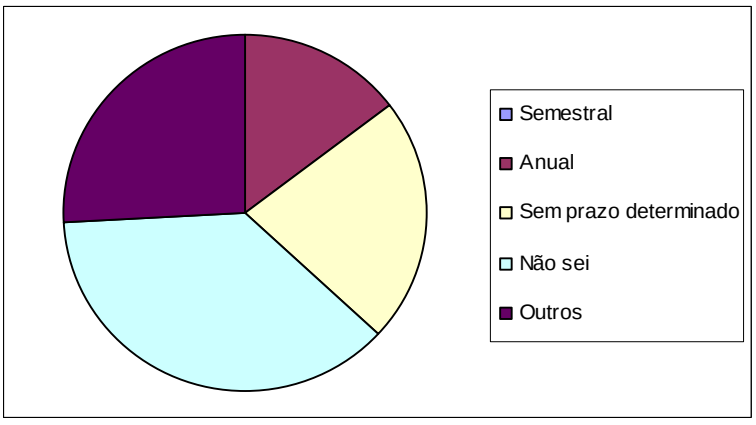


Gráfico 31: Freqüência do controle do investimento em segurança de TI
Fonte: Dados da pesquisa acadêmica da autora

4.1.5 Gestão de incidentes

Procura detectar fragilidades e eventos de segurança da informação associados com sistemas de informação que ocorrem e são comunicados, permitindo a tomada de ação corretiva em tempo hábil.

Questão 30: buscou verificar se existem instrumentos formais para a notificação de diferentes eventos de segurança e fragilidade que possam impactar na segurança do negócio e se os empregados, fornecedores e terceirizados estão conscientes sobre essas ações. 62% dos gerentes concordaram parcialmente com a afirmativa; 34% concordaram; 4% optaram por "outros", apresentando a seguinte observação: "Não é uma prática institucionalizada na Empresa, só algumas unidades utilizam". O Gráfico 32 apresenta o resultado.

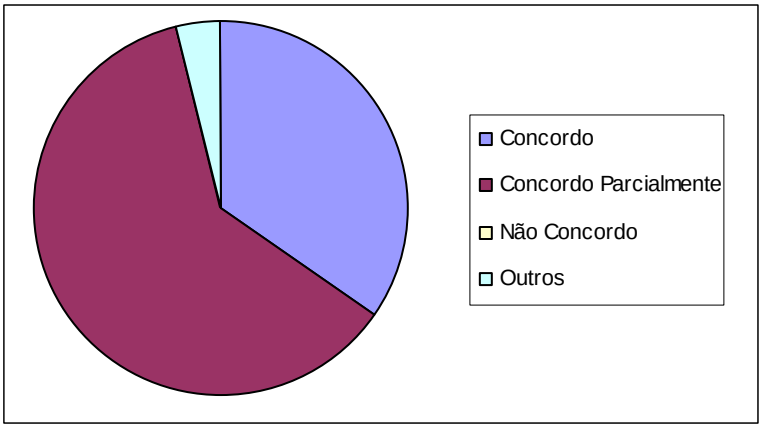


Gráfico 32: Instrumentos para notificação de incidente de segurança
Fonte: Dados da pesquisa acadêmica da autora

Questão 31: buscou verificar a que se relacionam com mais freqüência os incidentes de segurança. 26% dos gerentes disseram que os incidentes de segurança estão mais relacionados a ambiente operacional; 19% disseram estar relacionados a mau funcionamento ou sobrecarga de sistemas; 19% relacionados a erro humano; 12% relacionados a perda de serviço; 12% disseram estar relacionados a não-conformidade com

políticas ou diretrizes; e 12% disseram estar relacionados a violação de procedimentos de segurança. É preciso aprofundar o conhecimento sobre cada um dos problemas que mais recaem sobre os incidentes, destacando a importância de direcionamento de treinamento, de acordo com a indicação de estudo específico sobre o tipo e as causas do incidente. O Gráfico 33 apresenta o resultado.

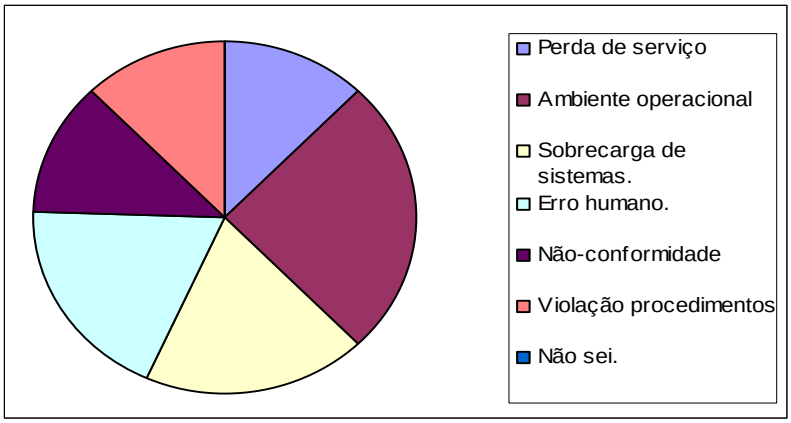


Gráfico 33: Motivos de incidentes de segurança
Fonte: Dados da pesquisa acadêmica da autora

Questão 32: buscou verificar se os incidentes de segurança são imediatamente notificados e tratados. 56% dos gerentes disseram concordar que os incidentes de segurança são imediatamente notificados e tratados; 37% disseram concordar parcialmente; 4% disseram não concordar e 4% optaram por "outros", apresentando as seguintes observações: "Os incidentes são tratados em nível de infra-estrutura, faltando ainda a correlação de serviços"; "Às vezes são tratados e não notificados". O Gráfico 34 apresenta o resultado.

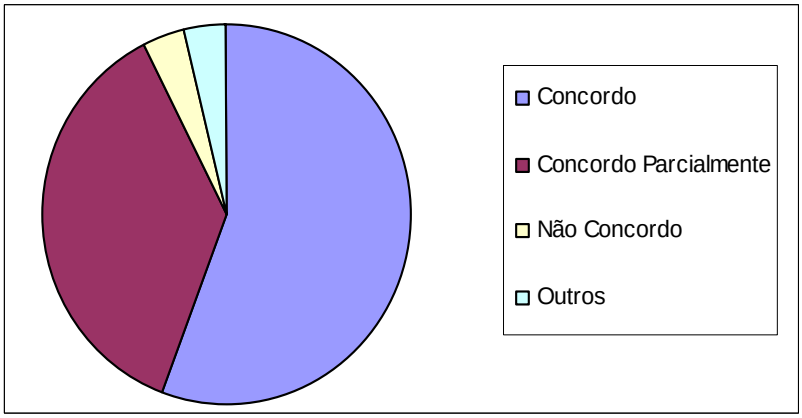


Gráfico 34: Incidentes de segurança são imediatamente notificados
Fonte: Dados da pesquisa acadêmica da autora

Questão 33: buscou verificar se as ações de resposta a incidentes são tomadas imediatamente após sua notificação, porque as responsabilidades e procedimentos estão definidos e disseminados entre os empregados, responsáveis pelas atividades. 55% concordaram com a afirmativa; 37% disseram concordar parcialmente; 4% disseram não concordar e 4% optaram por "outros", mas não ofereceram contribuições. A importância do tema e considerando o resultado do item 32, há necessidade de aprofundar conhecimento sobre o que motivou 37% dos gerentes a não concordarem plenamente com a premissa e porque outros 4% disseram não concordar. O Gráfico 35 apresenta o resultado.

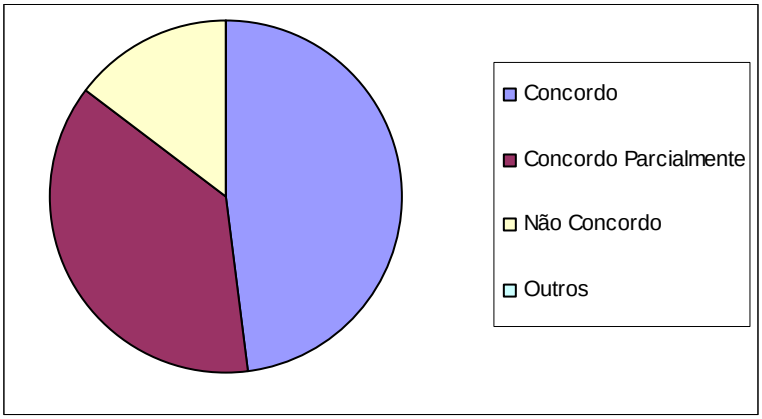


Gráfico 35: Resposta a incidente é imediata
Fonte: Dados da pesquisa acadêmica da autora

Questão 34: buscou verificar se os empregados estão treinados e orientados para, diante de incidente de segurança, colher as evidências a fim de assegurar a conformidade com as exigências legais, quando for o caso, e conhecer as falhas de segurança. 55% dos gerentes concordaram parcialmente com a afirmativa; 30% dos segmentos concordaram; 11% disseram não concordar e 4% optaram por "outros", mas não ofereceram contribuição. Considerando-se os resultados diferentes de "concordo", há indícios de que o procedimento não está disseminado no âmbito geral, carecendo de revisão a fim de identificar as necessidades de melhorias no treinamento ou reciclagem. O Gráfico 36 apresenta o resultado.

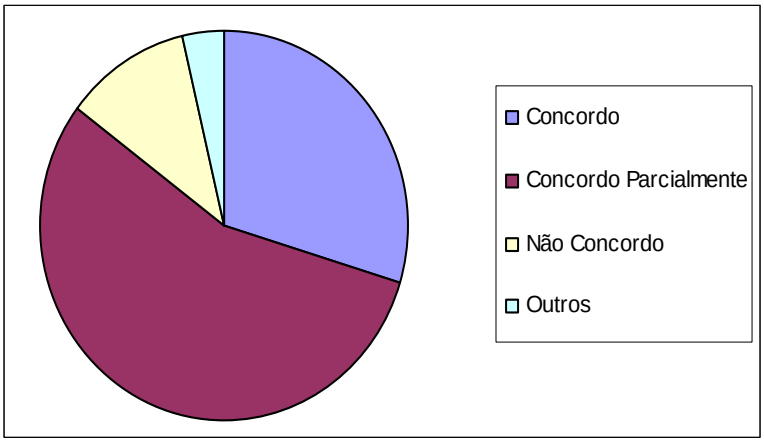


Gráfico 36: Empregados treinados para identificar evidências de incidentes
Fonte: Dados da pesquisa acadêmica da autora

4.1.6 Continuidade do negócio

A seção tem por objetivo verificar quanto está institucionalizado o processo continuidade do negócio, (processo que busca não permitir a interrupção do serviço e proteger os processos críticos contra efeitos de falhas de desastres significativos e assegurar sua retomada em tempo hábil).

Questão 35: buscou verificar se existe plano de continuidade para atender aos processos críticos do negócio. O resultado apresentou que 63% dos gerentes concordaram parcialmente com a afirmativa; 26% concordaram com a afirmativa; 7% não concordar; 4% optaram por “outros”, apresentando a seguinte observação: “A gestão da continuidade está em implantação”. Diante do resultado apresentado, há indícios de que o plano de continuidade para processos críticos não é conhecido pela maioria dos gerentes, necessitando de ações para institucionalizá-lo. O Gráfico 37 apresenta o resultado.

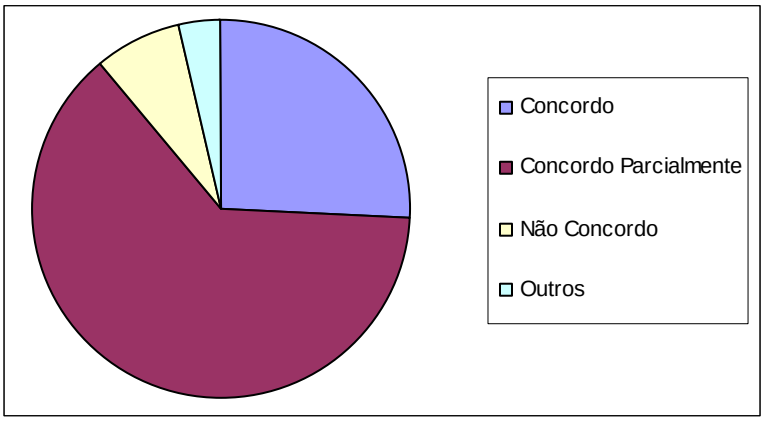


Gráfico 37: Plano de Continuidade para atender processos críticos
Fonte: Dados da pesquisa acadêmica da autora

Questão 36: buscou verificar se a gestão de risco identifica os processos críticos ligados ao negócio, sob a responsabilidade de cada segmento, porque faz parte do processo de gestão de continuidade adotado. O resultado indicou que 41% dos gerentes concordaram que a gestão de risco identifica os processos críticos ligados ao negócio; 41% disseram concordar parcialmente com a afirmativa; 11% dos segmentos não concordar; e 7% optaram por "outros", apresentando a seguinte observação: "Esta prática ainda não está internalizada". O Gráfico 38 apresenta o resultado.

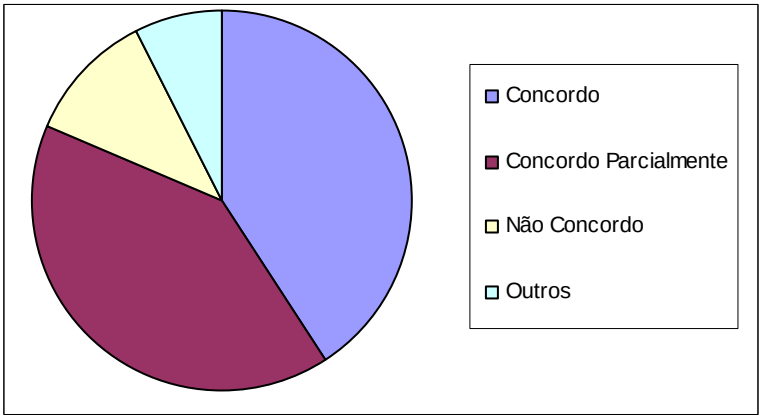


Gráfico 38: Gestão de riscos subsidia a continuidade do negócio
Fonte: Dados da pesquisa acadêmica da autora

Questão 37: buscou verificar se, em regra, ao ser definido um novo sistema ou serviço, consideram-se os requisitos de segurança necessários à continuidade do negócio e o planejamento dos recursos associados. O resultado da pesquisa indicou que 46% dos geren-

tes concordaram com a afirmativa; 48% concordaram parcialmente e 4% disseram não concordar com a afirmativa. O resultado sugere a necessidade de adoção de ações a fim de tornar as políticas de gestão de riscos, institucionalizadas. O Gráfico 39 apresenta o resultado.

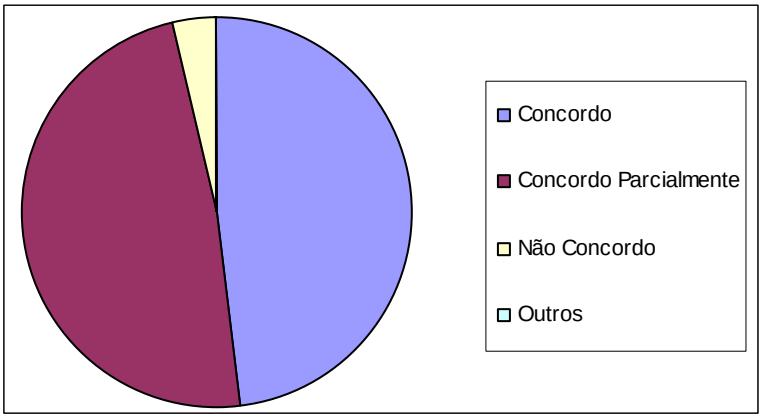


Gráfico 39: Construção de novos serviços alinhados aos requisitos de segurança
Fonte: Dados da pesquisa acadêmica da autora

4.1.7 Conformidade – requisitos legais

A seção Conformidade tem o objetivo de verificar o quanto os requisitos legais (legislação, normas, políticas, obrigações contratuais, entre outros instrumentos legais) são considerados no atendimento ao negócio.

Questão 38: buscou verificar se há garantia de que a avaliação da segurança da informação, no âmbito da unidade, é apropriada e está dentro da legalidade. O resultado indicou que 37% dos gerentes disseram há garantia de que a segurança está dentro da legalidade, “mas existem processos que estão sendo adequados à legislação e às regras internas”; 30% disseram que “a auditoria interna verifica periodicamente a legalidade dos processos de segurança da informação, sem que tenha havido notificação nos últimos doze meses”; 26% disseram não saber informar se há garantia de conformidade da segurança da informação com a legalidade e 7% disseram que não há garantia. Os resultados sugerem que há casos em que processos carecem de adequação a normas e procedimentos, resta identificar esses processos. O Gráfico 40 apresenta o resultado.

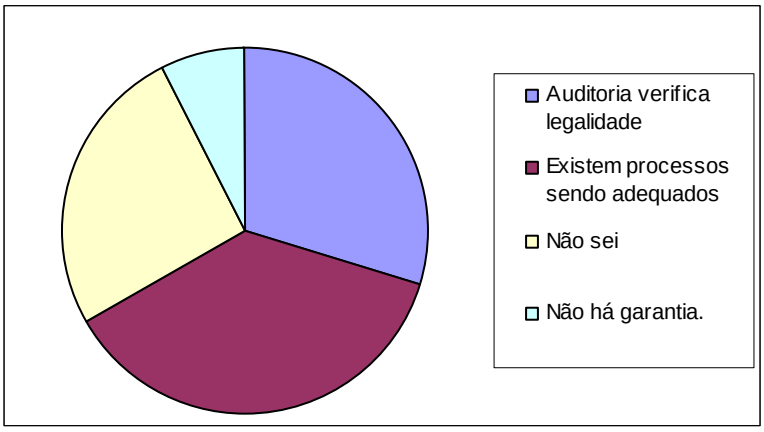


Gráfico 40: Avaliação da segurança conforme legalidade
Fonte: Dados da pesquisa acadêmica da autora

Questão 39: buscou verificar se os processos da área são executados corretamente para atender à conformidade com as normas e políticas de segurança. O resultado indicou que 41% dos gerentes concordaram que processos de sua área são executados corretamente para atender à conformidade às normas e políticas de segurança; 41% concordaram parcialmente; 11% disseram não concordar com a afirmativa e 7% optaram por “outros”, mas não ofereceram contribuição. O resultado corrobora o item 38, evidenciando que existem processos que necessitam ser adequados a normas e procedimentos. O Gráfico 41 apresenta o resultado.

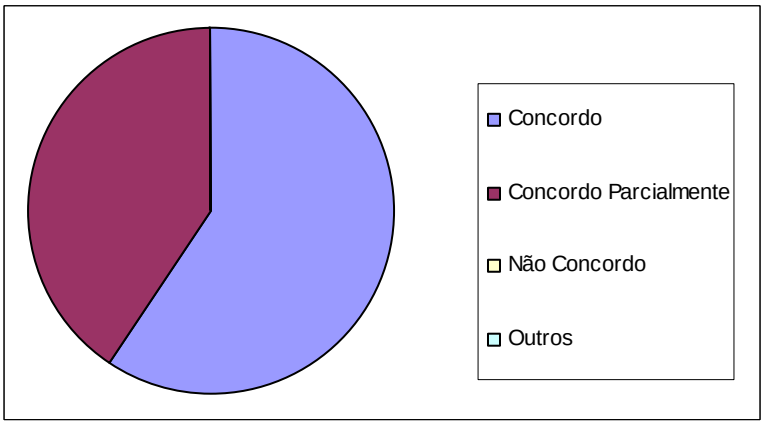


Gráfico 41: Conformidade dos processos
Fonte: Dados da pesquisa acadêmica da autora

Questão 40: buscou verificar se, diante da não-conformidade detectada em resultado de auditorias internas ou externas, as ações adotadas são: identificar as causas da não-conformidade, avaliar necessidade de ações para que a não-conformidade não se repita, analisar criticamente a ação corretiva e implementar a mais apropriada. O resultado indicou que 48% dos gerentes concordaram com a afirmativa; 48% disseram concordar parcialmente com a afirmativa e 4% optaram por "outros", com a observação de que "as auditorias não ocorrem de forma preventiva". O resultado, a exemplo dos itens 38 e 39, alerta para a necessidade de melhoria nas ações de legalidade e conformidade dos processos com as normas e procedimentos em vigor. O Gráfico 42 apresenta o resultado.

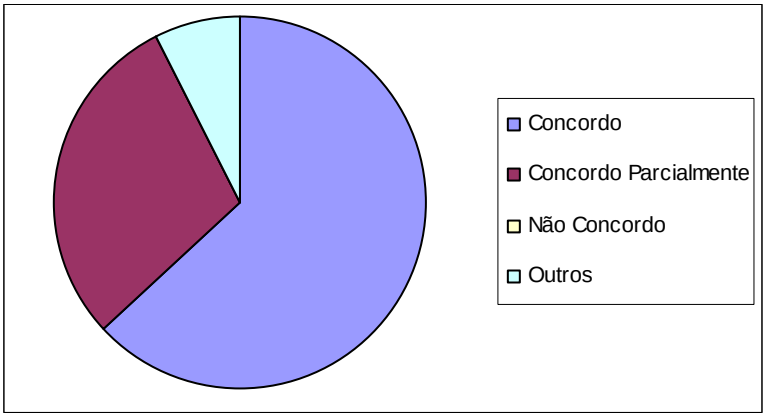


Gráfico 42: Ações de correção de não-conformidade dos processos
Fonte: Dados da pesquisa acadêmica da autora

4.2 Análise dos dados da pesquisa

4.2.1 Análise do perfil dos gerentes estratégicos

Este item não consta na pesquisa na forma como está sendo apresentado. O objetivo é mostrar o perfil institucional da liderança estratégica, que está localizado entre a liderança superior (que são os diretores e conselhos, administração e fiscal) e a liderança média (níveis táticos, operacionais, supervisores), representado na Figura 14.

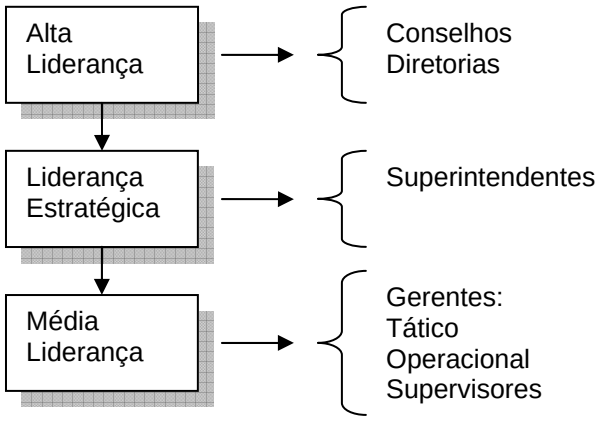


Figura 14 – Demonstração da estrutura de liderança formulada pela autora
Fonte: autora

O item foi construído a partir de duas questões da seção Segurança em Recursos Humanos, da pesquisa, e de informações da base de dados de recursos humanos da Empresa, disponibilizados em portal intranet.

Os líderes estratégicos têm cargo de superintendente ou equivalente. São no total 29 cargos, dos quais 27 responderam à pesquisa. Estão na Empresa, em média, há 25 anos e têm sob sua responsabilidade grande contingente de recursos humanos e complexas atividades.

Interrogados sobre a participação em treinamento voltado para a segurança da informação, nos últimos 12 meses (considerando o período de abril/2006 a abril/2007), no geral, 52% disseram que não participaram, sob a alegação de que não houve curso direcionado à especialidade da unidade ou por falta de tempo para dedicar-se a treinamentos. Os demais gerentes pesquisados (48%) disseram ter participado de treinamento em segurança, nos últimos 12 meses.

Diante dos resultados dos 52% dos gerentes que não participaram de treinamento, seria importante verificar:

- quando ocorreu a última participação em treinamento e qual foi o tema;
- qual o fator de maior relevância para justificar a “falta de tempo para treinamento”, a exemplo das Unidades de Produtos e Serviços (UPS), 17% e Unidades de Relacionamento com Clientes (URC), 14%;

- qual tema de segurança da informação é de interesse das lideranças, independente do segmento de atuação;
- qual a participação desses gerentes em algum tipo de treinamento em segurança e quando participaram, considerando a relevância de cada segmento de atuação, dos níveis gerenciais intermediários e do contingente de pessoas subordinadas por segmento;
- qual a efetiva necessidade de treinamento em segurança da informação, abrangendo todos os níveis gerenciais, no âmbito de cada segmento.

A participação em treinamento, de acordo com dados da pesquisa, carece de incentivos para melhoria, considerando que conscientização, educação e treinamento são pilares para a gestão adequada em qualquer especialidade de conhecimento.

Notadamente em segurança da informação, o conhecimento das políticas de segurança, das ameaças, das tendências de ameaças à segurança da informação, saber tratar reporte de incidentes, tratar incidentes de segurança, entre outros, são itens básicos e necessários à conduta da liderança estratégica e demais níveis gerenciais; são fundamentais para que a alta direção e gerentes intermediários tenham consciência de suas responsabilidades quanto ao valor da segurança da informação para a organização e interessados (clientes, empregados, sociedade). Enfim, para que possam comprometer-se com uma efetiva política de segurança direcionada ao negócio (ITGI, 2006, p.13).

De acordo com Wright (2000, p.302-303), a liderança estratégica difere dos outros níveis de liderança porque, entre outras, tem a responsabilidade de integrar e orientar suas equipes dentro de uma percepção de futuro quanto a cenários, processos e crescente complexidade das organizações, de forma a motivar essas equipes a se moverem na mesma direção. Diante disso, pode-se afirmar que a liderança carece estar bem treinada para ser referência e assumir suas responsabilidades.

4.2.2 Análise da questão Governança e Gestão

Governança ou gestão da segurança da informação é alicerçada em estrutura de decisão em que tecnologia, processos e pessoas são os pilares para que a informação tenha a proteção adequada ao negócio.

A tendência de globalização dos serviços converge para diversas tecnologias que possibilitam, além da nanotecnologia, biotecnologia, entre outras tecnologias emergentes, o processamento em tempo real da informação. Diante desse cenário, a governança da segurança da informação apresenta uma proposta em que a segurança da informação não seja direcionada apenas ao âmbito tecnológico, mas como parte integrante de toda a organização, em todos os segmentos (Bernardes e Moreira, 2005, p. 3-4).

Questões da pesquisa:

Questão 1 – buscou identificar quais funções existem sob a orientação dos líderes estratégicos, segundo sua percepção, mas dentro de uma relação de itens oferecidos, estimulados, havendo também a possibilidade de que outros itens pudessem ter sido citados.

Entre os itens não selecionados por algumas unidades vinculadas ao segmento Unidade de Produto e Serviço (UPS), a atenção é para o tema “Proteção de propriedade intelectual”, considerando que se trata de assunto que dispõe de legislação própria (Lei no. 9.610/98 e Lei no. 9.609/98, que tratam sobre direito autoral). O Serpro, por ser uma empresa que constrói produtos, tem uma Política de Propriedade Intelectual. Este resultado específico suscita a percepção de que o assunto deve ser revitalizado em todos os segmentos.

O resumo das respostas à questão está apresentado na Quadro 5, demonstrando que as funções de governança, citadas no questionário, que também estão no âmbito da gestão da segurança, estão inseridas nos segmentos da Empresa. Entretanto, foi observado

que, em alguns casos, a escolha do assunto não reflete o objetivo da área ou do próprio segmento, conforme explicitado após apresentação da Tabela.

Quadro 5: Resultado das funções de governança da segurança da informação, por segmento

Funções	**URC**	**UPS**	**UGE**	**UAE**	**Apoio**
Planejamento e estratégia de segurança para serviços de Cliente	•	•	•	•	•
Gestão da segurança em ambiente de TI	•	•	•	•	•
Implementação de segurança em serviços de clientes	•	•	•	•	•
Gestão da segurança para proteção de dados e informação	•	•	•	•	•
Gestão de segurança física e do ambiente	•	•	•	•	•
Controle de acesso	•	•	•	•	•
Gestão da continuidade do negócio	•	•	•	•	•
Gestão de Recursos Humanos	•	•	•	•	•
Gestão de incidentes	•	•	•	•	-
Proteção de propriedade intelectual	•	-	•	•	•
Segurança de rede	•	•	•	•	-
Desenvolvimento e manutenção de sistemas de informação	•	•	•	•	-
Gestão de contratos de serviços	•	•	•	•	•
Gestão financeira	•	•	•	•	•

Fonte: Dados da pesquisa acadêmica da autora

As funções que não refletem o objetivo do segmento são as seguintes:

- Gestão da segurança em ambientes de TI e Gestão da segurança para proteção de dados e informação. São atividades das áreas vinculadas à Unidade de Produto e Serviço (UPS) que, entre outras atividades, cuida dos ambientes de rede (Internet e intranet), centro de dados, enfim, todos os ambientes de TI. Os demais segmentos são usuários.
- Gestão da segurança física e do ambiente. É uma das atividades inerentes à Unidade de Gestão Empresarial (UGE). Os demais segmentos são usuários.
- Desenvolvimento e manutenção de sistemas de informação. São atividades da Unidade de Relacionamento com Cliente (URC). Os demais segmentos são usuários de produtos e serviços.

Questão 2 – verificou como os gerentes estratégicos percebem o apoio da alta direção: diretores, diretor-presidente, diretor-superintendente, conselho diretor e conselho

fiscal, nos negócios de segurança.

É importante destacar que o apoio da alta direção é o ponto mais relevante da governança da segurança da informação. Segundo o IT Governance Institute (ITGI, 2006, p. 21) – "a governança da segurança da informação é responsabilidade da alta direção e dos gerentes seniores", acrescentando que o apoio deve ser integral e transparente. Ressalta-se ainda que a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005 (p.8) recomenda o apoio da alta direção como um dos requisitos para garantir a gestão da segurança da informação.

O resultado da pesquisa mostrou que 55% dos gerentes consideraram parcialmente suficiente o apoio da alta direção, 41% consideraram suficiente o apoio e 4% consideraram insuficiente. A leitura desse resultado indica que não existe apoio sistemático da alta direção à segurança da informação, sugerindo que o apoio é manifestado em situações isoladas.

Observa-se que este ponto "particularmente fundamental para que haja efetiva governança da segurança da informação", conforme orientam as regras internacionais, não está sendo atendido na Empresa.

De acordo com Allen (2005, p.20), uma das barreiras à implementação da governança da segurança da informação é não obter o "apoio da alta direção e dos gerentes seniores". Nesse caso, cabe ao chefe da segurança mostrar a esse público sua responsabilidade com o direcionamento da política de segurança da informação para os negócios da Empresa, considerando ainda que a alta direção é legalmente responsável pela segurança do negócio.

A fim de apoiar a ação do chefe da segurança no empenho de buscar o apoio da alta direção, seria importante identificar em que situações ocorre esse apoio citado por 41% dos segmentos que disseram ser suficiente esse apoio, visando utilizar esses pontos como elementos para embasar o trabalho pela busca de apoio integral e transparente.

Questões 3, 4 e 5 – tratam de temas que se inter-relacionam e cada um observa um ponto da segurança que poderá subsidiar o outro ou mesmo formatar um ciclo para a

adoção de controles, mediante resultado de análise de riscos. Cada questão tem o seguinte objetivo:

- **A questão 3 -** verificou se a segurança atual, adotada na organização, atende às expectativas dos segmentos, considerando o nível de importância de cada unidade em relação à segurança da informação para o sucesso do negócio;
- **A questão 4** – verificou o nível de importância do segmento em relação à segurança do negócio da organização;
- **A questão 5** – verificou se a segurança adotada nos processos, por segmento, está compatível com a missão do negócio.

O relacionamento entre as questões 3, 4 e 5 é percebido na ordem, conforme estruturado na figura 15.

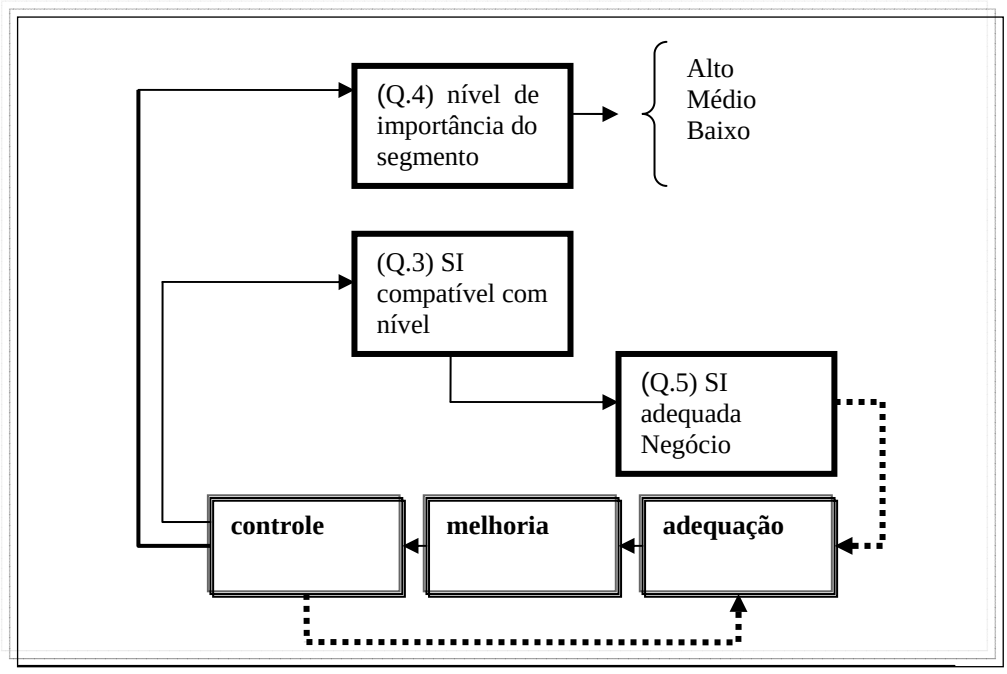


Figura 15 – Relacionamento entre as questões 3, 4 e 5 da pesquisa
Fonte: autora

O resultado da questão 3 indicou que a segurança atual atende a 52% dos segmentos, entretanto, num nível muito elevado, 48% disseram que atende parcialmente; para a questão 4, 52% dos segmentos têm alta importância para a segurança, 44% teriam média importância e 4% teriam baixa importância; e o resultado da questão 5 apresentou que 63% dos processos dos segmentos contribuem parcialmente para o nível adequado da segurança ao negócio e 37% afirmaram contribuir plenamente.

Diante desse resultado, seria importante conhecer as necessidades de segurança de cada unidade específica, de acordo com o resultado da pesquisa, principalmente as URC e UPS, concentrando-se em serviços e sistemas de missão crítica. Essa ação deve ser conduzida por processo de análise de risco, visando construir de forma sistematizada as ações de melhoria.

De acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005 (p.6), deve-se considerar que em segurança é muito importante conhecer os riscos, não subestimar nem superestimar, pois há riscos que necessitam ser mitigados, outros riscos, controlados e há riscos aceitáveis. Nesse contexto, conhecer o nível de importância do segmento para o negócio da organização é fundamental para obter o tratamento adequado.

Questão 6 – buscou identificar se os contratos existentes que consolidam a prestação do serviço ou produto traduzem claramente a responsabilidade das partes para garantir a segurança do negócio nas questões de confidencialidade, integridade e disponibilidade.

Para 67% dos gerentes, os contratos de seus segmentos atuais garantem parcialmente as responsabilidades das partes (empresa, clientes e fornecedores) enquanto 33% indicaram que seus contratos garantem plenamente.

Por ser o contrato uma das ferramentas mais importantes para definir responsabilidades, direitos e deveres das partes, o resultado da pesquisa evidencia a importância de, num contexto geral, revisar as regras sobre os contratos que regem as relações entre as partes, adequando-os, de acordo com o caso, segmento e necessidades de segurança. É importante ressaltar que os modelos de contratos utilizados por 33% dos demais segmentos devem ser elementos de análise para embasar o processo de melhoria.

Questão 7 – buscou identificar como os diversos segmentos percebem a gestão de análise de riscos como instrumento para nortear os gerentes a manterem os riscos em níveis

aceitáveis. Os resultados apresentados foram os seguintes:

- 66% disseram que o processo de gestão de risco do negócio, atualmente, favorece parcialmente as ações proativas para manter o risco em níveis aceitáveis;
- 30% entendem que o processo atual de gestão de risco favorece plenamente as ações de mitigação de riscos.

A ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005 (p. 6) diz que o conhecimento dos riscos é o elemento norteador da política de segurança a ser adotada para o negócio. Com o mesmo direcionamento, o Instituto Brasileiro de Governança Corporativa (IBGC) em seu Guia de Orientação para Gerenciamento de Riscos, (2007, p. 6) sugere que o modelo de gestão de riscos deve ser compatível com a realidade de cada organização.

Essas recomendações embasam a importância da gestão de riscos como norteadora das políticas de segurança para manter o risco em níveis aceitáveis. Diante do cenário apresentado, é fundamental que o modelo atual seja revisto, implementando as melhorias de acordo com o segmento especifico, observando que é responsabilidade da alta direção e dos gerentes seniores identificarem previamente os riscos e adotar planos para sua prevenção ou minimização.

Questão 8 – buscou verificar se a revisão periódica dos processos de segurança, por meio da gestão de riscos, é fundamental à sustentação da continuidade do negócio, da adequabilidade e efetividade da segurança.

Eis os resultados: no geral, 70% dos gerentes pesquisados concordaram com a afirmativa; 22% disseram concordar parcialmente e, finalmente, 4% disseram não considerar suficiente a gestão de riscos para garantir a continuidade do negócio. Outros 4% disseram não saber informar. Nesse item, a idéia era relacionar as duas questões e verificar se havia a prática da premissa, mas as respostas sugeridas no questionário não foram compatíveis ao objeto da verificação. Os itens para a questão deveriam ter sido os seguintes: “pratico, pratico parcialmente, não pratico, e não sei”. Diante disto, o resultado deste item não será analisado.

Questão 9 – buscou identificar se os controles de segurança utilizados são adequados e incluem os documentos de política, a atribuição de responsabilidade, o processamento correto nas aplicações, a gestão de vulnerabilidade técnica, a gestão da continuidade do negócio e a gestão de incidentes de segurança da informação e melhorias.

O resultado total foi que 50% dos gerentes disseram que os controles de segurança adotados atualmente são parcialmente adequados e 28% concordaram que os controles são suficientes.

A análise do resultado aponta para a necessidade de revisão dos controles, considerando que se insere nesta pesquisa a visão da auditoria que busca verificar nos controles o reflexo da conformidade das práticas com as normas e legislação. Adicionalmente, há que se considerar os 15% que disseram serem insuficientes os controles e os 7% que responderam não sei informar.

Questão 10 – buscou identificar se a segurança da informação faz parte da cultura da organização, tendo como termômetro o respeito às regras em todos os níveis organizacionais.

Constatou-se que 74% dos gerentes concordaram parcialmente que a segurança faz parte da cultura da organização e 19% acreditam que a segurança da informação efetivamente faz parte da cultura da organização.

É importante observar que a segurança da informação faz parte da cultura da empresa quando é percebida pela maioria absoluta de seus empregados, clientes, fornecedores e demais interessados. O resultado suscita a idéia de que a segurança da informação existe, mas precisa ser mais internalizada. Talvez isso reflita o pouco apoio da diretoria, apontado na pesquisa da questão 2, conforme Quadro 8.

Quadro 8: Apoio da alta direção

Itens	URC	UPS
Suficiente	43%	33%
Parcialmente suficiente	43%	67%
Insuficiente	14%	0%

Fonte: Questão 2 da pesquisa

Diante da importância de criar e manter uma cultura de segurança, cita-se a orientação da ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEV*E*LOPMENT (OECD, 2005, p. 6) de que "a cultura de segurança é fundamental para que haja a efetiva proteção a sistemas críticos e a infra-estrutura". Para Allen (2005, p.7), a governança da segurança da informação "direciona e controla a organização no estabelecimento e sustentação da cultura de segurança necessária à condução dos seus negócios".

Questão 11 – buscou identificar se a gestão da continuidade do negócio é uma função institucionalizada e faz parte da cultura da organização.

O resultado da pesquisa indicou que 56% dos gerentes concordaram parcialmente que o processo de continuidade do negócio esteja institucionalizado. Já 22% dos gerentes não concordaram e 19% afirmaram que sim: o processo de continuidade é institucionalizado. Há que se considerar, neste contexto, outras variáveis:

- A gestão de riscos, verificada na questão 7, apresentou que 66%, disseram que o processo de gestão de risco do negócio, atualmente, favorece parcialmente as ações proativas para manter o risco em níveis aceitáveis;
- Os controles de segurança utilizados são adequados ao negócio, verificado na questão 9, que apresentou que 50% dos segmentos afirmaram que os controles adotados atualmente são parcialmente adequados.

A gestão da continuidade do negócio é um processo que visa manter as atividades do negócio sem interrupção, protegendo os processos críticos. É requisito essencial à continuidade do negócio o alinhamento com o processo de gestão de riscos, que fornece o entendimento dos riscos a que a organização está exposta, no diz respeito a sua probabilidade de ocorrer o impacto e o controle dos planos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799:2005, p.103).

Diante desse contexto, convém que a Empresa tenha uma percepção mais clara dos riscos, identificando os processos críticos e integrados à gestão da segurança da informação, com as exigências inerentes à gestão da continuidade do negócio, inclusive

adotando os controles necessários à identificação e redução dos riscos. É importante considerar que o apoio da alta direção é fundamental, tendo em vista que recursos financeiros, organizacionais, técnicos e de pessoas devem ser suficientes para viabilizar a gestão da continuidade do negócio.

Questão 12 – buscou identificar o quanto os processos críticos estão protegidos contra ameaças que interferem na confidencialidade, integridade e disponibilidade.

Os índices apresentados foram: 56% disseram concordar parcialmente e 40% disseram concordar que os processos críticos estejam protegidos. O resultado apresentado, no geral, indicou que a maioria dos gerentes entende que os processos críticos estão protegidos, mas há necessidade de aperfeiçoamento.

É importante verificar que o resultado está compatível com o resultado da questão 11, em que se identificou que o processo de continuidade do negócio não está institucionalizado.

Questão 13 – buscou identificar como o processo de recuperação de desastre, para atendimento em níveis de serviços contratados pelo cliente, está institucionalizado ou garantido.

O resultado apresentado foi de que 56% concordaram parcialmente com a afirmativa e 33% concordaram, enquanto 11% dos respondentes discordaram.

A percepção dessa variável remete a uma análise conjunta das variáveis – processo de continuidade do negócio - que depende fortemente do processo gestão de risco e recuperação de incidentes, dentro de prazos contratuais.

A recomendação da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005, p.104, é que a continuidade do negócio deve ser sustentada por um processo de gestão de riscos, identificando os eventos que poderão causar interrupções. Com esse direcionamento, o plano de recuperação de incidente deve ser moldado para

atender aos níveis de serviço acordados com os clientes.

Diante disto, os dados da pesquisa apresentados podem ser interpretados como um alerta à necessidade de intensificar investimentos nesses processos para garantir a sustentabilidade dos negócios. Ressalta-se, ainda, que esses processos devem ser institucionalizados e creditados pela alta direção, patrocinadores, clientes e demais interessados.

Questão 14 – verificou se a certeza de que a segurança aplicada ao negócio tem sido suficiente para detectar e prevenir incidentes de segurança. Respalda-se no fato de que não houve registro de infecção de vírus nos últimos doze meses, que pudesse comprometer o negócio.

O resultado global da variável pesquisada indicou que: 52% concordam; 32% concordam parcialmente, e 16% não concordam. Não ficou claro e por isso as respostas carecem de mais elementos para formar uma análise melhor. Entretanto, a leitura sugerida é de que não houve nos últimos doze meses incidentes de segurança que comprometessem o negócio. Mas esse fato não garante que não existam eventos frágeis ou ameaças carecendo de revisão dos procedimentos ou análise de riscos em determinados ambientes.

Neste caso, é importante que empregados, patrocinadores, clientes, fornecedores e outros interessados sejam alertados sobre a importância de notificar eventos de segurança da informação, por meio de canais formais, devendo ser consolidado o processo de realimentação.

4.2.3 Análise da questão Recursos Humanos

O objetivo foi de verificar se existem, por segmento organizacional, pessoas qualificadas e dedicadas ao exercício das atividades de segurança no âmbito de suas áreas, considerando a complexidade das atividades desenvolvidas para atendimento ao negócio.

Questão 15 - verificou a quantidade de pessoas por segmento e o número foi extraído das bases disponíveis no portal de recursos humanos, no ambiente de intranet da Empresa. Será utilizado para ilustrar as análise ou interpretação dos dados, quando necessário. Os dados são apresentados na Quadro 9.

Quadro 9: Quadro de pessoal

URC	2.427
UPS	3.180
UGE	1.011
UAE	39
APOIO	124
TOTAL	6.781

Fonte: Banco de dados de RH do Serpro.

As unidades do segmento UPS são as que dispõem de maior contingente, ressaltando que, além das atividades de rede, centro de dados, teste, análise e homologação de ferramentas para ambientes seguros, também atende a clientes e suporte à rede em todos os estados brasileiros. As unidades do segmento URC desenvolvem produtos e serviços e têm presença nas 10 regionais fiscais do país. A UGE tem presença em todas as regiões fiscais. A UAE e Apoio são áreas de direcionamento estratégico e só existem na sede da Empresa.

Questão 16 – buscou identificar, por segmento organizacional, a quantidade de pessoas com atividades específicas em segurança da informação.

O resultado da variável pesquisada indicou que 62% dos segmentos organizacionais dispõem de 1 a 5 pessoas voltadas para as atividades de segurança no âmbito de suas Unidades; 15%, de 6 a 10 pessoas, e outros 15% dispõem de até 50 pessoas.

Para essa análise duas variáveis são importantes por segmento: complexidade das atividades *versus* quantidade de pessoas. Os resultados são:

- A URC, com quase 2.500 empregados, distribuídos nas 10 regiões fiscais, composta por 7 unidades (superintendências), apresentou a seguinte distribuição:

57% das unidades têm de 1 a 5 pessoas dedicadas à segurança; 29%, têm de 6 a 10 pessoas; e 14% têm até 50 pessoas com atividades voltadas à segurança da informação;

- A UPS, com quase 3.200 empregados, distribuídos nas 10 regiões fiscais e nas capitais dos demais Estados, composta por 6 unidades (superintendências), apresentou a seguinte distribuição: 17% dispõem de 1 a 5 pessoas dedicadas à segurança; 29%, dispõem de 6 a 10 pessoas e 50% têm até 50 de pessoas em atividades de segurança da informação;

- A UGE, com quase 1.050 empregados, distribuídos nas 10 regiões fiscais, composta por 4 unidades (superintendências), apresentou que 100% dispõem de 1 a 5 pessoas dedicadas à segurança;

- A UAE, com quase 40 empregados, todos lotados na Sede. Destaca-se que uma das unidades é responsável pelo processo de gestão da segurança da informação. Apresentaram a seguinte situação: 71 % dispõem de 1 a 5 pessoas dedicadas à segurança e 29% não dispõem de pessoas com conhecimento em segurança;

- Apoio, com quase 130 empregados, todos lotados na Sede. A situação é a seguinte: 100% dispõem de 1 a 5 pessoas dedicadas à segurança da informação.

No geral, a quantidade de recursos humanos dedicada a atividades de segurança apresenta-se compatível ou adequada ao tipo de segmento, considerando que as áreas URC e principalmente as UPS têm mais atividades direcionadas para ativos estratégicos.

Não foi possível verificar se a distribuição dos recursos humanos com atividades em segurança está adequada a cada área que compõe os segmentos URC e UPS. Um estudo mais aprofundado deve analisar a situação atual e buscar as adequações compatíveis com a real necessidade ou realizar adequações de melhoria.

Questão 17 – identificou se o investimento que as pessoas da unidade têm

recebido em treinamento, conscientização e educação em segurança da informação é adequado à necessidade do negócio.

O resultado da pesquisa apresentou que 48% dos segmentos organizacionais concordam que o investimento em treinamento é adequado ao negócio. Mas a maioria - 52% - não concordou e fez os seguintes comentários:

- "O investimento não é simplesmente 'eventual', mas ainda não pode ser considerado totalmente adequado".
- "Os treinamentos que existem são definidos em plano corporativo e não são suficientes".
- "Liberação de pessoas para treinamento em segurança é abaixo da oferta (há mais oferta). Motivo: falta de pessoal para atender à demanda".
- "Eventos de segurança não são bem difundidos".
- O resultado sugere que o treinamento em segurança da informação para atender à necessidade do negócio ainda não alcançou o estágio de maturidade, considerando as necessidades das áreas e os interesses do negócio. Enfim, a resposta à questão alerta para a necessidade de rever o planejamento de treinamento em segurança da informação, buscando torná-lo adequado às necessidades do negócio.

Questão 18 – verificou se o acompanhamento dos resultados dos treinamentos aplicados demonstra que as pessoas ficam mais motivadas, contribuem mais com a Área, compartilham o conhecimento e apresentam melhores níveis.

O resultado global indicou que 52% dos segmentos concordaram parcialmente que as pessoas treinadas são mais motivadas, contribuem mais e 44% dos segmentos concordaram, fazendo parte do resultado os seguintes comentários:

- "O treinamento não tem conseqüência direta na motivação";
- "É necessário mudança de atitudes; a motivação carece de trabalho mais eficiente e está associada a outros elementos";
- "Há necessidade de trabalho de conscientização".

Diante desse contexto, é importante considerar a relevância do resultado concordo

parcialmente. Foram 52% que disseram ter algum tipo de necessidade não atendida com o treinamento, buscando identificar o motivo dessa percepção e os fatores que têm contribuído para que o treinamento não esteja apresentando um bom retorno.

As questões 19 e 20 são complementares. Identificaram as certificações em segurança que existem e a quantidade de pessoal certificado de sua Unidade.

Todas as unidades do negócio têm pessoas com certificação em segurança da informação, exceto o segmento das UPS.

Obter certificação significa aferir e confirmar os conhecimentos em segurança da informação. As certificações existentes na Empresa são:

- CISSP - Certified Information Systems Security Professional
- MCSO - Security Officer;
- ACPCF – Axur Certified Professional Computer Forensics;
- Auditor Líder ISO 27001 ou BS 7799-2
- CERT - Computer Security Incident Response Team (certificação internacional)

A pesquisa não esclareceu se as certificações apresentadas por segmento estão compatíveis com a necessidade do negócio, se há mais de uma certificação por pessoa e qual o benefício dessas certificações.

Diante da importância e da tendência internacional de aprofundamento de conhecimento em segurança da informação com certificações, diferencial competitivo para as organizações, é importante identificar as necessidades por segmento e alinhar o planejamento de recursos humanos, de acordo com a questão 18, e motivar as pessoas a participarem. É necessário também considerar que segmentos como UGE disseram não existir pessoas certificadas.

A questão 21 é complemento da questão 19: buscou identificar se há melhor resposta das pessoas certificadas nas questões de segurança em relação aos demais.

O resultado global indicou que 59% dos segmentos organizacionais concordaram

que há melhor resposta das pessoas certificadas às questões de segurança; 37% disseram não saber informar e 4% disseram que não concordam com a afirmativa.

Convém salientar que segmentos como UPS concordaram que as pessoas certificadas dão melhores respostas sobre segurança da informação em suas unidades. Entretanto, dois pontos despertam maior atenção:

- 37% dos segmentos disseram não saber informar se há melhor resposta das pessoas certificadas;
- As UGE não dispõem de pessoa certificada, mas em seus segmentos há de 1 a 5 pessoas voltadas para atividades de segurança (questão 19); e 75% concordaram que o treinamento em segurança é adequado às necessidades do negócio (questão 17).

Na avaliação geral, registra-se a sugestão de que haja controle a fim de identificar se os investimentos que são feitos na certificação de pessoas que trabalham com atividades de segurança trazem resultados e se as certificações são compatíveis com as necessidades do negócio e se existem outras necessidades ainda não atendidas, mesmo em outros contextos de segurança.

Questão 22 – teve como objetivo identificar a participação da alta liderança em treinamento, em segurança, nos últimos 12 meses.

Foi tratado inicialmente no item 5.1, Análise dos dados funcionais dos gerentes estratégicos. O resultado apresentado foi que 49% dos lideres estratégicos disseram ter participado de algum treinamento em segurança da informação, com foco em sua área do negócio e outros 51%, por variadas razões, não participaram de treinamento algum em segurança.

Na concepção do modelo de governança da segurança da informação, esse tipo de resultado não é bom porque a orientação é que os gerentes sejam referências para seus grupos de trabalho (INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE, 2006, p.13).

Questão 23 – buscou verificar as ações adotadas pelos gerentes para garantir o uso ético das informações críticas da empresa.

O resultado global indicou que 85% dos gerentes dos segmentos organizacionais utilizam processos de conscientização para garantir o uso ético das informações críticas da empresa; 7% disseram não saber qual medida é utilizada e outros 4% afirmaram que aplicam ações disciplinares administrativas diante de situações de reincidência. Por sua vez, 4% responderam outros, com o comentário de que “nenhuma ação é tomada nesse sentido”.

Apesar de 85% dos segmentos terem dito que a ação de conscientização é a mais utilizada para garantir o uso ético das informações críticas da empresa, nenhum gerente ressaltou se adota algum critério de classificação da informação para orientar sobre a importância das informações e o grau de sigilo. Destaca-se ainda que 14% disseram não saber o tipo de ações adotadas nesses casos e que a unidade não toma providência alguma para garantir o uso ético das informações críticas da empresa, sob sua responsabilidade.

Registra-se que tanto a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005 quanto ITGI e outros institutos pesquisados neste trabalho recomendam que a informação tenha proteção adequada e um dos requisitos é o uso da classificação da informação. Esta questão traz à tona a legalidade (Decreto nº. 4.553 e Norma sobre a classificação da informação interna da Empresa), concluindo-se que conhecer as normas e tratar com ética as informações são atributos fundamentais tanto para a gestão quanto para a governança da segurança da informação, e todos os envolvidos precisam conhecer e praticar.

4.2.4 Análise da questão Planejamento

Teve como objetivo verificar se o planejamento em segurança está alinhado ao negócio, considerando as políticas estabelecidas, os objetivos, processos e procedimentos

para a gestão de riscos e melhoria da segurança da informação.

Questão 24 – verificou se o orçamento destinado à segurança, com prioridade para os processos críticos e de infra-estrutura, está alinhado ao planejamento estratégico da Empresa. Os índices apresentados foram os seguintes: 34% concordaram que o orçamento de segurança prioriza serviços críticos; 33% concordaram parcialmente e 33% não concordaram.

O resultado indicou que a prática não está internalizada, sugerindo que o orçamento destinado ao planejamento em segurança, na forma como está sendo administrado, não atende a esse requisito.

Num processo de governança da segurança da informação (ITGI, 2006, 11-14), é fundamental a integração e o alinhamento estratégico da segurança com o negócio da empresa. Para atender à questão explicitada, há que se considerar o seguinte fluxo:

- A gestão de riscos fornece os requisitos sobre as necessidades de investimento em infra-estrutura para proteger processos críticos;
- O item orçado é inserido no planejamento estratégico;
- O planejamento estratégico tem a aprovação da diretoria.

Os controles são adotados para verificar se os resultados foram obtidos e qual o impacto sobre o investimento.

Questão 25 – avaliou se um dos critérios considerados para priorizar os investimentos em segurança da informação direciona para os processos críticos. Com os índices de 56% dos segmentos que disseram concordar e 44% que não compartilharam da mesma opinião, pode-se entender que para alguns segmentos o procedimento é transparente, não ocorrendo o mesmo com outros segmentos, indicando que não é uma regra ou política da Empresa esse direcionamento.

Questão 26 – avaliou se um dos critérios considerados para priorizar os investimentos em tecnologia da informação direciona para os processos críticos em infra-estrutura. No geral, o resultado foi que 56% concordaram com a afirmativa e 45% não compartilharam da mesma opinião.

Na análise, percebe-se que as questões de infra-estrutura de TI são mais compatíveis ao segmento UPS e a posição foi de que 50% concordaram e 50% concordaram parcialmente. Diante deste resultado, a leitura é que não existe uma política orientadora neste sentido, deixando claras e transparentes as regras de prioridade em planejamento.

Questão 27 – avaliou se a adoção dos controles de segurança se respalda prioritariamente nos resultados das auditorias interna e externa, registros de incidentes e análise e gestão de risco.

O resultado aponta para os 56% dos segmentos que não compartilharam da afirmativa, registrando-se que para ue afiramm investimentote a premissa ocorre como algumas unidades “esta ainda não é uma prática disseminada, mas há iniciativas nesta direção” e que “há clientes que definem os controles de segurança para seus serviços”. Registra-se ainda que 44% concordaram com a afirmativa.

Diante disto, há indícios de que o processo não está institucionalizado, carecendo de revisão, avaliando inclusive como interagir com o cliente no sentido de estabelecer as regras para atendimento desses tipos de controle.

Questão 28 – avaliou se o controle existente sobre o investimento de segurança em tecnologia da informação é aferido pela relação do custo do investimento e do resultado no negócio.

O resultado indicou que 47% dos gerentes concordaram parcialmente; 24% não compartilharam da afirmativa e 9% dos segmentos concordaram com a afirmativa.

Alguns gerentes que não compartilharam da afirmativa fizeram as seguintes observações:

- “A unidade não tem esse direcionamento”;
- “Não há esse relacionamento com custo do investimento e resultado do negócio”.

Diante disto, o resultado da questão indicou que o controle existente não tem sido suficiente para aferir o retorno do investimento da segurança no negócio.

Questão 29 – vinculada à questão 28, buscou verificar a freqüência com que ocorre o controle do investimento em segurança de TI aferido pela relação do custo do investimento e resultado do negócio.

Nessa questão 63% dos gerentes afirmaram não saber; 15% disseram que a freqüência é anual e 22%, que não há prazo determinado para o controle.

O resultado apresentado corrobora a percepção da questão 28, em que a maioria dos gerentes disse não concordar que os controles sejam efetivos para identificar o resultado realizado pelo investimento em TI.

Considerando o resultado das questões 28 e 29, há indícios de que os controles não estão institucionalizados nem efetivamente implementados, carecendo de aperfeiçoamento no sentido de que os resultados sejam transparentes.

4.2.5 Análise da questão Gestão de Incidentes

O objetivo foi analisar que fragilidades e eventos de segurança da informação associados com sistemas de informação ocorrem e são comunicados, permitindo adotar ação corretiva em tempo hábil.

Questão 30 – verificou se existem instrumentos formais para notificação de eventos de segurança e fragilidade que possam impactar a segurança do negócio, e se os empregados, fornecedores e terceirizados estão conscientes dessas ações.

Entre os gerentes, 62% concordaram parcialmente com a afirmativa, 34% dos segmentos concordaram e 4% não concordaram que existem instrumentos formais para notificação de eventos de segurança. Entretanto, houve a seguinte observação: “Não é uma prática institucionalizada na Empresa, algumas unidades da UPS utilizam”. O resultado sugere que há instrumentos formais, mas não estão internalizados ou disseminados no âmbito da Empresa.

De acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005, p.98-101, devem existir nas organizações canais apropriados para o registro de eventos de segurança e a diretoria precisa orientar e manter a prática.

Ainda segundo a Norma, a empresa deve alertar empregados, fornecedores e terceiros sobre a responsabilidade de notificar eventos de segurança com rapidez, orientando quanto aos procedimentos a serem adotados para esse fim. Também as áreas internas devem estar treinadas para agir imediatamente a qualquer tipo de incidente.

Importante observar que o processo de gestão de incidente deve estar alinhado à gestão de continuidade do negócio.

Questão 31 – verificou a que se relacionam com mais freqüência os incidentes de segurança.

- 26% dos gerentes disseram que os incidentes de segurança estão mais relacionados a ambiente operacional;
- 19% dos segmentos disseram estar relacionados a mau funcionamento ou sobrecarga de sistemas;
- 19% disseram que relacionados a erro humano;
- 12% disseram estar relacionados a perda de serviço, a equipamento ou recursos;
- 12% disseram estar relacionados a não-conformidade com políticas ou diretrizes;

- 12% a violação de procedimentos de segurança.

De acordo com os índices apresentados, os três itens mais sensíveis, relacionados com mais freqüência a incidentes de segurança, são: “ambiente operacional” (29%), mau funcionamento ou sobrecarga de sistemas e erro humano, ambos com 19%.

Uma análise/avaliação de riscos deve ser direcionada a cada um dos segmentos a fim de identificar com mais qualidade e propriedade o risco real, de acordo com cada contexto, conhecendo objetivamente cada um para definir e implementar os controles apropriados para reduzir os riscos, mitigar ou tomar outras providências.

Questão 32 – verificou se os incidentes de segurança são imediatamente notificados e tratados.

Disseram concordar que os incidentes de segurança são imediatamente notificados e tratados, 56% dos segmentos; 37% disseram concordar parcialmente e 8% não concordaram, apresentando as seguintes observações:

- “Os incidentes são tratados em nível de infra-estrutura, faltando ainda a correlação de serviço”;
- “Às vezes são tratados e não notificados”.

Na análise desse item é importante considerar o resultado da questão 30 que considerou que existem instrumentos formais para registro de eventos de segurança, mas não estão internalizados ou devidamente disseminados no âmbito da Empresa.

A hipótese sugerida é que a falta de divulgação e internalização dos instrumentos para reporte de eventos de segurança faculte que as ações para tratar incidentes de segurança sejam adotadas isoladamente e os incidentes tratados em nível de infra-estrutura, faltando ainda a correlação de serviços não-notificados.

Questão 33 – verificou se as ações de resposta a incidentes são adotadas imediatamente após sua notificação, porque as responsabilidades e procedimentos estão

definidos e disseminados entre os empregados, responsáveis pelas atividades.

O resultado indicou que 55% dos gerentes concordaram; 37% concordaram parcialmente e 8% dos gerentes não concordaram. Na análise desse item é importante considerar o resultado da questão 30 que considerou existirem instrumentos formais para registro de eventos de segurança, mas não estão internalizados ou devidamente disseminados no âmbito da Empresa. Configurou-se a necessidade de internalização dos instrumentos e do canal de comunicação de eventos de segurança. Essa ação deve refletir-se na melhoria de procedimentos de ação isolada.

Também é importante observar que a resposta a incidentes de segurança às vezes requer ação célere, dispensado qualquer formalismo para evitar um desastre. Diante disto, a política de gestão de incidentes de segurança deve prever como agir em situações emergenciais. Neste caso, existe alinhamento com a gestão de continuidade do negócio.

Questão 34 – verificou se os empregados estão treinados e orientados para, diante de incidente de segurança, colher as evidências a fim de assegurar a conformidade com as exigências legais, quando for o caso, e conhecer as falhas de segurança.

O resultado indicou que 55% dos gerentes concordaram parcialmente com a afirmativa e 30% concordaram que as pessoas estão treinadas para manter e colher evidências de incidentes. No entanto, 15% não concordaram.

Esse é um item diretamente relacionado à Segurança em Recursos Humanos, questão 17, que identificou se o investimento que as pessoas da unidade têm recebido em treinamento, conscientização e educação em segurança da informação é adequado à necessidade do negócio.

4.2.6 Análise da questão Continuidade do Negócio

A questão teve o objetivo de verificar quanto está institucionalizado o processo continuidade do negócio, (processo que busca não permitir a interrupção do serviço e proteger os processos críticos contra efeitos de falhas de desastres significativos e assegurar sua retomada em tempo hábil).

Questão 35 – verificou se existe plano de continuidade para atender aos processos críticos do negócio.

O resultado mostrou que 63% dos gerentes concordaram parcialmente com a afirmativa de que “existe plano de continuidade para atender aos processos críticos do negócio”; 26% concordaram, enquanto 11% discordaram.

Esse item está relacionado ao tema Governança e Gestão, questão 11, que verificou se a gestão da continuidade do negócio é uma função institucionalizada e faz parte da cultura da organização e mais de 56% dos gerentes concordaram parcialmente, enquanto 22% não concordaram.

Diante dos resultados identificados, há indicações de que o processo de gestão de continuidade do negócio não é inerente às atividades de segurança, carecendo de ações eficazes no sentido de institucionalizá-lo.

Questão 36 – verificou se a gestão de risco identifica os processos críticos ligados ao negócio, porque faz parte do processo de gestão de continuidade adotado.

Entre os gerentes, 41% concordaram que a gestão de risco identifica os processos críticos ligados ao negócio, porque faz parte do processo de gestão de continuidade; outros 41% concordaram parcialmente, mas 18% não concordaram.

Está coerente com o resultado da questão 35, que buscou identificar se existe plano de continuidade para atender aos processos críticos do negócio, cujo resultado geral foi que

63% concordaram parcialmente com a afirmativa.

Diante desses resultados, a interpretação sugerida é que o processo de gestão de riscos é conhecido, mas não está alinhado com as atividades de segurança, no contexto da gestão de continuidade do negócio, carecendo de ações eficazes no sentido de tornar os processos integrados, institucionalizados e transparentes.

Questão 37 – verificou se, em regra, ao ser definido um novo sistema ou serviço, consideram-se os requisitos de segurança necessários à continuidade do negócio e o planejamento dos recursos associados. Resultou que 48% dos gerentes concordaram com a afirmativa, outros 48% disseram concordar parcialmente e 4%, não concordaram.

As respostas comprovam que a continuidade do negócio ainda não é inerente à gestão da segurança da informação. Diante disto, é importante observar a recomendação da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005, (p.105) sobre um plano de continuidade do negócio, com uma estrutura básica, a fim de manter e assegurar a disponibilidade da informação.

4.2.7 Análise da questão Conformidade – requisitos legais

O objetivo foi de conferir quanto os requisitos legais (legislação, normas, políticas, obrigações contratuais, entre outros instrumentos legais) são considerados no atendimento ao negócio.

Questão 38 – verificou se existe garantia de que a avaliação da segurança da informação, no âmbito da unidade, é apropriada e está dentro da legalidade.

O resultado foi o seguinte: 37% dos segmentos afirmaram que há garantia de que a segurança está dentro da legalidade, “mas existem processos que ainda estão sendo adequados à legislação e às regras internas”; 30% dos segmentos disseram que “a auditoria

interna verifica periodicamente a legalidade dos processos de segurança da informação, sem que tenha havido notificação nos últimos doze meses"; 26% dos segmentos disseram não saber informar se há garantia de conformidade da segurança da informação com a legalidade; 7% dos segmentos afirmaram que não há garantia.

Diante desse resultado, pode-se inferir que há sintomas de não-conformidade, suscitando a necessidade de identificar as causas e definir ações corretivas apropriadas.

Questão 39 – verificou se os processos das unidades são executados corretamente para atender à conformidade com as normas e políticas de segurança.

O resultado indicou que 41% dos gerentes concordaram que os processos atendem à conformidade com as normas e políticas de segurança; 41% disseram concordar parcialmente e 18% não concordaram.

Considerando a análise comparativa, sugere-se que os processos de adequação a políticas, normas de segurança e legislações sejam revisados para identificar possíveis causas dos desencontros de percepções.

A ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 17799/2005 (p.112) recomenda que os gestores garantam que todos os processos sejam executados em conformidade com as normas e políticas de segurança, buscando evitar a violação da lei, normas e qualquer procedimento legal.

É importante ressaltar que a conformidade é um dos pilares da governança da segurança da informação e atribui à alta direção a responsabilidade de garantir a conformidade com as leis (NIST, 800-100, 2006, p. 6).

Questão 40 – verificou se diante da não-conformidade resultante de auditorias internas ou externas, as ações adotadas são: identificar as causas da não-conformidade, avaliar a necessidade de ações para que a não-conformidade não se repita, analisar

criticamente a ação corretiva e implementar a mais apropriada.

O resultado mostrou que 48% dos gerentes disseram concordar com a afirmativa; 48% concordaram parcialmente e 4% não compartilharam da afirmativa.

Isto evidencia que a premissa ocorre, mas não se encontra incorporada, suscitando a necessidade de identificar quais fatores influenciam no sentido de que algumas das ações não sejam adotadas para assegurar que a não-conformidade não se repita.

É importante ressaltar que a conformidade com as leis, procedimentos e regulamentos é premissa básica a ser seguida tanto no Código de Governança quanto recomenda a ISO 17799:2005.

5. CONCLUSÃO

5.1 O problema da pesquisa

Este estudo teve o objetivo de investigar quanto a gestão da segurança da informação de uma empresa pública de tecnologia da informação está direcionada ao crescimento sustentável da organização, podendo convergir para um plano de Governança da Segurança da Informação. Diante disto, para estruturação da pesquisa, foi formulada a seguinte pergunta:

Qual é a real percepção dos gerentes executivos sobre a segurança da informação no âmbito de seu segmento de atuação?

Na dimensão da governança, a alta direção, conselhos, patrocinadores, gerentes executivos são responsáveis pela promoção das condições necessárias para proteger a infra-estrutura tecnológica e por prestar esclarecimentos sobre as medidas adotadas para manter o nível adequado de segurança ao negócio (Chairman, 2001, p. 1). Neste estudo, a opção para aplicar a pesquisa nos gerentes executivos, em nível de superintendência deveu-se ao fato de que são empregados estáveis, conhecem a organização e atendem ao requisito de governança, observando que, por se tratar de empresa pública, diretoria e conselheiros são instáveis, pois a cada quatro anos de gestão há sempre uma possibilidade de mudança.

Diante disto, a pesquisa foi estruturada visando obter informações relativas a temas de segurança da informação concernentes a:

- Governança e gestão;
- Segurança em Recursos Humanos;
- Planejamento;
- Gestão de incidentes;
- Continuidade do negócio;

- Conformidade (requisitos legais).

5.1.1 Governança e gestão

Na identificação das funções exercidas pelas unidades dos diversos segmentos, tanto em governança quanto na gestão, o tema “Proteção de propriedade intelectual” não foi selecionado por algumas unidades. A empresa pesquisada constrói produtos e para proteger o direito autoral dispõe de uma Política de Propriedade Intelectual, além das Leis nº. 9.610/98 e nº. 9.609/98, que tratam sobre direito autoral, às quais se subordina. Este resultado faz perceber que o assunto deve ser revitalizado na organização.

Outros resultados que se mostraram importantes, carecendo de aprimoramento, no contexto de um modelo de gestão ou governança da segurança da informação, serão abordados a seguir:

- A maioria dos gerentes - mais de 55% - considerou que o apoio da alta direção não é suficiente para garantir as ações de segurança no âmbito da empresa. O resultado dessa variável, considerando a recomendação dos institutos pesquisados, como IBGC, NIST, ITGI, e autores como Allen, Chairman, Caralli, entre outros, seria o primeiro ponto a ser considerado para garantir que o modelo de gestão ou governança de segurança da informação seja alinhado à estratégia do negócio da organização. Enfim, sem o compromisso e entendimento da alta direção sobre a importância da segurança para manter o negócio em níveis de resultados positivos, a gestão da segurança é uma ação isolada de gerentes envolvidos em parte sob sua responsabilidade, comprometendo a própria continuidade do negócio.

- Corroborando os problemas trazidos pelo insuficiente apoio da alta direção, os resultados da pesquisa, em questões fundamentais para a segurança da informação, refletiram essa realidade. Os pontos relevantes foram os seguintes:
  - Quanto à gestão de riscos, para 70% dos gerentes ela favorece parcialmente as ações proativas para manter o risco em níveis aceitáveis;
  - 81% dos gerentes não consideram que a segurança faça parte da cultura da organização.
  -

Diante desses resultados, há indícios de que a governança e gestão necessitam da participação efetiva da alta direção, carecendo que esta seja alertada sobre a necessidade de seu envolvimento, entendendo criticamente sua responsabilidade com a continuidade do negócio.

5.1.2 Segurança de Recursos Humanos

A variável buscou verificar o quanto gerentes e empregados estão preparados, com treinamentos em segurança, para desempenhar com responsabilidade seus papéis. A pesquisa demonstrou que todas as unidades de todos os segmentos têm uma a cinco pessoas voltadas para atividades em segurança no contexto da área e que para 52% dos gerentes o investimento destinado a treinamento em segurança está adequado às necessidades do negócio.

Quanto à aplicação e resultado do investimento em treinamento, a pesquisa indicou que 50% dos gerentes participaram nos últimos doze meses de algum treinamento em gestão de segurança. Outro dado relevante é o investimento em certificações em segurança. Todos os segmentos, exceto a Unidade de Gestão Empresarial (UPS), dispõem de pessoas certificadas. Entretanto, 44% dos gerentes concordaram que as pessoas treinadas são mais motivadas, contribuem mais e são mais assertivas. A maioria dos gerentes considerou que outros fatores influenciam no compartilhamento de conhecimento e contribuições.

No geral, a pesquisa demonstrou que existem pessoas preparadas para desenvolver com responsabilidade as atividades de segurança dentro dos vários segmentos. Entretanto, não ficou claro se a distribuição desses recursos humanos capacitados está adequada à necessidade dos segmentos. Outro ponto relevante é que metade dos gerentes não participou de treinamento em segurança pelo menos nos últimos doze meses.

5.1.3 Planejamento

A variável teve o objetivo de verificar se o planejamento em segurança está alinhado ao negócio, considerando as políticas estabelecidas, os objetivos, processos e procedimentos para a gestão de riscos e melhoria da segurança da informação. O resultado da pesquisa indicou que não existe a prática institucional do orçamento priorizar o planejamento em segurança. Trata-se de prática recomenda pelo ITGI, para a governança de segurança da informação, a fim de verificar os resultados do investimento refletido no resultado do negócio. Enfim, seria a aplicação de controles para verificar o resultado sobre o investimento.

Quanto ao investimento em tecnologia da informação, 56% dos gerentes concordaram que é direcionado para os processos críticos em infra-estrutura. Considerando os resultados, a leitura resultante é que não existe uma política orientadora neste sentido, deixando claras e transparentes as regras de prioridade em planejamento.

Percebe-se que falta política que oriente as prioridades do planejamento em segurança. É o que demonstra o total de 81% dos gerentes que disseram não existir controle para verificar o resultado do investimento de segurança em tecnologia da informação em relação ao custo do investimento e do resultado no negócio.

É importante registrar que o resultado da variável planejamento alerta para a necessidade de implementar uma política de planejamento orientado para a segurança do negócio, partindo da premissa da análise de riscos para direcionar o investimento e controles de aferição do resultado sobre o investimento.

5.1.4 Gestão de Incidentes

A variável teve como objetivo detectar se as fragilidades e eventos de segurança da informação, associados a sistemas de informação, ocorrem e são comunicados, permitindo a adoção de ação corretiva em tempo hábil. Para que a organização tenha essas

informações é necessário dispor de instrumentos e canais formais e institucionalizados. De acordo com 64% dos gerentes, existem instrumentos formais, mas não estão internalizados ou devidamente disseminados no âmbito da Empresa.

Outro resultado relevante foi verificado quanto a que mais se relacionam os incidentes de segurança: 26% dos gerentes disseram que os incidentes de segurança estão mais relacionados a ambiente operacional; 19% disseram estar relacionados a mau funcionamento ou sobrecarga de sistemas e erro humano; e para 12%, os incidentes estariam relacionados à perda de serviço, equipamento ou recursos, não-conformidade com políticas ou diretrizes ou violação de procedimentos de segurança.

Adicionalmente, a pesquisa mostrou que diante de um incidente de segurança, o tratamento é imediato, independentemente de registros e canais de comunicação.

Ressalta-se que, mediante o resultado sobre ocorrência de incidentes, uma análise/avaliação de riscos deveria ser direcionada a fim de identificar com mais qualidade e propriedade o risco real, de acordo com cada contexto, conhecendo objetivamente cada um para definir e implementar os controles apropriados para reduzir os riscos, mitigá-los ou tomar outras providências.

5.1.5 Continuidade do negócio

O objetivo da variável foi verificar o quanto está institucionalizado o processo continuidade do negócio (processo que impede a interrupção do serviço e protege os processos críticos contra efeitos de falhas de desastres significativos, assegurando a retomada do serviço em tempo hábil). Para viabilizar esse processo, as empresas definem um plano de continuidade a fim de atender aos processos críticos do negócio. O resultado indicou que existe um plano, mas não está institucionalizado, carecendo de ações eficazes no sentido de torná-lo inerente à gestão de segurança ou governança.

Outro ponto relevante a ser considerado é que 59% dos gerentes disseram que a

gestão de risco não identifica os processos críticos ligados ao negócio, não estando ainda alinhada à gestão de continuidade do negócio, adotada na Empresa. Diante desses resultados, há indícios de que a continuidade do negócio ainda não é inerente à gestão da segurança da informação.

5.1.6 Conformidade – requisitos legais

Teve a variável o objetivo de verificar quanto os requisitos legais (legislação, normas, políticas, obrigações contratuais, entre outros instrumentos legais) são considerados no atendimento ao negócio. Nesta questão, o resultado indicou que para 37% dos gerentes há garantia de que a segurança está dentro da legalidade, “mas existem processos que ainda estão sendo adequados à legislação e às regras internas”; 30% disseram que “a auditoria interna verifica periodicamente a legalidade dos processos de segurança da informação, sem que tenha havido notificação nos últimos dozes meses”; 26% dos segmentos disseram “não saber” se há garantia de conformidade da segurança da informação com a legalidade; 7% dos segmentos disseram que não há garantia. Esse resultado sugere que em alguns segmentos há sintomas de não-conformidade, levando à necessidade de identificar as causas e definir ações corretivas apropriadas.

5.2 Trabalhos futuros

O presente estudo não se esgota com os resultados obtidos. Propõe-se a contribuir para as discussões qualitativas sobre o tema segurança da informação no âmbito da empresa pesquisada. Diante disto, a corroboração ou contestações aos resultados obtidos por outros trabalhos poderão aprimorar ações de melhoria sob a perspectiva da evolução para um modelo de governança da segurança da informação, contribuindo, em última instância, para uma melhor gestão.

Novos estudos podem ser feitos na busca da relação da governança com a gestão, com aplicação de testes estatísticos, dessa feita, envolvendo a alta direção (conselhos e diretoria). Dada a amplitude do tema segurança da informação e sua importância estratégica para o negócio, outros estudos podem ser desenvolvidos buscando responder a questões como:

- Identificar ações de governança da segurança da informação para proteger os ativos de informação de uma empresa pública de TIC;
- Investigar como fatores endógenos afetam a gestão da segurança da informação e como é possível avaliar e promover ações de melhoria;
- Desenhar um modelo da relação endógena, identificando os níveis de relacionamento na dimensão estratégica, tática e operacional, que possa contribuir para o sucesso da segurança da informação numa estrutura de governança corporativa;
- Detectar os fatores que contribuem para que os conselhos e diretoria não conheçam suas responsabilidades em relação ao sucesso da gestão da segurança da informação, verificando ações de melhoria que possam ser desencadeadas.

Outra observação a ser considerada em termos de novos estudos seria investigar o modelo de segurança da informação que melhor atenda aos interesses da empresa, do cliente e da sociedade, no contexto da proteção de serviços críticos e infra-estrutura, com a finalidade de desenvolver uma cultura de segurança, nos moldes que recomenda a ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD).

Finalmente, analisando o resultado da pesquisa desta dissertação, sugere-se como proposta de trabalhos futuros o processo de ações de melhoria da segurança da informação na empresa que serviu de base ao estudo. O trabalho, com finalidade de aperfeiçoamento do modelo de segurança da informação, buscando atender aos interesses da empresa, do cliente e da sociedade, no contexto da proteção de serviços e infra-estrutura críticos, deveria respaldar-se nos quesitos da pesquisa que apresentaram mais fragilidade, partindo daquele que identificou a importância do envolvimento da alta direção (conselhos, diretoria e patrocinador) como apoiador estratégico. E assim, desenvolver uma cultura de segurança, nos moldes que recomenda a OECD e dentro dos preceitos da legalidade preconizados pelo Decreto nº. 6.021, de janeiro/2007.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT** ISO/IEC Guia 73:2005. **Gestão de Riscos.** Vocabulário. Recomendações para uso em normas.

_____. **ABNT** NBR ISO/IEC 17799:2005. **Tecnologia da Informação**. Técnicas de Segurança. Código de prática para a gestão da Segurança da Informação.

_____. **ABNT** NBR ISO/IEC 27001. 2006. **Tecnologia da Informação.** Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos

AUSTRALIAN STANDARD FOR RISK MANAGEMENT **AS/NZS** 4360:2004. Série Risk Management. **Gestão de Riscos.** A norma AS/NZS 4360:2004

_____. **AS/NZS** 4360:2004. Série Risk Management. **Gestão de Riscos**. Diretrizes para a implementação da AS/NZS 4360:2004

ALLEN, Julia, **Governing for Enterprise Security. Networked Systems Survivability Program**, June 2005. Carnegie Mellon University and Software Engineering Institute Material. Technical Note CMU/SEI–2005–TN–023. Disponível em: <http://www.sei.cmu.edu/publications/pubweb.html>. acesso em: jan. 2007.

BERNARDES, Mauro César, MOREIRA, Edson dos Santos. **Um Modelo para Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional. Instituto de Ciências Matemáticas e de Computação** (ICMC). Universidade de São Paulo, 13560-970 São Carlos - SP

BITTERLI, Peter R. IT Security Governance – **A Slow Start to a High Maturity Level. Information Systems Control Journal**. v.I, 2005. Information Systems Audit and Control Association (ISACA). Disponível em: <http://www.isaca.org>. Acesso em: jun. 2006.

BOOZ, Allen Hamilton. **Convergence of Enterprise Security Organization. Information Systems Security Association** (ISSA). Novembro, 2005. Information Systems Audit and Control Association (ISACA). Disponível em: <http://www.isaca.org>. Acesso em: jan. 2007.

BRITISH STANDARD **BS** 25999-1:2006, Business Continuity Management (BCM), Part 1: **Code of Practice**. British Standard Institute (BSI)

CARALLI, Richard A. **Managing for Enterprise Security. Networked Systems Survivability Program**, December 2005. Carnegie Mellon University and Software Engineering Institute Material. Technical Note CMU/SEI–2004–TN–046. Disponível em <http://www.sei.cmu.edu/publications/pubweb.html>. Acesso em: jan. 2007.

CARR, Nicholas G., **IT Doesn't Mattre.** Harvard Business Review Online. May 2003. On-line version. Disponível em: <http://harvardbusinessonline.hbsp.harvard.edu>. Acesso em: 12 mar. 2004.

CHAIRMAN, Thomas Horton. **Information Security Governance:** what Directors Need to Know. 2001. The Institute of Internal Auditors. ISBN 0-89413-457-4. Disponível em: <http://www.isaca.org>. Acesso em: jul. 2007.

CONNER, Bill, NOONAN, Tom, HOLLEYMAN, Robert W., **Information Security Governance:** Toward a Framework for Action. 2004. Business Software Alliance (BSA). Disponível em: <http://www.bsa.org>. Acesso em: mar. 2007.

CONNER, William, **Information Security Governance. Entrust** – Securing Digital Identities & Information. April 2003. Disponível em: <http://www.entrust.com>.

DOMINGUES, Heron; **Governança de TI** – um caminho sem volta. 2005. IT Governance Institute (ITGI). Disponível em: <http://www.itgi.org>.

ELOFF, M.M., SOLMS, S.H. **Information Security Management**: A Hierarchical Framework for Various Approaches. 2000. Computer & Security Vol. 19, No. 3, (2000) 243-256. Department of Computer Science, Rand Afrikaans University Johannesburg, South Africa.

FERNANDES, Aguinaldo Aragon, ABREU, Vladimir Ferraz de, **Implantando a Governança de TI:** da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport Livros e Multimídia Ltda. ISBN 85-7452-270.8. 2006

GARTNER. Gartner. **Structure and Content of an Enterprise Information Security Architecture**. G00136867. 2006. Disponível em: <http://www.gartner.org>.

HAES, Steven De, GREMBERGEN, Wim Van. **IT Governance Structures**, Processes and Relation Mechanisms: achieving IT/Business Alignment in a Malor Belgian Financial Group. 2005. University of Antwerp Management School. 0-7695-2268-8/05/(C) 2005 IEEE.

HÁFEZ, Andréa, **A governança corporativa não se limita a um conjunto de princípios, pode ser um instituto jurídico**. Espaço Jurídico – Notícias. Bovespa. 2005. Disponível em: <http://www.bovespa.com.br>.

HAMILTON, Booz Allen, **Convergence of Enterprise Security Organizations.** 2005. ASIS International; Information Systems Security Association (ISSA).; Information Systems Audit and Control Association (ISACA). Disponível em: <http://www.isaca.org>.

HESKETT, James, **What's the Future of Corporate Governance?** Harvard Business School. July 2001. Disponível em: <http://hbswk.hbs.edu/cgi-bin/>.

HÖNE, Karin, ELOFF, JHP. **Information Security Policy** – what do international information security standards say? 2002. Department of Computer science Rand Afrikaans University. 0167-4048/02US 2002. Disponível em: <http://harvardbusinessonline.hbsp.harvard.edu>.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **IBGC**. Código de Melhores Práticas. 2004. Disponível em: <http://www.ibgc.org.br>. Acesso em: mar.2007.

_____. **IBGC.** Guia de Orientação para Gerenciamento de Riscos Corporativos. 2007. Disponível em: <http://www.ibgc.org.br. Acesso em: jul. 2007.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **ITGI**. Information Security Governance: Guidance for Boards of Directors and Executive Management. 2006. 2a. Edition. Disponível em: <http://www.itgi.org>.

_____. **ITGI.** Board Briefing on IT Governance. Second Edition. 2004. ISBN 1-89209-64-4. Disponível em: <http://www.itgi.org>.

ISO Guide 73:2002. **Risk Management**. Guidelines for use in standards.

KRUTZ, Ronald L. and VINES, Russell Dean, **The CISSP Prep Guide**: Mastering the Ten Domains of Computer Security. Jonh Wiley & Sons. 2001. USA.

LEACH, John. **Improving user Security Behaviour.** 2003. Computer & Security, vol. 22, nº. 8, 0167-4048/03 2003. Elsevier Ltd.

MARCONI, Marina de Andrade e LAKATOS, Eva Maria, **Metodologia do trabalho Científico**. Editora Atlas S.A, 6ª edição, 2006. São Paulo.

MORESI, Eduardo, **Metodologia da Pesquisa**. UCB, 2004. Brasília - DF.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST**. Information Security. U.S. Department of Commerce. Recommended Security Controls for Federal Information Systems. NIST Special Publication 800-53. 2005. Disponível em: <http://www.nist.gov>.

_____. **NIST**, **Information Security.** U.S. Department of Commerce. Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100. 2006. Disponível em: <http://www.nist.gov>.

NORMA BRASILEIRA **NBR** 25999-1:2007, Gestão da Continuidade do Negócio, Parte 1**:** Código de práticas.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD.** Information and Communications Technologies. ISBN-9264-026444. 2006. Disponível em: <http://www.oecd.org>. Acesso em: mai. 2007.

_____. **OECD**, Organization for Economic Co-operation and Development. Principles of Corporate Governance. 2004. Disponível em: <http://www.oecd.org>. Acesso em: jul.2007.

_____. **OECD,** Organization for Economic co-operation and Development. **The Promotion of a Culture of Security for Information Systems**. JT00196105. 2005. Disponível em: <http://www.oecd.org>. Acesso em: 2006.

PFLEEGER, Charles P., **Security in Computing.** 2ª. Edition. Editorial Precision Graphic Services Inc. NJ 07458. 1997. USA

PIRONTI, John P., **Informations Security Governance:** Motivations, Benefits and Outcomes. ISACA. 2006. Disponivel em: http://www.isaca.org>.

RABELO, Flavio, SILVEIRA, José Maria da, **Estruturas de Governança e Governança corporativa:** avançando na direção da integração entre as dimensões competitivas e financeiras. IE/UNICAMP, Campinas, nº. 77, 1999.

RAUEN, André Tortato, **Revista Espaço Acadêmico** – nº. 69. fevereiro/2007. Mensal – Ano VI - ISSN – 1519.6186. Departamento de Economia da Universidade Extremo Sul Catarinense (UNESC).

RIBBEERS, Pieter M. A., PETERSON, Ryan R., PARKER, Marylin M., Designing Information Technology **Governance Processes:** Diagnosing Contemporary Practices and Competing Theories. Hawaii International Conference on System Sciences. 2002. 0-7695-1435-9/02 IEEE.

SCHUMACHER, Markus, BUGLIONI, Eduardo Fernandez, HYBERTSON, Duane, BUSCHMANN, Frank, SOMMERLAD, Peter, **Security Patterns**: Integrating Security and Systems Engineering. Jonh Wiley & Sons, Ltd. 2006. PO198SQ, England.

SETHURAMAN, Sekar, **Road Map for Information Security:** what to do after BS 7799 Certification. 2006. Isaca JornalOnline. Disponível em: <http://www.isaca.org>.

STEINBERG, Herbert, Vários colaboradores. **A Dimensão Humana da Governança Corporativa**: pessoas criam as melhores e piores práticas. 2003. São Paulo: Editora Gente. ISBN 85-7312-397-4.

Von SOLMS, Rossouw, **The 10 Deadly Sins of Information Security Managegement.** Elsevier: Computers & Security. 2004. Disponível em: <http://www.elsier.com>.

WEILL, Peter and WOODHAM, Richard., **Don't Just Lead, Govern**: Implementing Effective IT Governance. 2002. CISR WP nº.326. Massachusetts Institute of Technology. Disponível em: <http://web.mit.edu/cisr>.

WEILL, Peter, ROSS, Jeanne W., **Governança de Tecnologia da Informação**. 2006. São Paulo. M. Books do Brasil Ltda.

WEILL, Peter, ROSS, Jeanne W.; **IT Governance on One Page**. 2004. Center for Information System Research. CISR WP nº. 349 and Sloan WP nº. 4516-04. Massachusetts Institute of Technology, Cambridge. Disponível em: <http://web.mit.edu/cisr/>.

WEILL, Peter, WOODHAM, Richard, **Don't Just Lead, Govern:** Implementing Effective IT Governance. 2002. Center for Information System Research. CISR WP nº. 326. Massachusetts Institute of Technology, Cambridge. Disponível em: <http://web.mit.edu/cisr/>

Referências auxiliares

CERT/CC; CSO Magazine; United States Secret Service. **E-Crime Watch survey.** 2004. Carnegie Mellon University Software Engineering Institute. Pennsylvania. USA. Disponível em: <http://www.sei.emu.edu/publication>.

CERT-br; Estatísticas dos Incidentes Reportados. 2006, 2005, 2004, até 1999. Disponível em: <http://www.cert.br/stats/incidentes>.

_____. Cartilha de Segurança para Internet. Disponível em: <http://www.nbso.nic.br/docs/cartilha>.

CSI/FBI; Computer Crime and Security Survey. 2006. www.gocsi.com e www.austcert.or.au

DELOITTE, Touche Tohmatsu. TMT Global Security Survey 2006. Audit, Tax, Consulting, Financial Advisory. 2005. www.dexsurvey.deloitte.com

Legislação brasileira

BRASIL. Decreto nº. 3.505, de 13 de junho de 2000, **Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.**

_____. Decreto nº. 4.553, de 27 de dezembro de 2002, **Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.**

_____. Decreto nº. 6.021, de 22 de janeiro de 2007, **cria a Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União** – CGPAR, e dá outras providências.

Documentos normativos utilizados

SERPRO. Decisão de Diretoria – **Estrutura Orgânica do Serviço Federal de Processamento de Dados** – Serpro. OE-013/2006.

_____. Resolução SG-012/2005. **Política Corporativa de Segurança da Informação** – PCSI.

_____. Decisão de Diretoria – **Programa de Segurança do Serpro** (PSS), SG-144/ 2005.

_____. Decisão de Diretoria – **Gestão de Riscos de Segurança,** SG-113/2006.

_____. Norma - **Classificação dos Ativos de Informação do Serpro**. SG-005/2005.

_____. Metodologia de execução do Programa de continuidade do negócio do Serpro (PCN), 2006.

Apêndice A – Formulário da Pesquisa

Questionário da Pesquisa sobre a segurança da informação, no âmbito do SERPRO, sob o enfoque da Governança da Segurança da Informação.

Apresentação

Este questionário tem objetivo acadêmico e visa agregar valor à pesquisa qualitativa em segurança da informação cujo escopo é a Governança da Segurança da Informação.

Esta pesquisa será aplicada aos ocupantes de cargo de Superintendente das diversas áreas de conhecimento, por serem os líderes principais da linha de comando da estrutura organizacional. Nesta condição, dispõem de conhecimentos estratégicos e táticos sobre o negócio da Empresa e sobre a segurança da informação, que está alinhada a sua linha de negócio.

Sua cooperação em responder todas as questões no melhor de sua compreensão é fundamental para o trabalho que está sendo construído.

Classificação: restrito e controlado. Não identifica o pesquisado, apenas o segmento da estrutura organizacional – Consultoria e Apoio (AUDIG, COJUR, GABDP), UAE (Unidade de Alinhamento Estratégico), UPS (Unidade de Produto e Serviço), URC (Unidade de Relacionamento com Cliente) e UGE (Unidade de Gestão Empresarial).

Instruções de preenchimento

1 – Não existem respostas certas ou erradas, mas aquela que melhor expresse sua opinião.

2 – Todos os itens devem ser preenchidos, observando que

- na maior parte das questões, a resposta é única;
- alguns itens podem ter respostas múltiplas. Neste caso, haverá a informação “marque todas as aplicáveis”;
- se optar pelo item “outros”, o campo complementar “Cite” deve ser preenchido.

3 – Para marcar a opção ou opções escolhidas, quando for o caso, favor preencher o campo [ ] com a letra “X”.

4 – O prazo de preenchimento é de 3 dias, a partir desta data: 17/04/2007.

5 – Em caso de dúvida, contatar Maria do Carmo Mendonça, ramal ...

Governança e Gestão

Glossário

Governança: estrutura que determina os objetivos organizacionais e monitora o desempenho para assegurar a concretização desses objetivos (OECD).

Governança Corporativa: conjunto de práticas de gestão, envolvendo, entre outros, os relacionamentos entre acionistas ou quotistas, conselhos de administração e fiscal ou órgãos com funções equivalentes, diretoria e auditoria independentes, com a finalidade de otimizar o desempenho da empresa e proteger os direitos de todas as partes interessadas, com transparência e eqüidade, com vistas a maximizar os resultados econômico-sociais da atuação das empresas estatais federais". (IBGC – Instituto Brasileiro de Governança Corporativa).

Gestão da continuidade do negócio: tem o objetivo de não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e de assegurar sua retomada em tempo hábil. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC 17799:2005).

Gestão de incidentes de segurança da informação: tem o objetivo de assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. (ABNT ISO/IEC 17799:2005).

Escopo da Governança

1 – Quais das funções abaixo existem em sua Unidade? Marque todas as aplicáveis.
[ ] Planejamento e estratégia de segurança para serviços de clientes (relacionamento com cliente)
[ ] Gestão da segurança em ambiente de TI
[ ] Implementação de segurança em serviços de clientes (política, processos e tecnologia)
[ ] Gestão de segurança para proteção de dados e informação
[ ] Gestão de segurança física e do ambiente
[ ] Controle de acesso
[ ] Gestão de continuidade do negócio
[[Gestão de recursos humanos
[ ] Gestão de incidentes
[ ] Proteção de propriedade intelectual
[ ] Segurança de rede
[ ] Desenvolvimento e manutenção de sistemas de informação
[ ] Gestão de contratos de serviços
[ ] Gestão financeira
[ ] Nenhum dos itens
[ ] Outros. Cito: _____
_____
_____

2 – O apoio ou comprometimento da alta direção da empresa com os processos de segurança tem sido suficiente para garantir o resultado esperado.
[ ] É suficiente
[ ] É parcialmente suficiente
[ ] É insuficiente
[ ] Não sei

3 – A segurança adotada na organização tem sido suficiente para proteger patrocinadores, investidores, clientes, empregados e fornecedores, de acordo com as expectativas da Unidade.
[ ] É suficiente
[ ] É parcialmente suficiente
[ ] É insuficiente
[ ] Não sei

4 – O nível de importância de sua unidade em relação à segurança da informação para o sucesso do negócio da organização, em sua opinião, é considerado:
[ ] Alto
[ ] Médio
[ ] Baixo
[ ] Não sei

5 – A segurança adotada nos processos sob sua responsabilidade contribui para que a organização garanta e sustente um nível previsível, aceitável e adequado de segurança compatível com a missão do negócio.
[ ] Contribui plenamente
[ ] Contribui parcialmente
[ ] Não contribui
[ ] Outros. Cito: _____

6 – Os contratos que determinam responsabilidade das partes (empresa, clientes, empregados e fornecedores) garantem a confidencialidade, integridade e disponibilidade do negócio contratado.
[ ] Garantem plenamente
[ ] Garantem parcialmente
[ ] Não garantem
[ ] Outros. Cito: _____

7 – O processo de gestão de riscos do negócio favorece ações proativas para manter o risco em níveis aceitáveis.
[ ] Favorecem plenamente
[ ] Favorecem parcialmente
[ ] Não favorecem
[ ] Outros.Cito: _____

8 – A revisão periódica dos processos de segurança por meio da gestão de risco é mandatório para garantir a sustentação da continuidade do negócio, adequabilidade e efetividade da segurança.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Insuficiente
[ ] Não sei

9 – Os controles de segurança utilizados são adequados e incluem os documentos de política, a atribuição de responsabilidade, o processamento correto nas aplicações, a gestão de vulnerabilidade técnica, a gestão da continuidade do negócio e a gestão de incidentes de segurança da informação e melhorias.
[ ] Suficientes
[ ] Parcialmente suficientes
[ ] Insuficientes
[ ] Não sei

10 – A segurança da informação faz parte da cultura da organização; existe respeito às regras e ações de segurança em todos os processos de negócio, nos níveis gerenciais estratégico, tático e operacional.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____
_____
_____

11 – A gestão da continuidade do negócio é institucionalizada, faz parte da cultura da organização e inclui controles para identificar e reduzir riscos, protegendo os processos críticos contra falhas ou desastres significativos.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____
_____
_____

12 – Os processos críticos estão protegidos contra ameaças que interferem na confidencialidade, integridade e disponibilidade dos serviços.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____
_____
_____

13 – O processo de recuperação de desastre, para atendimento a níveis de serviço contratados pelo cliente está institucionalizado ou garantido.
[ ] Concordo
[ ] Concordo parcialmente

[ ] Não concordo
[ ] Outros. Cito: _____

14 – A certeza de que a segurança aplicada ao negócio tem sido suficiente para detectar e prevenir incidentes de segurança respalda-se no fato de que não houve registro de infecção de vírus nos últimos doze meses, que comprometesse o negócio.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

Segurança em Recursos Humanos

Glossário

Segurança em recursos humanos: busca assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de roubo, fraude ou mau uso dos recursos. (ISO/IEC 17799:2005).

15 – Qual o número de pessoas lotadas em sua Unidade?
[ ] Até 50 pessoas
[ ] 51 até 100 pessoas
[ ] 101 até 200 pessoas
[ ] Até 500 pessoas
[ ] Outro. Cito: _____

16 – Qual o número de pessoas lotadas em sua unidade que tem atividade específica de segurança?
[ ] 1a 5 pessoas
[ ] 6 a 10 pessoas
[ ] Até 50 pessoas
[ ] Outro. Cito: _____

17 – O investimento que as pessoas da Unidade têm recebido em treinamento, conscientização e educação em segurança da informação é adequado à necessidade do negócio.
[ ] Concordo
[ ] Eventualmente invisto em treinamento de segurança
[ ] Esse tipo de treinamento não é importante para a unidade
[ ] Outros. Cito: _____

18 – O acompanhamento dos resultados dos treinamentos aplicados demonstra que as pessoas ficam mais motivadas, contribuem mais com a Área, compartilham o conhecimento e apresentam melhores níveis de assertividade.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

19 – Quais são as certificações em segurança que existem no pessoal de sua Unidade? Marque todas as aplicáveis
[ ] CISSP (Certified Information System Security Professional)
[ ] MCSO (Modulo Certified Security Officer)
[ ] Auditor Líder ISO 27001 ou BS 7799-2
[ ] ACPCF (Axur Certified Professional Computer Forensics)
[ ] Outras. Cito: _____

20 – De acordo com a resposta 19, cite a quantidade de pessoas certificadas, por tipo de especialidade.
[ ] CISSP (Certified Information System Security Professional)
[ ] MCSO (Modulo Certified Security Officer)
[ ] Auditor Líder ISO 27001 ou BS 7799-2
[ ] ACPCF (Axur Certified Professional Computer Forensics)
[ ] Outras. Cito: _____

21 – Há melhor resposta das pessoas certificadas nas questões de segurança em relação aos demais?
[ ] Sim
[ ] Não
[ ] Não sei

22 – Nos últimos 12 meses você participou de algum programa de treinamento, visando ao conhecimento voltado para sua Unidade, sobre a segurança da informação?
[ ] Sim
[ ] Não houve programa de treinamento voltado para minha área
[ ] Não, porque não tenho tempo para dedicação a treinamento
[ ] Outros. Cito: _____

23 – Que ações estão sendo adotadas por seus gerentes para garantir o uso ético das informações críticas da empresa? Marque todas as aplicáveis
[ ] Conscientizando
[ ] Aplicando ações disciplinares administrativas diante de situações de reincidência

[ ] Não sei
[ ] Outros. Cito: _____

Planejamento

Glossário

Planejamento em segurança: estabelecer política, objetivos, processos e procedimentos relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização. (ABNT NBR ISO/IEC 27001).

Processo Crítico: devem ser identificados e integrados à gestão da segurança da informação com as exigências da gestão de continuidade do negócio com outros requisitos de continuidade relativos a tais aspectos como operações, funcionários, materiais, transporte e instalações. (ABNTNBR ISO/IEC 17799:2005).

24 – O orçamento destinado à segurança em sua Unidade, com prioridade para os processos críticos e de infra-estrutura, está em concordância com o planejamento estratégico da organização.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

25 – Um dos critérios considerados para priorizar os investimentos em segurança da informação direciona para os processos críticos.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito _____

26 – Um dos critérios considerados para priorizar os investimentos em tecnologia da informação direciona para os processos críticos em infra-estrutura.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

27 – A adoção dos controles de segurança respalda-se prioritariamente, nos resultados das auditorias internas e externas, registros de incidentes e análise e gestão de riscos.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

28 – O controle existente sobre o investimento de segurança em tecnologia da informação é aferido pela relação do custo do investimento e do resultado no negócio.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

29 – Em caso afirmativo na resposta 28, acima, com que freqüência o controle é realizado?
[ ] Semestral
[ ] Anual
[ ] Sem prazo determinado
[ ] Não sei
[ ] Outros. Cito: _____

Gestão de Incidentes

Glossário

Gestão de incidentes: busca assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. (ISO/IEC 17799:2005).

30 – Existem instrumentos formais para notificação de diferentes eventos de segurança e fragilidades que possam impactar na segurança do negócio, e os empregados, fornecedores e terceirizados estão conscientes sobre essas ações.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

31 – Os incidentes de segurança mais freqüentes estão relacionados a (Marque todas as aplicáveis):
[ ] Perda de serviço, equipamento ou recursos
[ ] Ambiente operacional (parada do serviço, gestão inadequada de *patch*)
[ ] Mau funcionamento ou sobrecarga de sistema
[ ] Erro humano
[ ] Não-conformidade com políticas ou diretrizes
[ ] Violação de procedimentos de segurança
[ ] Não sei.

32 – Os incidentes de segurança são imediatamente notificados e tratados.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

33 – As ações de resposta a incidentes são tomadas imediatamente após sua notificação, porque as responsabilidades e procedimentos estão definidos e disseminados entre os empregados, responsáveis pelas atividades.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

34 – Os empregados estão treinados e orientados para, diante de incidente de segurança, colher as evidências a fim de assegurar a conformidade com as exigências legais, quando for o caso, e conhecer as falhas de segurança.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

Continuidade do Negócio

Glossário

Continuidade do negócio: não permitir a interrupção do negócio e proteger os processos críticos contra efeitos de falhas de desastres significativos e assegurar sua retomada em tempo hábil. (ISO/IEC 17799:2005)

35 – Existe plano de continuidade para atender os processos críticos.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

36 – A gestão de riscos identifica os processos críticos ligados ao negócio sob a responsabilidade de sua Unidade, porque faz parte do processo de gestão de continuidade adotado.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

37 – Em regra, ao ser definido um novo sistema ou serviço, consideram-se os requisitos de segurança necessários à continuidade do negócio e o planejamento dos recursos associados.
[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

Conformidade (requisitos legais)

Glossário

Conformidade: busca evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. ISO/IEC 17799:2005.

38 – Há garantia de que a avaliação da segurança da informação, no âmbito da unidade, é apropriada e está dentro da legalidade?
[ ] Sim, a auditoria interna verifica periodicamente a legalidade dos processos de segurança da informação, sem que tenha havido notificação nos últimos doze meses
[ ] Sim, mas existem processos que estão sendo adequados à legislação e às regras internas
[ ] Não sei
[ ] Não há garantia. Cito: _____

39 – Os processos de sua área são executados corretamente para atender a conformidade com as normas e políticas de segurança.

[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

_____

_____

40 – Diante da não-conformidade verificada em resultado de auditorias internas ou externas, as ações tomadas são: identificar as causas da não-conformidade, avaliar a necessidade de ações para que a não-conformidade não se repita, analisar criticamente a ação corretiva e implementar a mais apropriada.

[ ] Concordo
[ ] Concordo parcialmente
[ ] Não concordo
[ ] Outros. Cito: _____

_____

_____

Agradeço sua colaboração.
Maria do Carmo Soares de Mendonça