

Fundação Getulio Vargas
Escola de Administração de Empresas de São Paulo

ANDRE SHIGUERU HORI

Modelo de Gestão de Risco em Segurança da
Informação: Um estudo de caso no mercado
brasileiro de Cartões de Crédito

São Paulo
2003

Modelo de Gestão de Risco em Segurança da
Informação: Um estudo de caso no mercado
brasileiro de Cartões de Crédito

ANDRE SHIGUERU HORI

Modelo de Gestão de Risco em Segurança da Informação: Um estudo de caso no mercado brasileiro de Cartões de Crédito

Banca Examinadora:

Prof. Orientador Dr. Jaci Corrêa Leite

Prof. Dr. Eduardo H. Diniz

Prof. Dr. Hiroo Takaoka – FEA/USP

Fundação Getúlio Vargas
Escola de Administração de Empresas de São Paulo

ANDRE SHIGUERU HORI

Modelo de Gestão de Risco em Segurança da
Informação: Um estudo de caso no mercado
brasileiro de Cartões de Crédito

Dissertação apresentada ao Curso de
Pós-Graduação da FGV-EASP
Área de Concentração: Sistemas de Informação
Como requisito para obtenção do título de
Mestre em Administração.

Orientador: Prof. Dr. Jaci Corrêa Leite

São Paulo

2003

*Dedico esta dissertação e o
próprio título de Mestre aos
meus pais, Yoichi e Anna,
e à minha esposa Delva..*

AGRADECIMENTOS

Registrar o agradecimento a todos aqueles que contribuíram para realização deste trabalho é o mínimo que posso fazer como forma de expressar meu reconhecimento aos esforços, incentivos e apoios que recebi e aos quais gostaria de prestar os meus mais sinceros agradecimentos.

Agradeço à minha família, minha esposa Delva Damaceno, e meus filhos, Willian e Jhessica, por sua grande paciência, incentivo e apoio em todos os momentos difíceis à realização deste trabalho.

Agradeço em especial ao professor e orientador Jaci Corrêa Leite, que me estimulou, aconselhou, e orientou de maneira segura este meu trabalho até sua conclusão, mesmo tendo o tempo como nosso grande inimigo. Aos professores Eduardo Diniz e Hiroo Takaoka, por se predisporem a analisar este trabalho. Ao professor Paulo Roberto Feldmann pelo incentivo e inspiração.

Agradeço aos amigos, Nelson Hirano e Sergio Schmidt, que sempre me incentivaram e apoiaram nas diversas situações profissionais, durante todos estes anos, para que eu pudesse executar e concluir este trabalho.

Agradeço a PricewaterhouseCoopers, na pessoa de Edgar Roberto D'Andrea, pela compreensão, incentivo e condições para que este trabalho pudesse ser finalizado.

Agradeço também à Visanet, especialmente ao Sergio Cloves pelo apoio e suporte necessário para a realização deste trabalho. Agradeço também todos os profissionais da Visanet que participaram e contribuíram para o estudo de caso.

Agradeço aos meus colegas, professores e funcionários da Fundação Getúlio Vargas que me ensinaram muitas coisas importantes e interessantes durante esta agradável convivência nestes últimos anos.

Deixo também meus agradecimentos aos amigos Andre Ohl, Iuzo Yokobatake, Ramon Bustamante, Frederico Seidi Hori, Fabio Odagui, Vladimir Seger, Augusta Takeda, Celso Fujita, Anísio Straub, Debora Morandim, Carolina Hori, Marcos Gama, Darli Cunha, Tayse Orlovas, Lorival Rangel Mattos e Luciana Damaceno, que me incentivaram e contribuíram direta ou indiretamente para realização deste trabalho.

Agradeço aos meus avós, Toshio e Yoshie Takeda, e Shiniti e Yoshie Hori, e muito aos meus pais, Yoichi e Anna Hori, que sempre acreditaram e investiram em mim muito esforço, amor, e educação. Obrigado por me ajudarem a alcançar minhas metas e sonhos.

“‘Há muitos Inimigos’ é uma técnica que se aplica nos combates contra muita gente.(...) O espírito deve ser enfrentar os inimigos em todas as direções, pois eles podem vir de todos os lados. Observe a sua ordem de ataque, e enfrente primeiro quem atacar primeiro.”

Miyamoto Musashi em O Livro de Cinco Anéis

RESUMO

As questões ligadas a gestão de riscos associados a segurança da informação já é uma realidade no cenário empresarial brasileiro. O crescimento das operações de negócios em direção aos sistemas de informação baseados em tecnologia fez com que os números de ameaças e de vulnerabilidades sobre as redes de computadores e comunicações aumentassem. Vários são os desafios de estruturação e implementação de uma área de segurança da informação dentro das empresas. Este trabalho analisa as diversas formas de construção de uma infra-estrutura de gestão de risco em segurança de informação, não só no âmbito tecnológico, mas também, no operacional e no mercadológico, de forma a estabelecer uma relação transparente às demais áreas internas da organização, aos clientes e a todo o mercado. A segurança da informação, vista freqüentemente como um assunto ligado a tecnologia, passa a ser entendida cada vez mais como um processo de negócio, e conseqüentemente, uma grande vantagem competitiva para o mundo empresarial.

PALAVRAS-CHAVE

- ?? Segurança da informação
- ?? Segurança de computadores
- ?? Segurança de redes
- ?? Gerenciamento da segurança da informação
- ?? Gerenciamento de risco
- ?? Modelo de gestão de risco

ABSTRACT

The concerns regarding managing information security risks are already part of the Brazilian enterprise environment's reality. The business processes' expansion towards the information systems based on technology made the number of threats grow as well as the vulnerability of the computer and communication networks. Several are the challenges regarding the security information area's infrastructure, and also the implementation of it within a given company. This study analysis the different ways of building up a managing information security risks' infrastructure, not only at the technology level but also at the operational level as well as on regarding the marketing concepts, establishing a clear relation to all other internal areas of the company, and also to customers and to the marketplace itself. The information security, often taken as a technology matter, is now seen as a business process; consequently, it is understood by the enterprise world as a real competitive advantage.

KEY WORDS

- ?? Information security
- ?? Computer Security
- ?? Network security
- ?? Information security management
- ?? Risk management
- ?? Risk management model

SUMÁRIO

1. Introdução	16
1.1. Definição do Problema	18
1.2. Justificativa do Estudo	21
1.3. Objetivos	23
1.3.1. Objetivo Geral.....	23
1.3.2. Objetivos Específicos	23
1.3.3. Delimitação do Objeto	24
2. Fundamentação Teórica.....	25
2.1. Gerenciamento de riscos	25
2.1.1. Conceito de risco.....	25
2.1.2. Classificação dos riscos.....	26
2.1.3. O processo de gerenciamento de risco.....	35
2.2. Gestão de risco e segurança da informação	47
2.2.1. Conceitos básicos sobre segurança da informação.....	48
2.2.2. Ameaças e seus elementos	51
2.2.3. Gerenciamento de risco e segurança da informação	56
2.2.4. Segurança da informação e auditoria de sistemas	62
2.3. Modelo de Gestão de Risco em Segurança da Informação.....	67
2.3.1. Direcionadores de negócio e agentes de implementação	67
2.3.2. Alinhamento estratégico da segurança da informação.....	71
2.3.3. Segurança das Operações	83
2.3.4. Gerenciamento de Identidades.....	102

2.3.5. Modelos de gestão de risco em segurança da informação.....	110
3. Metodologia da Pesquisa	114
3.1. Pesquisa Exploratória	114
3.2. Estudo de caso	115
3.3. Seleção do Caso Único	117
4. Estudo de Caso Resultados da Pesquisa	119
4.1. O negócio VISANET	119
4.1.1. Estrutura organizacional	121
4.1.2. Conceitos e terminologias da VISANET.....	122
4.1.3. A relação da VISANET com seus parceiros	125
4.1.4. Principais processos de negócio	126
4.1.5. Detalhes tecnológicos e operacionais	129
4.2. Segurança da informação na VISANET	130
4.2.1. Alinhamento estratégico.....	130
4.2.2. Segurança das operações.....	138
4.2.3. Gerenciamento de Identidades.....	154
5. Discussão dos Resultados	159
6. Conclusão	170
6.1. Conclusões	170
6.2. Limitações.....	172
6.3. Sugestões para novas pesquisas.....	173
7. Bibliografia	175
8. Glossário	186
Anexo 1: Questionários	193

LISTA DE FIGURAS

FIGURA 1: COMO O BRASILEIRO GASTA SEU DINHEIRO	19
FIGURA 2: ABECS EVOLUÇÃO ANUAL.....	19
FIGURA 3: EVOLUÇÃO DO MERCADO	22
FIGURA 4: TIPOS DE RISCO.....	31
FIGURA 5: CLASSIFICAÇÃO DE RISCO	32
FIGURA 6: PROCESSO DE GERENCIAMENTO DE RISCO DE CULP	36
FIGURA 7: OBJETIVOS DE NEGÓCIO X RISCOS.....	37
FIGURA 8: CÁLCULO DA PROBABILIDADE.....	39
FIGURA 9: IMPACTOS	40
FIGURA 10: CRITICIDADE.....	40
FIGURA 11: ESTRUTURA TEMPORAL.....	40
FIGURA 12: COMPARAÇÃO ENTRE OS MÉTODOS	42
FIGURA 13: MITIGAR O RISCO.....	44
FIGURA 14: CADEIA DE VALOR DE PORTER.....	47
FIGURA 15: AMEAÇAS	52
FIGURA 16: NATUREZA DOS ATAQUES	54
FIGURA 17: ATACANTES	55
FIGURA 18: RISK MANAGEMENT MODEL	58
FIGURA 19: RISK MANAGEMENT MODEL	58
FIGURA 20: INFORMATION SECURITY RISK MANAGEMENT PRINCIPLES	59
FIGURA 21: INFORMATION SECURITY RISK MANAGEMENT	62
FIGURA 22: COBIT PRINCIPLES	64
FIGURA 23: COBIT PROCESS	65
FIGURA 24: GERENCIAMENTO DA INFORMAÇÃO	65
FIGURA 25: INFORMATION RISK MANAGEMENT	68
FIGURA 26: ESTRUTURA ORGANIZACIONAL.....	76
FIGURA 27: ESTRUTURA ORGANIZACIONAL TRADICIONAL.....	77
FIGURA 28: ESTRUTURA PROPOSTA POR BYRNES.....	78
FIGURA 29: INFORMATION SECURITY RISKS.....	110
FIGURA 30: MANAGING INFORMATION SECURITY RISKS.....	111
FIGURA 31: INFORMATION RISK MANAGEMENT	111
FIGURA 32: MODELO DE GESTÃO DE RISCO EM SEGURANÇA DA INFORMAÇÃO.....	112
FIGURA 33: PROCESSOS VISANET	123
FIGURA 34: INFRA-ESTRUTURA DA VISANET	130
FIGURA 35: ESTRUTURA ORGANIZACIONAL DA ÁREA DE SEGURANÇA	133
FIGURA 36: MATRIZ DE RISCO: PROCESSO X CIA X IMPACTO	144
FIGURA 37: MATRIZ DE AVALIAÇÃO DOS RISCOS	144
FIGURA 38: MODELO DE FORÇAS DE PORTER APLICADO A VISANET	159
FIGURA 39: MATRIZ SWOT	160
FIGURA 40: CADEIA DE VALOR DE PORTER APLICADA A VISANET	161
FIGURA 41: ADERÊNCIA DA VISANET AO MODELO DE GESTÃO	169
FIGURA 42: MODELO DE GESTÃO DE RISCO EM SEGURANÇA DA INFORMAÇÃO.....	171

1. Introdução

Nos últimos anos, o mundo moderno tem vivenciado a velocidade da evolução da era da informação. Nessa era, a velocidade da propagação e da disponibilização da informação gera diversos avanços conjunturais e mercadológicos, dentre os quais vale a pena ressaltar:

- ✍ ✍ Competição global;
- ✍ ✍ Crescimento da dependência nos sistemas de informação baseado em tecnologia;
- ✍ ✍ Vulnerabilidades significantes das redes de computadores e comunicações;
- ✍ ✍ Grande número de colaboradores e trocas de informações;
- ✍ ✍ Uso de redes públicas, tais como a Internet;
- ✍ ✍ Crescimento do comércio eletrônico;
- ✍ ✍ Troca rápida na tecnologia;
- ✍ ✍ Desenvolvimento de novos tipos de aplicações;
- ✍ ✍ Demanda por melhores funcionalidades e performance.

Estes efeitos provenientes dos avanços tecnológicos e conjunturais têm exigido das empresas constantes evoluções organizacionais, operacionais, e tecnológicas. Neste cenário, produtos e serviços são criados dentro de um ambiente extremamente dinâmico. De um lado existe o desafio de inovar, agilizar e controlar novos processos continuamente, identificando e gerenciando riscos. Por outro lado, há o dilema, das organizações, de encontrar o equilíbrio entre construir uma relação de confiabilidade, dentro de um ambiente dinâmico, competitivo e dependente de tecnologia, e de proteger a reputação da instituição de fraudes, perda de informação, e de confiabilidade, e de outras formas de desvios que acarretem perdas financeiras, direta ou indiretamente.

Agora imagine-se a seguinte cena: o presidente da empresa chama o responsável pela segurança de TI e o responsável pela segurança física da corporação e pede um relatório sobre como a empresa está preparada para os

problemas referentes à segurança. O fato provavelmente observado será: os gerentes praticamente não se haviam encontrado ou conversado antes e, com certeza, nunca tinham desenvolvido uma estratégia de segurança coerente e amarrada.

Os executivos de negócios acham estranhos como dois departamentos com a missão de gerenciar e de reduzir os riscos do negócio não estejam coordenando seus esforços, sem considerar que há dois departamentos responsáveis pela segurança. A razão dessa discrepância é simples: as tecnologias e os processos para segurança tecnológica requerem um conhecimento diferente do de segurança física.

As empresas começam a olhar para o gerenciamento de risco como um processo de negócios da segurança e concluem esse processo é menos efetivo se for segregado em dois departamentos que não se interagirem. A gestão de segurança da informação tem que lutar em todos os *fronts*: nos *fronts* da TI, da cultura empresarial, da proteção dos ativos físicos, das negociações estratégicas, etc.

No passado não muito distante, a direção das empresas costumava entregar o gerenciamento de risco técnico para especialistas de TI, enquanto a equipe de segurança física se focava na segurança dos empregados, prevenção de crimes e gerenciamento de risco físico. De forma similar, os membros da equipe de TI tinham seus próprios interesses, como defesa da rede, de servidores e de estações de trabalho, além de cuidarem de gerenciamento de senhas, da prevenção a ataques de *hackers* e da segurança de *Web sites*.

Nestes últimos anos passou a ser comum analisar a segurança em termos de valor para os negócios e para os processos. Por exemplo, as preparações contra desastres, espionagem e terrorismo são fatores que causam impacto em toda a organização, atingindo dos acionistas aos empregados, e está ligada às estratégias de segurança.

A segurança da informação deve dirigir as atividades de segurança física e as funções de segurança lógica, de modo a coordenar e integrar uma ampla variedade de funções que guardem sinergia entre si.

Fica, portanto, evidente que a segurança é um serviço essencial que permeia toda a organização, o que significa também que a segurança está evoluindo rumo a um papel essencial, com responsabilidades não só em TI, mas também na melhoria da eficiência operacional dos negócios e na implementação de formas de gestão de risco a um custo compatível com a realidade da empresa.

Tudo isso fica claro quando as empresas tratam a segurança como um processo de negócios, atribuindo a responsabilidade a uma área específica para coordenar os diversos componentes do gerenciamento de risco de segurança da informação dentro da organização. Esta constatação levou ao surgimento da área de segurança da informação.

1.1. Definição do Problema

Segundo BEHAN (1990) o homem pré-histórico não tinha nada para comprar e vender e, portanto, não tinha a necessidade de um sistema de pagamento. Passados 100 mil anos, o homem sentiu a necessidade de armazenar e transacionar alimentos durante os tempos de escassez. O homem com sua inteligência criou o mais simples sistema de meio de pagamentos: um sistema de moedas, que não só desenvolveu suas habilidades para trabalhar com o metal, mas também ensinou-o a comunicar-se através de símbolos abstratos. Analisar a evolução dos sistemas de meio de pagamentos é analisar a própria história do homem moderno.

Segundo FORTUNA (1999), o dinheiro de plástico é mais um sistema de meio de pagamento que facilita a vida do homem moderno e representa um enorme incentivo ao consumo.

A evolução tecnológica e cultural proporciona cada vez mais a troca dos pagamentos em cheque por meios eletrônicos, como cartões de débito e crédito. Isto se deve ao fato de oferecer benefícios para todas as partes envolvidas. Para o estabelecimento comercial, este meio de pagamento garante o recebimento da venda e evita a perda de tempo no levantamento da ficha do cliente. Para o portador do cartão, ou comprador, a facilidade de utilização atrelada à

privacidade de seus dados pessoais, confirma a preferência cada vez maior da utilização deste meio de pagamento, conforme mostram os levantamentos da Visa do Brasil. DINIZ - REVISTA EXAME (15/07/2002).

O NEGÓCIO É DINHEIRO VIVO
Como o brasileiro paga suas contas — em %*

TIPO DE GASTO	DINHEIRO	CHEQUE	CARTÃO DE DÉBITO	CARTÃO DE CRÉDITO
Drogarias	87	15	9	19
Restaurantes	84	17	8	20
Supermercados	83	15	18	22
Postos de gasolina	82	23	16	17
Comércio de roupas	73	19	10	27
Móveis	62	3	2	25
Hotéis	61	30	10	36
Viagens aéreas	57	26	5	45
Compras pela internet	52	—	5	43

*As somas superam 100%, pois o consumidor pode escolher mais de um meio de pagamento ao responder à pesquisa

Fonte: Visa do Brasil

Figura 1: Como o brasileiro gasta seu dinheiro

De acordo com a Associação Brasileira das Empresas de Cartões de Crédito e Serviço - AB ECS (2002), o número de transações feitas apenas com cartões de crédito saltou de 516,7 milhões em 1997 para 1,03 bilhão no ano de 2001.

AB ECS

Período	Número de Cartões (Milhões)	VARIAÇÃO +(-)	Nº. de Transações (Milhões)	VARIAÇÃO +(-)	Valor de Transações (US\$) (Bilhões)	VARIAÇÃO +(-)
1991	7,9		105,7		5,2	
1992	7,8	(1,27)	151,6	43,42	5,1	(1,92)
1993	8,4	7,69	199,9	31,86	6,3	23,53
1994	11,2	33,33	210,3	5,20	10,3	63,49
1995	14,3	27,68	319	51,69	21,3	106,80
1996	17,2	20,28	437,1	37,02	25,5	19,72
1997	19,3	12,21	516,7	18,21	27,8	9,02
1998	22	13,99	641,2	24,10	32	15,11
1999	23,6		0,77		41,6	
2000	27,95	18,43	1,00	29,92	50,36	21,06
2001	35,3	26,30	1,03	3,0	62,9	24,90

Figura 2: AB ECS evolução anual

Além disto, segundo pesquisa realizada pela Credicard, o Brasil ocupa hoje a 7ª posição no ranking mundial de cartões de crédito. Os Estados Unidos continuam como o país com a maior emissão de cartões de crédito, com 583,8 milhões, seguidos pelo Japão, com 136,8 milhões, e pelo Reino Unido, com 80 milhões. O estudo mostra também que 34% dos brasileiros economicamente ativos possuem cartão. ABECS (2002).

Proporcionalmente ao crescimento da utilização deste meio de pagamento, crescem também os riscos inerentes a estas operações. Cada vez mais freqüentes, as fraudes neste tipo de transação provocam perdas anuais pesadíssimas para as instituições financeiras responsáveis pela operação do sistema.

Para manter esses riscos sob controle, é preciso elaborar uma gestão dos riscos tecnológicos, para que a segurança da informação seja gerenciada de forma eficaz, e constantemente manter essa gestão atualizada, seguindo boas práticas a serem empregadas no planejamento, desenho, implementação e manutenção dos sistemas da informação.

No entanto, nos últimos anos, a atenção sobre a segurança da informação esteve sempre mais voltada aos recursos de tecnologia. A mudança das arquiteturas de segurança e a crescente prioridade que o assunto vem ganhando dentro das corporações estão levando à emergência da criação da área de segurança da informação.

A maioria das instituições financeiras concorda que é apropriado colocar a segurança como prioridade. O que não parece apropriado, no entanto, é deixar decisões de risco para negócios estratégicos sob a responsabilidade da equipe de tecnologia. Os profissionais do departamento de TI certamente sabem avaliar riscos técnicos, mas esse time dificilmente está em condições de avaliar o risco de negócios, que é responsabilidade de gerentes e diretores, aconselhados por auditores e, sobretudo, pela área de segurança da informação.

1.2. Justificativa do Estudo

A gestão da segurança da informação é abordada como contexto deste estudo, pois a segurança de uma corporação é mais do que um conjunto de tecnologias. Atrelados a ela, estão questões legais, aspectos físicos e culturais da empresa, além da implicação em planejamento estratégico, negociações complexas e resolução de problemas. Esses desafios exigem, atualmente, o desenvolvimento de uma área altamente especializada em negócios e, ao mesmo tempo, com grande conhecimento tecnológico, de forma a prover segurança às informações da empresa. A criação de uma área específica em segurança da informação apareceu no cenário corporativo dos Estados Unidos e Europa nos dois últimos anos. Desde então, ela atraiu muita atenção, mas não se pode ainda dizer que seja comum nas empresas.

A escolha do tema “modelo de gestão” está relacionada ao desafio de dirigir tecnologias, processos, políticas e pessoas em relação a uma postura comum de segurança. É preciso mapear medidas de proteção, balancear as necessidades de negócios com as de segurança, auxiliar gerentes de negócios a compreender quais são as potenciais vulnerabilidades e os riscos de seus departamentos, além de apoiar os executivos em negociações nas quais questões de segurança têm um peso importante dentro das organizações atualmente. A prioridade da gestão da segurança da informação é certificar-se de que a segurança seja uma responsabilidade que permeie toda a corporação.

“Neste mundo globalizado, onde as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações. Uma falha, uma comunicação com informações falsas ou um roubo ou fraude de informações podem trazer graves consequências para organização, como perda de mercado, de negócios e, conseqüentemente, perdas financeiras.” (NAKAMURA, 2002, pág. 28).

A limitação deste estudo para a indústria de cartões de crédito se deve ao fato de que são grandes as expectativas sobre segurança da informação nas instituições financeiras.

"(...), uma fonte potencial de problemas é a preocupação dos clientes com privacidade e segurança, que poderia levar uma forte reação contra os fornecedores que utilizam tais sistemas ou simplesmente a sua não utilização por parte dos clientes." (ALBERTIN, 1999, pág. 154).

Além disto, se analisarmos o quadro comparativo entre os mercados desta indústria, podemos observar a crescente ascensão do mercado brasileiro neste segmento. Observamos que o Brasil, apesar da pequena participação perante os líderes de mercado, supera os maiores em alguns indicadores, como por exemplo, o número de transações mensais por cartão é maior que o principal líder, os Estados Unidos da América.

Evolução do Mercado										
	Brasil		Argentina		América Latina		EUA		Mundo	
	1999	2000	1999	2000	1999	2000	1999	2000	1999	2000
Faturamento US\$ BI	20,5	26,1	16,2	16,0	72,0	82,3	1.107,1	1.261,5	2.343,2	2.737,0
% share sobre o mundo	0,9%	1,0%	0,7%	0,6%	3,1%	3,0%	47,2%	46,1%	100%	100%
Nº de transações (MM)	579	731	270	281	1.315	1.507	11.120	12.560	26.063	30.386
Transação média (US\$)	35	36	60	61	55	55	100	100	90	90
Nº de cartões de crédito (MM)	23,5	29,2	11,6	11,8	62,7	70,0	511,0	538,0	1.045,0	1.136,3
% share sobre o mundo	2,2%	2,6%	1,1%	1,0%	6,0%	6,2%	48,9%	47,3%	100%	100%
Gasto médio anual, por cartão (US\$)	871	895	1.394	1.352	1.148	1.176	2.167	2.345	2.242	2.409
Nº de transações mensais por cartão	2,05	2,09	1,94	1,84	1,75	1,79	1,81	1,95	2,08	2,23
Nº de estabelecimentos (MM)	0,59	0,60	0,22	0,22	1,65	1,20	3,8	4,3	18,1	20,6

Fonte: Visa / MasterCard / Diners Club / American Express / Discover / JCB / RedeShop

Figura 3: Evolução do mercado

(REVISTA CARDNEWS, Nov. 2001, pág. 49)

A restrição deste estudo ao mercado brasileiro somente se justifica pelo fato de que o universo de estudo estaria sujeito às restrições impostas pelas políticas governamentais. Além disto, esta limitação justifica-se de forma a

permitir comparar a estruturação da gestão da segurança da informação com a de outros países onde existam estudos similares.

1.3. Objetivos

1.3.1. Objetivo Geral

Utilizando-se a metodologia do estudo de caso, o objetivo principal consiste em investigar como construir uma infra-estrutura de gestão de risco em segurança de informação, não só no âmbito tecnológico, mas também no operacional e no mercadológico, de forma a estabelecer uma relação transparente às demais áreas internas da organização, aos clientes e a todo o mercado.

1.3.2. Objetivos Específicos

Através da metodologia de estudo de caso, são objetivos específicos deste trabalho:

- ▣ Analisar o intento estratégico da empresa a ser estudada e seus objetivos de negócio
- ▣ Aplicar os quesitos de segurança da informação à situação da empresa
- ▣ Comparar os resultados através do desenho de um modelo de gestão da segurança da informação aderente e específico ao seu negócio.

A partir desta análise, pode-se verificar se a gestão da segurança da informação é tratada formalmente, através de uma área de gestão específica, ou se as responsabilidades sobre o assunto se encontram distribuídas entre as diversas áreas nas empresas administradoras de cartão de crédito. São então estabelecidas as seguintes hipóteses (nula e alternativa) a serem testadas:

H1: A empresa analisada pertencente a indústria de cartão de crédito trata a gestão da segurança da informação de forma centralizada e especializada.

Hipótese alternativa: Não existe tal tratamento centralizado e especializado na indústria de cartão de crédito.

Na hipótese de H1 ser verdadeira, propõe-se verificar de que forma a gestão da segurança da informação é tratada dentro da indústria. Para isto, estabelecem-se então as seguintes hipóteses (nula e alternativa) a serem também testadas:

H2: A empresa analisada pertencente a indústria de cartão de crédito executa uma análise de risco para a gestão da segurança da informação de forma aderente e específica ao seu negócio.

Hipótese alternativa: Não existe tal análise de risco para a gestão da segurança da informação na indústria de cartão de crédito.

1.3.3. Delimitação do Objeto

O campo de estudo deste trabalho está limitado à indústria de administração de cartões de crédito no Brasil. Todas as necessidades de segurança da informação apresentadas neste trabalho são relativas ao cenário sócio-econômico brasileiro.

2. Fundamentação Teórica

Neste capítulo, analisaremos as teorias relativas ao gerenciamento de riscos (amplamente exploradas e estruturadas sob uma visão de riscos financeiros e operacionais), os conceitos básicos sobre segurança da informação, segundo diversos autores; e o gerenciamento de riscos aplicado à segurança da informação, e finalizaremos com um modelo conceitual.

2.1. Gerenciamento de riscos

Segundo DOWD (1998), tudo muda, tanto para o bem quanto para o mal, e afeta as pessoas e as organizações. Mudanças sempre carregam riscos, sejam eles tanto para o ganho quanto para a perda, e lidar com eles faz parte tanto da vida das pessoas quanto da sobrevivência de uma organização. Lidar com os riscos não significa eliminá-los ou simplesmente ignorá-los. Significa que devemos gerenciar os riscos: decidir quais devemos evitar e como, quais riscos aceitar e em que condições, quais riscos devemos tomar, etc.

2.1.1. Conceito de risco

Existem diversas definições em torno da palavra ‘risco’. Podemos citar as definições de diversos autores:

“(...) 2. Situação em que há probabilidades mais ou menos previsíveis de perda ou ganho (...)”. (FERREIRA, 1999, pág. 1772).

“(...)a possibilidade de que os resultados realizados possam ser diferentes daqueles esperados.”. (GITMAN, 1997, pág. 17).

“Risco pode ser definido, de forma abrangente, como o potencial de eventos ou tendências continuadas causarem perdas ou flutuações em receitas futuras”. (MARSHALL, 2002, pág. 19).

“Risk is a condition in which there is a possibility of an adverse deviation from a desired outcome that is expected or hoped for.” (VAUGHAN, 1997, pág. 8).¹

Conforme VAUGHAN (1997), independentemente da definição, pode-se notar que o conceito de incerteza, seja de ganho ou de perda, está explícita ou implicitamente presente em todas elas, de maneira que, quando existe o risco, são possíveis dois resultados: certeza de ocorrência ou não. Da mesma forma, podem-se prever os resultado de perdas previstas ou perdas não-previstas.

2.1.2. Classificação dos riscos

Uma base para as diferentes classificações de riscos é a classificação baseada nas diferentes causas de perda e nos seus efeitos. A grande maioria dos autores citados classifica semelhantemente os tipos de riscos, principalmente os com foco nos riscos financeiros. A partir destas classificações, outras sub-classificações podem ser aplicadas.

a. Riscos financeiros e não financeiros

Segundo VAUGHAN (1997), a palavra ‘risco’ envolve a exposição da empresa a situações adversas, com perdas financeiras ou não.

¹ Risco é situação na qual há uma possibilidade de um desvio do resultado que é esperado ou aguardado.

São riscos financeiros aqueles que estão envolvidos no relacionamento entre uma organização e o ativo associado à geração das expectativas de resultados, os quais podem ser perdidos ou prejudicados. Portanto, três elementos estão presentes neste tipo de risco:

- ☞ Indivíduo ou organização que estão expostos ao risco
- ☞ Ativo ou receita, cuja destruição ou perda causará prejuízo financeiro
- ☞ Uma ameaça que pode causar a perda

O primeiro elemento explicita que alguém ou alguma coisa será afetada pela ocorrência do evento. Já os outros dois referem-se ao valor do ativo e o perigo sobre este.

Riscos não-financeiros podem ser representados por perdas não-passíveis de mensuração financeira. A aplicação desta forma de classificação é apresentada no seguinte exemplo:

“During the devastating midwestern floods of 1993, millions of acres of farmland as well as thousands of buildings were severely damaged by floodwaters, causing billions of dollars in financial loss to owners. In addition, according to the game commissions in the affected states, the effect of the flood on wildlife in the area was severe. Although the loss of thousands of deer, pheasants and trees perhaps diminished the quality of life for residents of the area, there was no financial loss resulting from the destruction of the wildlife and fauna.” (VAUGHAN, 1997, pág. 13).²

² Durante a devastadora inundação de 1993, milhões de acres de fazendas tão como dezenas de construções foram destruídas causando bilhões de dólares em perdas financeiras para os proprietários. Além disto, de acordo com o levantamento realizado por uma comissão, o efeito da inundação sobre a vida selvagem da área atingida foi severa. A perda de veados, faisões, e árvores talvez diminuíram a qualidade de vida dos residentes da área, e portanto, não há como mensurar as perdas financeiras resultantes da destruição da fauna e flora selvagem.

b. Riscos estáticos e dinâmicos

Segundo VAUGHAN (1997), mudanças na economia, a partir de dois conjuntos de fatores, geram riscos dinâmicos. O primeiro conjunto é formado por aqueles fatores relacionados com o ambiente externo: setor de atividade, política econômica, mudanças tecnológicas, competidores e clientes do mercado. Alterações nestes fatores são incontrolláveis e muitas vezes imprevisíveis, gerando muitas vezes grandes perdas financeiras a uma empresa. O segundo conjunto está relacionado com às decisões estratégicas internas da empresa: decisões sobre o que produzir, como produzir, como financiar, quais insumos comprar, etc. A estratégia traçada determina se a empresa será lucrativa ou não, se ela terá prejuízos ou não.

Riscos estáticos, por sua vez, são aqueles não estão relacionados a mudanças na economia. Por exemplo, mesmo se fosse possível não ocorrerem mudanças na economia, conforme descrito acima, as empresas ainda estariam sujeitas aos riscos de natureza não-econômica, como desastres naturais, fraudes, roubos, abalo de imagem ou de reputação, falhas de tecnologia ou aspectos legais. Segundo VAUGHAN (1997), as perdas estáticas são mais regulares e geralmente mais previsíveis.

c. Riscos fundamentais e particulares

Esta classificação baseia-se na origem e na natureza do grupo atingido. Riscos fundamentais são aqueles que são impessoais em origem e em natureza do grupo. São riscos causados por fenômenos econômicos, políticos e sociais, resultando em consequências que atingem indiferentemente diversos grupos ou organizações.

Riscos particulares, por sua vez, estão relacionados a um evento pontual que atinge um determinado grupo ou uma empresa em específico.

d. Riscos especulativos e puros

Riscos especulativos são aqueles que possuem tanto a probabilidade de perda quanto de ganho. Diferentemente, os riscos puros são aqueles que possuem apenas a probabilidade de perda.

Esta classificação é importante, pois apenas os riscos puros são seguráveis, enquanto os especulativos são mais aceitos, pois possuem uma característica de oportunidade.

VAUGHAN (1997) ainda sub-classifica os riscos puros como:

- I. Riscos pessoais: consiste na possibilidade de perda de receitas ou ativos, sendo divididos em quatro perigos: morte prematura, velhice não assistida, doença e desemprego.
- II. Riscos de propriedade: toda pessoa que possui uma propriedade está sujeita à ameaça de perda ou mau uso da propriedade, acarretando perdas de receitas ou ativos.
- III. Riscos de responsabilidade: riscos referentes à difamação (intencionais ou não) sobre o indivíduo ou organização, causando perdas de receitas ou ativos.
- IV. Riscos gerados a partir da falha de outros: este risco existe a partir do momento em que uma pessoa concorda em executar um trabalho para outra e existe a possibilidade de que a mesma falhe, resultando em perdas de receitas ou ativos.

e. Riscos como fator de oportunidade, fator negativo e variância de resultado

Outra classificação importante de risco é dada por MARSHALL (2002). Segundo ele, pode-se dividi-los em quatro tipos: risco como resultado médio, risco como variância de resultado, risco como fator catastrófico e risco como fator positivo de oportunidade.

O risco como fator positivo de oportunidade está centrado no investimento e tem base em iniciativas estratégicas. Ele está relacionado à

estratégia de crescimento da instituição e ao retorno dos investimentos. Quanto maior o risco, maior o potencial do retorno e, paralelamente, maior pode ser o potencial de perda. Nesse contexto, a ousadia é um requisito e o gerenciamento do risco requer técnicas orientadas para maximizar ganhos diante dos obstáculos.

O risco como resultado médio refere-se à preocupação com os resultados esperados. Desta forma, o risco de um evento afeta o resultado potencial da empresa e, conseqüentemente, todos os interessados nela.

O risco como variância de resultado refere-se à preocupação com a eficiência operacional. Neste contexto, o gerenciamento de riscos consiste em adotar técnicas para reduzir qualquer variação que possa ocorrer entre o resultado projetado e o real.

O risco como fator catastrófico negativo refere-se à ocorrência de potenciais efeitos negativos, como fraude, roubo, abalo de imagem ou reputação, falhas de tecnologia ou aspectos legais. Neste contexto, o gerenciamento de riscos tem um foco tradicional e defensivo e significa adotar técnicas de controle e alocar recursos para minimizar o impacto de um evento negativo sem incorrer em custos excessivos ou em paralisação total ou parcial das atividades da instituição.

f. Classificação segundo a natureza do risco

Outra forma de classificar o risco é através de sua natureza específica. MARSHALL (2001) afirma que essas categorias de risco não são, necessariamente, mutuamente excludentes e devem-se ajustar seus significados para adaptá-las ao contexto específico do negócio. Nestas categorias estão incluídas, mas não se limitam a:

Risco

Contábil	de auditoria	de negócios	de Continuidade de negócios
De concorrentes	de conformidade	de controle	de país
De crédito	de cliente	Fiduciário	de fraude
de financiamento	de RH	Jurídico	Liquidez
de mercado	de operações	de ativo físico	Político
De projeto	de regulamentação	de reputação	Estratégico
de fornecedor	de tecnologia	de transações	de liquidação

Figura 4: Tipos de risco

(MARSHALL, 2002, pág. 405-439)

Segundo GREENSTEIN (2000) podemos ainda agrupar esta forma de classificação de MARSHALL (2002) em três grandes grupos:

1. Riscos estratégicos: são aqueles relacionados às estratégias adotadas pela empresa e que possam ameaça-la de não atingir suas metas ou de obter perdas financeiras. Os riscos estratégicos podem ser divididos em dois: externos (como pressões do concorrente, adaptações a mudanças, mercado financeiro instável, etc) ou internos (como lançamento de produtos, falhas de comunicação, etc.)
2. Riscos financeiros: são os riscos associados às transações financeiras que uma empresa realiza. Estes riscos podem ser: de precificação, como os relacionados a encargos financeiros altos, volatilidade cambial, etc; de liquidez, como o fluxo de caixa inadequado, concentração de capital, etc; e de crédito, como garantias insuficientes, realização difícil, etc.
3. Riscos operacionais: são os riscos que englobam a integridade dos processos de negócios e a condição de fornecer produtos e serviços de forma consistente e oportuna. Estes riscos podem ser sub-divididos em: de conformidade, como legal, aderência a regulamentação, etc; de processos, como ineficiência, inadequação, obsolescência tecnológica, falta de foco, etc; de tecnologia e processamento de informações, como confidencialidade da informação, integridade da informação, acesso indevido, aderência dos sistemas de informação, etc; de RH, como

pressão dos sindicatos, desmotivação, condições de segurança e saúde inadequadas, etc; e de retidão e ética, como práticas ilícitas, fraudes, propriedade intelectual, etc.

Podemos observar a mesma classificação através de SANTOS (2002), apenas dividindo os riscos estratégicos em: riscos do macro-ambiente e riscos do ambiente setorial.

RISCO EMPRESARIAL TOTAL				
Riscos Oriundos do Ambiente Externo		Riscos Oriundos do Ambiente Interno		
Riscos do Macroambiente	Riscos do Ambiente Setorial	Riscos Financeiros	Riscos Operacionais	
<ul style="list-style-type: none"> – político-legais – econômicos – demográficos – naturais – tecnológicos – sociais 	<ul style="list-style-type: none"> – de fornecedores – de clientes – de concorrentes – de produtos alternativos 	<ul style="list-style-type: none"> – de liquidez – de crédito – de mercado – legais 	Gerais	Funcionais
			<ul style="list-style-type: none"> – da estrutura de custos – de sucessão – de fraudes – corporativos – de sistemas – de greves – de erros – de infra-estrutura 	<ul style="list-style-type: none"> – da área administrativa – da área de compras – da área de marketing – da área de vendas – da área de produção/ logística – da área de sistemas/ Internet – da área contábil/fiscal – da área de distribuição

Figura 5: Classificação de risco

(SANTOS, 2002, pág. 25)

2.1.3. Conceito de gerenciamento de risco

Como observamos anteriormente, as empresas estão sujeitas a diversos tipos de riscos. Qualquer tipo de negócio possui risco. No entanto, estes riscos, atualmente, nem sempre são corretamente mensurados ou sequer identificados, levando as organizações a grandes prejuízos. Desta forma, é necessário que as organizações implementem áreas responsáveis pelo gerenciamento de riscos. Por isso, diversas empresas treinam atualmente profissionais para se tornarem especializados e dedicados exclusivamente à atividade de gerenciamento de riscos. (VAUGHN, 1997, pág 26). Mas o que se entende por gerenciar riscos?

Diversos são os autores que definem ‘gerenciamento de riscos’. Citaremos a seguir alguns deles:

“ Risk management is the process by which organizations try to ensure that the risks to which they are exposed are the risks to which they thin they are and need to be exposed to operate their primary business.” (CULP, 2002, pág. 199).³

“Risk management is a scientific approach to dealing with pure risks by anticipating possible accidental losses and designing and implementing procedures that minimize the occurrence of loss or the financial impact of the losses that occur.” (VAUGHAN, 1997, pág. 30).⁴

“Risk management is a methodology for: assessing the potential of future events that can cause adverse affects; and implementing cost-efficient strategies that can deal with theses risks” (GREENSTEIN, 2000, pág. 171)⁵

Segundo KING (2001), entre os diversos benefícios de gerenciar riscos podem-se citar:

“There are many benefits to managing the risks (...), including:

- 1. Avoid unexpected losses and improve operational efficiency. Understanding the important operational risks enables management to focus on ways to reduce routine loss and improve efficiency. This also reduces the like hood of incurring large losses and improves the quality of the operational processes.*

³ Gerenciamento de risco é o processo pelo qual as organizações tentam assegurar que os riscos os quais elas estão expostas estão compatíveis aos riscos que elas acreditam ser necessários para operar o seu negócio.

⁴ Gerenciamento de risco é uma abordagem científica para lidar com os riscos puros de forma antecipar possíveis perdas futuras e elaborar e implementar procedimentos que minimizem a ocorrência da perda ou de impactos financeiros que estas possam causar.

⁵ Gerenciamento de risco é uma metodologia para: levantar o potencial dos eventos futuros que possam causar mudanças prejudiciais; e implementar estratégias de custo-eficiência que possam lidar com estes riscos.

2. *Efficient use of capital. A business allocates capital based on expected earnings in much the same way an investor values a company. The efficient use of a firm's capital implies optimizing the risk/return trade-off for capital allocation decisions within the firm.*
3. *Satisfy stakeholders. Regulators, credit agencies, and other stakeholders are increasingly interested in a firm's risk management practices. The operations of the firm are an integral part of this risk management, and a major contributor to earnings volatility that can affect the value of the firm. Risk measurement can help influence stakeholder views and improve areas that are needed to avoid stakeholder surprises.*
4. *Comply with regulation. Corporate governance recommendations and requirements view risk management as a board-level responsibility. (...)" (KING, 2001, pág. 08).⁶*

Podemos concluir que o gerenciamento de riscos não só é importante mas também vital para a existência e a sobrevivência do negócio, sendo portanto,

⁶ Existem muitos benefícios para o gerenciamento de riscos, incluindo:

1. Evitar perdas não esperadas e aumentar a eficiência operacional. Entender a importância dos riscos operacionais permite a gerência dar foco nas soluções que permitam reduzir as perdas nos processos e aumentar a eficiência. Isto também reduz a possibilidade de incorrer a grandes perdas e aumentar a qualidade do processo operacional.
2. Utilização eficiente do capital investido. Um negócio investe capital baseado nas expectativas de ganho da mesma forma que um investidor avalia uma companhia. O uso eficiente do capital de uma empresa implica na otimização da relação risco-retorno do capital investido na empresa.
3. Satisfazer os acionistas/interessados. Regulamentadores, financiadores, e outros interessados estão aumentando seus interesses em entender as práticas utilizadas pelas empresas em gerenciar os riscos. As operações de uma empresa são parte integral do gerenciamento de riscos, e um maior contribuinte para volatilidade dos ganhos que possam afetar o valor da empresa. A avaliação de riscos pode influenciar a visão dos acionistas e apontar melhorias necessárias para evitar supresas.
4. Estar de acordo com a regulamentação. Requisitos e recomendações de domínio corporativo tornam o gerenciamento de riscos uma responsabilidade do conselho da empresa.

classificado como um processo de negócio fundamental à competitividade das empresas hoje.

“O objetivo de competir pelo futuro não é estimular enormes riscos, mas sim trabalhar para tornar nossas ambições menos arriscadas.” (PRAHALAD, 1995, pág. 143).

Segundo KOLLER (1999), gerenciar os riscos permite que as empresas realizem suas decisões estratégicas de forma muito mais estruturada, permitindo um melhor direcionamento para a empresa.

2.1.3. O processo de gerenciamento de risco

Não existe uma divisão unânime das fases que compõem o processo de gerenciamento de risco. A estruturação por fases facilita o entendimento e a identificação da necessidade de conhecimentos técnicos e específicos, da participação de áreas e de profissionais-chave da empresa. Dos diversos autores analisados, concluímos que, apesar dos nomes diferentes, as atividades são praticamente as mesmas, mas muitas delas são de grande complexidade. Uma característica observada em todos estes autores é que o processo de gerenciamento de risco é um processo cíclico, ou seja, repete-se continuamente.

A característica cíclica do processo é possível de ser observada, por exemplo, em CULP(2002), propõe o processo dividido em 5 atividades: identificar e determinar as tolerâncias, medir os riscos, monitorar e relatar os riscos, controlar os riscos e, finalmente revisar, auditar e realinhar os riscos.

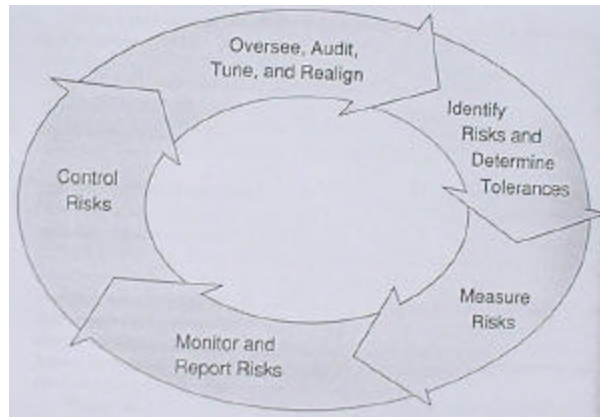


Figura 6: Processo de Gerenciamento de Risco de CULP

(CULP, 2002, pág.200)

No entanto, este modelo, como alguns outros, não exploram, ou melhor, não explicitam a atividade de planejamento e de implementação dos mecanismos contra o risco. Especificamente, uma grande parte deles deixa implícito, dentro da atividade de análise de risco, a decisão e o planejamento sobre as contramedidas a serem adotadas em relação ao risco.

Devido a este fato, apresentaremos a proposta de VAUGHAN(1997) dividindo-se o processo de gerenciamento de risco em 6 grandes atividades:

a. Determinação dos objetivos

A primeira etapa no processo de gerenciamento de riscos é decidir precisamente qual o objetivo deste gerenciamento. Para se obter o máximo benefício, é necessário o desenvolvimento consciente de um objetivo, pois, de outra forma, a tendência é que o processo de gerenciamento de risco se torne uma série isolada de problemas e que não seja visto como um problema único que envolva toda a organização. Não existem regras para se elaborar um plano consistente e objetivo para lidar com os riscos da organização, mas é fundamental a obtenção do entendimento dos objetivos estratégicos e operacionais da instituição, incluindo fatores críticos de sucesso, ameaças e oportunidades relacionadas.

Entre os vários objetivos possíveis, podemos citar: minimizar custos, proteger ativos, proteger os funcionários de acidentes que possam causar sérios danos aos mesmos, difamação, processos trabalhistas, etc. Mas, sem dúvida, o principal objetivo do gerenciamento do risco é a sobrevivência da empresa, isto é, a garantia de continuidade e existência da organização. Fixar os objetivos ajuda as empresas a manterem a sua atenção nos objetivos e metas a serem atingidos. Desta forma, elaborar os objetivos para o gerenciamento de riscos é revisar também as metas de negócios da empresa. Um exemplo disto pode ser bem observado através do quadro ilustrativo elaborado por MARSHALL (2002).

Objetivos Operacionais	Objetivos de Negócios	Componentes de Risco	Raciocínio
Eficiência	Redução de custos	Perdas esperadas	Custos mais baixos Impostos mais baixos Menores custos de seguro
Gerência de mudanças	Crescimento	Perdas inesperadas	Facilidade de planejamento Menor utilização de financiamento externo
Controle interno	Utilização eficiente de capital	Perdas catastróficas	Menor probabilidade de dificuldades financeiras Maior utilização de financiamento de endividamento com mecanismos de economia fiscal Satisfação de exigências regulamentares
Oportunismo	Aumento de receita	Potencial positivo	Tipicamente opções estratégicas como as oferecidas por investimentos em infra-estrutura

Figura 7

Figura 7: Objetivos de negócio x riscos

(MARSHALL, 2002, pág. 37)

Segundo VAUGHAN (1997), os objetivos do gerenciamento de risco devem estar formalizados numa “Política de Gerenciamento de Risco Corporativo”, que engloba os objetivos, a política e as normas para o assunto. Idealmente, os objetivos e a política de gerenciamento de risco devem ser produtos da alta direção da empresa, responsável em última instância pela preservação dos ativos da organização.

b. Identificação dos riscos

É difícil generalizar os riscos de uma organização, pois os processos operacionais e as condições em que as empresas se encontram são muito particulares a cada uma delas. Alguns riscos são óbvios, mas muitos deles estão

escondidos e, por isso, nesta etapa, é necessário que se utilize uma abordagem sistemática para o problema de identificação dos riscos.

A identificação do risco deve ser perseguida de forma sistemática dentro das instituições, utilizando-se as principais técnicas como:

- ✍ ✍ Entendimento da indústria à qual a empresa pertence
- ✍ ✍ Análise dos registros históricos da empresa
- ✍ ✍ Mapeamento dos processos da empresa
- ✍ ✍ Inspeção das atividades críticas da empresa
- ✍ ✍ Estudo das políticas e normas internas da empresa
- ✍ ✍ Questionários de análise de risco
- ✍ ✍ Análise dos relatórios financeiros
- ✍ ✍ Entrevistas
- ✍ ✍ Estudo da regulamentação da indústria

Combinando estas técnicas com a simulações de situações hipotéticas em conjunto e com o entendimento das operações da empresa, pode-se ajudar a garantir que riscos inerentes não estejam mascarados.

c. Análise de Risco

Uma vez identificados os riscos, é necessário avaliá-los corretamente. Isto envolve medir o potencial de perda e a probabilidade de ocorrência, podendo-se, a partir daí, classificá-los e priorizá-los. Certos riscos, devido à severidade de possibilidade de perda ou à alta taxa de exposição, demandarão mais atenção que outros. Classificar os riscos, por meio de uma sistemática que permita priorizar os investimentos e analisar a relação custo-benefício, é fundamental para a sobrevivência das empresas.

Segundo MARSHALL (2002), existem cinco componentes associados ao risco que devem ser detalhados nesta etapa:

- I. Probabilidade de o evento ocorrer. Estimar a probabilidade de o evento ocorrer no futuro, seja por métodos subjetivos ou objetivos é muito difícil. O substituto mais comumente utilizado para a probabilidade de um evento freqüente é o número de ocorrências deste evento dividido pelo período de tempo.

$$\text{Probabilidade de evento em um período futuro} = \frac{\text{Nº de ocorrências durante um período de tempo historicamente representativo}}{\text{Extensão do período de tempo histórico}}$$

Figura 8: Cálculo da probabilidade

(MARSHALL, 2002, pág. 44)

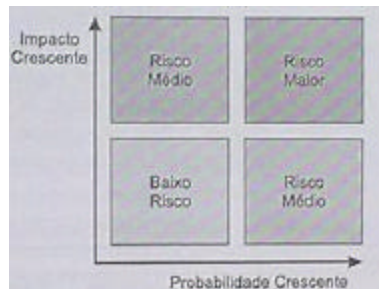
- II. Impacto do evento sobre a empresa: isto envolve três tipos gerais de impacto financeiro sobre a empresa: custos diretos, indiretos e de oportunidade. Impactos de custos diretos são aqueles que causam perdas financeiras diretas, impactos de custos indiretos são resultantes de danos à reputação da empresa ou efeitos sobre outros eventos de perdas da empresa e impactos de custos de oportunidade são aqueles que resultam na não-realização dos lucros potenciais máximos, representando um sacrifício por parte da empresa.

Tipos de Custo		Definição	Exemplos
Custos Diretos	Perda de lucros	Custos marginais incorridos diretamente como resultado da ocorrência de um evento	Custos não-orçados de pessoal para investigação e mitigação, ou seja, horas extras Erros irreversíveis Penalidades regulamentares
	Perda de valor	Custos fixos alocados ao evento Redução no valor de ativos e aumento no valor de obrigações	Custos orçados de pessoal Despesas administrativas Danos físicos Perda de registros Roubo de ativos Baixas de perdas de ativos Perda de principal Exposição de mercado
Custos Indiretos	Custos diretos de outros eventos causados ou tornados mais prováveis pela ocorrência do evento.	Perda de lucros	Custos de juros Custos legais e de litígio Custos de seguros aumentados Retirada de contrapartes/clientes Custos operacionais adicionais
	Outros custos indiretos	Perda de valor	Perda de pessoal-chave Perda de mercado Aumento de custo de capital Perda de fluxo de caixa normal Perda de reputação
Custos de Oportunidade	Perda de lucros Perda de valor		Oportunidades de negócios perdidas Recursos perdidos Processos perdidos

Figura 9: Impactos

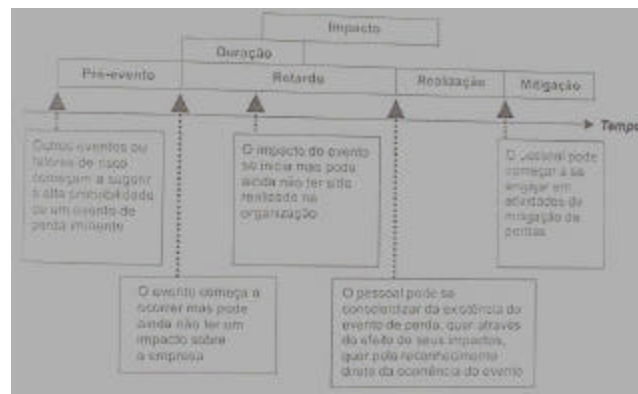
(MARSHALL, 2002, pág. 45)

- III. **Criticalidade do evento:** é a medida mais simples do risco de um evento, calculado através do produto entre probabilidade do evento e o seu impacto. Ao analisarmos esta relação poderemos facilmente diferenciar um risco alto de um risco mais baixo.

**Figura 10: Criticalidade**

(MARSHALL, 2002, pág. 46)

- IV. **Estrutura temporal do evento:** em alguns eventos complexos, também chamados de incidentes, pode ser útil analisar a estrutura detalhada dos mesmos. Diagramas elaborados, como apresenta MARSHALL (2002) podem ser utilizados para formalizar incidentes ou estudos de caso de eventos de alto impacto e revelar lições importantes para eventos similares no futuro.

**Figura 11: Estrutura temporal**

(MARSHALL, 2002, pág. 46)

- V. Incerteza do evento: este componente está relacionado às distribuições de probabilidades, tanto de frequência quanto de impactos. Estas distribuições são conhecidas apenas de forma imprecisa e estão sujeitas à incerteza além de quaisquer riscos. Para os riscos mais frequentes, podem-se produzir estimativas de risco mais precisas, mas para eventos menos frequentes, aqueles em que as empresas têm pouca ou nenhuma experiência, a incerteza do evento influi muito na forma de quantificar ou qualificar o risco.

Uma vez analisados os componentes associados ao risco, são empregadas diversas técnicas para se avaliar melhor cada risco em específico. Estas técnicas estão basicamente divididas em dois grupos: técnicas quantitativas e técnicas qualitativas.

✍ ✍ Análise quantitativa

Nesta análise, utilizaremos técnicas para quantificar o risco, ou seja, encontrarmos valores em que possamos comparar e classificar os riscos. Muitas teorias matemáticas foram desenvolvidas nesta área, principalmente por ela estar intrinsecamente ligada a estatística. KOLLER (1999) apresenta as seguintes técnicas: análise estatística, análise de Bayes, árvores de decisões, análise de fatores, simulações de Monte Carlo, etc. VAUGHAN (1997) apresenta o modelo binomial e de Poisson e técnicas de correlação e regressão linear para uma análise quantitativa do risco. VALLBHANENI (2002) apresenta conceitos importantes para a quantificação do risco:

- a. *Exposure factor* (EF): ou fator de exposição, é o percentual da perda do ativo causado pela ameaça.
- b. *Single Loss Expectancy* (SLE): ou expectativa de perda pontual, é o valor do ativo multiplicado pelo fator de exposição. Este valor representa uma quantificação para comparação futura nos cálculos. ($EF \times AV$ *Asset Value*)
- c. *Annualized Rate of Occurance* (ARO): ou frequência do evento ocorrer por ano.
- d. *Annualized Loss Expectancy* (ALE): ou expectativa de perda anual. É resultado do produto entre a expectativa de perda pontual e a frequência de ocorrência ($SLE \times ARO$).

✍ ✍ Análise qualitativa

Nesta análise, os riscos são comparados qualitativamente, a partir do seus atributos, e em conjunto, com a sensibilidade dos avaliadores em questão. VALLBHANENI (2002) cita como exemplo as técnicas de julgamento, intuição e a técnica Delphi. Julgamento e intuição, segundo o autor, geralmente são muito importantes no processo de avaliação de risco de uma empresa. Sob esta abordagem, o risco é classificado em alto, médio e baixo. Já na técnica Delphi, um grupo de pessoas participam destas classificações, de forma independente e anônima, e listam os riscos de acordo com suas visões pessoais. A partir daí, é realizada uma avaliação e priorizados os riscos mais votados. Então realiza-se uma nova votação, independente e anônima em cima da lista compilada. Novamente, é realizada uma avaliação e priorizados os riscos mais votados. Estas rodadas serão executadas até se obter o consenso do grupo. Devido a isto, esta técnica é denominada de *group decision-making*⁷.

Não é foco deste estudo detalhar cada uma das técnicas apresentadas, uma vez que existem muita teoria e muitos conceitos por trás de cada uma delas.

KRUTZ (2001) apresenta um quadro comparativo entre as duas abordagens. O método quantitativo, por analisar o risco através de números, apresenta como vantagens: análises de custo x benefício, estimativas de custos financeiros, facilidade de comunicação dentro da empresa, a possibilidade de serem automatizados e menos dúvidas nos resultados. Por outro lado, o método qualitativo, por ser subjetivo, atrelado à visão dos profissionais da empresa, apresentam como vantagens: baixa complexidade, menor quantidade de informação, menor tempo e esforço envolvidos.

Propriedade	Quantitativo	Qualitativo
Custo x Benefício	Sim	Não
Estimativa custos financeiros	Sim	Não
Pode ser automatizado	Sim	Não
Precisão (guesswork)	Baixo	Alto
Complexidade	Alta	Baixo
Volume de informação	Alta	Baixo
Tempo e esforço envolvido	Alta	Baixo
Facilidade de comunicar	Alta	Baixo

Figura 12: Comparação entre os métodos

(KRUTZ, 2001, pág. 22)

⁷ Decisão tomada pelo grupo.

d. Selecionando e planejando o tratamento do risco

Conforme CULP (2002), o objetivo de se gerenciarem riscos não significa eliminá-los completamente. Toda vez que vamos atravessar a rua, estamos correndo o risco de sermos atropelados. Neste caso, eliminar o risco completamente significaria não atravessarmos mais a rua, o que tornaria nossa vida praticamente inviável. Para a maioria das pessoas, gerenciar o risco, neste caso, significaria olhar os dois lados da rua antes de atravessá-la e atravessá-la na faixa de pedestre.

As empresas não diferem do caso apresentado. As empresas nada mais são que negócios nos quais riscos são assumidos por investidores interessados em um retorno futuro.

Para se lidar com o risco, são possíveis quatro técnicas descritas pela maioria dos autores citados:

I. Eliminar o risco

Quando uma organização se recusa a aceitar um determinado risco em um determinado instante, a exposição a este risco não permite à empresa se encontrar nesta situação. Segundo VAUGHAN (1997) esta técnica é mais negativa do que positiva, pois a utilização constante desta abordagem faz com que o negócio perca as oportunidades de lucro e, conseqüentemente, a possibilidade de atingir seus objetivos.

II. Mitigar o risco:

Conforme MARSHALL (2002), mitigar o risco é desenvolver mecanismos para se reduzir o risco até um nível aceitável para a organização. Segundo VAUGHAN (1997), isto pode ser feito em cima da prevenção contra perdas, reduzindo-se o impacto e a probabilidade de esta ocorrer. Programas de saúde e medidas de prevenção, como posto médico, plano de saúde, brigada de incêndio, sistemas de sprinklers, segurança física e patrimonial, sistemas de alarmes, etc, são exemplos de mitigar o risco através da prevenção contra perdas. Outra forma de mitigar o risco é diluí-lo em grandes volumes, desde que se tenha um bom controle sobre as probabilidades de ocorrência. Por exemplo, uma

seguradora pode assumir a possibilidade de perda da exposição de um indivíduo do grupo e ainda assim, não afetar sua rentabilidade.

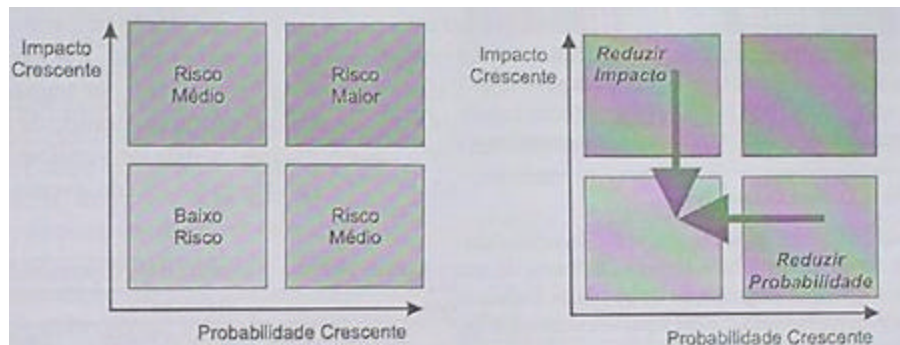


Figura 13: Mitigar o risco
(MARSHALL, 2002, pág. 45-46)

III. Reter o risco

Esta técnica talvez seja a mais utilizada para se lidar com o risco. As empresas, como os indivíduos, visualizam uma série de riscos e, na maioria dos casos, não fazem nada a respeito. De acordo com VAUGHAN (1997), a retenção do risco pode ser: consciente, quando a organização identifica o risco, mas não toma nenhuma atitude em relação ao mesmo, ou inconsciente, quando a organização não conseguiu identificar o risco. Pode ser também: voluntário, quando a empresa identificou o risco, sabe que é possível evitá-lo, mitigá-lo ou transferi-lo, mas prefere nada fazer, assumindo os possíveis prejuízos e as demais consequências; ou involuntário, quando a empresa inconscientemente reteve o risco ou quando o risco não é possível de ser evitado, mitigado ou transferido. A retenção do risco é um método legítimo e, em muitos casos, a melhor solução. De forma genérica, pode-se dizer que se devem reter os riscos que representem uma perda relativamente insignificante para a organização.

IV. Transferir o risco

O risco deve ser transferido quando o tomador de risco não pode arcar com o mesmo e, portanto, o transfere para outro que seja capaz de toma-lo. A transferência de risco serve tanto para riscos especulativos como para riscos puros. Um exemplo clássico é o processo de *hedging*, executado nas principais bolsas de mercadorias. *Hedging* é o método de transferir o risco das variações de preço de uma entrega futura. Um

exemplo de transferência de risco puro é realizar o seguro de algum bem patrimonial.

V. Dividir o risco

Dividir o risco é um caso específico de transferência do mesmo e também uma forma de sua retenção. Quando o risco é dividido, a possibilidade de perda é transferida de um indivíduo para o grupo, que de certa forma reteve este risco. Aplicar em um fundo de ações e realizar um seguro são exemplos de formas de dividir os riscos.

Segundo VAUGHAN (1997), esta fase é a mais delicada do processo pois envolve uma tomada de decisão sobre cada risco. As atuações dos gestores de risco sobre as decisões a serem tomadas variam de organização a organização. Se a política de gerenciamento de risco é rígida e detalhada, o gerente de risco tomará menos decisões e se tornará um mero administrador da política, diferentemente de um gestor pró-ativo da política de risco sobre os processos e riscos associados. É necessário também, nesta fase, a definição de ações que minimizem e monitorem os riscos identificados, além da validação do balanceamento entre risco e retorno de investimento.

e. Implementando o controle do risco

A decisão de tratar um risco deve ser executada com ou sem reservas, e com ou sem orçamento. No entanto, a sua implementação, uma vez decidida, necessita de reservas, que na maioria das vezes não foram previstas, mas devem ser desenhadas e implementadas através de um programa de prevenção ao risco.

GREENSTEIN (2000) afirma que a implementação de um ambiente de controle para a instituição requer uma visão corporativa dos riscos envolvidos, sejam eles decorrentes da estratégia adotada ou dos processos existentes nas áreas operacionais e financeiras, sejam eles dos sistemas e das tecnologias aplicadas ou da regulamentação e da legislação vigentes.

A implementação de um ambiente de controle é a base para o efetivo gerenciamento de riscos. Para que os procedimentos de controle possam ser implementados e monitorados, é importante existir:

- ✍✍ Comprometimento da alta administração;
- ✍✍ Uniformidade de linguagem e processos;
- ✍✍ Coordenação na implementação e no gerenciamento das mudanças;
- ✍✍ Envolvimento das áreas de negócio, tecnologia, controles internos, conformidade, segurança de informações e auditoria;
- ✍✍ Alinhamento contínuo entre os objetivos da instituição, e a implementação dos controles;

f. Avaliando e revisando os riscos

Segundo VAUGHAN (1997), a avaliação e a revisão dos controles e dos riscos devem ser feitas por duas razões. Primeiro, o gerenciamento de riscos não é estático, ou seja, novos riscos aparecem, riscos antigos desaparecem, técnicas de controle ficam obsoletas, etc e, segundo, erros ocorrem continuamente. Avaliar e revisar o gerenciamento dos riscos permite ao gestor revisar as decisões e corrigir os erros antes que estes se tornem onerosos. Para isto são necessários:

- ✍✍ Comunicação, aprendizado e acultramento efetivos;
- ✍✍ Alinhamento contínuo entre os objetivos da instituição, e o gerenciamento de riscos;
- ✍✍ Acompanhamento das ocorrências de sucesso e insucesso;
- ✍✍ Monitoramento dos processos de gerenciamento de riscos;
- ✍✍ Revisão contínua do ambiente de controle.

2.2. Gestão de risco e segurança da informação

A tecnologia da informação trouxe mudanças expressivas no mundo empresarial, alterando constantemente a forma das empresas operarem.

“A tecnologia da informação alterou o mundo dos negócios de forma irreversível. Desde que a tecnologia da informação foi introduzida sistematicamente em meados da década de 50, a forma pela qual as organizações operam, o modelo de seus produtos e a comercialização destes produtos mudaram radicalmente.” (MCGEE, 1994, pág. 5).

A tecnologia de sistemas de informação é um componente fundamental na cadeia de valor, como apresenta PORTER (1990).

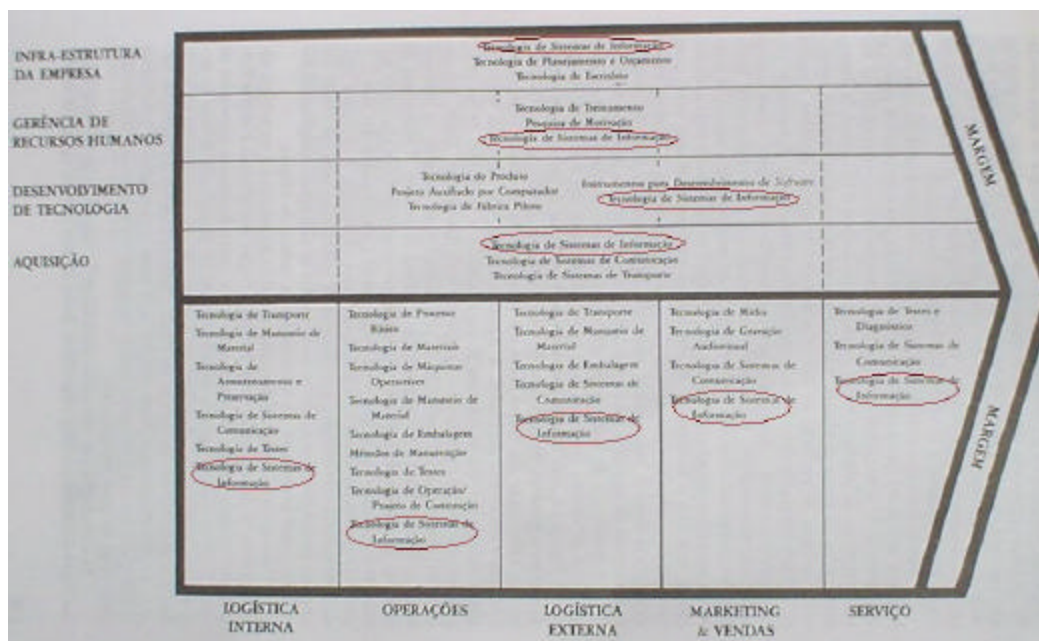


Figura 14: Cadeia de valor de Porter

(PORTER, 1990, pág. 155)

“A tecnologia de sistemas de informação é particularmente penetrante na cadeia de valores, visto que cada atividade de valor cria e utiliza a informação.” (PORTER, 1990, pág.156)

Segundo TAPSCOTT (1996), enquanto na velha economia o fluxo de informação era físico, como dinheiro, cheque, faturas, comprovantes, etc, na nova economia digital a informação está armazenada digitalmente em computadores e fluindo na velocidade da luz através das redes.

Segundo NAKAMURA (2002), os benefícios trazidos pela tecnologia da informação resultam em uma maior produtividade e ,conseqüentemente, em maiores lucros dentro da organização. A segurança da informação significa permitir que as empresas busquem os lucros através das novas oportunidades de negócio implementadas através de soluções, utilizando-se os recursos de informática. Logo, a segurança deve ser tratada não apenas como um mecanismo de proteção, mas sim como um elemento habilitador para que os negócios de uma empresa sejam executados.

2.2.1. Conceitos básicos sobre segurança da informação

a. Confidencialidade, Integridade e Disponibilidade

De acordo com KRUTZ e VINES(2001), a tríade que compõe os princípios básicos da segurança da informação são: integridade, confidencialidade e disponibilidade. Quando aplicados, esses princípios permitem adotar controles e medidas em relação a segurança da informação, reduzindo, dentre outros, os riscos de vazamento e divulgação não autorizada da informação, fraudes financeiras, apropriação indevida de informações, reputação da imagem da instituição:

- ✎ Integridade: Princípio que trata sobre a proteção da informação ou dos bens de informação contra a criação ou a modificação não autorizada. Perda de integridade pode estar relacionada com erro humano, ações intencionais ou contingência. A perda de integridade de uma informação pode torna-la sem valor, ou mesmo, torna-la perigosa. A consequência de utilizar dados incorretos pode ser desastrosa.
- ✎ Confidencialidade: Princípio que trata sobre a disponibilidade de informações à apenas pessoas autorizadas. Controles devem ser implementados para garantir que o acesso a informação seja sempre restrito àquelas pessoas que necessitam efetivamente tê-los. Muitos crimes cibernéticos acontecem através da quebra da confidencialidade

e do roubo da informação. Podem-se considerar dois momentos distintos desse princípio: ser confidencial e manter-se confidencial. A informação, para ser confidencial, deve ter uma classificação que determine as medidas de segurança necessárias quando ela estiver sendo tratada. Manter-se confidencial significa que o meio utilizado para tratar a informação permite proteção adequada.

- ✎✎ Disponibilidade: Princípio que trata sobre prevenir que a informação ou o recurso de informação esteja indisponível, quando requerida pelo cliente, pelo órgão regulador ou mesmo pela própria instituição. Aplica-se não só à informação, mas, também, aos canais eletrônicos, equipamentos de uma rede e outros elementos da infra-estrutura tecnológica. Não conseguir acesso a um recurso de informação desejado é chamado de Denial of Service, técnica muito utilizada pelos hacker. Os ataques intencionais contra infra-estrutura tecnológica podem ter finalidade de tornar os dados indisponíveis, assim como de roubar a informação.

b. Outros conceitos

Segundo VALLABHANENI (2002), são conceitos importantes a serem considerados no estudo da segurança da informação:

- ✎✎ Entidade: usuário, processo ou dispositivo que irá acessar uma determinada informação ou serviço;
- ✎✎ Atributos: características únicas pertencentes a entidade que permite distingui-la das demais entidades;
- ✎✎ Identificação: processo de reconhecimento da entidade através de seus atributos;
- ✎✎ Autenticação: processo de validação da identidade da entidade;
- ✎✎ Autorização: processo de prover ou retirar privilégios de uma entidade;
- ✎✎ Contabilização (*accountability*): processo para realizar o *log* das ações realizadas por uma entidade;
- ✎✎ Controle (*assurance*): garantir que os princípios básicos de segurança (tríade CIA) e de contabilização estejam assegurados;
- ✎✎ Não -repúdio: assegurar para uma entidade a negação de uma ação realizada;

✍ ✍ Auditoria (*audit*): revisão por uma entidade independente sobre os controles e a conformidade dos requisitos de segurança.

c. Classificação da informação

De acordo VALLABHANENI (2002), a classificação da informação é fundamental a segurança da mesma e para isso deve ser classificada em:

✍ ✍ Sensível: Esta classificação aplica-se às informações que necessitam de precauções especiais para assegurar a integridade da informação, bem como para protegê-la de modificações ou exclusões não autorizadas. Este tipo de informação requer um nível de confiança, exatidão e integralidade maior do que o normal. Incluem-se nesta classificação transações financeiras da companhia, ações legais, dentre outros.

✍ ✍ Confidencial: Esta classificação aplica-se às mais sensíveis informações de negócio destinadas estritamente para o uso interno da companhia. A revelação não autorizada destas informações poderia causar um sério impacto adverso para a empresa, seus acionistas, seus parceiros de negócio, e/ou seus clientes. As classificações *Secret* e *Top Secret* são variações da classificação "Confidencial".

✍ ✍ *Secret*: Esta classificação indica dados confidenciais com um alto grau de sensibilidade.

✍ ✍ *Top Secret*: Esta classificação indica dados confidenciais com o mais alto grau de sensibilidade.

✍ ✍ Privada: Esta classificação aplica-se a informações pessoais destinados para uso interno da companhia.

✍ ✍ Pública: Esta classificação aplica-se a todas as informações que não se encaixam adequadamente nas classificações mencionadas acima. Sua divulgação não autorizada não possui um efeito adverso para a companhia, funcionários e/ou clientes.

✍ ✍ Sem classificação: Esta classificação aplica-se a informações que não são sensíveis ou classificadas.

✍ ✍ Sem classificação porém sensível: Esta classificação aplica-se a informações cuja perda, mau uso, acesso não autorizado ou modificação desta informação poderá afetar de modo adverso os interesses da empresa. Incluem-se nesta classificação: testes para

contratação de funcionários, registros de investigativos, manuais para investigações, dentre outros.

Segundo KRUTZ e VINES (2001), deve-se designar um responsável pela classificação da informação. Recomenda-se que esta tarefa seja desempenhada pelo proprietário da informação ou sistema. Todas as informações geradas devem receber uma classificação. Periodicamente, o proprietário da informação deverá revisar a classificação fornecida, pois a criticalidade da informação pode ser alterada ao longo do tempo. Por exemplo, o desenvolvimento e o lançamento de um novo produto, somente deve ser classificada como informação confidencial e tratada como tal até o lançamento do produto, pois após esse evento, ela deixa de ser uma informação confidencial, e passa a ser pública.

2.2.2. Ameaças e seus elementos

Segundo PELTIER (2002), a segurança existe para proteger os ativos contra as ameaças existentes contra estes. Identificar as ameaças contra os ativos, que necessitam ser protegidos, é o primeiro passo para a segurança destes ativos.

Podemos definir a ameaça como:

“Prenúncio ou indício de coisa desagradável ou terrível (...)” (FERREIRA, 1999, pág. 118).

“Expressão de uma intenção de dano ou prejuízo.” (OXFORD, 1992, pág. 432).

A grande bibliografia existente referente a segurança da informação, também denominada de segurança digital, está voltada para área técnica e lista as ameaças existentes neste de meio de forma bastante semelhante.

Outra questão interessante sobre as ameaças digitais é que:

“(...) as ameaças no mundo digital espelham as ameaças no mundo físico. Se bancos físicos são roubados, então bancos digitais serão roubados.” (SCHNEIR, 2002, pág. 27).

Segundo PELTIER (2001), podemos identificar os seguintes elementos em cada ameaça:

- ✎ Agente: é o catalisador que executa a ameaça. O agente pode ser um ser humano, uma máquina ou a natureza.
- ✎ Motivo: é aquilo que incentiva o adversário a atuar. Esta ação pode ser acidental ou intencional.
- ✎ Resultado: é o efeito causado pela execução da ameaça. No caso da segurança da informação poderá ser: perda de acesso, acesso não autorizado, perda de privacidade, indisponibilidade de serviços, divulgação, alteração ou destruição de informações.

De acordo com PELTIER (2001) baseados nestes elementos, as ameaças existentes à segurança da informação podem ser divididas em três grandes grupos: humana, acidental, e de desastre natural. Isto é observado pelo desenho apresentado pela SYMANTEC (2002) em seu *Security Reference Handbook*.

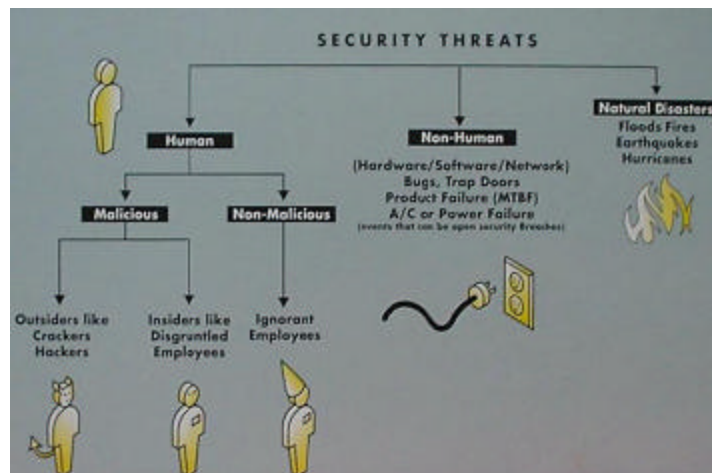


Figura 15: Ameaças

(SYMANTEC, 2002, pág. 24)

a. Ameaça de natureza humana

São aquelas que cujo agente é o ser humano. Podem ser acidentais ou intencionais.

Ameaças de intencionais são amplamente exploradas por literaturas especializadas. MCCLURE (2000) e SPYMAN (2000) são dois exemplos de autores que exploram tecnicamente as formas de ataque à sistemas computacionais. Eles ensinam sobre ameaças intencionais e suas contra-medidas, como muitos outros autores técnicos em segurança de redes. Podemos a partir deles identificar as diversas ameaças intencionais:

- ✎✎ *Footprinting*: ou rastreamento de alvos, é a utilização de ferramentas e técnicas para descobrir informações relacionadas a tecnologias utilizadas pela empresa, como: Internet, *intranet*, acesso remoto e *extranet*. A partir desta técnica, o invasor seleciona a empresa-alvo a ser explorada. MCCLURE (2000).
- ✎✎ *PortScan*: ou varredura de portas, a partir dos endereços IPs escolhidos a partir de um *footprinting*, os atacantes exploram mais detalhadamente cada um deles, encontrando as brechas necessárias para invasão e obtenção de informações valiosas como: servidores de rede, servidores DNS, servidores de correio eletrônico, nomes de funcionários e até telefones. SPYMAN (2000).
- ✎✎ *Sniffer*: ou coleta de dados trafegados na rede, é a técnica para capturar as informações que trafegam na rede, como *logins* e senhas não criptografadas, para utilização posterior. SPYMAN (2000).
- ✎✎ *Spoofing*: ou enumeração, atacantes assumem a identidade de um outro computador baseado na confiança entre servidores, que acreditam na credibilidade do endereço de origem. Esta é a principal técnica utilizado por atacantes intencionais para realizar um ataque através de um atacante não-intencional, ou acidental. MCCLURE (2000).
- ✎✎ *Hacking*: a partir de diversas informações coletadas, os atacantes exploram as vulnerabilidades do sistema operacional de um determinado computador. A partir daí, o atacante pode tentar invadir outros computadores pertencentes a rede ao qual o computador invadido pertence. MCCLURE (2000).
- ✎✎ DoS: da sigla *Denial of Service* ou ataque por negação de serviço, consiste, basicamente, em atacar um certo serviço no servidor alvo

de forma a travar todo o sistema. Desta forma, *hackers* conseguem indisponibilizar serviços e informações.

✍ ✍ Vírus de computador: programa que pode infectar outro programa de computador através da modificação dele, de forma a incluir uma cópia de si mesmo. A denominação de vírus vem de uma analogia com o vírus biológico, que altera a célula internamente e produz cópias dele. Atualmente a sofisticação desta ameaça tem causado diversos prejuízos as empresas.

Por não ser objetivo deste trabalho, o ensino didático das técnicas e tecnologias utilizadas para a execução de um ataque, sugiro para maiores detalhes e explicações, a leitura dos autores acima citados.

Segundo pesquisa realizada e divulgada em outubro de 2002 pela revista InformationWeek e a empresa de consultoria PricewaterhouseCoopers, a maioria da natureza das violações identificadas são os vírus, conforme mostra a seguir:



Figura 16: Natureza dos ataques

(InformationWeek, Outubro de 2002, pág.45)

SCHNEIER (2001) cita diversos responsáveis por estes ataques, mas resumidamente podemos escolher os seguintes quatro grupos:

- ⚡ *Hackers*: possui várias definições, desde um administrador de sistema corporativo perito para criar defesas até um criminoso adolescente com pouca ética que se diverte em realizar ataques.
- ⚡ Criminosos solitários: são criminosos que começam a se especializar em tecnologia para executar seus crimes de forma digital.
- ⚡ *Insiders* maliciosos: são os funcionários ou prestadores de serviço que possuem como objetivo prejudicar a empresa, seja por causa de motivos de descontentamento, ou por motivos para obtenção de ganhos pessoais .
- ⚡ *Insiders* inocentes: são funcionários ou prestadores de serviços que não utilizam corretamente os recursos tecnológicos por falta de conhecimento, disponibilizando desta forma uma série de vulnerabilidades para empresa.

Segundo pesquisa realizada e divulgada em outubro de 2002 pela revista InformationWeek e a empresa de consultoria PricewaterhouseCoopers, a maioria dos ataques partem de ataques internos (considerando usuários autorizados e não-autorizados temos o total de 39%), conforme mostra a seguir:

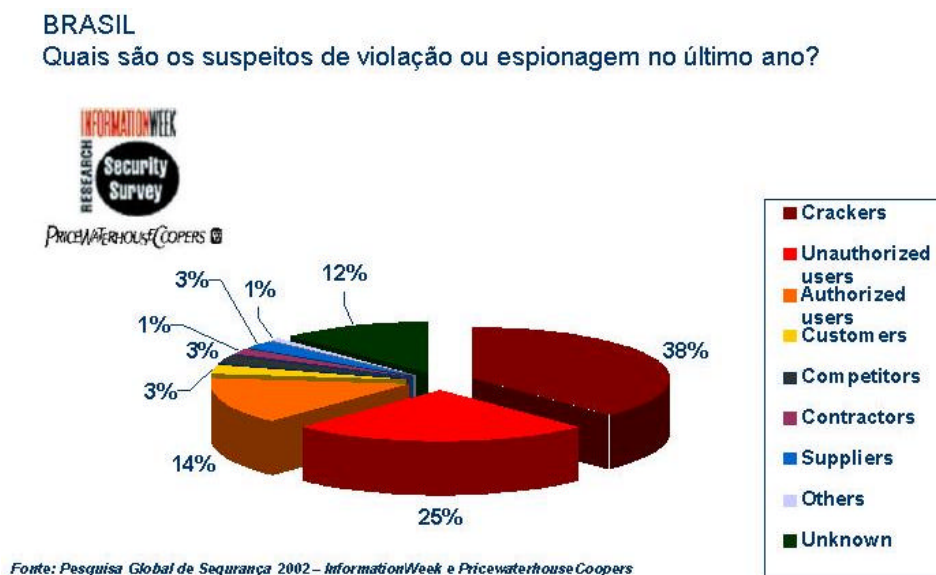


Figura 17: Atacantes

(InformationWeek, Outubro de 2002, pág.45)

b. Ameaça acidental

São aquelas que cujo agente é uma falha tecnológica, interna ou externa ao ambiente da organização. De acordo com WADLOW (2001), são exemplos de ameaça acidental: sobrecarga do circuito de energia, falta de energia, umidade, problemas com a temperatura do local dos servidores, etc.

c. Desastre natural

São desastres cujo agente é a natureza. De acordo com HUMPHREYS (1998), são exemplos de desastre natural: terremoto, inundações, incêndios, tempestades, etc.

2.2.3. Gerenciamento de risco e segurança da informação

A primeira forma de analisar o gerenciamento de risco da segurança da informação é aplicar os conceitos de gerenciamento de risco diretamente sobre o tema da segurança da informação. Desta forma podemos aplicar as classificações de risco segundo VAUGHAN (1997), para podermos entender melhor a natureza dos riscos associados a segurança de informação e melhor classificá-los. Os riscos associados a segurança da informação são:

- ✎✎ Financeiros: pode-se dizer que os riscos a segurança da informação são na sua grande maioria riscos financeiros, pois causam, direta ou indiretamente perdas de receita ou financeiras.
- ✎✎ Estáticos ou dinâmicos: dependendo da situação podem ser riscos estáticos, como por exemplo, uma invasão pontual ao sistema computacional, um incêndio no CPD, ou dinâmico, como, mudanças na tecnologia, um vírus mundial, etc.
- ✎✎ Particulares ou fundamentais: os riscos da segurança da informação podem ser ainda particulares, como um ataque específico ao *website* da organização, ou fundamentais, como a propagação de e-mails com vírus.

☞ Puros: pode-se dizer que a grande maioria dos riscos em segurança da informação são puros, pois há possibilidade apenas de perdas.

Em relação à questão do gerenciamento em si do risco, pode-se dizer que muito tem sido desenvolvido na área de risco, principalmente na área financeira.

“Both the theory and the practice of risk management have developed in the last two and a half decades. The theory has developed to point where risk management is now regarded as a distinct sub-field of the theory of finance (...)” (DOWD, 1998, pág. 4)

Isto talvez esteja relacionado ao próprio tempo de estudo do gerenciamento da área financeira; em relação nas demais áreas, como o gerenciamento da informação.

“Os conhecimentos relativos ao gerenciamento de finanças e operações vêm sendo acumulados e ensinados por mais de um século. Os conhecimentos sobre o gerenciamento da informação apenas recentemente começaram a ser reunidos.” (MCGEE, 1994, pág. 23).

Uma das formas encontradas nos autores pesquisados para o gerenciamento de riscos em segurança da informação é aplicar os conceitos de gerenciamento de risco sobre o tema de segurança da informação. BRAITHWAITE (2002) apresenta o modelo proposto por CAMPBELL e SANDS (1979) com esta finalidade. Podemos observar todas as fases tradicionais do gerenciamento de riscos e suas diversas atividades ao longo do processo.

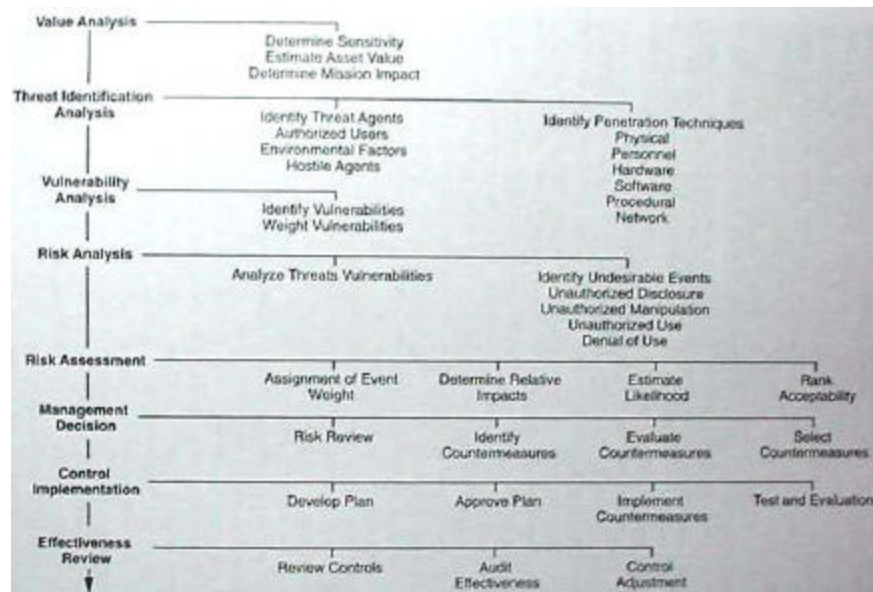


Figura 18: Risk Management Model

(CAMPBELL e SANDS, 1979, v. 48)

Seguindo esta mesma linha de raciocínio, ALBERTS (2002) apresenta o seguinte processo de gerenciamento de risco para segurança da informação.

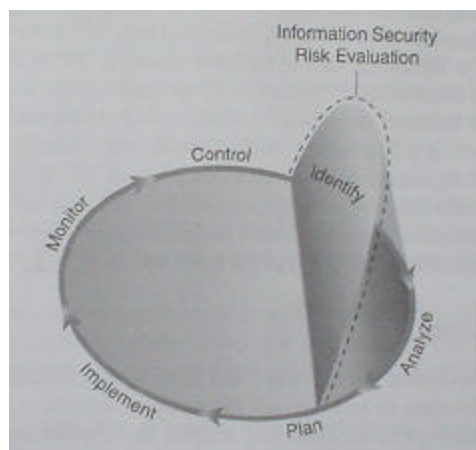


Figura 19: Risk Management Model

(ALBERTS, 2002, pág. 11)

Podemos notar uma pequena diferença entre os modelos tradicionais de gestão de riscos como de VAUGHAN (1997) e CULP (2002). ALBERTS (2002) propõe que a fase de avaliação do risco englobe a fase de identificação dos riscos e a análise do risco.

ALBERTS (2002), ainda em seu modelo, define que o gerenciamento de risco em segurança da informação deve seguir os seguintes princípios:

- ▬ Princípios de avaliação de risco em segurança da informação
- ▬ Princípios de gerenciamento de risco
- ▬ Princípios organizacionais e culturais

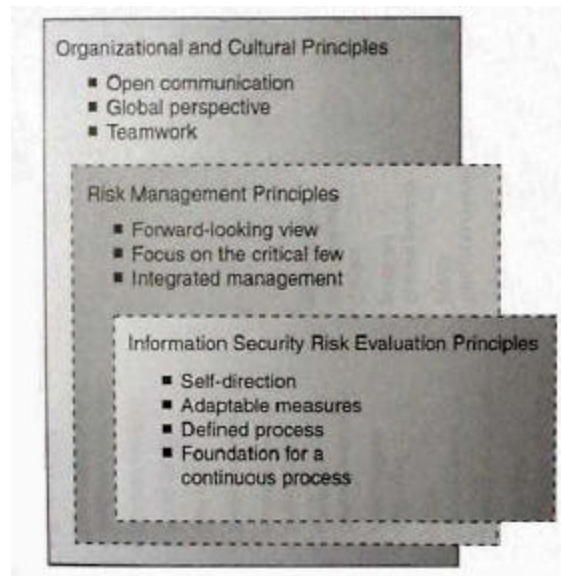


Figura 20: Information Security Risk Management Principles

(ALBERTS, 2002, pág. 20)

a. Princípios de avaliação do risco em segurança da informação

Estes princípios focam o direcionamento das avaliações de risco em segurança da informação. Estes princípios asseguram que a segurança da informação permeie toda a organização. São eles: auto-gestão, medidas adaptativas, formalização de processos de risco, estrutura para um processo contínuo.

- ▬ Princípio de auto-gestão: este princípio descreve que todos na organização devem estar preocupados com a identificação e avaliação do risco em segurança da informação. Somente desta forma é possível considerar que a empresa esteja em condições de avaliar os riscos em todas as esferas e processos de negócio.

- ✍ ✍ Princípio de medidas adaptativas: uma avaliação flexiva pode se adaptar as constantes mudanças e avanços tecnológicos. Este princípio afirma que para uma boa avaliação de risco, o modelo de riscos e ameaças não deve ser rígido e muito menos tentar ser o mais perfeito possível.
- ✍ ✍ Princípio de formalização de processos de risco: este princípio define que processos formalizados facilitam a institucionalizar a aplicação destes processos, assegurando que os processos sejam aplicados.
- ✍ ✍ Princípio de estrutura para um processo contínuo: este princípio baseia-se que uma organização deve implementar estratégias de segurança baseadas nas lições aprendidas no passado. A melhoria da segurança deve ser um processo contínuo e deve ser planejado e estruturado para tal.

b. Princípios de gerenciamento de risco

Estes princípios estão baseados nas práticas genéricas de gerenciamento de risco, e portanto, não são exclusivos a segurança da informação. São eles: visualizar sempre a frente, foco em poucos pontos críticos, e gerenciamento integrado.

- ✍ ✍ Princípio de visualizar sempre a frente: este princípio define que devem existir pessoas preocupadas não apenas com os problemas atuais mais que estejam focados com os ativos mais críticos da organização e visualizem quais os riscos futuros a estes ativos.
- ✍ ✍ Princípio de foco em poucos pontos críticos: este princípio afirma que a organização deve focar apenas nas questões mais críticas de segurança da informação.
- ✍ ✍ Princípio de gerenciamento integrado: este princípio afirma que as políticas e estratégias de segurança devem ser consistentes com as políticas e estratégias da organização.

c. Princípios organizacionais e culturais

Estes princípios analisam as questões organizacionais e culturais da empresa. Conforme ALBERTS (2001), as pessoas não comunicarão e muito menos tratarão os riscos chave, caso não exista um ambiente propício aberto a discussão e troca de idéias. Para isto é fundamental, os seguintes princípios: comunicação aberta, perspectiva global, e trabalho em equipe.

- ✍ ✍ Princípio da comunicação aberta: este princípio é o mais difícil de se implementar. Ele afirma que o conceito fundamental atrás do gerenciamento de risco é a cultura organizacional que suporta a comunicação dos riscos de informação através de uma forma colaborativa.
- ✍ ✍ Princípio de perspectiva global: segundo este princípio é necessário que as pessoas enxerguem os riscos de segurança, não de forma pontual, mas sim com uma perspectiva global de toda empresa. Ou seja, é necessário que as pessoas encarem que a empresa deve tratar a segurança da informação como um todo e não localmente.
- ✍ ✍ Princípio do trabalho em equipe: é impossível que uma única pessoa entenda as questões de segurança de uma empresa como um todo. Este princípio afirma que o gerenciamento de risco deve ser uma abordagem inter-disciplinar e portanto há necessidade de um trabalho em equipe.

PELTIER (2002) apresenta uma outra forma de abordagem, cujo enfoque é identificar as necessidades de negócio e os riscos associados, e a partir daí estabelecer um processo de gerenciamento destes riscos. O gerenciamento do risco na segurança da informação é apresentado através do seguinte processo: identificação das necessidades e análise de riscos, implementação de políticas e controles, conscientização e treinamento, monitoramento e revisão dos controles. Todo este processo deve estar centralizado em um ponto focal, seja uma pessoa ou área de segurança.

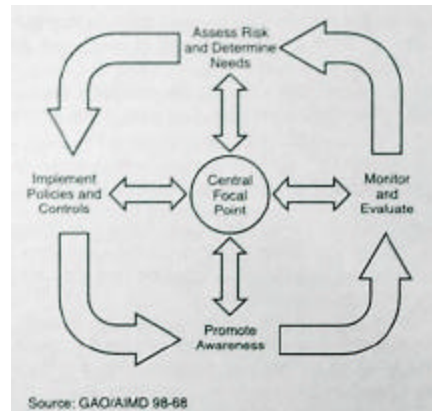


Figura 21: Information Security Risk Management

(PELTIER, 2002, pág. 18)

2.2.4. Segurança da informação e auditoria de sistemas

Segundo o Relatório do Comitê de Conceitos Básicos de Auditoria da Associação Americana de Contabilidade, citado por BOYTON (1996), a auditoria é um processos sistemático de obter e avaliar evidências enfocando afirmações sobre ações e eventos econômicos para avaliar o grau de correspondência entre estas afirmações e os critérios estabelecidos para comunicação dos resultados aos interessados.

Segundo BOYTON (1996), pode-se classificar a auditoria em três tipos:

- ✎ Auditoria de demonstrações financeiras: envolve a análise das evidências sobre as demonstrações financeiras de uma empresa, com o objetivo de opinar se tais demonstrações foram desenvolvidas obedecendo a um critério estabelecido.
- ✎ Auditoria de conformidade (*compliance*): envolve a análise das evidências de algumas atividades financeiras ou operacionais de uma empresa, com o propósito de verificar se estas estão em conformidade com as condições e regulamentos específicos ao assunto.
- ✎ Auditoria operacional: compreende a análise das evidências sobre a eficiência e a eficácia das atividades operacionais de uma empresa em relação a objetivos específicos.

Qualquer atividade empresarial necessita ser conduzida dentro de determinados padrões, e este conjunto de padrões, que direciona a empresa no sentido dela atingir seus objetivos, pode ser chamado de controle interno.

A importância do controle interno para os trabalhos de auditoria é reconhecida há um certo tempo. Segundo BOYTON (1996), a publicação do AICPA (*American Institute of Certified Public Accountants*) de 1947 já reconhecia e definia o termo *Internal Control*.

A preocupação com controles internos ultrapassou as fronteiras da auditoria e contabilidade. Em 1987, a *Treadway Commission*, uma comissão formada pelo Congresso dos Estados Unidos, divulgava o relatório final denominado *National Commission on Fraudulent Financial Reporting*, no qual recomendava as empresas públicas a manter controles internos que forneçam segurança mínima para evitar fraudes e problemas aos relatórios financeiros. Também recomendava que as organizações patrocinadoras da comissão cooperassem para o desenvolvimento de instruções adicionais de um sistema de controles internos.

Em 1992, o comitê das organizações patrocinadoras da comissão de 1987 - COSO (*Committee of Sponsoring Organizations*) lançou o relatório chamado *Internal Control – An integrated framework* com os seguintes objetivos:

- ✍✍ Estabelecer uma definição de controle interno atendendo as necessidades de diversos parceiros envolvidos.
- ✍✍ Fornecer um padrão para que as empresas e outras organizações pudessem avaliar o seu sistema de controle interno e determinar como melhorá-lo.

Segundo o relatório do COSO (1992), para a existência de controles internos na organização é necessário uma estrutura de controle, descrita a seguir:

- ✍✍ Ambiente de controle
- ✍✍ Avaliação de riscos
- ✍✍ Atividades de controle
- ✍✍ Informação e comunicação
- ✍✍ Monitoração

Segundo BOYTON (1996), os controles internos aplicados aos sistemas de informações computadorizados podem ser executados por controles gerais e controles de aplicação. Os controles gerais são:

- ✍ ✍ Controles organizacionais e operacionais
- ✍ ✍ Controles de documentação e de desenvolvimento de sistemas
- ✍ ✍ Controles de equipamentos e de sistemas operacionais
- ✍ ✍ Controles de acesso
- ✍ ✍ Controles de dados e processamento

Já os controles de aplicação são:

- ✍ ✍ Controles de entrada
- ✍ ✍ Controles de processamento
- ✍ ✍ Controles de saídas

Em 1996, uma associação mundial de auditores de informática envolvendo mais de 100 países, denominada ISACA – *Information Systems Audit and Control Association* com apoio de instituições como Unisys e Coopers & Lybrand, desenvolveu uma estrutura denominada COBIT – *Control Objectives for Information and Related Technology* para facilitar os trabalhos de auditoria em sistemas computadorizados. Baseando-se nos componentes de controles definidos no relatório do COSO, o COBIT avalia se os requisitos do negócio estão sendo atendidos pela tecnologia de informação da empresa.

A estruturação do COBIT define que os recursos de tecnologia de informação implementam os diversos processos de TI com o objetivo de atender os requisitos do negócio.



Figura 22: COBIT principles
COBIT

A execução das atividades de TI deve ser feita de forma que se atinjam os objetivos de controle. Atendendo a estes objetivos, o COBIT afirma que existe uma relativa segurança que os requisitos de negócio foram atendidos. É responsabilidade da organização assegurar a execução destes processos e se os objetivos de controle correspondentes estão sendo atingidos.



Figura 23: COBIT process

COBIT

Agora sob a óptica de GREENSTEIN (2000), podemos classificar os riscos associados a segurança da informação como uma sub-classificação de um risco operacional.



Figura 24: Gerenciamento da informação

(elaborado pelo autor)

Para situarmos a segurança da informação em relação aos trabalhos de auditoria e as principais teorias desenvolvidas, elaborou-se o seguinte quadro comparativo:

	Segurança da informação	Auditoria de Sistemas	Auditoria de Controles Internos
1. Área responsável	Riscos de alteração, indisponibilização e destruição da informação	Riscos associados aos recursos de Tecnologia da Informação	Riscos operacionais
2. Metodologia	BS7799 ISO 17799	COBIT: Control Objectives for Information and related Technology (9 dimensões)	<i>Internal Control: Integrated framework – COSO</i>
3. Organização desenvolvida da metodologia	BS: British Standards OSI: Organization of International Standards	ISACA: Information System Audit and Control Association	COSO: Committee of Sponsoring Organizations of the Treadway Commission
4. Certificação profissional	CISSP: Certified Information System Security Professional	CISA: Certified Information System Auditor	-----
5. Órgão emissor da Certificação	ISC2: International Information Systems Security Certification Consortium	ISACA: Information System Audit and Control Association	-----
6. Foco de estudo	Processos de Segurança da Informação	Processos de TI	Processos Operacionais
7. Riscos analisados	<ol style="list-style-type: none"> 1. Risco alinhamento estratégico do plano de Segurança da informação 2. Segurança do Código 3. Risco em segurança de invasão na mudança da plataforma tecnológica 4. Segurança dos dados 5. etc. 	<ol style="list-style-type: none"> 1. Risco de alinhamento estratégico do plano de TI 2. Qualidade e eficiência do código 3. Risco nas aplicações e performance na mudança da plataforma tecnológica 4. Qualidade dos dados 5. etc. 	<ol style="list-style-type: none"> 1. Falta de Controles de processos 2. Falha de produto / serviço 3. Inadequação da capacidade de produção 4. Obsolescência do estoque 5. Obsolescência tecnológica 6. etc.

2.3. Modelo de Gestão de Risco em Segurança da Informação

De acordo com NAKAMURA (2002), a necessidade de segurança está transcendendo o limite da produtividade e funcionalidade. Enquanto que a eficiência e eficácia nos negócios significam vantagem competitiva, a falta de segurança nos meios tecnológicos pode resultar grandes prejuízos.

“According to the Computer Security Institute, the computer-related crime costs an organization about \$500,000 while an average bank robbery results in only about \$2,500 in losses.” (KANELLAKIS, Canadian HR Reporter, Dec. 2, 2002, v. 15-21, pág. G4)

Segundo WADLOW (2001), a administração da segurança, seja como função ou seja como responsabilidade de uma área específica dentro da instituição, é requisito fundamental dentro do processo de estabelecimento da arquitetura da segurança corporativa.

Para fins didáticos e de organização, o modelo de gestão de risco em segurança da informação foi dividido em quatro componentes:

- ▬ Direcionadores de negócio e agentes de implementação
- ▬ Alinhamento estratégico da segurança da informação ao negócio
- ▬ Segurança das operações
- ▬ Gerenciamento das identidades

2.3.1. Direcionadores de negócio e agentes de implementação

LAUDON (2002) propõe o seguinte modelo para a gestão da segurança da informação:

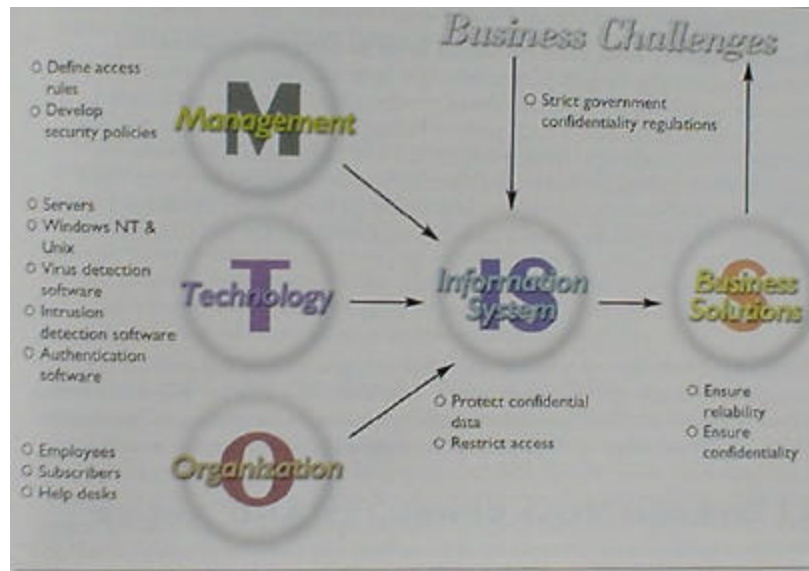


Figura 25: Information Risk Management

(LAUDON, 2001, pág.433)

Podemos identificar e classificar a partir deste modelo os seguintes elementos:

- ≡ Agentes implementadores: tecnologia, pessoas e processos.
- ≡ Direcionadores de negócio: *Business Challenges*
- ≡ Áreas de interesse: definição de regras de acesso, desenvolvimento de políticas de segurança, arquitetura de segurança (representados por *Servers, Window NT, Intrusion detection software, etc*)

a. Direcionadores de negócio

Segundo ALBERTS (2002), planejar as estratégias de segurança da informação alinhada com os objetivos de negócio da organização é fundamental para a sua implementação de segurança. Os direcionadores de negócio estão relacionados as questões de planejamento e estratégia. São em última instância os objetivos finais da área de segurança da informação. Os direcionadores de negócios são três:

Agregar Valor ao Negócio

Conforme PELTIER (2001), a segurança da informação está intimamente relacionada com as necessidades de negócio da organização. Determinar estas necessidades e identificar os riscos associados à estas, são fundamentais para o gestor de segurança.

Segundo o princípio de gerenciamento integrado de risco proposto por ALBERTS (2002), as questões de segurança devem estar incorporadas no negócio da organização e as estratégias e metas de negócio devem ser perseguidas pelas estratégias e políticas de segurança.

De acordo com PELTIER (2001), este direcionador visa minimizar a lacuna existente entre o valor da informação e os esforços para segurança da informação. Para isto responder, é necessário que a área de segurança responda as seguintes questões:

- ☞ ☞ Quais são as estratégias e metas de negócio da empresa?
- ☞ ☞ Como a segurança pode contribuir para atingir as metas e objetivos da empresa?
- ☞ ☞ Quais são os processos críticos da empresa e os riscos associados?
- ☞ ☞ Qual o valor da segurança da informação sobre os processos críticos?

Gerenciar o Custo Total em Segurança

De acordo com ATKINSON (1999) , com o desenvolvimento do controle gerencial no século XX, administrar e apresentar o retorno sobre o investimento é fundamental para as áreas que compõe a organização. Portanto trata-se de um direcionador importante para a área de segurança da informação.

Segundo LOEB (2002) , otimizar o custo total da segurança dentro da instituição, e apresentar de forma clara e transparente para as demais áreas é uma tarefa árdua e necessária. Primeiro que quantificar o retorno do investimento para os projetos de segurança é extremamente difícil, uma vez que lida-se com parâmetros muitas vezes intangíveis, como por exemplo: má fé de

funcionários ou mudanças tecnológicas. Segundo, é uma atividade necessária, pois sem gastos em segurança não há proteção aos negócios da empresa.

Esta comunicação, segundo ALBERTS (2002) é fundamental, pois somente com uma comunicação aberta, clara e transparente, pode-se criar uma cultura organizacional propícia ao gerenciamento de riscos de segurança da informação.

Gerenciar as Expectativas dos Investidores

De acordo com BYRNES (2002), é fundamental administrar as expectativas dos acionistas e da alta cúpula em relação ao risco da instituição associado a segurança da informação. Uma das funções implícitas do gestor de segurança é entender as estratégias do negócio e enviar mensagens de marketing alinhadas as mesmas para alta administração e acionistas. O gestor da segurança da informação deve se preocupar em responder:

- ❏ O nível de segurança às informações é satisfatório em relação aos investimentos?
- ❏ Existe a aplicação das melhores práticas de segurança sobre as informações do negócio?
- ❏ O negócio está dentro das conformidades legais de segurança?
- ❏ Quais certificações poderiam ser obtidas em relação ao estágio de maturidade de segurança da organização?

c. Agentes implementadores

Tendo em vista os direcionadores de negócio, são necessários agentes para tratar a implementação, levando em consideração os princípios apresentados por ALBERTS (2002) que consideram os aspectos técnicos, humanos e procedurais. Os agentes implementadores do Modelo de Gestão, que são:

Pessoas

De acordo com os princípios organizacionais e culturais apresentado por ALBERTS (2002), para implementação efetiva da gestão de segurança dentro de

uma organização, o agente mais importante, e no entanto, menos observado durante a implementação, são as pessoas. As questões culturais para assimilação e implementação da segurança da informação são fundamentais para a eficácia da gestão de segurança.

Processos

Como já anteriormente descrito por ALBERTS (2002), através do princípio da formalização dos processos de risco, o desenho e uma boa definição dos processos de segurança são essenciais para o sucesso da implementação da segurança da informação.

Tecnologia

Segundo SCHNEIER (2001), a tecnologia é o item ,que na prática, é o primeiro ser implementado e leva o estigma de ser entendido dentro da organização como o único responsável pela gestão da segurança.

Conforme FONTES(2000), a utilização inadequada deste componente, em nada ajudará em proteger os sistemas de informação da empresa. Apenas trará um falso conforto para aqueles que a implementaram.

*“O truque é projetar sistemas que sejam protegidos contra as ameaças reais, e não usar tecnologias de segurança a esmo, acreditando que isso fará algo útil.”
(SCHNEIER, 2001, pág. 303)*

2.3.2. Alinhamento estratégico da segurança da informação

Este tópico aborda as questões estratégicas com relação a segurança da informação e aborda as principais ações para o efetivo alinhamento estratégico da segurança da informação com os objetivos e processos de negócio da organização. Para fins didáticos foram divididas nas seguintes áreas de interesse:

- ✍ ✍ Visão e apoio estratégico
- ✍ ✍ Organização e competências
- ✍ ✍ *Compliance* e aderência
- ✍ ✍ Políticas e normas de segurança
- ✍ ✍ Monitoramento e prevenção
- ✍ ✍ Treinamento e conscientização

a. Visão e apoio estratégico

Segundo BYRNES (2002) a definição da missão e visão da área de segurança da informação é fundamental, não só para área de segurança da informação, mas também para o conhecimento de toda a organização. Para isto é essencial que a área tenha o apoio da alta administração da instituição. É necessário que toda a alta administração tenha consciência da importância da segurança da informação tendo uma participação ativa nas aprovações das estratégias a serem adotadas.

Ainda de acordo com BYRNES (2002), como produto desse item é necessário o desenvolvimento de um *Security Charter*, documento formal, contendo toda a estratégia de segurança corporativa da instituição, que reflita o desejo da alta administração da instituição, quanto a proteção dos ativos de informação e das operações internas da empresa.

b. Organização e competências

De acordo com KURTZ e VINES (2001), a estrutura organizacional da área de segurança da informação e o estabelecimento de competências específicas, para tratar as questões de segurança de forma direcionada as necessidades, é fundamental para a Gestão da Segurança da Informação. Para isto, todas as responsabilidades das entidades abaixo mencionadas devem ser formalmente definidas na Política de Segurança da Informação.

☞ Comitê de Segurança da Informação : a composição de um Comitê é fundamental para estabelecer o programa de segurança para a organização, suas metas, objetivos e prioridades para suportar a missão da organização. O comitê deve ser composto por executivos das diversas áreas representativas da organização ou delegados por eles com conhecimento das estruturas internas e com autonomia de forma a deliberar e suportar as decisões tomadas sobre as questões de segurança que afetem os negócios da empresa. As responsabilidades do Comitê de Segurança da Informação incluem, mas não se limitam a:

- ☞ Direcionar os esforços e recursos propostos pela Área de Segurança conforme a estratégia de negócios da organização.
- ☞ Aprovar a Política e Normas de Segurança da Informação e suas atualizações, bem como as responsabilidades atribuídas a esta.
- ☞ Aprovar os controles a serem utilizados para garantir a segurança das informações.
- ☞ Acompanhar os indicadores de segurança e incidentes reportados pela área de Segurança da Informação.
- ☞ Deliberar sobre a aplicação de penalidades em casos de violações à Política de Segurança da Informação cuja gravidade seja alta.
- ☞ Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados.
- ☞ Aprovar planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação.
- ☞ Garantir que todo profissional de segurança da informação obtenha treinamento específico para condução de suas atividades, inclusive permitindo e gerando contatos com empresas especializadas.
- ☞ Delegar as funções de segurança da informação aos profissionais responsáveis.

☞ Gerência de Segurança da Informação: esta gerência possui como responsabilidade, atuar de forma pró-ativa nas questões de segurança para toda a organização, bem como coordenar e intermediar todas as interações com entidades internas ou externas em todos os assuntos relacionados a segurança da informação. Algumas das atividades da área de segurança incluem, não se limitando a:

- ✍ Monitorar as violações de segurança e tomar ações corretivas para assegurar que as ações necessárias para que não haja recorrência foram adotadas.
- ✍ Testar a infraestrutura de tecnologia para avaliar os pontos fortes e detectar possíveis ameaças, com o suporte da área de Tecnologia e Infraestrutura.
- ✍ Revisar periodicamente as Políticas e Normas de Segurança da Informação e sugerir as alterações necessárias.
- ✍ Definir as principais funções e responsabilidades quanto à segurança da informação de todas as áreas da organização.
- ✍ Gerenciar o desenvolvimento, a implementação e o teste dos controles técnicos e processuais de segurança, necessários para garantir a segurança do ambiente de tecnologia.
- ✍ Desenvolver, manter e implementar programas de treinamento e de conscientização aos funcionários e prestadores de serviço sobre a Política de Segurança da Informação, a forma como ela está estruturada e os principais conceitos de segurança da informação.
- ✍ Participar dos planejamentos anuais de segurança, considerando as diversas áreas da empresa e seus planos específicos, para definir as estratégias, alocar os recursos tecnológicos, financeiros e humanos e priorizar os investimentos, submetendo os projetos ao Comitê de Segurança da Informação para aprovação.
- ✍ Elaborar, implementar, analisar e divulgar os indicadores da segurança da informação, tomando as ações necessárias para que estes atendam às necessidades da empresa.
- ✍ Assessorar as demais áreas da empresa no processo de classificação das informações.
- ✍ Implementar programas regulares de avaliação de riscos nas áreas de negócio, auxiliando os responsáveis por estas, quando necessário.
- ✍ Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios.
- ✍ Assegurar que exista um processo apropriado para o reporte dos incidentes e violações de segurança detectados pelos funcionários e prestadores de serviço, independentemente dos recursos tecnológicos utilizados.

- ✍ Garantir a tomada de ações rápidas caso sejam detectados incidentes de segurança.
- ✍ Reportar periodicamente à Alta Administração o nível de segurança da organização, incluindo informações sobre as áreas que apresentem problemas, com recomendações para aprimoramento;
- ✍ Desenvolver e assegurar a utilização de dispositivos adicionais de segurança, não se limitando aos mencionados nas Políticas e Normas de Segurança da Informação.
- ✍ A área de segurança da informação deverá auxiliar as áreas de desenvolvimento durante a fase de planejamento dos sistemas para que sejam abrangidos os controles de segurança.

De acordo com WADLOW(2001), a área de segurança da informação deve estruturar as seguintes equipes multidisciplinares:

- ✍ Equipe de Monitoramento: esta equipe representa os alertas e alarmes da organização de segurança, vinte quatro horas por dia em sete dias da semana. Esta equipe realiza tarefas rotineiras necessárias além de testar vários sistemas regularmente de forma a verificar que tudo está funcionando conforme o projetado. No caso de um ataque, esta equipe é responsável pela declaração de um estado de emergência e de proteger os sistemas de informações até a equipe de resposta e a equipe de investigação assumirem a situação. Deve-se também capacitar esta equipe para lidar com questões rotineiras sem a declaração de um estado de emergência. Enquanto as demais equipes tratam do ataque, a equipe de monitoramento deve ter condições de continuar a monitoração da rede e dos sistemas de informação.
- ✍ Equipe de Resposta: a equipe de resposta é responsável pelo combate a qualquer ataque a organização. Seus membros operam as defesas ativas da empresa e visam avaliar e coordenar o combate a qualquer dano causado pelo incidente. Também asseguram que qualquer brecha das defesas utilizadas por um atacante será descoberta e consertada, e que qualquer modificação e estrago realizado pelo invasor será encontrado e restaurado inteiramente às configurações corretas. Além de responder os ataques, a equipe de resposta é responsável pelo estudo de métodos de ataque e pelo sistema de monitoração ativa e sistema de registros (logs). Desta forma, a todo o novo método de ataque é planejado uma forma de defesa para conter e derrotar o mesmo. De forma mais abrangente essa equipe também é responsável

pela coordenação da elaboração do plano de contingência de toda a organização, interagindo com os gerentes, proprietários das aplicações, equipes de segurança, e demais entidades.

- ✎ Equipe de Investigação de Crimes Eletrônicos: esta equipe fornece pesquisa e ajuda detalhada à equipe de resposta. Num incidente, a equipe de investigação de crimes eletrônicos é responsável por investigar exaustiva e cuidadosamente de forma a confirmar, refutar ou adicionar qualquer avaliação trazida pela equipe de resposta. Vale lembrar ainda que as funções de segurança não se restringem a algumas equipes, mas sim devem ser cobertas por diversas áreas de organização.



Figura 26: Estrutura organizacional

(WADLOW, 2001, pág. 52)

De acordo com VALLABHANENI (2002), existem diversas funções de segurança que não estão dentro da área de segurança, como:

- ✎ Proprietário da Informação: preferencialmente, cada sistema e as informações nele contidas, devem possuir um proprietário atribuído. Especificamente, os proprietários são responsáveis por definir o nível de segurança e o perfil de acesso para os dados, arquivos e sistemas que estejam sob sua responsabilidade. Adicionalmente, o proprietário é responsável por classificar as informações que estejam sob sua responsabilidade, de acordo com os critérios definidos pela área de Segurança da Informação.
- ✎ Administradores de Sistemas: são os gerentes e técnicos que desenham e operam os sistemas de computadores. Eles são responsáveis pela implementação da segurança técnica no sistema do computador e por estarem familiarizados com a tecnologia de segurança que corresponde aos seus sistemas. Eles também precisam garantir a continuidade dos serviços que realizam para suprir as necessidades funcionais dos

gerentes das áreas de negócio bem como analisar vulnerabilidades técnicas nos seus sistemas (e na implementação segura).

- ✎ Equipe de Telecomunicações: normalmente são responsáveis por prover serviços de comunicação, incluindo voz, dados, vídeo e fax.
- ✎ *Help Desk*: ou serviço de atendimento e suporte, é incumbido de tratar os incidentes. Deve ser capaz de reconhecer os incidentes de segurança e direcionar a solicitação para o funcionário ou organização apropriada responsável.
- ✎ Auditores: são responsáveis por examinar os sistemas para determinar se estes estão atendendo os requisitos de segurança estabelecidos, incluindo as políticas organizacionais e dos sistemas, e se os controles de segurança estão apropriados.
- ✎ Segurança Patrimonial: a área de Segurança Patrimonial é normalmente responsável pelo desenvolvimento e pelo reforço dos controles de segurança física após prévia consulta aos demais gerentes da organização. Esta área deve assegurar a segurança física em toda a dependência da empresa, assim como o transporte e armazenamento das mídias e documentos externos.
- ✎ Qualidade: muitas organizações têm estabelecido um programa/área de qualidade para melhorar os produtos e serviços oferecidos aos clientes. O gerente da qualidade deve ter um conhecimento dos princípios de tecnologia e como eles podem ser usados para melhorar o programa de qualidade. Estes princípios incluem a melhoria da integridade das informações do computador, a disponibilidade dos serviços e a confidencialidade da informação do cliente.

Segundo BYRNES (2001) a estrutura organizacional tradicional para a área de segurança da informação seria os especialistas no assunto estarem subordinados às gerências de desenvolvimento de sistemas e *data center*.

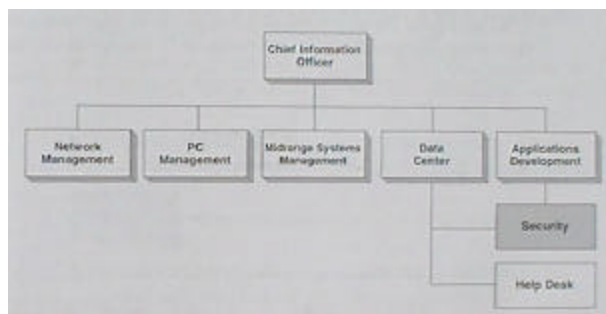


Figura 27: Estrutura Organizacional Tradicional

(BYRNES, 2001, pág. 9)

BYRNES (2001) propõe a seguinte estrutura organizacionais para uma efetiva gerência de segurança da informação. Neste caso a área de segurança da informação responde diretamente ao *Chief Information Officer*.

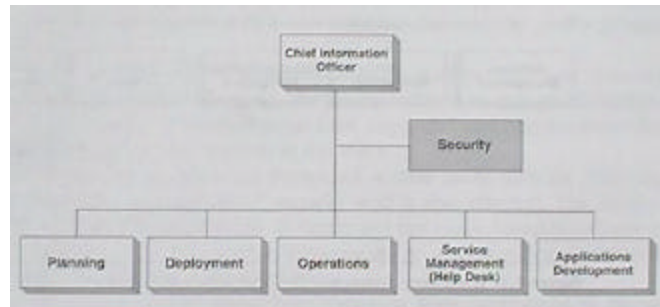


Figura 28: Estrutura proposta por Byrnes

(BYRNES, 2001, pág. 10)

Já ROSS e WEILL (2002) propõe que a área de TI não devesse liderar o processo de gerenciamento de riscos de segurança e privacidade, pois podem dar ênfase excessiva em segurança e tornar os processos inconvenientes para os clientes e funcionários.

Segundo NAKAMURA (2002), a segurança da informação deve ser tratada como um processo de negócio e para isto deve ter independência total para atuar.

A área de segurança de informação por ter características de auditoria e propósitos diferentes de tecnologia não deveriam estar subordinadas a área de tecnologia. Neste sentido, o modelo proposto por BYRNES (2001) fere questões de auditabilidade caso a área de segurança de informação fosse subordinada a área de tecnologia.

c. Compliance e aderência

Segundo PELTIER (2002) a estratégia para se obter um alcance amplo e corporativo em relação à segurança de informação está na avaliação da aderência da estratégia da segurança de informação aos objetivos de negócio da empresa. É

necessário, criar indicadores para avaliar qual a efetiva participação da área de segurança da informação nas demais áreas de negócio da instituição.

A aderência visa a atender dois princípios importantes apresentados por ALBERTS(2002), o princípio do foco em poucos pontos críticos, e o princípio de gerenciamento integrado.

De acordo com VALLABHANENI (2002), os projetos de segurança desenvolvidos deverão estar em conformidade com as necessidades de negócio da empresa. Dessa forma, a área de segurança da informação deverá estar em constante contato com os gestores das áreas de negócio com o propósito de identificar as necessidades de segurança inerentes ao processo produtivo. Todos os projetos que apresentem riscos para as informações da empresa, devem ter o envolvimento formal da área de segurança da informação, visto que esta área possui conhecimentos que a permitem identificar quais os controles de segurança necessários para que a integridade, confidencialidade e disponibilidade sejam preservadas. A área de segurança da informação juntamente com as demais áreas deverão definir qual será o fluxo a ser seguido para que seja solicitado o envolvimento da área de segurança da informação em todos os projetos.

d. Política, normas e procedimentos de segurança da informação

De acordo com a NBR ISO/IEC 17799 (2001), uma etapa fundamental para a elaboração das políticas de segurança é a classificação e controle dos ativos de informação.

De acordo com KRUTZ e VINES (2001), a área de segurança da informação deverá definir quais critérios os proprietários das informações e sistemas deverão adotar durante a classificação dos mesmos. Dependendo da classificação recebida, a informação deverá receber controles apropriados, os quais serão definidos pelas políticas e normas de segurança da informação.

VALLABHANENI (2002) afirma que é necessário também que sejam definidos quais são os receptores autorizados a receber informações classificadas em cada um dos níveis de classificação definidos. A lista de receptores

autorizados deverá ser periodicamente revisada, pelo proprietário da informação, juntamente com a área de segurança da informação.

Segundo SCHNEIER (2001), as políticas e normas de segurança da instituição devem fornecer um conjunto estruturado de diretrizes e ações com o propósito de minimizar a possibilidade de ocorrência de incidentes de segurança da informação.

Já VALLABHANENI (2002) afirma que as Políticas e Normas de Segurança da Informação têm como principal objetivo definir princípios e responsabilidades para assegurar que a informação esteja adequadamente segura e para criar uma estrutura de ambiente computadorizado na qual os controles internos possam se basear. Todos os funcionários e prestadores de serviço devem estar aderentes as Políticas e Normas de Segurança da Informação, que devem ser constantemente atualizadas de forma que reflitam as alterações dos processos e da organização. Segundo o autor, para a elaboração das Políticas e Normas de Segurança da Informação deve-se:

- ✎ obter o comprometimento da alta administração da empresa, suportando os objetivos e princípios da segurança da informação;
- ✎ definir quais tópicos serão abordados pela política;
- ✎ incluir no documento da política o objetivo da política e a justificativa da importância desses documentos;
- ✎ o enunciado das políticas e normas deve ser claro o bastante, não deixando dúvidas quanto a sua aplicabilidade (onde, como, quando, para quem e/ou para o que a política se aplica);
- ✎ estabelecer um fluxo de relacionamento com outras funções envolvidas nos assuntos organizacionais de segurança, como Auditoria Interna, Departamento Jurídico, Departamento Organizacional, Segurança Patrimonial, dentre outros;
- ✎ estabelecer um fluxo de aprovação no qual esteja prevista a revisão por consultores especialistas em segurança, Departamento Jurídico e Desenvolvimento Organizacional, dentre outros;
- ✎ sinalizar toda a documentação como rascunho até que todo o processo de revisão esteja concluído;

- ✎✎ definir no planejamento de segurança um período para revisão das Políticas e Normas de Segurança da Informação;
- ✎✎ definir as responsabilidades e as diretrizes de segurança a serem observadas;
- ✎✎ assegurar que as normas elaboradas preservem as propriedades das informações (confidencialidade, disponibilidade e integridade);
- ✎✎ definir quais ações são consideradas violações de segurança;
- ✎✎ estabelecer as ações disciplinares que serão tomadas contra os indivíduos que violarem as Políticas e Normas de Segurança da Informação;
- ✎✎ elaborar as normas e políticas que reflitam a realidade atual da empresa, dessa forma o tempo verbal deverá ser o presente; e
- ✎✎ abordar no mínimo os aspectos de segurança definidos na BS7799, em consonância com a realidade da empresa; e submeter este documento a aprovação das áreas de negócio.

De acordo com KRUTZ e VINES (2001), para implementação da Política e Normas de Segurança da Informação deve-se:

- ✎✎ obter a atenção e o interesse dos funcionários e prestadores de serviço da empresa informando sobre a iminência da aprovação e da adoção das Políticas e Normas de Segurança;
- ✎✎ publicar o documento contendo as Políticas e Normas de Segurança da Informação na intranet e no formato impresso;
- ✎✎ antes de conceder o acesso dos recursos de informação da empresa aos funcionários e prestadores de serviço solicite que os mesmos assinem um termo de responsabilidade atestando que entenderam e conhecem as normas de segurança definidas; e
- ✎✎ elaborar programas de conscientização para os funcionários da empresa, seguindo as diretrizes de segurança.

A NBR ISO/IEC 17799 (2001) determina as seguintes áreas de interesse a serem cobertas pela política, normas e procedimentos da segurança da informação:

- ✎✎ Classificação e controle dos ativos de informação
- ✎✎ Segurança em pessoas

- ☞ Segurança física e do ambiente
- ☞ Gerenciamento das operações e comunicações
- ☞ Controle de acesso
- ☞ Desenvolvimento e manutenção de sistemas
- ☞ Gestão da continuidade do negócio
- ☞ Conformidade

Além disto, o mesmo documento, recomenda a elaboração de termos de confidencialidade e responsabilidade; e a elaboração de treinamentos de conscientização e materiais de apoio, como manuais de utilização da política e normas de segurança.

e. Monitoramento e prevenção

De acordo com VALLABHANENI (2002), a aplicação das normas e procedimentos estabelecidos para instituição devem ser constantemente monitoradas. Esse monitoramento pode identificar situações futuras de risco e gerar ações preventivas. A adoção de metodologia de gerenciamento de riscos, que ajude a instituição em identificar e monitorar sistematicamente os riscos é fundamental para a gestão da segurança da informação.

Ainda segundo o autor, a área de segurança da informação deverá avaliar a adoção de penalidades decorrentes do não cumprimento das diretrizes fornecidas nas políticas e normas de segurança. Entretanto, deve ser levado em consideração que, muitas vezes, os usuários incorrem em violações de segurança de forma não intencional, e sim devido ao desconhecimento.

Conforme cita VALLABHANENI (2002), de acordo com o grau de aderência alcançado, a área de segurança da informação poderá reavaliar os controles estabelecidos e os recursos necessários para adoção dos mesmos, por exemplo, a adoção de ferramentas de criptografia, soluções de monitoramento, dentre outros.

A área de segurança também deverá definir como será feita a avaliação do nível de aderência das áreas de negócio aos padrões de segurança definidos. Adicionalmente, como será feita a implementação de contramedidas para correção das divergências encontradas durante o processo de diagnóstico de riscos.

f. Treinamento e Conscientização

De acordo com PELTIER (2001), um dos fatores relevantes para se obter eficácia da segurança da informação está no comprometimento de todos os funcionários, prestadores de serviço e demais colaboradores internos e externos da instituição. A criação de programas de treinamento sobre segurança da informação, que aborde desde mensagens de conscientização ampla, até treinamentos técnicos específicos; é fundamental neste item.

Segundo KRUTZ e VINES (2001), a empresa deve elaborar um Programa de Conscientização sobre Segurança da Informação para todos os funcionários e prestadores de serviço que utilizam ou têm acesso às suas informações. Este programa deverá ser conduzido internamente se a empresa possuir uma equipe especializada em segurança, caso contrário esse trabalho deverá ser realizado por empresas terceirizadas que atuam nesse segmento.

Ainda de acordo com KRUTZ e VINES (2001), as sessões de conscientização deverão abordar aspectos de segurança relacionados com as atividades desempenhadas pelos funcionários e prestadores de serviço e estarem condizentes com as necessidades e experiências prévias que os mesmos possuem. O programa de conscientização deverá ser realizado periodicamente e todos os funcionários e prestadores de serviço deverão ser convocados a participar.

2.3.3. Segurança das Operações

De acordo com HUMPHREYS (1998), a segurança da informação deve identificar os riscos e vulnerabilidades das operações de negócio da empresa e

implementar as devidas soluções de segurança, não só através da tecnologia, mas também, de processos e de pessoas. Essa área pode ser subdividida em:

- ✍✍ Arquitetura de segurança
- ✍✍ Segurança das operações
- ✍✍ Telecomunicações
- ✍✍ Segurança física
- ✍✍ Desenvolvimento de sistemas
- ✍✍ Resposta à incidentes

a. Arquitetura de Segurança

De acordo com KRUTZ e VINES (2001), é necessário estabelecer uma arquitetura de segurança, que trata das questões de segurança da informação e controles, em todos os níveis técnicos e operacionais para as diversas áreas de negócio. Ela abrange os conceitos, princípios, estruturas e padrões utilizados para desenhar, implementar, monitorar os sistemas operacionais seguros, equipamentos, redes, aplicações e controles para reforçar os diferentes níveis de confidencialidade, bem como garantir a integridade e a disponibilidade dos meios.

Para KRUTZ e VINES (2001), a arquitetura de segurança do ambiente computacional refere-se a um conjunto de estruturas e aos detalhes necessários para o seu funcionamento. Para tanto, esta arquitetura deve endereçar os princípios básicos relacionados a segurança da informação incluindo privacidade dos dados, integridade, disponibilidade e confidencialidade.

Segundo VALLABHANENI (2002), de modo geral a arquitetura de segurança está envolvida com os sistemas operacionais, hardware, protocolos utilizados nas redes, circuitos e programas de sistema de operações, mas normalmente não envolve sistemas de aplicações, os quais são requisitados para executar uma tarefa, mas não para fazer o sistema funcionar. A seguir segue um tipo de arquitetura de segurança que pode ser agregado no ambiente computacional das organizações:

- ✍✍ Internet Protocol Security – IPSEC. IPSEC é projetado para oferecer segurança e interoperabilidade, baseado em criptografia para *Internet*

Protocol – IP v4 e IP v 6. O conjunto de serviços de segurança oferecido inclui controle de acesso, disponibilidade, integridade, autenticação da origem, proteção contra ataques e confidencialidade limitada do fluxo do tráfego. Esses serviços são fornecidos na camada *IP*, oferecendo proteção também para as camadas superiores, como *Transmission Control Protocol- TCP*, *User Datagram Protocol - UDP*, *Internet Control Message Protocol - ICMP* e *Border Gateway Protocol - BGP*.

A série de protocolos IPSEC e algoritmos padrões associados são projetados para oferecer segurança de alta qualidade para o tráfego da Internet. Contudo, a segurança oferecida pelo uso desses protocolos depende da qualidade da sua implementação.

b. Segurança das Operações

De acordo com VALLABHANENI (2002), a segurança das operações é utilizada para identificar os controles sobre o hardware, as mídias e sobre os operadores com acesso privilegiado a esses recursos. Auditoria, monitoramento, ferramentas e recursos são os mecanismos que permitem a identificação dos eventos de segurança e subsequentemente ações para identificar os elementos chaves e reportar a ocorrência ao responsável, equipe ou área pertinente. Dentre as várias atividades relativas a segurança das operações o autor cita como principais as:

☞ Segregação das funções

A segregação de funções deve existir para garantir que nenhum indivíduo e/ou área desempenhe um processo completo como geração, entrada, autorização, verificação ou distribuição de dados. Porém, muitas vezes devido a estrutura da organização, mais de uma dessas funções acabam sendo executadas por um único indivíduo e/ou área. Para tanto, devem existir procedimentos e controles que autorizem, administrem e monitorem o desenvolvimento das funções exercidas. O recomendado é que exista uma estrutura propiciando a revisão e/ou aprovação entre as funções que completam um processo. Recomenda-se evitar que um único indivíduo e/ou área seja responsável por um processo do início até seu final.

O objetivo da separação de tarefas é assegurar que nenhum indivíduo sozinho possa comprometer uma aplicação, política, procedimentos, atividades ou controles. É uma diretriz básica de segurança que

atividades de alto risco sejam segregadas. Nenhum funcionário deve ser responsável por monitorar as atividades que ele próprio tenha executado.

☞ Administração do anti-vírus

Controles devem ser adotados para evitar a introdução de vírus de computador no ambiente interno da empresa. Atualizações constantes na lista de vírus devem ser realizadas, evitando assim que a empresa se torne suscetível ao ataque. Preferencialmente essas atualizações deverão ser feitas automaticamente, sem que haja intervenção manual. Entretanto, um funcionário da empresa deverá acompanhar o processo, assegurando que o mesmo tem sido realizado com sucesso.

Todos os servidores e microcomputadores devem ser atualizados quando surgirem novas listas de definições de vírus. Todos os arquivos recebidos via disquete ou enviados eletronicamente devem ser verificados quanto a existência de vírus. Esta configuração deverá estar pré-configurada no antivírus.

Os usuários devem estar instruídos a não desabilitarem o *software* antivírus de suas máquinas. Preferencialmente, esses *software* deverão ter essa opção bloqueada. Periodicamente a empresa deverá verificar se todos os equipamentos possuem o sistema antivírus instalado, ativo e atualizado. O *software* antivírus deve estar sempre ativo e ser executado para verificação do dispositivo que protege sempre que houver a suspeita da existência de vírus, ou sob comando do usuário do equipamento.

☞ Procedimentos de *backup*

As empresas deverão possuir procedimentos adequados para geração e retenção das mídias de *backup* e dos sistemas utilizados para geração dessas informações.

A existência de mídias de *backup* é crucial para continuidade dos negócios caso ocorram incidentes de segurança. Devem ser atribuídas as mídias de *backup* os mesmos cuidados destinados às informações originais.

Periodicamente, devem ser geradas cópias de segurança das informações e dos sistemas utilizados na geração dos mesmos. Esta periodicidade poderá variar, dependendo do intervalo no qual os dados originais são atualizados. Por exemplo, uma informação que é atualizada mensalmente, o *backup* deverá ser realizado em um período igual ou superior a um mês, não havendo necessidade de serem realizados, por exemplo, *backups* diários.

Durante o processo de geração de *backup*, deverão ser considerados os arquivos de dados, os bancos de dados, o código fonte dos sistemas em desenvolvimento, utilitários, dentre outras informações que os proprietários da informação julguem necessárias. A decisão sobre a periodicidade de realização de *backup* de determinados arquivos está baseado no custo de realizar o *backup*, *versus*: (1) o custo de falha; (2) a capacidade de recriar o arquivo sem um *backup*; e (3) tempo necessário para realizar uma cópia de segurança.

☞☞ Inventário dos ativos

O inventário de todos os *hardware* de computador, como processadores, monitores, *notebooks*, *modems*, equipamentos de telecomunicação, roteadores, *fax*, PABX, devem ser registrados no inventário de ativos físicos. Esse inventário de ativos da informação deverá ser revisado sempre que esses *hardware* forem removidos, descartados, realocados, atualizados ou sofrerem qualquer outro tipo de alteração.

As empresas também deverão inventariar todos os sistemas aplicativos, ferramentas, pacotes adquiridos de terceiros, *software shareware* e *freeware* autorizados. Esse inventário de ativos da informação também deverá ser feito de forma automatizada via rede, possibilitando identificar discrepâncias da configuração padrão homologada pela empresa. O inventário de *software* deverá registrar informações semelhantes ao inventário de *hardware*.

A realização de inventários de ativos da informação periodicamente permite a empresa identificar a utilização de *software* não homologados ou piratas em seu ambiente. Para melhor controle de seus ativos, o processo de aquisição de *hardware* e *software*, bem como a instalação dos mesmos, deverá estar centralizado.

☞☞ Documentação das Operações

É necessário formalizar todos os procedimentos operacionais executados por suas áreas de negócio. Entretanto, num primeiro momento, essa atividade deverá ser priorizada nas áreas onde há o manuseio de informações sensíveis e a utilização de um volume muito grande de mão de obra terceirizada, buscando dessa forma, minimizar a dependência desses terceiros.

O objetivo da formalização dos procedimentos executados pela área é assegurar o uso adequado das aplicações, soluções tecnológicas e desempenho adequado das atividades da área, bem como garantir que na ausência dos funcionários que executam a tarefa, esta continuará sendo desenvolvida. A formalização dos procedimentos em um nível adequado de detalhes ajuda a eliminar as falhas de segurança os

descuidos, fornece aos recém-contratados instruções suficientemente detalhadas, e assegura a qualidade das atividades, garantindo assim a execução correta e eficiente, bem como a continuidade e a consistência dos processos.

☞ ☞ Manuseio e destruição de mídias

Devem-se elaborar Políticas, Normas e Procedimentos de Segurança referentes ao armazenamento e ao descarte das mídias que contenham informações de alta criticalidade. Adicionalmente, a adoção de dispositivos apropriados de armazenamento de descarte é necessária.

Após a definição da política de classificação de informações, a área de segurança da informação deverá realizar um trabalho, junto aos Gestores das áreas, para o mapeamento das necessidades de segurança decorrentes da classificação realizada, por exemplo, necessidade de adoção de cofres para armazenamento de mídias, de picotadores para destruição de relatórios, de disponibilização de um espaço maior no ambiente de rede para armazenamento das informações locais, da adoção de cuidados especiais durante o envio de informações impressas ou em formato digital (duplo envelopamento, criptografia, etc.), dentre outros.

☞ ☞ Monitoramento das trilhas de auditoria

Durante o desenvolvimento dos sistemas, é necessário atentar para que os mesmos estejam parametrizados de forma que permitam a geração de trilhas de auditoria. Estas trilhas são registros históricos das transações ocorridas e que permitem percorrer uma transação de seu princípio até seu fim, ou vice-versa. As trilhas de auditoria, as quais são gravadas em arquivos de *log*, auxiliam na detecção de violações de segurança, de problemas de performance e de falhas nos sistemas. Em virtude de os arquivos de *log* serem recursos passivos, visto que eles somente coletam dados e não tomam nenhuma ação, sua maior utilidade está na detecção e intimidação de ações consideradas impróprias.

Deve ser definido pelo proprietário do sistema, juntamente com o suporte da área de segurança da informação, quais módulos, bem como quais eventos dentro dos módulos (inclusão, alteração, dentre outros) deverão permitir a gravação de trilhas de auditoria. Para os sistemas existentes, deve ser avaliada a possibilidade da geração desses arquivos e a implementação dos mesmos no menor prazo possível.

O recurso de trilha de auditoria deve ser desenvolvido de tal forma que permita a ativação/desativação mediante as necessidades de negócio. Somente a área de segurança da informação, juntamente com os

responsáveis pelo processo de auditoria na empresa, deve possuir permissão para desativar tal recurso.

☞☞ Análise de risco

As empresas devem utilizar a análise de risco para todas as informações e/ou sistemas, incluindo aqueles que ainda estão em fase de desenvolvimento. A alta administração da empresa e todos funcionários responsáveis por aplicações críticas ao negócio, ambientes de processamento de informação, redes de comunicação e desenvolvimento de sistemas devem estar conscientes da necessidade quanto à realização da análise de risco.

Os riscos oferecidos ao negócio, associados aos sistemas e às informações, devem ser avaliados usando-se um método formal de análise de risco, o qual deve ser documentado, flexível, de fácil compreensão, aprovado pela alta administração e periodicamente revisado, para assegurar que ele atinja as necessidades de negócio.

c. Telecomunicações

De acordo com VALLABHANENI (2002), esta área de interesse aborda os métodos de transmissão, as formas de tráfego de informações e as medidas de segurança utilizadas para fornecer integridade, disponibilidade, autenticação e confiabilidade para as transmissões ocorridas, utilizando redes de comunicação pública e privada. Para a segurança desta área, são necessários:

☞☞ Modems

A empresa deve elaborar procedimentos descrevendo os passos a serem seguidos pelos funcionários e prestadores de serviço para a obtenção de aprovação e a instalação de *modems* nas estações de trabalho da rede.

Além disso, deve-se adquirir uma ferramenta que permita controlar e identificar todo o *hardware* existente nos diversos computadores da rede, de modo que VISANET mantenha um inventário de *hardware* sempre atualizado.

☞☞ PABX

A organização deve assegurar a integridade dos dados do sistema de PABX. Aplicações, correções, suplementos e programas são normalmente necessários para testar e atualizar este sistema. Sendo assim, o administrador do PABX precisará algumas vezes prover dados corretos *real-time* para o *firmware software* e programadores. Dados sensíveis devem ser manipulados de maneira adequada à sua classificação, evitando a

exposição do PABX. A segurança de operações também deve envolver a proteção contra modificações não autorizadas de *software* e *hardware*.

☞☞ Firewalls

Os *firewalls* devem ser vistos como a primeira linha de defesa contra ameaças externas e de proteção da rede interna da empresa.

De acordo com MCCLURE (2000), existe uma série de vantagens que justificam o uso *firewall*, dentre as quais destacam-se com um dos principais dispositivos: proteção contra serviços vulneráveis; habilitação somente dos protocolos definidos pelos administradores; segregação do acesso para alguns sistemas, redes e dispositivos; e identificação de vírus e códigos maliciosos.

Os ambientes de *firewall* são compostos de dispositivos, de sistemas associados e de aplicações projetadas para se trabalhar em conjunto. As configurações em um *firewall* devem visar à minimização do gerenciamento, e, ao mesmo tempo, a fornecer a proteção adequada à empresa.

☞☞ Cabeamento

Em relação à estruturação do cabeamento, a empresa deverá avaliar a utilização de cabeamentos estruturados, (ou seja, aqueles que obedeçam às seguintes condições: segregação do cabeamento elétrico e lógico através da utilização de dutos distintos) e utilizar dutos adequados ao meio a que esse estiver exposto, a fim de evitar problemas como, por exemplo, interferência eletrônica. O cabeamento ainda deverá estar devidamente identificado, ser testado e certificado e as instalações deverão apresentar documentação referente ao cabeamento.

☞☞ LAN

As LANs (Local Area Network) devem manter a confidencialidade e a integridade dos dados quando forem armazenados, processados ou transmitidos através dela; devem também manter a disponibilidade dos dados armazenados, assim como a habilidade de processar e transmitir os dados de maneira precisa e garantir a identidade do emissor e do receptor de uma mensagem.

☞☞ Computação remota

A computação remota ocorre na medida em que funcionários da empresa passam a ter a necessidade de acesso às informações ou aos recursos da companhia remotamente. Tal situação expõe a organização à utilização da computação remota, que deve ser controlada para que apenas usuários autorizados possam acessar os componentes e os recursos remotamente.

Para tanto, os servidores segundo NAKAMURA (2002), devem ser capazes de identificar e autenticar as solicitações dos usuários remotos,

utilizando recursos como um *token* ou componentes biométricos para incrementarem o processo de autenticação do usuário. Além disso, outros fatores devem ser agregados, como o emprego de *VPN*, a fim garantir a privacidade utilizada durante a transmissão das informações.

☞☞ Sistemas operacionais de rede

A empresa deve atentar para a revisão, a configuração e a atualização dos sistemas operacionais utilizados na rede, a fim de incrementar a segurança do ambiente. Para tanto, as seguintes práticas de mercado devem ser consideradas, dentre outras: atualizar o *software* e instalar *patches* de segurança, configurar o sistema operacional seguindo *checklist* de segurança, remover as aplicações desnecessárias, especialmente aquelas que não são homologados, utilizar *software* de antivírus para a proteção dos sistemas operacionais, e arquivos e implementar *firewalls* pessoais nos computadores considerados críticos.

☞☞ Wireless

As redes *Wireless* são um elemento importante da infra-estrutura da comunicação. Estes sistemas, incluindo sistema de redes e celulares, estão fornecendo níveis de mobilidade e flexibilidade sem precedentes durante o desenvolvimento dos sistemas aos usuários. As redes de celulares e de satélites têm vantagens sobre redes terrestres, porque elas são potencialmente acessíveis de qualquer lugar do planeta, sem o custo de instalação de fios ou cabos.

Entre os principais objetivos de segurança *wireless* cabe ressaltar: segurança física dos dispositivos *wireless*; implementação de *Public Key Infrastructure (PKI)* a fim de garantir a privacidade das informações e utilização do *Wireless Transport Layer Security Protocol (WTLS)* em aplicações que utilizem o protocolo WAP.

☞☞ WAN

Uma *Wide Area Network (WAN)* refere-se a uma rede que interliga sistemas localizados em áreas geográficas distantes, tal como uma cidade, um continente, ou muitos continentes. Uma rede complexa pode constituir-se de WANs que possuem a amplitude de continentes ou regiões geográficas dentro de continentes e de conexões menores, como LANs ou MANs.

As seguintes metas devem ser consideradas para a implementação de um programa eficiente de segurança voltado à WAN: manter a confidencialidade, a integridade e a privacidade dos dados quando forem armazenados, processados ou transmitidos pela WAN; manter a disponibilidade dos dados, assim como a habilidade de processar e transmitir os dados de maneira precisa; e garantir a disponibilidade dos *links* envolvidos nas transmissões.

⚡️ Aprimorar controles sobre o uso da Internet

A empresa deverá elaborar políticas e procedimentos com relação ao uso da Internet. Estes documentos deverão definir qual o critério a ser adotado para liberação do acesso à Internet para seus funcionários e prestadores de serviço. O acesso aos *sites* de *Webmail* deverá ser bloqueado, bem como sites cujo conteúdo seja impróprio, como pornografia, atividades criminais ou não-éticas e raciais. A realização de *downloads* pelos funcionários e prestadores de serviço também deverá ser avaliada. Preferencialmente, este recurso deverá estar habilitado somente para os funcionários que necessitarem deste acesso para execução de suas atividades. Não deverá ser permitido o acesso à Internet via *modem*. Todos os acessos à Internet deverão ser feitos por meio da rede interna da VISANET, passando obrigatoriamente por um *firewall*. Todas as exceções a esse procedimento deverão ser formalmente autorizadas pelo gestor responsável pelo funcionário ou pelo prestador de serviço. Os *notebooks* que efetuam acesso via *modem* deverão possuir *firewall* próprio.

⚡️ Intranet

Segundo VALLABHANENI (2002), de maneira geral uma intranet é uma rede que emprega o mesmo tipo de serviços, aplicações e protocolos presentes em uma aplicação Internet, mas sem envolver conectividade externa ao ambiente computacional.

Dentro da rede interna (intranet), muitas *intranets* podem ser criadas com o uso de firewalls internos.

Dado que as *intranets* utilizam os mesmos protocolos, aplicações e serviços presentes na Internet, muitos assuntos de segurança inerentes às aplicações Internet também estão presentes nas aplicações da intranet.

⚡️ Extranet

Segundo NAKAMURA (2002), enquanto o escopo da *intranet* é limitado aos funcionários da organização, o escopo da *extranet* inclui fornecedores ou organizações de clientes fazendo negócio com a empresa. As *extranets* são redes restritas baseadas em *intranets* com audiências selecionada como fornecedores, consumidores, clientes e outras partes interessadas fora da organização. A *intranet* se conecta com a *extranet* através de tecnologia baseada em Internet. As *extranets* são geralmente uma *intranet business-to-business*, isto é, duas *intranets* ligadas via Internet. A *extranet* permite o acesso limitado e controlado a usuários remotos via formulário de autenticação e criptografia, tal como é fornecido pela *Virtual Private Network* – VPN. As *extranets* compartilham de quase todas as características da *intranet*, com a exceção de a *extranet* ser designada a existir fora do ambiente de *firewall*. Por definição, a proposta da *extranet* é

fornecer acesso às informações potencialmente sensíveis, sem permitir que usuários remotos acessem à *intranet*. As *extranets* empregam protocolos *Transmission Control Protocol/Internet Protocol – TCP/IP*, junto com as mesmas aplicações e serviços padrões. Assim, a *extranet* é uma rede baseada em *IP* que facilita o fluxo de informações entre uma companhia e seus funcionários e prestadores de serviço. Dentro da *extranet*, algumas opções estão disponíveis para reforçar a variação dos níveis de segurança como identificação e autenticação, criptografia e uso de *firewall* para proteção das redes.

✍️ VPN

Uma *Virtual Private Network – VPN* é uma rede baseada em *Internet Protocol – IP* que usa uma configuração especial de roteador tais como filtros e caminhos estatísticos. Qualquer conexão entre um *firewall* com redes públicas deve utilizar *VPN* criptografada para assegurar a privacidade e integridade dos dados que estão passando pela rede pública. Todas as conexões de *VPN* devem ser aprovadas e gerenciadas pelo administrador de serviços da rede. Formas apropriadas para distribuir e manter as chaves de criptografia devem ser estabelecidos antes do uso operacional da *VPN*. Muitas organizações possuem redes e as informações dos servidores propagam-se através de múltiplos locais. Quando uma grande organização acessa a informação ou outra fonte baseada em *LAN*, linhas privadas são normalmente usadas para conectar as *LANs* nas *WANs*. Linhas alugadas são relativamente mais caras para configurarem e se manterem, transformando a Internet em uma alternativa atraente para conectar fisicamente *LANs* separadas. A desvantagem de usar a Internet para este propósito é a quantidade de dados confidenciais correntes na Internet entre *LANs*, assim como a vulnerabilidade de *spoofing* e outros ataques. As *VPNs* usam criptografia para prover o serviço de segurança requerido. Normalmente a criptografia é feita entre *firewalls* e a conectividade segura é limitada para um número limitado de *sites*.

✍️ Segurança em E-mail

Os principais protocolos de *e-mail* na Internet são: *Simple Mail Transport Protocol (SMTP)*, *Post Office Protocol – POP* e *Internet Mail Access Protocol (IMAP)*. Um servidor de *SMTP* aceita mensagens de *e-mail* de outros sistemas e as armazena para os destinatários. Um servidor *POP* permite a um cliente realizar *download dos e-mails* recebidos por outro servidor de *e-mail*. A assinatura digital é uma analogia à assinatura escrita, porém eletronicamente, e que pode ser usada para provar a um receptor, ou um terceiro que a pessoa que deu origem à mensagem a assinou. Assinaturas digitais são também criadas para verificar a integridade de dados e

programas a todo instante. Desse modo, as assinaturas digitais autenticam a integridade dos dados assinados e a identificação do signatário. Assinatura digital garante, para um terceiro, que aqueles dados foram verdadeiramente assinados pelo gerador da assinatura. Além disso, essas assinaturas são usadas em *e-mail*, transferência eletrônica de fundos, transferência eletrônica de dados, distribuição de *software*, armazenamento de dados e outras aplicações que requerem garantia da integridade dos dados e autenticação da origem dos dados.

Um algoritmo proporciona a capacidade de gerar e verificar as assinaturas. A geração de assinaturas utiliza-se da chave privada para gerar uma assinatura digital. Para a verificação de uma assinatura utiliza-se uma chave pública correspondente à chave privada. Cada usuário possui um par de chaves, privada e pública. Qualquer um pode verificar a assinatura de um usuário utilizando a chave pública do mesmo. Somente a pessoa que possui a chave privada (o usuário) pode gerar a assinatura. A segurança de um sistema de assinatura digital depende de manter em segredo a chave privada dos usuários. Estes devem, portanto, proteger-se contra a utilização não autorizada de suas chaves privadas.

Para a criação das assinaturas é utilizada uma função *hash* para se obter uma versão condensada de dados, chamada de *message digest*, a qual é então inserida no algoritmo da assinatura digital para gerá-la. A assinatura digital é enviada para o verificador pretendido junto com os dados assinados (normalmente chamados de mensagem). O verificador de mensagens verifica a assinatura utilizando a chave pública de quem o enviou. A mesma função *hash* também deve ser usada no processo de verificação. Procedimentos similares podem ser usados para gerar e verificar assinaturas dos armazenamentos e dados transmitidos.

Uma assinatura digital também pode ser usada para verificar se a informação não foi alterada depois que foi assinada; isto proporciona uma mensagem íntegra. Uma simples alternativa para a assinatura digital é a função *hash*. A característica do não-repúdio (*non-repudiation*) da assinatura digital conta com a suposição matemática de que é impraticável computacionalmente derivar a chave privada de uma chave pública e/ou um grupo de mensagens e assinaturas preparadas utilizando a chave privada. A característica de não-repúdio da assinatura digital também conta com a suposição prática de que a chave privada é, ou pode ser, associada a uma única entidade (o assinante), que somente este assinante conhece ou usa a chave privada, e que a esta poderá estar e estará mantida em segredo.

Assinaturas eletrônicas (digitais) são muito difíceis de serem forjadas, porém assinaturas escritas à mão são facilmente forjadas.

IDS

Os sistemas de detecção de intrusão, segundo NAKAMURA (2002), na sua maioria, detectam ataques que ocorreram, mas normalmente não podem evitar o ataque. Portanto, normalmente eles apenas estão disponíveis para detectar ataques que têm sido anteriormente vistos e analisados pelo vendedor IDS. Estes ataques recentemente publicados podem não ser detectados pelas redes que utilizam IDS. Alguns IDS podem criar respostas limitadas aos ataques detectados, mas estas respostas normalmente não são suficientes para parar ataques mais sofisticados. O IDS é um mecanismo de segurança robusto, o qual deve ser utilizado em conjunto com uma série de técnicas preventivas de segurança, tais como controles de identificação e autenticação. Os IDS podem ser *software* ou *hardware* que automatizam esses processos de monitoração e análise. Há diversas razões pelas quais a empresa deve adquirir e usar IDS para o monitoramento de suas redes entre as quais destacamos:

- Detectar os ataques e outras violações da segurança que não são prevenidos por outras medidas de segurança;
- Tomar as ações cabíveis em tempo real sobre os ataques identificados;
- Documentar ameaças existentes no ambiente computacional;
- Rastrear as violações de usuários referentes às políticas existentes.
- Fornecer informações úteis sobre as intrusões que ocorrerem, permitindo melhor diagnóstico, recuperação e correção dos fatores causadores.

d. Segurança Física

Segundo KRUTZ e VINES (2001), este tópico estabelece todos os requisitos de segurança física a que a empresa deverá atentar, desde procedimentos até a adoção de dispositivos específicos, como detectores de incêndio, sensores, câmeras, soluções de controle de acesso físico, dentre outros. Para isto são necessários:

Segurança das Áreas Restritas

Os acessos ao Centro de Processamento de Dados (CPD) e outras áreas consideradas como críticas devem ser diferenciados de tal forma que

apenas as pessoas devidamente credenciadas e identificadas poderão obter acesso a esses locais.

☞ Controle de Acesso Físico

Os controles de acesso físicos devem restringir a entrada e a saída das pessoas através de, dispositivos eletrônicos e mídias nos edifícios nos quais a empresa tenha as suas operações.

Os controles de acesso físicos não devem restringir-se a área onde se hospedam os equipamentos críticos, mas também cobrir toda a área em que o cabeamento da *Local Area Network (LAN)* está disposto, nos locais onde ocorrem os serviços de suporte e a operação como cabine primária (energia elétrica), sala com os equipamentos de ar condicionado, sala com os *links* de comunicação e todos os outros elementos requeridos para a operação dos sistemas.

Além disso, é importante ser destacado que os controles de acesso físicos devem ser planejados tanto durante o horário comercial quanto fora do expediente normal de trabalho.

Os alarmes podem ser associados a outros dispositivos de detecção já mencionados e podem ser interligados a centrais de monitoramento a fim de acompanhar os ambientes-alvo.

Existem alguns recursos tecnológicos que podem ser utilizados para controlar o acesso às áreas críticas. Para tanto, destacam-se os seguintes itens relacionados:

- Sistema de Detecção Fotoelétrico

Esse sistema detecta passivamente qualquer mudança no nível de luz de um determinado ambiente. Com essa sensibilidade ao nível de claridade recomenda-se a utilização deste apenas em locais que não tenham janelas.

- Sistema de Detecção de Movimento

Existem três tipos de sistemas de detecção de movimento:

- ☞ Sistema de detecção sônico opera em uma faixa audível de 1,500 a 2,000 hertz e maior. Este sistema utiliza transmissores e receptores para monitorar todas as ondas sonoras do ambiente.

- ☞ Sistema de detecção ultra-sônico utiliza alta frequência de ondas som aproximadamente entre 19,000 – 20,000 hertz; e

- ☞ Sistema de detecção de microondas que opera de maneira similar ao sistema ultra-sônico, utilizando ondas de rádio para a detecção.

- Sistema de Detecção Acústico-Sísmico

Este sistema utiliza recursos de microfonia para detectar sons que excedam o nível de barulho do ambiente que está sobre proteção. O sistema sísmico utiliza os mesmos princípios de detecção de áudio com alta sensibilidade em detectar vibrações.

- Sistema de Detecção de Proximidade

Existem vários tipos de sistemas de proximidade, que detectam a aproximação ou a presença de um objeto ou de um indivíduo. Em princípio, um sistema de proximidade utiliza um campo elétrico que quando é invadido por um corpo, dispara um alarme.

Os sistemas de proximidade são designados para serem suplementares, não podendo ser usados efetivamente como um sistema primário, isto por causa da sensibilidade de alarmes falsos causados pela oscilação do fornecimento de energia. Portanto, o sistema de proximidade deve ser suportado por outro sistema de segurança.

☞ Controles Preventivos do Sistema de Suporte Ambiental

Os sistemas e as pessoas que os operam necessitam de um ambiente razoavelmente bem controlado. Conseqüentemente, falhas relacionadas ao sistema de ventilação (ar-condicionado), à eletricidade e aos outros dispositivos geralmente causarão danos e até mesmo a interrupção nos serviços, podendo ainda danificar o funcionamento dos equipamentos críticos.

e. Desenvolvimento e Manutenção de Sistemas

Segundo VALLABHANENI (2002), este tópico se refere aos controles incluídos dentro dos sistemas e aos aspectos a serem atentados durante o ciclo de desenvolvimento e de manutenção dos sistemas: codificação segura, segregação de ambientes, metodologia de desenvolvimento, estabelecimento de acordo de nível de serviço com os prestadores, controle de versão, dentre outros. Para isto, é necessário atentar a:

☞ Projeto de desenvolvimento

O planejamento de segurança deve começar durante a fase de planejamento do ciclo de vida do sistema, tanto para novos sistemas quanto para uma atualização dos mesmos.

Este planejamento ajuda o gestor a tomar decisões sobre qual tipo de solução terá um custo efetivo. Se o gestor do sistema esperar o sistema ser construído para considerar aspectos de segurança, o número de alternativas para se implementar a segurança será menor do que se o gerente tivesse planejado anteriormente e as opções remanescentes poderão ser mais caras.

O projeto e a implementação de segurança trata dos recursos de um sistema, da aplicação ou de um componente que atendam aos requisitos e as especificações de segurança e como serão desenhados e construídos. O planejamento e a implantação da segurança consideram o desenho do sistema, o desenvolvimento e a instalação. Eles são normalmente associado às fases de desenvolvimento/aquisição e implementação do ciclo de vida do sistema, entretanto, eles também devem ser considerados durante o ciclo de vida, nas ocasiões em que o sistema é modificado.

O projeto e a implementação da segurança devem ser examinados sob dois pontos de vista: o componente e o sistema. O componente de segurança direciona-se para a segurança de um produto específico ou de um componente, tal como um sistema operacional, aplicações, *security add-on* ou módulo de telecomunicações. A segurança do sistema direciona-se para a segurança de um sistema como um todo, incluindo a interação entre produtos e módulos.

✍ ✍ Testes

O teste pode tratar da qualidade do sistema durante o desenvolvimento, a implementação ou a operação de um sistema. Portanto, ele pode ser feito no ciclo de desenvolvimento, depois da instalação do sistema e durante sua operação. Algumas técnicas comuns de testes incluem testes funcionais (para se ver uma função está de acordo com os requisitos) ou teste de penetração (para ver se a segurança pode ser transgredida). Estas técnicas de testes podem variar desde testes de tentativas a profundos estudos, usando métricas, ferramentas automatizadas ou múltiplos tipos de testes.

A certificação é um processo formal de testes dos sistemas ou dos componentes contra requisitos específicos de segurança. A certificação é normalmente realizada por um revisor independente, pois assim a revisão será feita de forma mais impessoal do que se estivesse sendo realizada por uma pessoa envolvida no desenvolvimento do sistema.

Testes de conformidades e testes de validação são feitos para determinar se um produto (*software, hardware, firmware*) possui as especificações-padrão definidas. Estes testes são desenvolvidos para padrões específicos e utilizam muitos métodos. A conformidade com

os padrões pode ser importante por muitas razões, incluindo a interoperabilidade ou a resistência da segurança fornecida.

Metodologia

No desenvolvimento ou na manutenção de sistemas tanto os produtos de prateleira como os mais personalizados como, o uso de arquiteturas avançadas e confiáveis de sistemas, as metodologias de desenvolvimento ou as técnicas de engenharia de *software* podem proporcionar segurança. Exemplos incluem *design* seguro e revisões de desenvolvimento, modelagem formal, provas matemáticas, técnicas de qualidade ISO 9000 ou uso de conceitos de arquitetura segura, tais como uma base de computadores segura um ou monitor de referência.

São intrinsecamente mais confiáveis algumas arquiteturas de sistemas tais como sistemas que usam tolerância de erros, redundância, espelhamento ou *Redundant Array of Independent Disks – RAID*.

A habilidade de descrever os requisitos de segurança e de como eles foram alcançados pode refletir o grau em que o desenvolvedor do sistema ou do produto entende os aspectos de segurança aplicáveis. Sem um bom entendimento dos requisitos, provavelmente o desenvolvedor não estará apto a atingir bons resultados.

Documentação

A documentação de segurança pode referir-se a um sistema ou a um componente específico. O nível de documentação do sistema deve descrever os requisitos de segurança do sistema e como eles foram implementados, incluindo as inter-relações entre as aplicações, o sistema operacional ou rede. Ele trata, além do sistema operacional, sistema de segurança e das aplicações ele descreve a integração e implementação de um ambiente em particular.

Garantias

A certificação de um produto ou de um sistema para operar em situação similar pode ser usada somente para proporcionar alguma segurança. Portanto, é importante perceber que uma certificação é específica de um ambiente e de um sistema.

Garantia é outra fonte de segurança. Se um fabricante, produtor, desenvolvedor de sistemas ou integrador está disposto a corrigir erros dentro do tempo de estrutura ou no próximo lançamento, isto deve dar ao administrador do sistema um nível de segurança maior em relação à qualidade do produto. Uma afirmação de integridade é uma declaração ou certificação do produto. Ela pode ser suportada pela promessa de corrigir o item (garantia) ou pagar pelas perdas (dívidas)

se o produto não estiver conforme a afirmação de integridade. A divulgação de uma asserção ou uma declaração formal de um fabricante ou desenvolvedor proporciona uma quantidade limitada de segurança baseada exclusivamente na reputação.

Freqüentemente é importante saber que o *software* foi entregue sem modificações, especialmente se ele é distribuído eletronicamente. Em alguns casos, *checkbits* ou assinaturas digitais podem proporcionar uma boa garantia de que o código do programa não foi modificado. Antivírus pode ser usado para checar *software* que veio de fontes com confiabilidade desconhecida.

✍ ✍ Ambientes de desenvolvimento

A empresa deve obrigatoriamente possuir ambientes separados para desenvolvimento, testes e produção.

A responsabilidade pela transferência do *software* do ambiente de desenvolvimento para o ambiente de produção deve ser formalmente definida e documentada.

A segregação entre os ambientes de desenvolvimento e de testes também é de grande importância para assegurar a completa funcionalidade do sistema, visto que, se forem realizados testes no ambiente de desenvolvimento, o sistema estará utilizando recursos muitas vezes não encontrados no ambiente de produção e poderá não funcionar corretamente quando for realizada a migração.

Nenhum desenvolvedor deve ter acesso ao ambiente de produção. Isso assegura que nenhuma alteração será feita nos sistemas em produção sem a autorização do funcionário responsável pela migração dos sistemas, bem como sem a realização de testes. Adicionalmente, existem informações no ambiente de produção que não necessariamente precisam ser fornecidas à equipe de desenvolvimento.

f. Resposta a Incidentes

Desenvolve os planos de continuidade que permitam à instituição não só continuar a realização de seus negócios em situação de contingência, como também gerenciar os riscos de possíveis interrupções e retornar o funcionamento normal das operações.

Permite ainda identificar as ameaças e os riscos de a instituição não estar preparada para dar continuidade às operações críticas do negócio, dependentes ou não de tecnologia; como por exemplo, a necessidade de suporte jurídico.

“O planejamento de segurança e a recuperação de desastres andam de mãos dadas. A reputação sólida de uma empresa pode ser destruída em um único dia na Internet; por isso, é importante visualizar vários cenários de desastres e ter um plano para lidar com cada um.”
(KALAKOTLA, 2001, pág. 442)

Um Plano de Contingência Corporativo deve vislumbrar diretamente a continuidade das operações em circunstâncias anormais. Desse modo, as seguintes etapas descrevem as tarefas a serem realizadas para a elaboração de um plano de contingência:

- ✎ Realizar uma Análise de Impacto nos Negócios (*Business Impact Analysis*), a fim de verificar quais os processos e os recursos críticos para os negócios da empresa, que devem ser incluídos no Plano de Contingência;
- ✎ Atribuir um responsável (ou responsáveis) pela elaboração, teste e manutenção do Plano de Contingência;
- ✎ Identificar as ameaças às quais os processos críticos de negócio estão sujeitos. A partir dessa análise, definir as contra medidas necessárias para minimizar as ameaças, bem como as medidas necessárias para recuperar o ambiente tecnológico;
- ✎ Determinar as metas de tempo de recuperação para cada processo crítico de negócio no evento de uma contingência;
- ✎ Mapear detalhadamente os recursos necessários para recuperar os processos críticos de negócio;
- ✎ Identificar os controles preventivos a fim de reduzir os possíveis efeitos de interrupções do sistema, e os riscos potenciais os custos do ciclo de vida da contingência;
- ✎ Considerar as estratégias alternativas para *backup* de dados, a fim de selecionar um tipo de armazenamento *off-site* apropriado. Determinar a frequência e o conteúdo dos *backups*;

2.3.4. Gerenciamento de Identidades

A administração de identidade não é apenas um conjunto de soluções, mas uma estratégia de negócio que envolve todas as áreas da instituição. A administração das identidades, assim como as outras duas áreas de interesse, não devem ser abordadas de forma isolada, e sim, trabalhada em conjunto com os demais tópicos.

a. Administração de Usuários e *Workflow*

Segundo VALLABHANENI (2002), a administração de usuários é o processo de disponibilizar direitos de acesso baseados na política corporativa para funcionários, clientes e parceiros. Em uma estratégia de segurança efetiva, há uma centralização (ou *single point*) da administração para habilitar ou desabilitar os direitos de acesso. Ela ainda abrange desde dados e aplicações, como também recursos, tais como cartões de crédito, telefones, PCs, cartões de estacionamento e todos os outros pertencentes à instituição. Já *Workflow* é o processo automatizado para viabilizar e suportar a administração de usuários. Como na liberação / revogação de direitos de acesso há um envolvimento de diversas áreas (Desenvolvimento Organizacional, Administração de Rede, Segurança da informação, etc), o processo de Workflow rastreia os eventos e disponibiliza, de forma apropriada, notificações sobre ações de risco realizadas por aplicativos e por indivíduos.

Segundo KRUTZ & VINES (2001), todos os usuários devem possuir contas únicas e individuais. Não devem ser criados usuários genéricos, os quais inviabilizam a identificação do responsável pelas ações executadas nos sistemas operacionais e nos aplicativos. Contas inativas devem ser removidas do sistema. Também somente os funcionários autorizados, preferencialmente os proprietários dos recursos, poderão autorizar o acesso aos mesmos, mediante uma justificativa válida de negócio.

Quando o funcionário é contratado, demitido, promovido, transferido, etc., ocorre normalmente um atraso, até que essa mudança seja refletida nos

sistemas. Esse atraso pode acarretar, principalmente, dois problemas: possíveis falhas de segurança e redução da produtividade.

Segundo o relatório *Risk Management Forecast* da PRICEWATERHOUSECOOPERS (2000), atrelado ao processo de concessão e remoção de acessos, existe também a questão do gerenciamento das identidades, o qual não é uma solução tecnológica única. O gerenciamento de identidades é a coleção de tecnologias e de disciplinas que gerenciam as identidades dos usuários e seu acesso às informações, aos sistemas e aos recursos para o desempenho de suas responsabilidades. Este gerenciamento é feito em um curto período de tempo, com um custo razoável e de maneira efetiva, quando obedecendo a uma política de segurança.

É considerada uma identidade um conjunto de informações que descrevem um indivíduo e seus direitos de acesso dentro da organização. As informações referentes à identidade do funcionário em geral estão espalhadas dentre diversos sistemas e banco de dados, os quais em geral não compartilham de um mesmo módulo de controle de acesso. Em função da inexistência de interligação entre os diversos sistemas, o custo de gerenciar os usuários acaba sendo multiplicado pelo número de sistemas existentes, tornando dessa forma o processo de criação do usuário extremamente oneroso.

A estratégia de Gerenciamento de Identidades atua pro-ativamente no gerenciamento da identidade, desde a chegada do funcionário até seu desligamento. Os acessos fornecidos ao usuário estarão baseados nas funções que o mesmo executar na companhia. Para a adoção de uma solução de gerenciamento de identidades, deverão ser abordados os seguintes aspectos:

- ▣ *Directory Services*;
- ▣ Controle de Acesso baseado na função;
- ▣ Serviços de Autenticação e Autorização;
- ▣ Infraestrutura de Gerenciamento de Permissões;
- ▣ Provisionamento das Contas do Usuário;
- ▣ Políticas de Controle de Acesso;
- ▣ Serviços Adequados de Senhas; e

Delegação da Administração e Serviços de Auto-Registro.

b. Gerência de Permissões

Segundo VALLABHANENI (2002), o processo de concessão e controle de acesso deve estar baseado na função que o funcionário e/ou prestador de serviços executa. Todos os funcionários que exercerem uma determinada função deverão possuir os mesmos níveis de acesso. Os usuários deverão estar reunidos em grupos, facilitando dessa forma o gerenciamento dos mesmos.

Em nenhum momento deverá ser utilizado o método de liberação de acesso a todos os funcionários. Preferencialmente, o acesso deverá estar bloqueado a todos os funcionários e ser liberado somente à medida que forem solicitados pelos proprietários ou responsáveis pelos sistemas.

Adicionalmente, todos os sistemas que efetuam o manuseio de informações críticas devem possuir recursos de controle de acesso, internamente como um módulo do sistema, ou por meio de *software* específicos para essa finalidade.

Segundo WADLOW (2001), desta forma é possível estabelecer um conjunto de permissões de acesso, garantindo a efetiva aplicação dessas políticas, e permitindo que a organização responda a questões como:

- Quem acessará nossos sistemas e aplicativos?
- Onde eles estão autorizados a ir?
- O que eles estão autorizados a fazer?
- Como nós forneceremos/ revogaremos os acessos?
- Quem gerenciará as identidades e as permissões?
- Quais as considerações sobre privacidade?

c. Estrutura de Diretórios

Este item aborda os benefícios e a importância da implementação de uma estrutura de diretórios como parte de uma estratégia para a implementação da segurança corporativamente.

Segundo VALLABHANENI (2002), um serviço de diretórios possibilita a um usuário, administrador ou programa localizar objetos em uma rede e obter informações a respeito desse objeto. Um componente-chave de um serviço de diretórios é o seu repositório de informações, ou seja, o diretório. Diretórios geralmente são exibidos em interface gráfica como árvores ramificadas. Por exemplo, cada ramificação de uma árvore de diretório pode consistir em um escritório remoto de rede contendo sub-ramificações, tais como PC's remotos, impressoras e configurações de privilégios para usuários em um escritório específico. Muitos serviços de diretórios também são extensíveis, ou seja, podem incluir novos tipos de objetos, tais como imagens ou vídeos dos seus colaboradores.

Ainda segundo o autor, os diretórios podem ser utilizados associados a políticas de autorização com identificação de usuários, assim como para aplicar políticas globais para toda ou parte da hierarquia de segurança. Muitas redes corporativas são atualmente globais em seu alcance e o gerenciamento efetivo de informações credenciais de servidores e usuários é extremamente importante. A integração e a utilização de diretórios que são baseadas em padrões de múltiplos fornecedores podem incrementar a capacidade de gerenciamento de plataformas, de recursos humanos, e dessa forma, mesmo os ambientes de aplicações heterogêneas podem se tornar interligados.

d. Criptografia

Este tópico aborda a necessidade de a empresa atentar para a utilização de recursos criptográficos em alguns dos seus processos críticos de negócio, bem como em algumas de suas atividades específicas.

De acordo com KRUTZ e VINES (2001), a encriptação tem como objetivo mascarar uma mensagem para que a mensagem original possa ser recuperada apenas por pessoas autorizadas. A criptografia é normalmente implementada em um módulo de *software*, *firmware*, *hardware*, ou alguma combinação dessas. Este módulo contém o algoritmo criptografado, alguns parâmetros de controle, e facilidades temporárias de armazenamento para a chave ser usada pelo algoritmo. Para a função correta da criptografia são necessários o *design* e a implementação segura do módulo de criptografia. Isto inclui proteger o módulo contra alterações e a verificação quanto à entropia utilizada neste. As tecnologias de criptografia reúnem um conjunto de técnicas e aplicações para a transformação de informação em uma forma impossível de leitura se não houver conhecimento de um algoritmo específico.

Segundo NAKAMURA (2002), a encriptação e a decriptação geralmente necessitam da utilização de algumas informações secretas, as quais são chamadas chaves. Com a chave simétrica (ou chave compartilhada), a mesma chave é utilizada tanto para encriptação quanto para decriptação. Com a chave pública, chaves diferentes são utilizadas para encriptação e decriptação. A manutenção dos componentes de criptografia é crucial para assegurar a operação segura e a disponibilidade de um módulo ou produto.

Ainda segundo o autor, o primeiro nível de teste sobre componentes criptográficos é quanto ao algoritmo utilizado no módulo criptográfico. O próximo nível de testes é realizado sobre as aplicações. Este nível de teste também é chamado de teste de certificação, que é uma análise compreensiva dos controles técnicos e não técnicos de segurança e outras medidas de segurança de um sistema. O teste de certificação estabelece a extensão na qual um sistema particular se encontra, com requisitos de segurança para sua missão e com necessidades de operação. A certificação não requer somente o exame dos controles técnicos, mas também de todos os outros controles de segurança, como

por exemplo, controles físicos, procedimentos administrativos e controles pessoais.

e. Autenticação

Esta atividade assegura que usuários e os aplicativos foram devidamente identificados antes de ganhar acesso às informações. A autenticação confiável assegura o controle de acesso, à informação, permite trilhas de auditoria e assegura a legitimidade do acesso.

Segundo WADLOW (2001), a utilização de senhas de acesso como técnica de autenticação é largamente utilizada. Entretanto essa prática requer alguns cuidados especiais, visto que podem ser facilmente distribuídas a outras pessoas, ou até mesmo esquecidas. A utilização de senhas de acesso pode ser altamente efetiva se corretamente gerenciada, porém essa prática raramente ocorre

De acordo com CLARK (2003), a tecnologia de *Single Sign On* – SSO permite aos usuários se autenticarem apenas uma vez e acessarem todas as aplicações às quais possuam acesso autorizado. Quando devidamente implementado, o SSO aumenta a produtividade dos usuários da rede, reduz o custo de gerenciamento das operações da mesma e aumenta a segurança, reduzindo a possibilidade de os usuários utilizarem senhas de fácil inferência, senhas idênticas em todas as plataformas e sistemas aplicativos, compartilhá-las ou simplesmente anotá-las para consulta posterior. O propósito do sistema de SSO é tornar o uso de múltiplas senhas transparentes para o usuário. Este processo é realizado de várias formas:

- ✍ ✍ Alguns sistemas de SSO simplesmente criam *scripts* que contém a identificação do usuário e a senha de acesso, bem como os comandos de *logon*. Esse processo remove esta obrigação dos usuários com relação às senhas e a transfere para a equipe responsável pela administração dos *scripts*. Esses *scripts* também necessitam do armazenamento adequado, visto que o mau uso poderia acarretar problemas para a organização; e
- ✍ ✍ Outras soluções de SSO, como aquelas baseadas em Kerberos, utilizam técnicas de criptografia para enviar os privilégios para cada rede ou servidor onde o usuário necessita de acesso. Estes sistemas necessitam

estabelecer e operar os privilégios no servidor, bem como integrar a tecnologia de SSO em cada sistema a ser acessado.

Segundo BYRNES (2001), o acesso seguro, a instalações físicas, as informações, as contas bancárias ou outros têm sido baseados por muito tempo numa combinação de dois conceitos, o que você tem e o que você sabe. Porém, esse tipo de segurança é considerado de baixo nível e insuficiente para proteger o acesso a áreas de alto risco. Em situações que exigem maior segurança, esse conceito se expande para incluir “o que voce é” – que pode ser comprovado com o uso da biometria. O que voce é deve ser um elemento verdadeiramente único e incapaz de ser negado.

Ainda segundo o autor, a biometria envolve a avaliação de uma característica biológica única usada para verificar a identidade exigida de uma pessoa através de equipamentos automatizados. A característica biológica pode ser baseada em características fisiológicas ou comportamentais. As características fisiológicas medem os traços físicos, como a impressão digital ou face. As características comportamentais medem uma reação ou resposta do indivíduo, tal como uma assinatura ou padrão de voz. Controles de acesso baseados em biometria são implementados usando-se controles físicos e lógicos. Eles são mais caros e mais seguros quando comparados aos outros tipos de controles de acesso.

As biometrias disponíveis sob *smart identification cards* incluem *scanner* de impressão digital, geometria da mão, reconhecimento da face, *scanner* da íris (o mais seguro)e reconhecimento da voz (o menos seguro).

De acordo com NAKAMURA (2002), certificados digitais são basicamente recipientes para chaves públicas e agem com o propósito de identificação eletrônica. O certificado e chaves públicas são documentos públicos que, a princípio, ninguém pode acessar. Uma chave privada associada, pertencente somente a uma entidade à qual o certificado foi definido, é usada com o propósito de estar ligando o certificado com àquela entidade. Usuários que não possuem esta chave privada não podem usar o certificado com o intuito de autenticação. Entidades podem provar suas posses de uma chave privada por dados conhecidos digitalmente ou demonstrando conhecimento sobre a troca de segredos, usando métodos criptográficos de chaves públicas.

Ainda conforme o autor, na prática qualquer um pode gerar um par de chaves privadas e certificados digitais; conseqüentemente, é necessário determinar quando o dono do certificado é digno de confiança. Por esta razão, um modelo confiável de terceiros é usado com certificado digital. O terceiro usado no domínio de certificados digitais é um Certificado de Autoridade (CA – *Certificate Authority*). Um CA pode emitir certificado usando chaves públicas proporcionadas por clientes, ou pode ser gerado por um par de chaves pública-privada apresentado pelo cliente e então emitir o certificado junto com esse par de chaves. Em ambos os casos, o cliente deve demonstrar sua identidade para o CA por algum meio confiável. Por exemplo, o cliente planeja um encontro face a face com o CA e apresenta a prova da identidade. O CA então emite um certificado com a assinatura digital dele, incluindo a chave pública deste cliente e informações sobre a identidade do cliente. As pessoas que possuem a chave pública do CA verificam a assinatura digital, e então se estabelece a cadeia confiável entre os clientes e a CA.

f. Integração de Sistemas Legados

De acordo com VALLABHANENI (2002), não basta implementar a administração das identidades nas novas plataformas, deixando partes dessa administração isoladas dentro dos Sistemas Legados e nos ERPs (*Enterprise Resource Planning*). A conscientização dos fornecedores tecnológicos em relação a integração dos diversos ambientes permite que novos conceitos, como por exemplo *Single Sign On* (tecnologia que permite aos usuários serem autenticados em uma única vez) já sejam criados de forma a permitir a integração às antigas tecnologias e aplicativos.

2.3.5. Modelos de gestão de risco em segurança da informação

O modelo proposto por BRAITHWAITE (2002) divide o gerenciamento da segurança de informação em quatro grandes áreas de interesse não-técnicas permeado as áreas técnicas: segurança física, segurança pessoal, procedimentos de segurança e proteções legais. No centro do modelo, observam-se as tecnologias ou áreas técnicas a serem tratadas pela segurança: sistemas aplicativos, processos cliente-servidor, processamento central ou distribuído, gerenciamento de banco de dados e rede, comunicações e Internet.

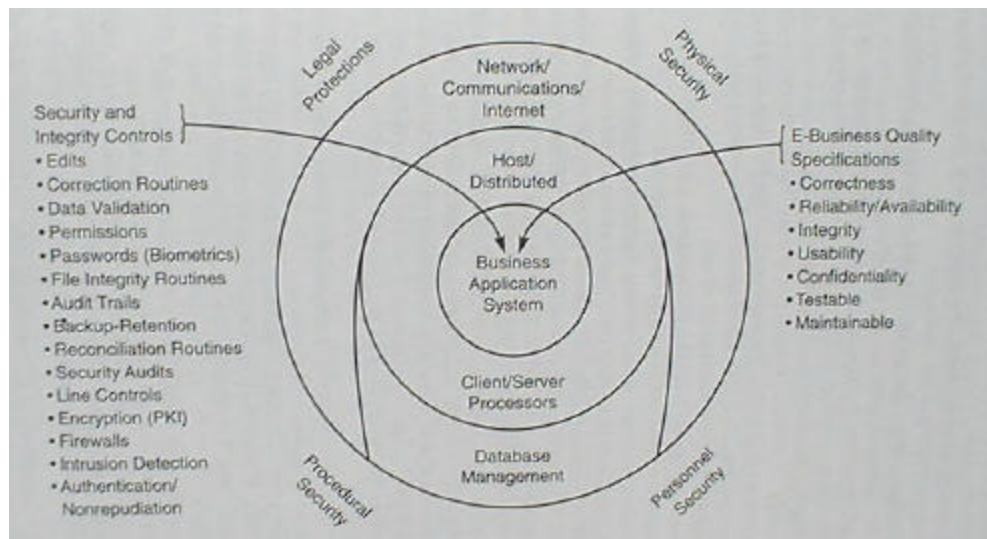


Figura 29: Information Security Risks

(BRAITHWAITE, 2002, pág. 143)

Já o modelo de CLARK (2003) apresenta uma abordagem em camadas, no qual o centro representa decisões mais estratégicas e as camadas externas, medidas de segurança e contra-medidas de ataque. Quanto mais externa a camada, maior o potencial de risco de ataques. Portanto, temos ao centro as decisões estratégicas em relação à segurança da informação, como a política de segurança da empresa e a divulgação das melhores práticas.

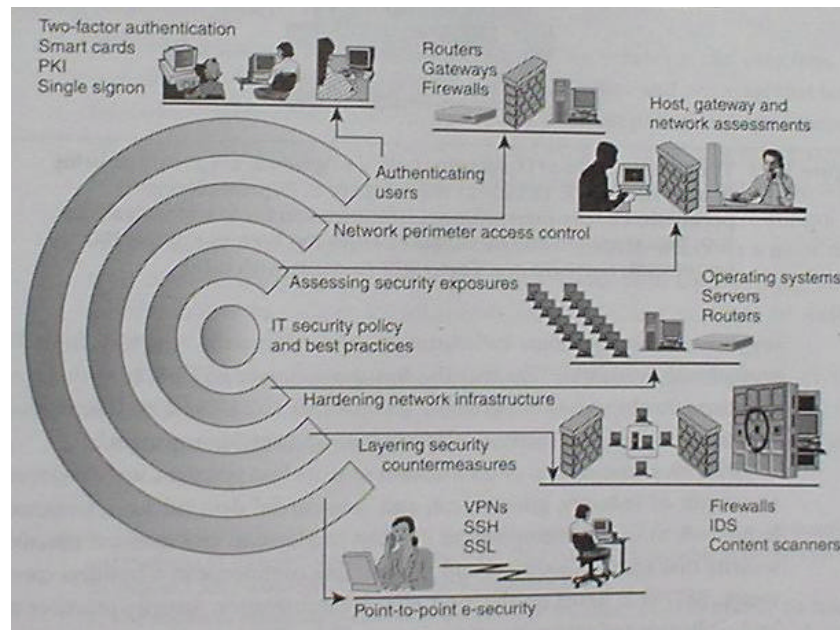


Figura 30: Managing Information Security Risks

CLARK (2003) pág. 150

O modelo proposto por LAUDON (2002), apesar de muito mais simples, apresenta importantes conceitos como os direcionadores de negócio, os agentes implementadores e as áreas de interesse.

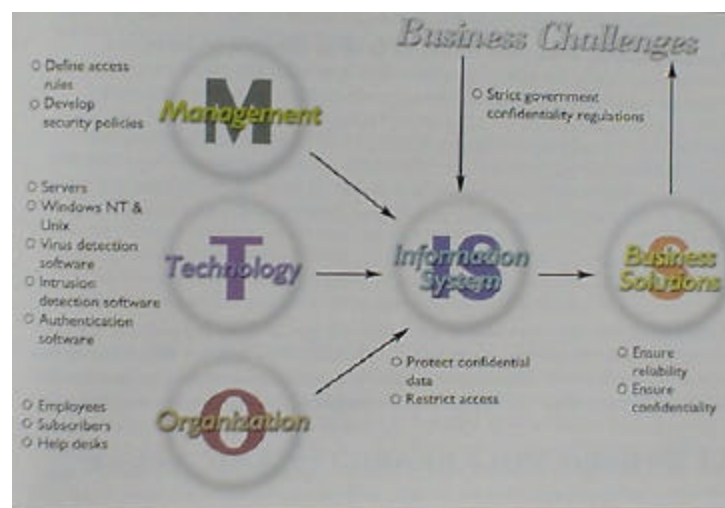


Figura 31: Information Risk Management

(LAUDON, 2001, pág.433)

A partir dos modelos e dos textos estudados, foi elaborado o seguinte desenho para a melhor visualização de todos os componentes anteriormente descritos.

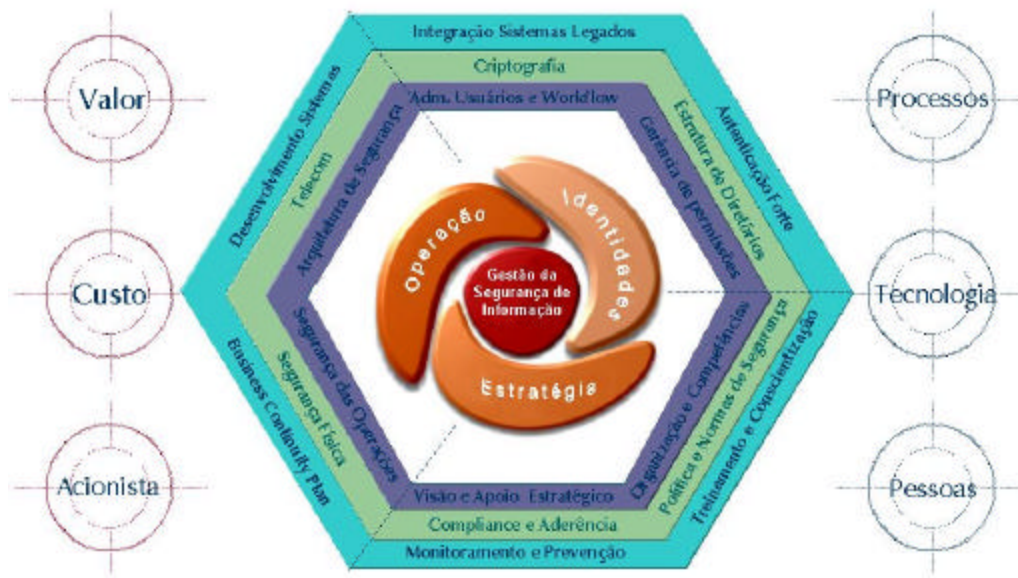


Figura 32: Modelo de gestão de risco em segurança da informação
(elaborado pelo autor)

Podemos inicialmente dividir o modelo em duas grandes metades. Na primeira metade, no lado esquerdo do desenho, estão as questões que orientarão o planejamento da segurança da informação. Conforme já descrito anteriormente, estas são os direcionadores de negócio e estão divididas em três: agregar valor ao negócio, gerenciar o custo da segurança da informação e administrar as expectativas dos investidores.

Na segunda grande metade do modelo, localizada no lado direito do desenho, encontramos as questões relacionadas à implementação, que devem levar em consideração os aspectos técnicos, humanos e procedurais. Os agentes implementadores, anteriormente descritos, são: processos, tecnologia e pessoas.

No centro do modelo, encontramos a gestão da segurança da informação e, como no modelo de CLARK (2003), esta gestão está dividida, de dentro para

fora, em três grandes assuntos de interesse. Estas áreas de interesse são os grande focos de concentração em que um gestor da segurança de informação deve atuar:

- ✍✍ Alinhamento estratégico: trata as questões estratégicas da área de gestão da segurança de informação.
- ✍✍ Gerenciamento da segurança das operações: visa a garantir a segurança das operações de negócio da instituição.
- ✍✍ Administração das identidades: trata da administração das identidades de todas as pessoas e entidades que possuem acesso à instituição.

A partir de cada área de interesse, são subdivididas, cada uma delas, em seis sub-áreas de interesse, para a segurança da informação.

Vale a pena ressaltar que as três áreas de interesse e suas subdivisões são altamente inter-relacionadas e que a divisão proposta no modelo visa apenas à elucidação didática e ilustrativa. Na prática, qualquer ação em uma das áreas gera automaticamente conseqüências nas demais outras duas.

3. Metodologia da Pesquisa

De forma geral, os critérios utilizados para definir os tipos de pesquisa variam entre os diversos autores. A opção pela utilização da metodologia de estudo de caso com seleção de caso único foram devidos aos conceitos e argumentos abaixo apresentados.

3.1. Pesquisa Exploratória

O objetivo principal da pesquisa exploratória é a busca pelo entendimento sobre a natureza geral de um problema. A pesquisa exploratória é tradicionalmente utilizada em áreas onde existe pouco conhecimento acumulado e sistematizado sobre o assunto e ser pesquisado. A pesquisa visa aprofundar questões a serem estudadas e ganhar maior conhecimento sobre um tema. Possui uma forma de investigação mais flexível e menos estruturada do que a realizada em uma pesquisa conclusiva devido a sua natureza de sondagem. Segundo BOYD e WESTFALL (1984), o estudo exploratório tem como principal objetivo encontrar idéias e novas relações para elaborar explicações prováveis. Uma vez que existem poucos estudos acadêmicos e científicos publicados sobre os aspectos de gerenciamento de risco em segurança da informação, tema deste trabalho, a opção pela adoção da pesquisa exploratória parece ser a mais adequada conforme o conceito exposto acima. Desta forma, a abordagem exploratória irá permitir o detalhamento do conhecimento sobre o assunto estudado, aumentando a sua compreensão através de uma investigação flexível.

De acordo com YIN (2001), a abordagem exploratória pode ser utilizada em qualquer um dos cinco tipos principais de estratégias de pesquisa: experimento, levantamento, análise de arquivos, pesquisa histórica e estudo de caso.

3.2. Estudo de caso

Conforme BOYD e WESTFALL (1984), o método do caso é um estudo intensivo de um número pequeno de casos, que tem por objetivo a obtenção de uma compreensão das relações dos fatores em cada caso, independentemente do número de casos envolvidos. É útil quando um problema envolve a inter-relação de vários fatores e quando for difícil compreender os fatores individuais sem considerá-los em suas relações com os outros. Através desta abordagem é possível o aparecimento de relações entre os fatores do caso e, que de outras formas, não poderiam ser descobertas.

O estudo de caso não é apenas um método de coleta de dados, mas sim, uma estratégia de pesquisa abrangente. Conforme a definição proposta:

“Um estudo de caso é uma investigação empírica que:

- ?? Investiga um fenômeno contemporâneo dentro de seu contexto na vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos; (...)*
- ?? Enfrenta uma situação em que o número de variáveis de interesse é muito maior do que o número de pontos de dados;*
- ?? Baseia-se em várias fontes de evidências necessitando de uma triangulação para a convergência dos dados;*
- ?? Beneficia-se do desenvolvimento de proposições teóricas prévias para conduzir a coleta e a análise dos dados.” (YIN, 2001, pág. 32).*

A partir do conceito de estudo de caso proposto por YIN (2001), a utilização do método do caso como estratégia para guiar a realização desta pesquisa justifica-se pelas seguintes razões:

- ✍ A gestão da segurança da informação na indústria de cartão de crédito é um fenômeno no mercado competitivo que ainda não está claramente definida;*

- ✍✍ A quantidade de variáveis envolvidas no estudo é significativamente maior que o número de casos estudados;
- ✍✍ O estudo baseia-se em várias fontes de evidência, tais como: revisão de literatura de teorias de gerenciamento de risco e segurança da informação, entrevistas com gestores da indústria de cartão de crédito;

A proposição teórica apresentada no capítulo de revisão de leitura englobando as teorias de modelos de gestão de riscos em segurança da informação orientou a condução e análise do estudo de caso.

De acordo com os conceitos e as justificativas apresentados, a opção pela utilização do método do caso parece adequada para atingir os objetivos propostos pela pesquisa, quais sejam, analisar o intento estratégico da VISANET e seus objetivos, aplicar os modelos de gestão de segurança da informação à situação da VISANET e comparar os resultados dos modelos com os objetivos estratégicos para a segurança da informação da VISANET. A questão norteadora da pesquisa: “como a estruturação da área de segurança da informação adotada pela VISANET alinha-se com as proposições de alguns modelos de gestão de risco em segurança da informação?”, também justifica a escolha do método, pois, segundo YIN (2001), o método de estudo de caso é indicado quando se deseja responder questões do tipo “como” e “porque” ao longo da pesquisa.

Entretanto, uma das principais críticas em relação à metodologia do estudo de caso é o fato de oferecer poucas bases para se fazer uma generalização científica ou estatística. De acordo com YIN (2001), uma vez que o objetivo dos estudos de caso é o de prover análises “generalizantes” e não “particularizantes”, eles devem se basear em generalizações analíticas, ao invés de estatísticas. Na generalização analítica o pesquisador procura generalizar um conjunto particular de resultados à uma teoria mais abrangente. Este trabalho não tem o objetivo da realização de generalizações estatísticas.

3.3. Seleção do Caso Único

Segundo YIN (2001) o estudo de caso único é indicado quando um conjunto de condições, ou de fundamentos lógicos, está presente para justificar sua adoção:

- ☞ O estudo de caso representa o caso decisivo para testar uma teoria ou um conjunto de teorias e proposições bem formuladas sobre um determinado assunto;
- ☞ O caso representa um caso raro ou extremo, ou seja, possui características especiais e únicas que por si só merecem ser analisadas e documentadas;
- ☞ O caso é um caso revelador, ou seja, é analisável pelo pesquisador que tem uma oportunidade especial para observar e investigar um caso é praticamente inacessível aos demais membros da comunidade científica.

Segundo YIN (2001), os resultados de um estudo de caso provavelmente serão mais convincentes e precisos quando baseados em fontes distintas de informação. Desta forma, para buscar maior riqueza de informações para a dissertação optou-se pela utilização das três formas de coleta de informações, determinando as seguintes três fases de coleta de dados:

☞ Estudo de Dados Secundários

Na primeira fase da pesquisa foram utilizadas as fontes secundárias para aprofundar a revisão bibliográfica. Foram pesquisados livros, artigos de jornais e revistas, artigos científicos e demais publicações que possibilitassem a obtenção de dados relevantes e atualizados sobre segurança da informação e sobre companhias de cartão de crédito. Esta fase da pesquisa teve início em 2002, com a execução do projeto da dissertação.

☞ Entrevista com profissionais da empresa

Neste período foram entrevistados: os principais executivos da VISANET e os diversos gerentes de segurança e de tecnologia da

informação. Os dados foram obtidos entre maio de 2002 até outubro de 2002.

☞☞ Análise dos dados

Segundo YIN (2001), a análise dos dados, consiste em examinar, categorizar, classificar em tabelas ou recombina as evidências encontradas na pesquisa tendo em vista as proposições teóricas iniciais do estudo. Uma vez que principal função do método do caso é a explicação sistemática dos fatos que ocorrem no contexto social e que se relacionam com uma multiplicidade de variáveis, os dados podem ser apresentados sob a forma de tabelas, quadros, gráficos e por meio de uma análise descritiva que os caracterizam.

4. Estudo de Caso Resultados da Pesquisa

A VISANET nasceu em novembro de 1995, resultado da associação entre própria VISA International a um grupo de bancos emissores do cartão. A empresa é a única adquirente do sistema VISA no Brasil. Isto significa que, a empresa é a única responsável pelo relacionamento e processamento de todas as transações do cartão dos 685 mil estabelecimentos comerciais afiliados ao sistema VISA no país. Através da plataforma da VISANET passam todas as transações com cartões VISA, crédito e débito, realizadas nesses estabelecimentos. São mais de 620 milhões de transações em 2001, totalizando um faturamento do sistema de 32,7 bilhões de reais. Em 2002, a previsão é atingir 800 milhões de transações, resultando num faturamento total de 41 bilhões de reais. (SPOSITO, REVISTA INFO CORPORATE, Outubro de 2002)

4.1. O negócio VISANET

A Companhia Brasileira de Meios de Pagamento, conhecida no mercado como VISANET, é uma das 10 maiores empresas do seu segmento em todo mundo. Iniciou suas operações em fevereiro de 1996 com o objetivo de administrar para os então bancos adquirentes: Bradesco, Banco do Brasil, Banco Real e Banco Nacional, a rede de estabelecimentos comerciais afiliados para aceitar os cartões VISA como meio de pagamento, afiliando novos estabelecimentos e recadastrando os estabelecimentos já afiliados pelos bancos.

No último trimestre de 1996, a VISANET começou a prestar todos os serviços típicos de uma empresa adquirente, compreendendo os principais processos de negócio: afiliação de novos estabelecimentos comerciais, serviços à rede, autorização e captura de transações, pagamento ao comércio, treinamento, e promoções nos pontos de venda entre outros.

A VISANET foi inicialmente constituída pela associação entre VISA International e grandes bancos brasileiros, que então formam o Conselho de

Administração da empresa. A VISANET conta com vinte oito grandes bancos entre seus acionistas e tem em cada uma das agências espalhadas por todo Brasil, um canal de distribuição para produtos VISA e para afiliação de novos estabelecimentos comerciais à sua rede.

A VISANET mantém 53 filiais operativas cobrindo mais de quatro mil municípios brasileiros, atendendo 685 mil estabelecimentos comerciais em todo o país. Todas as filiais estão interligadas ao sistema de processamento principal, facilitando o planejamento e execução das atividades comerciais da empresa.

A criação da VISANET representa para VISA e os bancos acionistas a oportunidade de: prestar um ótimo serviço ao comércio, expandir a rede para o interior do país, duplicar o volume de faturamento a cada três anos, criar plataformas de lançamento de novos produtos, duplicar o índice de automação das transações e conseqüentemente, fortalecer a marca VISA no mercado brasileiro.

A VISANET conta com uma forte estrutura financeira, distribuindo dividendos trimestrais aos seus acionistas e com independência à financiamento de terceiros para executar seus investimentos necessários à infra-estrutura requerida pelo crescimento de em torno 40% ao ano no volume de transações processadas.

A VISANET possui em sua estratégia a seguinte missão e visão:

“Missão da VISANET

Fazer com que a rede credenciada ao sistema VISANET tenha nos produtos o seu meio de pagamento preferido, não só pela agilidade no processamento da transação, mas também pela segurança no recebimento e oportunidade de incremento de vendas

Visão

Que todos os gastos efetuados no Brasil sejam processados através de um terminal conectado ao sistema VISA.”

Em entrevista a um alto executivo da VISANET, foi passado os seguintes objetivos empresariais:

- ✍✍ Personalização da gestão da rede de estabelecimentos comerciais para aumentar o índice de fidelização de cada estabelecimento para com os produtos VISA.
- ✍✍ Aumento das receitas do negócio, sempre oferecendo à rede de estabelecimentos comerciais, produtos e serviços criativos e de qualidade, além de promoções que ajudem alavancar o volume de negócios para esses estabelecimentos.
- ✍✍ Incorporação de novos nichos de mercado e expansão da aceitação dos produtos VISA como meio de pagamento no mundo digital.
- ✍✍ Aperfeiçoamento da gestão de risco para melhorar a rentabilidade dos emissores e da VISANET. Utilização da capacidade instalada na rede para trafegar transações de produtos não concorrentes e alavancar a aceitação dos produtos VISA. Oferecimento de uma rentabilidade superior aos acionistas e valorização da empresa no tempo.
- ✍✍ Comprometimento com a qualidade e com a eficiência em todos os processos que compõe a nossa cadeia de valores.
- ✍✍ Reconhecimento pelo mercado e por seus clientes como uma empresa líder, inovadora e voltada para o interesse de seus clientes.

4.1.1. Estrutura organizacional

O conselho de administração da VISANET é composto de onze membros e tem como presidente, o Sr. Ricardo Ancede Gribel, da VISA do Brasil, e como vice-presidente, o Rs. Arnaldo Vieira, do Bradesco. O Bradesco participa com quatro membros no conselho, o Banco do Brasil, com três, e o Banco ABN Amro Real, VISA International e Banespa com um membro cada um.

Segundo um relatório interno de 08 janeiro de 2002, os principais bancos acionistas são: Bradesco, Banco do Brasil, Banco ABN Amro Real, Banco Alfa, Banco Baneb, Banespa, Banestado, Banestes, BankBoston, Banrisul, BBV Banco,

BRB Banco de Brasília, Banco Cidade, HSBC Bank Brasil, Banco Santander, Banco Panamericano, Banco Rural, Banco Santos e Banco Sudameris.

A diretoria executiva é composta pelo presidente, Sr. Ruben H. Osta, e por sete diretores executivos referentes as diretorias de: Vendas & Negócios, Tecnologia & Operações, Finanças & Administração, Desenvolvimento Organizacional, Riscos & Fraudes, Processos & Auditoria, e Marketing & Produtos.

4.1.2. Conceitos e terminologias da VISANET

Antes de qualquer coisa é preciso definir os principais participantes dos processos de negócio da VISANET:

- ✍ ✍ Portador: pessoa física que possui o cartão de crédito ou débito. O portador é que realiza uma compra de um produto ou serviço em um estabelecimento comercial.
- ✍ ✍ Banco emissor: banco que emitiu o cartão para o portador. Quando se trata de um banco, em geral o portador possui conta corrente neste banco. O portador paga ao banco emissor a fatura mensal de seus gastos pessoais.
- ✍ ✍ Estabelecimento comercial: estabelecimento (pessoa jurídica) de caráter comercial aonde o portador realiza uma compra, ou seja, uma transação financeira.
- ✍ ✍ Banco adquirente: banco no qual o estabelecimento comercial possui uma conta corrente. Nesta conta são depositadas diariamente os valores das vendas realizadas à 30 dias atrás.
- ✍ ✍ VISA: empresa proprietária da bandeira VISA. Existe a matriz mundial, VISA International que interliga as diversas empresas processadoras das transações de cartão de crédito espalhadas pelo mundo. E a VISA do Brasil, responsável pela administração da bandeira no território nacional e pelas interligações tecnológicas entre a VISA International, bancos emissores e a VISANET.
- ✍ ✍ Rede de captura: rede que interliga todos os estabelecimentos comerciais que aceitam o cartão de crédito VISA e o cartão de débito VISA Electron.

⚡ VISANET: empresa processadora das transações dos cartões VISA. Ela é responsável pela expansão e manutenção da rede de captura, não só no âmbito tecnológico, mas também no âmbito mercadológico. Toda transação trafegada pela rede de captura da VISANET é cobrado do estabelecimento comercial um percentual do valor transacionado. Este percentual é dividido entre a VISA, a VISANET e o banco emissor. Todos os dias a VISANET realiza a transferência de valores dos bancos emissores (faturas pagas pelo portador) para os bancos adquirentes nas contas corrente dos estabelecimentos comerciais.

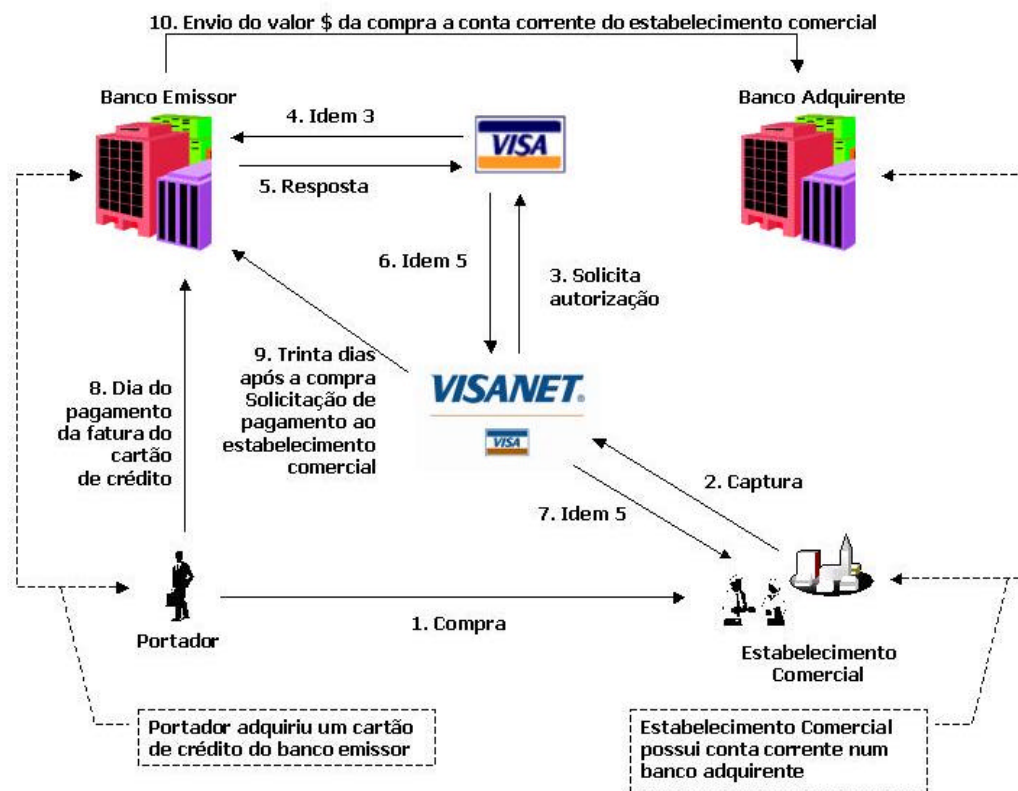


Figura 33: Processos VISANET

(elaborado pelo autor)

Outros conceitos são importantes para o entendimento dos processos de negócio da VISANET:

⚡ Rede corporativa: é a rede interna, de baixa plataforma, para acesso dos funcionários da VISANET realizarem suas operações

diárias. Tecnicamente, a rede corporativa é totalmente isolada da rede de captura.

- ✍ ✍ Rede de captura: é uma rede WAN exclusiva e totalmente isolada. O serviço de interligações, conexões e cabeamento dos diversos municípios à rede é realizado pela EMBRATEL. Também são utilizados os serviços de *co-location*⁸ dos concentradores de transações. pertencentes a VISANET ficam em *data centers* exclusivos rede que interliga todos os estabelecimentos comerciais que aceitam o cartão de crédito VISA e o cartão de débito VISA Electron.
- ✍ ✍ PIN-PAD: teclado numérico que se interliga ao POS ou ao PDV, para digitação da senha eletrônica do cartão de débito. Possui um microprocessador para criptografar a senha utilizando uma chave criptográfica randômica. A senha do cartão de débito já sai criptografada do equipamento. Toda vez que o gabinete do equipamento é aberto, por questões de segurança, todos os algoritmos de criptografia são destruídos.
- ✍ ✍ POS: da abreviação de *Point-of-sales*, são os equipamentos pertencentes a VISANET, que são alugados aos estabelecimentos comerciais de pequeno e médio porte. Estes equipamento estão ligados diretamente à rede de captura da VISANET. Podem ser dedicados ou discados. Os POS discados são os mais antigos, pois necessitam uma linha telefônica para ligar em uma central a cada transação. Os POS dedicados são aqueles que ficam conectados a rede de captura enquanto estão ligados. Lojas, restaurantes e postos de gasolina são exemplos típicos que possuem este tipo de aparelho.
- ✍ ✍ PDV: apesar de possuírem o mesmo significado literalmente, pois PDV vem da abreviação de Ponto de Venda, que é a tradução de *Point-of-Sales*, significam, não só para VISANET mas para o mercado nacional de cartão de crédito, um outro tipo de solução para a captura das transações. O PDV é uma solução no qual o estabelecimento comercial possui muitas caixas registradoras. Neste caso, somente o PIN-PAD pertence a

⁸ Enquanto que o serviço de *hosting* é um serviço pelo qual a empresa contratante paga a empresa contratada por disponibilizar os serviços de uma solução desenvolvida e pertencente a empresa contratante em um *data center* da empresa contratada, e esta deve fornecer toda a infra-estrutura tecnológica para suportar a solução. O serviço de *co-location* é um serviço de *hosting* no qual a empresa contratante é proprietária dos servidores que hospedaram suas soluções, ficando para empresa contratada, apenas as questões de segurança física e telecomunicações. O *co-location* pode ser administrado ou não por funcionários especializados da empresa contratada.

VISANET, pois a leitora do cartão de crédito faz parte da caixa registradora. O software totalmente componentizado também pertence a VISANET, e é disponibilizado ao estabelecimento comercial para integração ao seu sistema de automação das vendas. Nesta solução, sendo as caixas registradoras terminais PC, todas as informações passam por um servidor central que concentra as informações das transações dos cartões e enviam para a VISANET. Em grandes cadeias de supermercados e lojas, pode ocorrer mais níveis de concentração até a interligação com a rede de captura da VISANET. Pouco menos utilizado, Segundo, BEHAN (1990), o nome utilizado em inglês para esta solução como um todo é EFT – *Electronic Funds Transaction*, mas no Brasil o termo é utilizado apenas como concentrador TEF – Transação Eletrônica de Fundos, significando apenas o nome do software que roda no terminal de caixa.

4.1.3. A relação da VISANET com seus parceiros

Segundo as entrevistas realizadas com a alta direção, a VISANET adota como estratégia a terceirização de muito de seus serviços. Esta estratégia faz com que até mesmo operações *core* sejam realizadas através de fornecedores. Pode-se dizer que o quadro enxuto da empresa foca as questões de estratégia e direcionamento do negócio enquanto que as questões de implementação e execução ficam nas mãos dos parceiros. Conforme um dos principais executivos:

“...os fornecedores não são tratados como apenas fornecedores, mas sim como parceiros estratégicos para operação da empresa. Esta relação de confiança e parceria já faz parte da cultura da empresa. Hoje, se você entrar dentro da empresa, é difícil saber quem é fornecedor e quem é funcionário. O comprometimento de nossos parceiros com o sucesso de nosso negócio é tão alto quanto o de nossos funcionários.” (diretor executivo da VISANET, em entrevista realizada em julho de 2002)

Os principais fornecedores da VISANET são a EDS e a Proceda, fornecendo todos os serviços de autorização eletrônica e manual e

processamento de transações financeiras. Esta estratégia de terceirização também pode ser observada através de seu principal concorrente a REDECARD. Comparativamente, a REDECARD utiliza a empresa Orbitall para execução destes serviços.

4.1.4. Principais processos de negócio

Os principais processos de negócio da VISANET são:

- ✎ Afiliação: para trabalhar com os cartões VISA o estabelecimento comercial necessita afiliar-se ao sistema VISANET. Além da equipe de vendas dos bancos acionistas, existe uma equipe de vendas da VISANET que atua como agente afiliador.
- ✎ Autorização Eletrônica: autorização realizada através da rede de captura eletrônica da VISANET. O processo inicia-se em um terminal denominado POS (*Point of Sales*) ou em um PDV (Ponto de Venda) pertencente a rede da VISANET, localizado em um estabelecimento comercial afiliado. Ao passar o cartão na leitora magnética, os dados do cartão e da transação financeira são transferidos a concentradores intermediários que por sua vez enviam a duas centrais de autorização, localizados em: São Paulo, que atende as regiões Sul, Sudeste e Centro-Oeste; e Salvador, que atende as demais regiões. A partir destas centrais de processamento, ainda pertencentes a VISANET, os dados da transação são encaminhados a terminais interligados a rede internacional da VISA International, denominados de VAP – *VISA Access Point*. A rede da VISA International, decide e envia para o banco emissor responsável por aquela autorização. O banco emissor realiza ou não a autorização e devolve a rede da VISA International. Esta por sua vez joga de volta para as centrais de processamento da VISANET, que envia a resposta para o estabelecimento comercial de origem. Todo este processo de resposta da autorização demora no máximo seis segundos. Caso contrário a transação é abortada.
- ✎ Autorização Manual: quando o estabelecimento comercial possui as seguintes características: é de pequeno porte, possui um volume extremamente pequeno de vendas no cartão, não tem condições para alugar um POS, e não pertence a um

segmento de mercado classificado pela VISANET como de alto risco; o estabelecimento comercial pode realizar as vendas utilizando a 'maquineta', ou popularmente chamada de 'mata-pulgas'. Este equipamento consiste em tirar uma cópia em carbono do auto-relevo dos dados do cartão, e em conjunto obter um número de autorização telefonando para uma central de atendimento da VISANET. Este número é anotado ao comprovante de venda pelo cartão de crédito. Fica sob responsabilidade do estabelecimento comercial depositar as cópias dos comprovantes no seu banco adquirente. Após trinta dias após a data de autorização, o estabelecimento comercial recebe o valor em sua conta corrente.

- ✎ Captura Eletrônica: ao final de cada dia, tanto o POS quanto a solução de PDV, necessitam fechar seus lotes e transmitir para a VISANET, para que as transações sejam consideradas encerradas e concluídas. Somente após o fechamento dos lotes, o POS ou PDV poderá ser desligados. A cada novo dia de transações, os POS e PDVs devem ser inicializados gerando novos valores de lotes.
- ✎ Captura Manual: nas vendas realizadas manualmente, o comprovante de venda é emitido em três vias: 1a. via pertence ao portador do cartão, a 2a. via pertence a VISANET e a 3a. via pertence ao estabelecimento comercial. No máximo a cada 50 comprovantes de vendas, o Estabelecimento Comercial deve preencher um documento denominado Resumo de Operações R.O., o qual é um relatório sumariado de todas as vendas realizadas manualmente. Após preenchimento do R.O., e uma vez anexado os comprovantes de venda manual, o R.O. já pode ser entregue em uma das agências do banco adquirente. Todas as R.O possuem um número único de identificação. Os bancos adquirentes enviam por sua vez os comprovantes a duas empresas captadoras da VISANET: TRANSPEV e PROSERVVI. Ambas digitalizam os comprovantes, e enviam a VISANET para serem processadas.
- ✎ Captura *Batch* ou MOTO: Os Estabelecimentos Comerciais que recebem pedidos de compra por meio de *mail order* ou *telephone order*, utilizam o sistema de EDI via Interchange para transmitir as informações referentes a estas vendas para a VISANET. Neste caso, todas as transações são autorizadas uma a uma da mesma forma que uma autorização eletrônica.

- ✍ ✍ **Processamento (Edit Package):** A EDS, empresa responsável pelo processamento das informações capturadas, recebe os dados para processamento das seguintes fontes: PROCEDA(Captura Eletrônica), INTERCHANGE (Vendas Mail-Order e Phone-Order), TRASPEV/ PROSERVVI (Captura Manual). É realizada uma série de consistências e processados para a geração do arquivo a ser enviado a VISA International, contendo: grade de liquidação financeira, transações autorizadas, tratamento de rejeitadas, ajustes, reenvio de transações, etc. São processados também a inclusão e manutenção do cadastro de estabelecimentos afiliados.
- ✍ ✍ **Intercâmbio:** No processo de intercâmbio de transações, o portador do cartão entra em contato com o banco emissor com o objetivo de tentar identificar a origem da transação. Caso não seja possível a identificação, a VISA é acionada e caso ela também não consiga identificar a transação, o problema é passado para VISANET, no qual, busca em seus registros a origem da transação. Caso não seja encontrado, é iniciado um processo de solicitação de cópias ao estabelecimento comercial. Este por sua vez possui um prazo a cumprir, pois caso contrário, o valor será descontado e adicionado pontos em relação ao risco do estabelecimento.
- ✍ ✍ **Chargeback:** Operações de *chargeback* são aquelas em que o banco emissor gera uma transação de débito a VISANET, por ela não ter cumprido corretamente o processo de Intercâmbio. Diversas razões podem acarretar em um processo de *chargeback*, dentre elas: não atendimento a solicitação de cópia por parte da Visanet, cumprimento fora do prazo estabelecido, fornecimento de cópia ilegível, fornecimento de cópia errada, dentre outros. As solicitações de *chargeback* somente poderão ocorrer se o banco já tiver solicitado previamente um pedido de cópia.
- ✍ ✍ **Liquidação Financeira:** a partir das informações alimentadas no sistema de agenda financeira, a área de Tesouraria elabora a grade financeira, que do ponto de vista da VISANET, contempla como crédito os valores enviados pelos emissores de cartão e como débito os pagamentos aos estabelecimentos comerciais, tanto para as transações de débito VISA Electron quanto para as transações de crédito. Os valores a serem pagos pelos bancos emissores à VISANET são informados à VISA com um dia de antecedência. Este sistema calcula qual a melhor grade de liquidação possível para VISANET e a partir dessa informação gera um relatório informando os valores que os bancos possuem

a receber ou a pagar, para outras instituições financeiras. Dificilmente os bancos contestam os valores a serem creditados ou debitados, entretanto, caso isso ocorra, a VISANET intervém no processo.

4.1.5. Detalhes tecnológicos e operacionais

Como explicado anteriormente, a VISANET utiliza os serviços da EDS e Proceda para processamento das transações. Para o entendimento e a análise de risco da segurança da informação é necessário detalhar um pouco mais a infraestrutura que suportam as operações.

Como explicado anteriormente, existem duas centrais de processamento: uma em São Paulo e outra em Salvador. A primeira responsável por atender as regiões do sul, sudeste e centro-oeste; e a segunda, pelas regiões nordeste e norte do país.

A central de São Paulo está dividida em dois *data centers*: da EDS em São Bernardo do Campo e da Proceda, localizado no Centro Empresarial São Paulo CENESP. Ambos operam processos distintos. A Proceda tem como responsabilidade a captura e autorização das transações. Ao final do dia envia os lotes de transações capturadas, denominado de BASE I - Autorizações. Enquanto que a EDS é responsável por processar todas os lotes de transações já autorizados, com problemas e pendentes, enviadas pela Proceda São Paulo e a central de Salvador; e enviar para VISA International, denominado de BASE II - Liquidação e Intercâmbio. Além disto a EDS também administra as liquidações financeiras entre bancos emissores e bancos adquirentes; também calcula as comissões para a VISA, VISANET e banco emissor; e os devidos impostos.

A central de processamento de Salvador pertence a VISANET, mas é operada através de funcionários da Proceda. Tem como objetivo apenas a captura e autorização das transações. Ao final do dia, envia para EDS em São Paulo, os lotes de transações capturadas (BASE I).

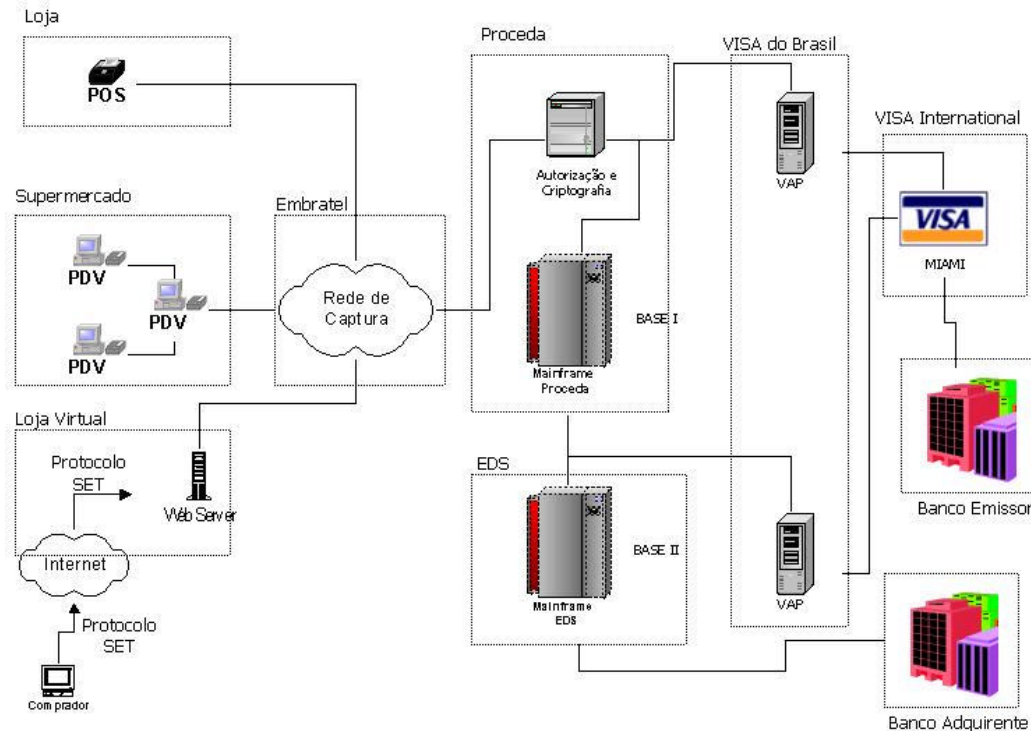


Figura 34: Infra-estrutura da VISANET

(elaborado pelo autor)

4.2. Segurança da informação na VISANET

Seguindo o modelo de gestão de risco de segurança da informação apresentado na fundamentação teórica, e através de uma série de entrevistas com o gerente de segurança da informação da VISANET, foi identificado o seguinte panorama.

4.2.1. Alinhamento estratégico

Conforme a estratégia de focar apenas a gestão do negócio, a área de segurança, extremamente enxuta como será descrita a seguir, contrata diversos serviços especializados em segurança para a VISANET. No início de 2002, a VISANET contratou a consultoria especializada da PricewaterhouseCoopers para

ajudar o redesenho e estruturação da área de segurança da empresa através de um Plano Diretor de Segurança da Informação.

Em entrevista com o Security Officer da VISANET, este trabalho estruturou a maior parte das informações de caráter estratégico para área a serem apresentados a seguir.

a. Visão e apoio estratégico

A área de segurança possui um Security Charter, conforme recomendado por BYRNES (2001), muito bem estruturado. Neste documento é possível encontrar a missão da área de segurança:

“Garantir o nível de proteção física e lógica dos dados e informações de nossa rede e nossos produtos, de forma a diminuir ou eliminar o risco de perda, destruição e indisponibilidade das mesmas.”

De forma bastante estruturada e complementar, a VISANET possui formalmente descrita também uma visão da área de segurança:

“A área de segurança da VISANET tem como visão os seguintes processos:

Prevenir

- ≡≡ Estabelecer requisitos mínimos que assegurem a confidencialidade, integridade e disponibilidade das informações sensíveis da empresa, dos estabelecimentos comerciais, dos portadores de cartões e dos bancos associados.*
- ≡≡ Desenvolver políticas, normas e procedimentos de segurança relacionados aos meios de pagamentos eletrônicos e a rede corporativa em conjunto com as áreas da empresa.*
- ≡≡ Implementar, soluções tecnológicas em conjunto com as demais áreas da empresa, os padrões e práticas que*

maximizem a segurança das informações nas transações de débito e crédito.

- ≡≡ Implementar em conjunto com as demais áreas da empresa, soluções tecnológicas de segurança da informação nas operações de negócio da VISANET.*

Monitorar

- ≡≡ Assegurar que as várias entidades, que estão envolvidas na atividade de meios de pagamentos eletrônicos, cumpram os requisitos mínimos de segurança estabelecidos pela VISA e pelos padrões e normas internacionais que regulam a indústria.*
- ≡≡ Assegurar que todas as entidades envolvidas na atividade de meios de pagamentos eletrônicos estejam em conformidade com as políticas, normas e procedimentos de segurança adotados pela VISANET.*
- ≡≡ Revisar em conjunto com as outras áreas da empresa os controles e a conformidade da execução, implementação e monitoramento dos requisitos e atividades de segurança da informação.*

Reagir

- ≡≡ Implementar normas e procedimentos que possibilitem a continuidade do negócio em caso de um ataque ou desastre aos sistemas de informação da empresa.*
- ≡≡ Estabelecer em conjunto com as demais áreas da empresa procedimentos para suporte técnico, jurídico e organizacional para resposta à incidentes e captura de evidências."*

Segundo entrevista com o Information Security Officer, o sucesso das ações e iniciativas segurança contam com o apoio estratégico da alta administração. Segundo ele, o trabalho para a estruturação do plano diretor da área, houve envolvimento direto do presidente e demais diretores executivos em mais de 40 horas.

O comprometimento do presidente e alta direção com a segurança da informação pode ser observada também nas divulgações e comunicações relativas a normas e padrões de segurança da informação.

b. Organização e competências

Segundo levantamentos com a área de Desenvolvimento Organizacional, a estruturação da área de segurança da informação na VISANET é formada por três gerências ligadas diretamente ao diretor executivo de risco, com o papel de *CRO – Chief Risk Officer*. Diferentemente das demais gerências não existe um diretor intermediário entre os gerentes e o diretor executivo. Segundo o gerente de segurança da informação, esta estruturação permite maior velocidade para tratamento dos assuntos.

A estrutura organizacional para área de segurança da informação na VISANET é a seguinte:

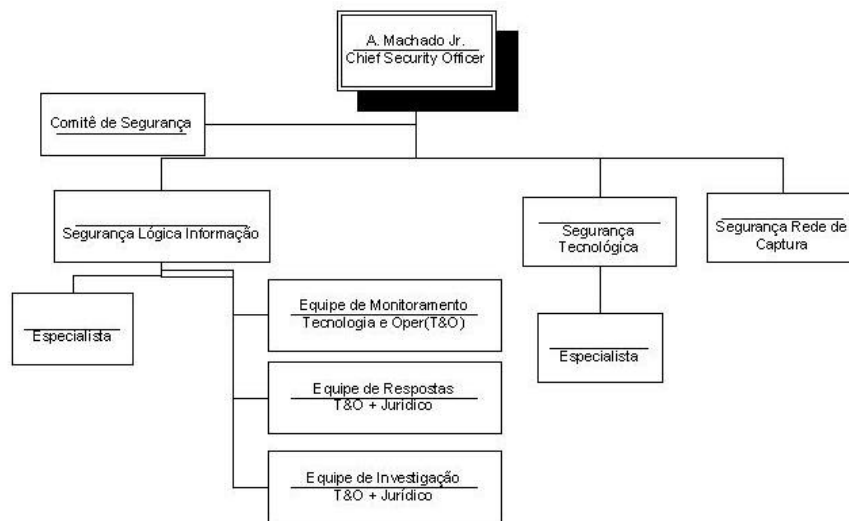


Figura 35: Estrutura Organizacional da área de segurança
(elaborado pelo autor)

A gerência de segurança da informação trata exclusivamente das questões de segurança da informação relativas a área corporativa da empresa. Ou seja, ela é responsável por toda a segurança das informações que trafegam dentro da empresa. Esta gerência é composta pelo gerente de segurança da informação e dois analistas em segurança da informação.

A gerência de segurança tecnológica é especializada nas questões de segurança relativas as tecnologias criptográficas aplicadas na ponta da rede de captura (entenda-se estabelecimento comercial) e no servidores de processamento das transações (dentro da VISANET). Esta gerência é composta pelo um gerente de segurança tecnológica e um especialista técnico.

E a gerência de segurança da rede de captura é responsável por tratar as questões de segurança do meio pelos quais os dados trafegam e são manipulados através da rede de captura. São analisados os riscos de segurança da informação em estabelecimentos que possuem uma rede interna distribuída, como por exemplo uma rede de supermercados, onde as informações dos cartões são armazenados, manipulados e transmitidos internamente antes do envio a VISANET. Esta gerência é composta apenas pelo gerente de segurança da rede de captura.

Como pode se observar, a área de segurança da informação é bastante enxuta. Segundo o gerente de segurança da informação, trabalhos específicos e pontuais em segurança da informação são implementados por fornecedores. Avaliações e implementações tecnológicas são realizadas através do acionamento de outras áreas dentro da empresa. Por exemplo, a área de segurança da informação não é responsável por disponibilizar a infra-estrutura tecnológica necessária, cabe a área de Tecnologia & Operações desempenhar essa função. Além desta, outras atividades da área de segurança da informação serão suportadas por outras áreas da VISANET, como por exemplo, Departamento Jurídico, Departamento Organizacional, Segurança Patrimonial, etc.

Conforme a explicação do gerente de segurança da informação, a equipe de monitoramento e resposta são equipes multidisciplinares formadas através de equipes pertencentes a área de Tecnologia & Operações e Risco & Fraude.

Segundo o gerente de segurança da informação, a VISANET possui um comitê de segurança da informação desde a sua criação. No entanto, até o final do ano de 2001, era composta por membros das áreas de Tecnologia & Operações e Risco & Fraude. A partir do ano de 2002, com a reestruturação das áreas, o comitê atual se tornou uma equipe multidisciplinar, envolvendo todas as áreas da empresa exceto a área de Vendas & Negócio. Participam atualmente deste comitê: um diretor financeiro representando a diretoria executiva de Finanças & Administração, dois gerentes da área de Tecnologia & Operações, um gerente da área de Processos & Auditoria, um diretor do Desenvolvimento Organizacional, uma gerente de Marketing & Produtos, além do próprio diretor executivo de Risco & Fraude e do gerente de segurança da informação.

c. Conformidade e aderência

Em entrevista com o gerente de segurança da informação, os projetos de segurança desenvolvidos pela VISANET estão em conformidade com as necessidades de negócio da VISANET.

Segundo ele, todos os projetos que apresentem riscos para as informações da VISANET, possuem o envolvimento formal da área de segurança da informação, visto que cabe a ela identificar e determinar os controles de segurança necessários para que a integridade, confidencialidade e disponibilidade da informação sejam preservadas.

Este envolvimento formal da área de segurança da informação só é possível devido ao trabalho conjunto com a área de Processos, no qual definiu o fluxo de atividades a serem seguidas para o desenvolvimento de novos projetos.

Além disto, isto permite que a área de segurança da informação esteja em constante contato com os gestores das áreas de negócio facilitando o propósito de identificar as necessidades e riscos de segurança inerentes ao processo produtivo.

d. Política e normas de segurança

Segundo o gerente de segurança da VISANET, no ano de 2001 foi contratada uma consultoria especializada para a elaboração da política de segurança da informação para rede corporativa.

De acordo com ele, ao longo do ano de 2002, a VISANET reestruturou a política e as normas de segurança internamente através do envolvimento e esforços das diversas áreas, acionadas a partir da equipe multidisciplinar do comitê de segurança da informação.

Durante a entrevista com o gerente de segurança da informação foram apresentadas as políticas e normas de segurança da informação da VISANET. Segundo ele, tanto para elaboração quanto para a reestruturação e detalhamento das políticas, foram seguidos rigorosamente as diretrizes da NBR ISO/EC toda as políticas e normas. Por questões estratégicas, a política e as normas de segurança não podem ser apresentadas neste trabalho.

e. Monitoramento e prevenção

Segundo o gerente de segurança da informação, são realizados periodicamente trabalhos com a área de Auditoria e Compliance para avaliar se os controles e responsabilidades de segurança definidos por meio das Políticas, Normas e Procedimentos de Segurança da informação, após publicação dos mesmos, estão sendo adequadamente cumpridos. Este monitoramento é necessário pois os bancos associados e acionistas realizam auditorias constantemente.

f. Treinamento e conscientização

Segundo entrevista com o Security Officer, garantir a segurança das informações é uma responsabilidade de todos os funcionários, prestadores de serviço e demais indivíduos que tenham acesso as informações e recursos do ambiente da VISANET. Por isso no ano de 2002, a VISANET realizou um treinamento de conscientização da segurança da informação para mais de 600

peçoas, englobando funcionários e todos os prestadores de serviços. Estas sessões contemplaram, dentre outros aspectos, os seguintes:

- ▬ a importância da Política de Segurança da Informação;
- ▬ aplicabilidade das Normas de Segurança;
- ▬ descrição dos principais elementos de segurança do ambiente de tecnologia (segurança física e segurança lógica);
- ▬ engenharia social;
- ▬ descrição do propósito da Análise de Risco realizada pela VISANET;
- ▬ penalidades decorrentes da não aderência a Política de Segurança da Informação;
- ▬ procedimentos para reporte de incidentes, falhas de segurança e suspeitas de fraudes;
- ▬ os riscos que a VISANET está sujeita decorrentes de falhas de segurança;
- ▬ casos práticos ocorridos na VISANET decorrentes de falhas de segurança;
- ▬ medidas de prevenção contra incidentes já ocorridos; e
- ▬ classificação das informações.

Ao final da sessão de conscientização ou do treinamento de segurança os funcionários e prestadores de serviço foram submetidos a uma avaliação, o que permitiu a VISANET mapear o nível de conscientização de segurança de seus colaboradores, possibilitando identificar falhas ocorridas no processo, e assegurando a efetividade de cada elemento do programa de conscientização.

Além disto, segundo o gerente de segurança da informação, foram adotadas as seguintes medidas para a conscientização de seus funcionários e prestadores de serviço:

- ☞ periodicamente, são anexados *posters* em pontos estratégicos, com pequenas mensagens sobre segurança. Os *posters* são realocados periodicamente de forma a evitar que passem despercebidos;
- ☞ são distribuídos, periodicamente, folhetos informativos que contenham artigos sobre segurança e casos práticos ocorridos;
- ☞ serão distribuídos prêmios e brindes que contenham bons empenhos de segurança ou idéias que reforçarão a atitude da companhia no sentido da segurança;
- ☞ serão adotadas competições para motivar os funcionários e prestadores de serviço na aderência as medidas de segurança; e
- ☞ será avaliada a efetividade do Programa de Conscientização por meio de pesquisas e questionários, das avaliações dos cursos e dos treinamentos realizados, da frequência e tipo de falhas de segurança ocorridas no ambiente da VISANET.

4.2.2. Segurança das operações

De acordo como gerente de segurança da informação, a VISANET é obrigada a seguir os padrões de segurança definidos pela VISA International, com a possibilidade de pesadíssimas multas no caso de não cumprimento. Para isto a VISA International disponibiliza os seguintes guias: *Visa Account Information Security - Best Practices Guide: 4.9 Software* e *Visa Account Information Security - Standards Manual: 4.6 Software*. Devido a isto, a área de segurança é responsável por dar o devido direcionamento em diversas implementações em segurança tecnológica.

a. Arquitetura de Segurança e Segurança das operações

Em relação a segregação de funções, através de entrevistas com analistas da área de Tecnologia & Operações foram encontradas uma boa segregação nas funções de tecnologia em relação à:

- ☞ operações e programação de aplicações;
- ☞ operações e agendamento da produção;
- ☞ operações e análise de controle de *jobs*;
- ☞ operações e controle de documentação;

- ▬ operações e *help desk*;
- ▬ operações e administração do banco de dados;
- ▬ operações e sistemas de segurança; e
- ▬ operações e gerência de mudanças; dentre outros.

Em entrevista com o gerente de segurança da informação, os aplicativos e documentos recebidos do meio externo são sempre ser verificados quanto à existência de vírus antes de serem inseridos no ambiente da VISANET, o mesmo processo é realizado com os documentos recebidos via *e-mail*, que neste caso são checados no momento em que forem recebidos no servidor de *Webmail*.

O *software* de antivírus está instalado nos *desktops*, em dispositivos de acesso remoto, servidores e *gateways* de Internet e a proteção também é integrada com navegadores *Web* para verificação de *ActiveX* ou Java *applets*. A VISANET utiliza uma combinação de *gateway* vírus *scanners* e produtos para *desktops* a fim de aumentar a possibilidade de identificar códigos potencialmente maliciosos.

A VISANET possui procedimentos formais para detecção e combate à infestação por vírus. Esse procedimento foi elaborado pela área de Tecnologia & Operações responsável pelas estações de trabalho em conjunto com a área de Segurança da Informação.

Os equipamentos em manutenção são verificados quanto à existência de vírus antes de serem conectados na rede interna da VISANET.

Os equipamentos infestados por vírus são isolados da rede interna da VISANET até que se tenha certeza de que o problema foi solucionado e não haja nenhum risco de proliferação do vírus.

Os incidentes com vírus ocorridos no ambiente interno da VISANET não são divulgados para entidades externas à VISANET.

Foi encontrado as diversas alternativas para geração dos *backups* dos sistemas e informações de forma a assegurar o sucesso do mesmo:

- ✎ Normal: efetua cópias de segurança de todos os arquivos e marca cada um para ser copiado em *backup*;
- ✎ Incremental: copia somente aqueles arquivos que sofreram modificações desde o último *backup* incremental;
- ✎ Diferencial: efetua a cópia somente daquelas informações que sofreram alterações desde o último *backup* normal; e
- ✎ Diário: armazena todos os arquivos selecionados que sofreram modificações naquele dia.

A VISANET definiu os procedimentos para geração, teste e restauração das mídias de *backup* gerados. Neles estão inclusos as seguintes informações:

- ✎ sistema utilizado para geração de *backup*;
- ✎ periodicidade de gravação da informação;
- ✎ definição das informações a serem geradas cópias de segurança, bem como os aplicativos que as geraram quando necessário;
- ✎ forma de armazenamento (incluindo procedimentos para armazenamento *off-site*);
- ✎ tabela de erros esperados e tratamento para os mesmos;
- ✎ identificação apropriada das mídias;
- ✎ instruções para restauração das mídias; e
- ✎ ambiente a ser utilizado para teste de restauração das mídias.

Todas as cópias de segurança geradas são registradas, permitindo dessa forma sua rastreabilidade e controle.

Para cada informação pela qual foram geradas cópias de segurança, são gravadas duas mídias distintas na VISANET, sendo que uma delas é armazenada *off-site*, pois caso ocorram incidentes que prejudiquem todo o *site* principal, é possível efetuar a restauração das informações a partir das mídias armazenadas remotamente.

De acordo com a área de Conformidade & Processos, a VISANET efetua um controle efetivo dos equipamentos de *POS* em posse de terceiros. A realização deste inventários permite a VISANET identificar o real valor dos ativos que possui. Os equipamentos de *POS* adquiridos são registrados em um

inventário no momento da aquisição dos mesmos. Este inventário contém informações como:

- ▬▬ descrição do equipamento;
- ▬▬ descrição do sistema instalado (quando aplicável);
- ▬▬ fabricante;
- ▬▬ marca;
- ▬▬ modelo;
- ▬▬ número de série;
- ▬▬ empresa de manutenção onde está alocado o equipamento;
- ▬▬ configurações do equipamento; e
- ▬▬ localização do equipamento.

A VISANET estuda a possibilidade de serem adotados sistemas automatizados para efetuar o controle e registro do inventário de equipamentos POS.

Segundo entrevista com o gerente de qualidade, a VISANET possui seus procedimentos formalmente documentados para as seguintes áreas:

- ▬▬ Intercâmbio;
- ▬▬ Processamento EDS;
- ▬▬ Afiliação de Estabelecimentos;
- ▬▬ Conferência Financeira;
- ▬▬ Liquidação Financeira; e
- ▬▬ *BackOffice*.

Foi designado um funcionário na área de negócio pela documentação formal dos procedimentos executados pela área. Esse funcionário é um profundo conhecedor das atividades realizadas pela área. O procedimento contém, dentre outros:

- ▬▬ descrição das atividades a serem executadas;
- ▬▬ entradas utilizadas e as saídas esperadas;
- ▬▬ parâmetros ou configurações necessárias;

- ▬▬ abrangência do procedimento;
- ▬▬ aplicação;
- ▬▬ responsabilidades;
- ▬▬ indicadores que permitam avaliar se os resultados obtidos estão dentro do esperado;
- ▬▬ ações a serem realizadas em caso de problemas;
- ▬▬ responsáveis a serem acionados em caso de problemas; e
- ▬▬ glossário contendo a definição de terminologias próprias do negócio ou de tecnologia utilizada.

Segundo ainda ele, todos os procedimentos são periodicamente revisados, e sempre que os processos sofram alterações significativas que impactem no conteúdo dos mesmos. Os procedimentos são formalmente implementados, o que permite a identificação de inconsistências no detalhamento dos mesmos. Estes estão acessíveis somente para os funcionários autorizados, que deles necessitam para a execução de suas atividades. Todos os procedimentos são revisados pelo Gestor da Área, de forma a assegurar que o documento represente corretamente a forma de atuação da VISANET.

Em entrevista com o gerente de segurança da informação, todos os funcionários da VISANET foram instruídos a não armazenarem informações referentes as atividades que desempenham no *hard-disk* de suas estações trabalho. Num primeiro momento, a VISANET dimensionou e disponibilizou um espaço em rede necessário para transferências das informações das estações de trabalho para o servidor, e em seguida solicitou que todas os funcionários efetuem a transferência das informações consideradas críticas. Periodicamente, a área de Segurança da Informação escolhe uma amostra (principalmente nas áreas mais críticas) com o propósito de assegurar que o procedimento correto tenha sido adotado. Os funcionários que não estiverem cumprindo a norma e não apresentarem uma justificativa válida de negócio, são punidos de acordo com as penalidades definidas na Políticas e Normas de Segurança da Informação.

Em entrevista com a área de auditoria, a VISANET contém trilhas de auditoria com as seguintes principais informações:

- ▬▬ a identificação do usuário;

- ▬ a data e a hora da operação;
- ▬ os tipos de operações realizadas;
- ▬ módulo utilizado para execução da operação; e
- ▬ um *flag* indicando a gravidade do evento ocorrido.

Dependendo da criticalidade do módulo, conforme definido pelo proprietário do sistema, são incluídas informações adicionais na trilha de auditoria.

Segundo o gerente de segurança da informação, o acesso as trilhas de auditoria é restrita ao proprietário do sistema, a área de segurança da informação e a área de auditoria. Existe uma segregação de funções entre a pessoa que está realizando a revisão das trilhas de auditoria e o responsável pela execução das atividades que estão sendo monitoradas.

De acordo com o gerente de segurança da informação, a VISANET possui métodos de análise de risco constituídos pelas seguintes etapas:

- ▬ Definição do escopo;
- ▬ Envolvimento de representantes das áreas chaves da organização, tais como os gestores do negócio, usuários chaves, profissionais de Tecnologia da Informação -TI (para as aplicações consideradas críticas ao negócio) e pessoas com experiência em análise de risco para auxiliar o processo de coleta e análise das informações pertinentes;
- ▬ Determinação do risco do negócio levando em consideração a criticalidade da operação, o impacto causado ao negócio da VISANET em caso de perda de confidencialidade, integridade ou disponibilidade, e as vulnerabilidades;
- ▬ Consideração as vulnerabilidades conhecidas; e
- ▬ Monitoração da efetividade deste trabalho.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
			Ponto de dependência financeira (R&D)			Risco de perda de produtividade (distúrbio das transações operacionais (processador))			Violação da legislação ou contratos estabelecidos			Comprometimento da imagem/reputação			Perda de oportunidade de negócio			Interrupção das atividades do negócio		
			A	M	B	A	M	B	A	M	B	A	M	B	A	M	B	A	M	B
1																				
2																				
3																				
4	Disponibilidade	Redução do número de socos Estabelecimentos Comerciais afetados																		
5	Confidencialidade	Diligência da Base de Estabelecimentos Comerciais																		
6		Pagamento equivoocado para Estabelecimentos Comerciais																		
7		Cobrança de taxas acima do abato do autor apropiado																		
8	Integridade	Envio de mensagens de transações, supérfluas e sobrecarga para Estabelecimentos Comerciais em massa																		
9		Aumento no número de transações rejeitadas																		
10		Ativação automática PDH/DPH																		
11	Disponibilidade	Redução do número de estabelecimentos afetados																		
12		Instalação de manutenção nos equipamentos com problemas																		
13	Confidencialidade	Diligência da Base de Estabelecimentos Comerciais																		
14		Instalação de equipamentos em endereço incorreto																		
15	Integridade	Controle físico dos Estabelecimentos que possuem equipamentos pertencentes à Visanet																		
16		Equipamentos afetados com mesmo número lógico																		
17		Aumento do número de transações rejeitadas																		
18		Automação Manual																		
19	Disponibilidade	Redução do número de transações feitas pelos portadores de cartão																		
20		Impossibilidade do cancelamento de transações																		
21	Confidencialidade	Diligência do número de cartões de crédito válidos																		

Figura 36: Matriz de risco: processo x CIA x impacto
(VISANET)

Os resultados da análise de risco ainda incluem uma clara indicação dos principais riscos associados, um diagnóstico dos impactos potenciais ao negócio e recomendações para as ações necessárias visando reduzir o risco a um nível aceitável.

Nº da Macro Ação	Macro Ações	Nº da Ação na Matriz	Risco Ocorrência	Tempo Implementação	Investimento Financeiro	Impacto
1	Revisão dos controles do processo captura manual		2,2	2,4	1,4	1,8
	Grupo de Análise e Prevenção	4	3	2	1	2
	Lacre dos maletins	2	2	2	1	2
	Planos	5	2	2	1	2
	Cópia verificador base 10	6	2	3	3	1
	Controle Resumo das Operações	1	2	3	1	2
	Processo abertura de maletins	3	1	1	1	2
2	Formalização de procedimentos		6	4	2,5	4,5
	Procedimento de Custódia de Senhas	0	3	1	1	2
	Processamento Interchange	8	3	1	1	2
	Procedimentos da Área de Produção	7	3	2	1	2
	Procedimentos formalmente documentados - Intercolinas	12	3	2	1	2
	Procedimento formalizado correção de problemas	48	3	2	1	2
	Procedimentos de Controle de Equipamentos	9	3	2	1	2
	Procedimentos de Backup e Restore	40	3	2	1	2
	Procedimentos Operacionais	42	3	2	1	2
	Plano de Contingência	41	3	3	3	3
3	Revisão dos contratos firmados com prestadores de serviço		2,75	1,5	1	2,5
	Processamento Interchange	8	3	1	1	2
	Acordo de Nível de Serviço	8	3	2	1	2
	Acordo de Nível de Serviço B2B	15	3	2	1	2
	Quantidade transações processadas Interchange	13	2	1	1	2
4	Integração base plataforma mainframe		3	3	3	3
	Transporte de CDs	10	3	3	3	3
5	Política, normas e procedimentos de controle de acesso		3,45-45-455	2,22-22-223	1,22-22-227	3,18-18-2
	Usuário genérico	30	3	1	1	3
	Controle de Acesso ao Sistema Online de Cartas	44	3	1	1	3
	1. Instalação de dispositivos de segurança habilitados	83	3	1	1	3

Figura 37: Matriz de avaliação dos riscos

(VISANET)

São realizados ainda testes de penetração para avaliação dos riscos tecnológicos através de uma metodologia estruturada para a sua aplicação. Os testes, por sua vez, consideram os seguintes objetivos:

- ✎ Analisar as reais ameaças para o ambiente tecnológico alvo;
- ✎ Proporcionar uma análise dos impactos das vulnerabilidades técnicas identificadas relacionando-as aos riscos potenciais ao negócio; e
- ✎ Assegurar a análise da segurança realizada e garantir a identificação dos riscos.

Com relação a periodicidade dos testes, a VISANET realiza-os com uma frequência pelo trimestral, ou quando a área responsável pela análise de risco julgar necessário.

Adicionalmente, a VISANET contrata consultorias externas especializadas pois desta forma, é possível adotar uma visão externa e imparcial para a real análise dos componentes de segurança utilizados no ambiente computacional, tendo em vista que muitas vezes uma visão interna pode não identificar todas as vulnerabilidades de presentes no ambiente.

b. Telecomunicações

Segundo entrevista com o gerente de tecnologia da rede corporativa, a VISANET assegura o controle rígido quanto a instalação de *modems* na rede corporativa. Só é possível *modems* em equipamentos previamente autorizados. Em entrevista com o gerente de tecnologia da rede de captura, o mesmo tipo de controle é realizado na rede de captura.

Conforme conversa com o gerente de segurança patrimonial, a VISANET possui controles relacionados a segurança física e patrimonial dos ativos visando a manutenção das operações e dos serviços relacionados ao PABX. A estrutura de armazenamento do sistema de PABX é discreta e mostra o mínimo sobre o seu propósito.

De acordo com a coordenadora técnica responsável pelos firewalls da VISANET, são aplicados de todos *patches* e atualizações pertinentes. Os *backups* do *firewall* são executados internamente através em um mecanismo *tape drive*. Os *firewalls* registram todas as atividades inclusive aquelas realizadas pelos administradores. O protocolo *Network Time Protocol - NTP* é usado para sincronizar os registros com outros sistemas registradores tais como a detecção de intrusão.

Conforme o gerente de segurança da informação, todo o cabeamento pertencente a VISANET é estruturado. São ainda verificados periodicamente as estruturas de cabeamento nos principais fornecedores: EDS, PROCEDA, INTERCHANGE, etc.

Com relação a segurança da LAN, a VISANET considera dois aspectos fundamentais:

- ✍ Estruturação e gerenciamento de dados centralizados apropriados, o qual contemple medidas como a realização de *backup*, contingência entre outras; e
- ✍ As estações de trabalho possuem mecanismos adequados de proteção. Para minimizar os riscos dessa situação, utiliza-se ferramentas que protejam os dados contidos nos discos locais como, por exemplo, através do emprego de recursos criptográficos.

Em relação a computação remota, de acordo com o gerente de segurança da informação, são utilizados *tokens* em combinação com senhas fortes para identificar e autenticar as solicitações dos usuários remotos. Além disso, o emprego de VPN na VISANET é utilizado para garantir a privacidade utilizada durante a transmissão das informações.

Durante os levantamentos, a VISANET estava homologando a implantação de soluções *wireless* para a rede corporativa. Uma preocupação do gerente de segurança corporativa é assegurar o emprego de mecanismos de segurança física, *Public Key Infrastructure - PKI* e utilização do *Wireless transport layer security protocol - WTLS* em aplicações WAP.

Segundo o gerente de telecomunicações, a sua área em conjunto com a área de segurança da informação atenta o modo que os fornecedores de *links* terrestres endereçam os princípios básicos relacionados a segurança da informação (privacidade dos dados, integridade, disponibilidade e confidencialidade) durante a prestação de serviços à VISANET.

Em relação ao uso área de segurança da informação em conjunto com a área de qualidade e processos definiram as normas para concessão de acesso à Internet, assim como o uso da mesma.

Em relação a intranet, a VISANET possui os controle de segurança sobre os *Webservers* seguindo as seguintes melhores práticas de mercado:

- ✂ ✂ Atualização de *software* e instalação de *patches* - Essa medida é uma das mais simples e ainda mais eficientes técnicas para reduzir os riscos e vulnerabilidades.
- ✂ ✂ Utilização dos servidores para uma única finalidade - Os *Webserver* devem ser dedicados exclusivamente a uma tarefa/ serviço a ele associado.
- ✂ ✂ Remoção das aplicações desnecessárias - *Software* privilegiados são definidos como aqueles que funcionam com privilégios de administrador. Todo *software* privilegiado que não for especificamente exigido para o funcionamento dos servidores deve ser identificado e removido.
- ✂ ✂ Proteção do Servidor com Filtro de Pacotes ;
- ✂ ✂ Segregação dos privilégios - A segregação de privilégios é um conceito chave para a proteção do *host* quando esse eventualmente for penetrado. Para tanto, deve-se estabelecer controles os quais utilizem contas distintas para o funcionamento dos diversos serviços utilizados pelo *webservers*.

Durante os levantamentos, a VISANET estava avaliando a implementação de uma metodologia de codificação segura a ser disponibilizada nos diversos projetos de desenvolvimento internos e também como referencial para os acordos de nível de serviço em projetos de desenvolvimento efetuados por terceiros que serão disponibilizados na *intranet*.

Conforme entrevista com o gerente de segurança da informação, a construção das VPNs que suportam as comunicações da VISANET foi implementada com base na aplicação das melhores práticas, seguindo os padrões de mercado.

De acordo com entrevista com o gerente de segurança da informação, para garantir a confidencialidade, a integridade e a disponibilidade dos serviços ao correio eletrônico a VISANET adota as seguintes medidas, dentre outras:

☞ As mensagens de *e-mail* são verificadas a fim de identificar:

- Códigos maliciosos;
- Expressões ofensivas; e
- Frases chaves conhecidas, como aquelas normalmente usadas em correntes de *e-mail*.

☞ Os sistemas de *e-mail* são protegidos:

- Bloqueando mensagens que se originam de *sites* ou usuários indesejáveis, por exemplo, evitar o *spamming*;
- *Hashing* de mensagens ajudando a manter a integridade daquelas que são confidenciais; e
- Garantindo a não repúdio das mensagens, por exemplo, provando a origem de uma mensagem usando mecanismos de assinaturas digitais.

Além disso, segundo ele, a VISANET define uma política relativa ao assunto privacidade e de monitoração das contas de *e-mail*. Através do teste interno de dados, a área de segurança da informação assegura a correção do risco de *relay de fake-mail*

Segundo o gerente de segurança da informação, através de IDS, usando técnicas de monitoramento dos eventos que ocorrem em um sistema computadorizado ou em uma rede, a VISANET está apta a prevenir, detectar, corrigir e reportar intrusão ocorridas em seu sistemas e na rede. As intrusões podem ser causadas por usuários não autorizados que tentam acessar os sistemas/redes, ou por usuários autorizados que tenta ganhar privilégios adicionais os quais esse não está autorizado.

c. Segurança física

Segundo o gerente de segurança da informação, a VISANET implementa os seguintes controles que julga necessários:

- ☒☒ Identificação de todos os funcionários por meio de crachá;
- ☒☒ Utilização de fechaduras especiais (*Eletronic Key System, Eletronic Combination Locks*) com combinações individuais de acesso nas salas onde os equipamentos críticos encontram-se instalados;
- ☒☒ Sistema de autenticação biométrica;
- ☒☒ Ante-sala utilizando o conceito de *man trap*;
- ☒☒ Uso de catracas eletrônicas para a restrição de acesso nas entradas dos locais;
- ☒☒ Monitorando dos ambientes 24 (vinte e quatro) horas por dia através de vigilantes;
- ☒☒ CPD com piso elevado;
- ☒☒ Utilização de desumidificador na fitoteca;
- ☒☒ Sistema de ventilação exclusivo;
- ☒☒ Sinalização indicativa de emergência;
- ☒☒ Extintores de incêndio contemplando as quatro classes de materiais combustíveis;
- ☒☒ Detectores de temperatura, água e fumaça; e
- ☒☒ Sistema para a contenção de incêndios.

Segundo ele, a VISANET também utiliza diversos mecanismos que auxiliam o controle de acesso físico. Entre as principais medidas adotadas estão:

- ☒☒ Uso de catracas eletrônicas para a restrição de acesso nas entradas dos locais;
- ☒☒ Monitorando dos ambientes 24 (vinte e quatro) horas por dia por meio de vigilantes;
- ☒☒ Identificação de todos os funcionários por meio de crachá; e

- ✎✎ Utilização de fechaduras especiais (Eletronic Key System, Eletronic Combination Locks) com combinações individuais de acesso nas salas onde os equipamentos críticos encontram-se instalados.

A VISANET possuem também as seguintes medidas relacionadas ao acesso físico:

- ✎✎ Todos os visitantes são identificados e são acompanhados pelos funcionários responsáveis;
- ✎✎ Todos os empregados, parceiros e prestadores de serviço estão devidamente identificados, por meio da utilização de crachás;
- ✎✎ Os crachás são usados sempre em local visível;
- ✎✎ Todos os empregados tem a obrigação de comunicar imediatamente a área de responsável a perda do crachá. Os parceiros e prestadores de serviço devem comunicar aos seus responsáveis na VISANET pela perda do crachá
- ✎✎ Os crachás extraviados são bloqueados imediatamente, restringindo seu uso.

Com relação a utilização de dispositivos portáteis por funcionários da VISANET, como *notebooks* são adotadas as seguintes medidas relacionadas a segurança:

- ✎✎ Utilização de cadeados nas mesas/dockstations para se evitar furtos;
- ✎✎ Sistema que bloqueia inicialização dos equipamentos utilizando senhas fortes;
- ✎✎ Autenticação Forte com mais um fator como, por exemplo, uso de um token;
- ✎✎ Utilização de sistema operacional com configurações de segurança nível C2 da Trusted Computer System Evaluation Criteria-TCSEC; e
- ✎✎ Ferramentas para criptografia dos dados contidos no disco rígido.

A VISANET assegura que os dispositivos de controles preventivos do sistema de suporte ambiental operam com as mínimas condições adequadas e que atendam os requisitos de segurança. Para isto são utilizados os principais controles:

- ✎✎ Protetores de picos de energia;

- ✎✎ Instalação de reguladores automáticos de energia (Estabilizadores de linha);
- ✎✎ Nobreak;
- ✎✎ Geradores Elétricos; e
- ✎✎ Cabeamento estruturado.
- ✎✎ Realização de manutenção preventiva segundo padrões e procedimentos do fabricante; e
- ✎✎ Utilização de geradores de energia para suportar os equipamentos das áreas consideradas críticas.

d. Desenvolvimento de sistemas

Segundo o gerente de segurança da informação, alguns controles são adotados para assegurar a segregação de ambientes:

- ✎✎ Os sistemas em desenvolvimento e produção, operam em diferentes microcomputadores, ou diferentes domínios ou diretório;
- ✎✎ As atividades de teste e desenvolvimento estão segregadas;
- ✎✎ Diferentes procedimentos de logon são utilizados para os ambientes de produção e testes, reduzindo assim o risco de erros. Os usuários são forçados a utilizar diferentes senhas para estes ambientes.

A grande maioria dos sistemas desenvolvidos para a VISANET possuem documentação técnica e para os usuários. A documentação técnica possibilita que qualquer funcionário consiga efetuar alterações, correções ou parametrizações a partir desta. Esta documentação deve ser precisa, completa e prática. Dentre outros itens, ela contém:

- ✎✎ consistente descrição dos requisitos, projetos e funções;
- ✎✎ data e versão das modificações;
- ✎✎ requisitos necessários para funcionamento;
- ✎✎ uso de tabelas, índices, glossários;
- ✎✎ organização lógica; e
- ✎✎ terminologia utilizada.

Outra preocupação destacada pelo gerente de segurança da informação é que o acesso a documentação técnica esteja restrito aos funcionários autorizados.

Segundo ele, os testes de aceitação na VISANET seguem as seguintes diretrizes:

- ▣ envolver os usuários da área de negócio;
- ▣ simular o ambiente de produção;
- ▣ envolver todo o conjunto que suporta o sistema, tais como funcionalidade da aplicação, gerenciamento do banco de dados e o sistema operacional de suporte;
- ▣ realizar avaliações da segurança do sistema; e
- ▣ incluir tentativas de quebra de segurança do sistema.

São verificados ainda:

- ▣ a completa funcionalidade dos requisitos de negócio;
- ▣ a funcionalidade dentro de condições normais e em caso de exceções;
- ▣ o impacto de dados incorretos;
- ▣ a interface com outros sistemas, tais como chamadas de outros programas e *hyperlinks*;
- ▣ a efetividade dos controles;
- ▣ a performance do sistema quando lidando com grandes volumes de trabalho (por exemplo testar o volume real dos dados manuseados/transações efetuadas);
- ▣ identificação da capacidade máxima do sistema;
- ▣ os critérios de validação dos dados durante a entrada de informações;
- ▣ a funcionalidade dos controles de acesso instaurados; e
- ▣ a funcionalidade das trilhas de auditoria.

Segundo o gerente de desenvolvimento, os procedimentos antes do desenvolvimento dos aplicativos ser conferida a terceiros a VISANET são:

- ▣ verificar a idoneidade do prestador;
- ▣ identificar sistemas críticos cujo desenvolvimento seja interessante mantê-lo internamente;
- ▣ realizar um processo formal para seleção de terceiros;

- ✍✍ identificar os riscos e avaliar as práticas de segurança empregados pelos prestadores de serviço; e
- ✍✍ acordar os controles de segurança.

O contrato formal estabelecido entre a VISANET e o prestador de serviço determina as seguintes obrigações para o prestador de serviços:

- ✍✍ obedecer as boas práticas de negócio, reportar os incidentes e fornecer relatórios periódicos sobre a atividade de desenvolvimento;
- ✍✍ manter a confidencialidade/integridade da informação obtida na execução do trabalho, limitando o acesso a usuários não autorizados;
- ✍✍ manter a continuidade dos negócios no caso de um incidente/desastre;
- ✍✍ aplicar controles de segurança, assegurando o cumprimento dos requisitos legais, incluindo a privacidade dos dados;
- ✍✍ permitir que suas atividade sejam auditadas; e
- ✍✍ estabelecer um critério de compensação se os objetivos do serviço não forem atendidos.

e. Resposta à incidentes

Segundo o gerente de segurança da informação, a VISANET possui uma política relacionada ao Plano de Contingência contendo:

- ✍✍ os propósitos do Plano de Contingência;
- ✍✍ situações em que o Plano de Contingência deverá ser utilizado ;
- ✍✍ as ações a serem tomados imediatamente após a ocorrência de um sinistro;
- ✍✍ os procedimentos detalhados a serem seguidos em caso de emergência;
- ✍✍ as atribuições de todos os envolvidos na recuperação do ambiente;
- ✍✍ listas de contatos, mapas da rede, diagramas e outras informações que auxiliem no processo de recuperação do ambiente de tecnologia;
- ✍✍ ações/listas de serviço a serem recuperados em ordem de prioridade; e
- ✍✍ controles de segurança a serem adotados durante a recuperação.

4.2.3. Gerenciamento de Identidades

a. Administração de usuários e workflow

Conforme entrevista com a área de segurança, a VISANET definiu um processo único de concessão de acesso a todas as plataformas e sistemas. Esse processo é suportado por um sistema de workflow, o qual permite garantir a autenticidade do solicitante e do aprovador, bem como otimizar todo o processo de concessão de acesso.

A solicitação de acesso é iniciada pela área de Desenvolvimento Organizacional, no momento da contratação, a qual indicará que o cargo do funcionário na VISANET, permitindo a partir daí os sistemas identificarem os privilégios mínimos necessários que o funcionário poderá receber. Desta maneira, a VISANET possui um mapeamento de todos os privilégios existentes, de acordo com o cargo do funcionário e/ou prestador de serviço.

Segundo o gerente da área, os principais benefícios decorrentes da adoção da estratégia de Gerenciamento de Identidades são:

- ▣ Redução no prazo para concessão de acesso;
- ▣ Redução do custo do processo em função da centralização da administração dos usuários;
- ▣ Aumento da aderência a Política de Segurança da Informação da companhia;
- ▣ Permite um processo contínuo de auditoria das regras de negócio adotadas para concessão de acesso;
- ▣ Permite a revogação imediata do acesso do funcionário em todos os sistemas que o mesmo acessava; e
- ▣ Adoção de um repositório único utilizado por toda a corporação.

b. Gerência de permissões

Segundo o gerente de segurança da informação, a VISANET adota o princípio do mínimo privilégio no qual é realizada a concessão a seus funcionários somente os privilégios necessários para a execução de suas tarefas. A adoção do menor privilégio não impede que alguns funcionários tenham privilégios significativos, desde que suas funções justifiquem a necessidade dos mesmos. A adoção desse critério reduz o número de perdas resultantes de acidentes, erros ou uso não autorizado do sistema.

c. Estrutura de Diretório

Segundo o gerente de segurança da informação, apesar dos serviços de diretórios poderem fornecer uma solução adequada de aplicação da política de segurança, para que seja completamente efetiva, esta precisa estar alinhada com políticas de segurança corporativa, normas e procedimento da VISANET. Devido a este fato, a implementação da estrutura de diretórios para rede corporativa na VISANET ainda está sendo elaborada, principalmente porque as políticas necessitam detalhar e complementar os processos de autenticação, controle de acesso, encriptação e trilhas de auditoria.

d. Criptografia

De acordo com a entrevista com o gerente de segurança da informação, a VISANET possui os seguintes aspectos para a implementação do ciclo de vida do produto criptografado:

- ⌘ *Hardware/firmware* (ex.: novas capacidades, expansão do sistema para acomodar mais usuários, substituição de equipamentos fora de funcionamento, mudança de plataforma e atualização de componentes de *hardware*;
- ⌘ *Manutenção/atualização de software* (ex.: novas capacidades, arrumando erros, melhorando a performance e substituição de chaves);

- ✍✍ Manutenção da aplicação (ex.: mudança de função e responsabilidades, atualizações remotas, atualização de senhas e exclusão de usuários da lista de acessos);
- ✍✍ Manutenção das chaves (ex.: arquivamento, destruição e a mudança de chaves); e
- ✍✍ Manutenção das permissões de acesso.

Além disto, segundo ele, os testes de certificação são realizados por uma área da organização que não seja o desenvolvedor dentro da organização. Isto se torna necessário para assegurar independência e objetividade no teste. Os testes de certificação são feitos por meio de vários padrões e requisitos particulares da VISANET.

A VISANET avalia a utilização de soluções criptográficas no ambiente como um todo a fim de proteger as informações e passar a utilizar serviços de segurança, como assinaturas eletrônicas.

e. Autenticação Forte

Segundo entrevista com o gerente de segurança tecnológica, a política de senhas utilizada pela VISANET considera os seguintes aspectos:

- ✍✍ critérios de formação da senha de acesso, adoção de senhas seguras;
- ✍✍ troca no primeiro acesso;
- ✍✍ período de expiração: os sistemas utilizados devem estar preparados para efetuar a expiração de senhas;
- ✍✍ configuração do histórico da senha, não permitindo a reutilização das mesmas;
- ✍✍ cuidados a serem adotados com a senha: não anotar a senha em papel, não compartilhar senhas com outros funcionários, não enviar senhas no formato *clear-text*;
- ✍✍ não inserção de senhas nos códigos-fonte e macros;
- ✍✍ procedimentos a serem seguidos no caso do bloqueio do usuário;

- ✂ não armazenamento de senhas no formato *clear-text* impressas ou em arquivos eletrônicos;
- ✂ adoção de senhas de difícil inferência;
- ✂ alteração da senha padrão dos aplicativos;
- ✂ descaracterização das senhas exibidas em monitores e documentos impressos; e
- ✂ não devem ser adotadas senhas de conhecimento genérico.

Além disto, são complementadas através das seguintes diretrizes no tratamento das senhas:

- ✂ estabelecer uma política de controle de acesso;
- ✂ criptografar as senhas durante a transmissão e armazenamento, visto que a rede está suscetível a ataques como *sniffing* e *hijacking*;
- ✂ utilizar aplicações disponíveis para testar a validação das senhas dos usuários (senhas fracas e fortes);
- ✂ desabilitar as contas e senhas inativas por um determinado período de tempo;
- ✂ instruir os funcionários sobre a possibilidade de sua senha ser espiada por outros funcionários;
- ✂ utilizar mecanismos para reduzir o número de tentativas inválidas de logon sem sucesso; e
- ✂ auxiliar os usuários a descobrir se sua senha foi ilicitamente obtida, exibindo a data e hora do último logon com sucesso cada vez que o usuário efetuar sua autenticação. Os usuários devem ser conscientizados sobre a necessidade de observarem a data e a hora e reportarem qualquer anomalia.

Segundo o gerente de segurança da informação, por um lado existem diversas vantagens do sistema de SSO, incluindo conveniência, administração centralizada, auditoria, alarmes, *logon* remoto, e proteção das senhas; mas por outro, a tecnologia SSO é considerada um *single point of failure*.

Tanto para soluções tecnológicas de sistema de SSO, quanto para as soluções tecnológicas para biometria, a VISANET ainda está estudando pesquisando estratégias e formas de implementação.

f. Integração dos sistemas legados

Segundo entrevista com o gerente de segurança da informação, a VISANET implementa projetos para integração da alta e baixa plataforma de modo que tal medida proporcione a integração das aplicações, dados e redes atualmente implementadas na VISANET, preservando assim os investimentos realizados na infra-estrutura lógica. Além disso, essa integração facilita o gerenciamento, a administração, autenticação e controles às requisições providas de ambas plataformas.

5. Discussão dos Resultados

Com o objetivo de estudar e analisar o intento estratégico da VISANET, a partir das entrevistas realizadas, elaborou-se o seguinte modelo baseado nas cinco forças de PORTER (1986) para análise estrutural da indústria de cartão de crédito.

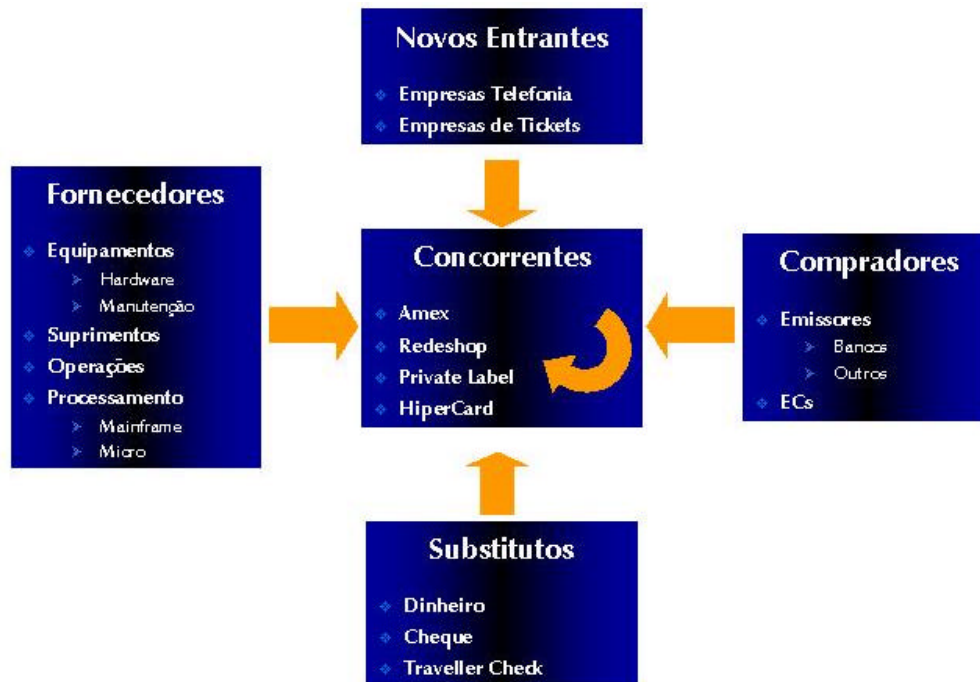


Figura 38: Modelo de forças de Porter aplicado a VISANET

(elaborado pelo autor)

- ✎ Compradores: bancos emissores e estabelecimentos comerciais. Segundo o presidente, existe uma pressão forte por preços pelos estabelecimentos comerciais.
- ✎ Concorrentes: concorrentes diretos da VISANET são: REDECARD e AMEX. Existem os cartões Private Label (emitidos pelos hipermercados, postos de gasolina, dentre outros), mas segundo o presidente da VISANET, não foi realizada nenhuma ação para conter a proliferação desse tipo cartão. No ano de 2000, a REDECARD procurou aumentar sua base de cartões emitidos, conseguindo um volume quase que equiparado ao número de cartões emitidos pela VISA. No segmento de crédito, o *market share* da VISANET atinge a marca de 47,4%. No segmento de débito, a participação da VISANET

alcança 60%. A diferença do alcance maior da VISANET está diretamente relacionado a rede de agências de seus acionistas. Entre os concorrentes diretos não existe briga de preços, pois o componente de custos destas empresas é praticamente igual.

- ✍ Fornecedores: EDS, PROCEDA, INTERCHANGE, etc. Como descrito no capítulo anterior, os fornecedores possuem um forte comprometimento com a VISANET, e possuem uma relação de parceria de ganha-ganha desde o início das operações.
- ✍ Novos entrantes: talvez empresas de telefonia e empresas emissoras de ticket. Segundo um alto executivo da empresa, a VISANET não enfrenta grandes problemas em relação a novos entrantes.
- ✍ Substitutos: dinheiro, cheque e *traveller* cheque. Deles o cheque no Brasil possui a característica de pré-datado, no qual concorre, diretamente com o cartão de crédito.

Além disto, foi elaborada a matriz SWOT a partir das observações realizadas através das várias entrevistas com os executivos da VISANET:

Strengths	Weakness	Opportunities	Threats
<ul style="list-style-type: none"> • Marca Visa; • Único acquire Visa no Brasil; • Oligopólio das bandeiras de cartões; • Solidez dos bancos acionistas e abrangência de suas redes; • Foco • Capital Humano de qualidade e com forte comprometimento. 	<ul style="list-style-type: none"> • Conflito de interesses entre o banco acionista e a Visanet; • Processo de antecipação descentralizado; • Inexistência de legislação que suporte o negócio. 	<ul style="list-style-type: none"> • Meios de pagamentos eletrônicos em expansão; • Novos produtos, ampliando o potencial de crescimento. 	<ul style="list-style-type: none"> • Pressão de preços por parte dos Estabelecimentos Comerciais; • Conflito de interesses do banco acionista; • Economia informal; • Banco do Brasil e Bradesco deixarem de ser acionistas.

Figura 39: Matriz SWOT

(elaborado pelo autor)

E também a cadeia de valor de PORTER (1990) para a VISANET:



Figura 40: Cadeia de valor de Porter aplicada a VISANET

(elaborado pelo autor)

Segundo pode-se observar em entrevista com os principais executivos da VISANET, que o cartão de débito está cada vez mais em expansão pois toda a potencialidade do mercado ainda não foi explorada. A tendência é que o meio de pagamento eletrônico substitua cada vez mais o volume de pagamentos em dinheiro e cheque. Nos últimos anos está ocorrendo uma redução entre o número de cheques compensados e um aumento do número de transações realizadas com cartão de débito. Entretanto, existem algumas características dos cheques que ainda não podem ser substituídas pelos cartões de débito, pois alguns estabelecimentos utilizam os cheques como forma de pagamento aos seus fornecedores sem que haja o depósito em suas contas correntes e conseqüentemente o pagamento de impostos como CPMF e IR. Nesse aspecto, não é interessante para alguns estabelecimentos comerciais, a aceitação de cartão de débito em substituição aos cheques emitidos por seus clientes.

Sob o aspecto legal, foram analisadas também os principais regulamentos que impactaram as atividades da Visanet:

- ▣ Implantação do SPB: A implantação do Sistema de Pagamentos Brasileiro foi encarado como uma oportunidade para a VISANET, pois a tendência é que sejam utilizados cada vez mais meios eletrônicos de pagamento.
- ▣ Lei Federal 9.532, de 10 de dezembro de 1997 que trata sobre a obrigatoriedade do uso de Emissor de Cupom Fiscal:

"Art. 33 - A emissão do comprovante de pagamento relativo a operação ou prestação efetuada por cartão de crédito ou débito automático em conta corrente, por contribuinte obrigado ao uso de equipamento emissor de cupom fiscal (ECF), será efetuada, somente, por meio de equipamento emissor de cupom fiscal (ECF) e o comprovante deverá: I - estar vinculado ao documento fiscal referente à operação ou prestação; II - ser arquivado e conservado, nos termos do art. 193 do Regulamento do ICMS, aprovado pelo Decreto nº 33.118, de 14 de março de 1991." (Portaria CAT-55/98 – Fonte: VISANET)

- ▣ As transações com cartão de crédito passaram a ser consideradas transações em moedas e qualquer crime envolvendo cartões de crédito passou a se enquadrar na legislação de crime financeiro. No entanto, não existem regulamentos específicos para o segmento de cartões de crédito, o que de certa forma acaba por prejudicar o segmento. Por exemplo, em situações de fraude dificilmente o fraudador é punido.

Pode-se observar através desta pesquisa que a VISANET se encontra em um estágio avançado no que diz respeito a segurança da informação. É possível afirmar que os modelos apresentados na fundamentação teórica estão quase que completamente cobertos pelas atividades e funções da área de segurança da informação da VISANET.

Este estágio avançado condiz com a natureza do negócio da indústria de cartões de crédito, onde a proteção às informações são fundamentais tanto para as operações quanto para a imagem da empresa. Pode-se concluir que a empresa se encontra neste estágio de segurança devido, em grande parte, ao comprometimento da alta direção da empresa em relação à segurança da informação. Isto comprova a afirmação de BYRNES (2001), que a estruturação da segurança da informação deve ter a participação ativa dos principais executivos da empresa.

De forma surpreendente, a gestão da segurança da informação na VISANET pode ser caracterizada como centralizada sob os aspectos de gestão. E no entanto, sob a óptica de implementação e execução pode-se dizer que ela é distribuída. Pois, de acordo com as necessidades e conhecimentos específicos a implementação dos controles de segurança de cada assunto, a área de gerenciamento de segurança da informação envolve e aciona as áreas específicas e detentoras dos conhecimentos necessários.

Outra descoberta interessante, é a estruturação da área de segurança de informação subordinada a uma diretoria exclusiva para o gerenciamento do risco. Esta estruturação vai segue a proposta de ROSS e WEILL (2002) mas contrariam a proposta de BYRNES (2001) que sugere a área de segurança subordinada a área de tecnologia de informação. Esta estruturação permite maior independência de atuação e cobrança das questões de segurança da informação nas demais áreas da empresa.

Em termos das políticas e normas de segurança observamos na VISANET foi é um dos primeiros assuntos a serem implementados em termos de segurança da informação, pois provém tanto o direcionamento necessário para organização, quanto o início de conscientização sobre o assunto.

Pode-se observar na prática que a segurança de informação necessita de processos bem definidos e formalizados, conforme propõe VALLABHANENI (2002). Além disto, os processos de segurança encontrados seguiam uma rígida aderência e alinhamento com os processos de negócio da organização, indo de encontro totalmente com a afirmação que a segurança da informação deve ser um processo de negócio, de NAKAMURA (2002).

Foi observado que apesar de bem segregada, a área de Segurança da Informação avalia periodicamente a inexistência de segregação de funções nas áreas críticas. Pode-se observar também que, a área de segurança da informação assegura a existência de procedimentos e instrumentos que garantam o combate de vírus no ambiente tecnológico da VISANET.

Foi notado que, o processo de *backup* na VISANET é automatizado, minimizando dessa forma erros decorrentes de intervenção humana. A

periodicidade de geração dos arquivos de *backup* varia de acordo com o arquivo. A estratégia de *backup* da VISANET antecipa a possibilidade de falhas em cada passo do ciclo de processamento, ou seja, os *backups* permitem a recuperação da informação antes da alteração ter sido gerada.

Observa-se que periodicamente a VISANET efetua visitas nos prestadores de serviço onde estão alocados os equipamentos para que seja feita uma verificação amostral da existência dos mesmos. De posse do inventário realizado inicialmente, e do volume de instalações realizadas, a VISANET tem de identificar o extravio de equipamentos, e de solicitar o ressarcimento por parte das empresas de manutenção se identificados problemas dessa natureza.

Foi descoberto que na documentação dos processos, são mencionados os controles de segurança adotados em cada uma das fases do processo. Esses controles são revisados pela área de Segurança da Informação da VISANET. Periodicamente, são realizadas revisões independentes para avaliar se os procedimentos estão sendo seguidos corretamente na prática, e se os controles estão sendo observados.

Contata-se que, o armazenamento das mídias na VISANET é feito de forma organizada, utilizando etiquetas nas fitas e cartuchos para identificação dos mesmos. O armazenamento de mídia magnética é feito em local limpo nos *data centers* das empresas parceiras: EDS e PROCEDA. Além de armazenar as mídias apropriadamente, a VISANET tem a preocupação de remover os dados da mídia quando não for mais necessário utilizá-las, pois conforme VALLABHANENI (2002), apagar indevidamente os dados pode deixar resíduos físicos que possibilitam a reconstituição dos dados.

Foi constatado que a avaliação das trilhas de auditoria geradas pelo sistema são realizadas periodicamente na VISANET. A frequência dessas revisões depende dos riscos envolvidos. Os seguintes riscos são considerados:

- ⚡ a criticalidade do processo realizado pela aplicação;
- ⚡ valor, a sensibilidade ou criticalidade da informação envolvida; e
- ⚡ a quantidade de interconexões, principalmente com a redes públicas de comunicação.

Pode-se notar que os sistemas de maior risco como: os que permitem alteração do domicílio bancário, acesso a números de cartão de crédito, cancelamentos de transações e a realização de ajustes, são monitorados constantemente e possuem trilhas de auditoria com um nível satisfatório de informações. Isto atende as proposições de KRUTZ e VINES (2001).

Outra constatação surpreendente, foi encontrar um processo bem definido para análise de risco específico em segurança da informação. A empresa possuía um processo de avaliação no qual são analisados os processos mais críticos da organização, seguindo as recomendações de VAUGHAN (1997), e classificados de forma, qualitativa segundo proposto por VALLABHANENI (2002). Esta análise, apesar de menos sofisticada que as demais, permite maior agilidade na identificação e priorização dos risco de segurança da informação. Também foi possível constatar que a avaliação dos riscos dos processos críticos de negócio, que assegurassem os princípios de a integridade, a disponibilidade e a confidencialidade de cada um deles, como recomendado por PELTIER (2001). Seguindo também a proposta de ALBERTS (2002), todos os processos da VISANET são implementados controles diretivos, preventivos, detectivos, corretivos e de recuperação para proteger contra os riscos associados.

Foi constatado que a VISANET assegura o controle rígido quanto a instalação de *modems* em ambas as rede tecnológicas dela. Isto é fundamental e está de acordo com as recomendações de VALLABHANINI (2002).

Observa-se que a VISANET possui políticas rígidas para os seus *firewalls*, as quais são baseadas no resultado das análises de risco. Estas políticas são sempre atualizadas a fim de garantirem proteção aos novos ataques ou novas vulnerabilidades identificadas. Como cita MCCLURE (2000), todas as políticas de *firewall* devem ser verificadas pelo menos com uma periodicidade trimestral.

Nota-se que a VISANET, no que diz respeito aos requisitos tecnológicos de LAN e computação remota implementam soluções satisfatórias e não as mais avançadas, que preservem a segurança das informações transmitidas em um nível necessário, e ao mesmo tempo, realizando uma boa relação custo-benefício sobre o assunto. A segurança destes itens vai de acordo com as recomendações de NAKAMURA (2002).

Pode-se perceber que a VISANET antecipa-se tanto nas questões de segurança na aplicação de novas tecnologias, como por exemplo o *wireless*, quanto nas questões de processos e procedimentos, como nos controles sobre o uso da Internet na organização. Esta atividade pró-ativa pode-se perceber na expectativa de uma implementação de uma metodologia de codificação segura a ser disponibilizada nos diversos projetos de desenvolvimento internos e também como referencial para os acordos de nível de serviço em projetos de desenvolvimento efetuados por terceiros que serão disponibilizados na *intranet*.

Devido ao fato de ser uma tecnologia utilizada há mais tempo, o emprego de VPN e suas melhores práticas descritas por VALLABHANENI (2002) já é prática no mercado, e portanto, não foi constatado nada surpreendente sobre o assunto na VISANET.

Em relação a segurança do correio eletrônico, foi contatado que a área de segurança da informação mantém um controle restrito na: implementação de uma solução de assinatura digital no seu ambiente computacional; nos servidores de *e-mail*, para que sejam revisados quanto as regras de filtro de segurança e bloqueio contra *spam*; e a implementação de uma política de Privacidade no ambiente computacional.

Contatou-se que através de IDS a VISANET está apta a prevenir, detectar, corrigir e reportar intrusão ocorridas em seu sistemas e na rede.

Contata-se que a segurança física da VISANET é implementada por diversos recursos avançados. Câmeras monitoram os principais pontos de acessos e são definidas rotinas específicas para periodicamente serem testados os dispositivos de detecção de incêndio, umidade, intrusão, com o propósito de assegurar que eles estão realmente funcionando. Constata-se ainda que a área de Segurança da Informação instrui todos os funcionários e prestadores de serviço com relação aos cuidados a serem adotados com os notebooks, incluindo armazenamento fora de expediente e a utilização de trava durante as ausências.

Foi possível constatar a criticalidade da segurança da informação nos processos de desenvolvimento, através da análise das medidas adotadas pela VISANET:

- ✍✍ as áreas de desenvolvimento e manutenção de sistemas possuam e utilizem ambientes segregados para as atividades de desenvolvimento, teste e homologação.
- ✍✍ as áreas de desenvolvimento e manutenção de sistemas possuam procedimentos para homologação dos aplicativos a serem colocados no ambiente de produção.
- ✍✍ existam recursos possibilitando a identificação das alterações realizadas no código fonte dos executáveis do ambiente de produção.
- ✍✍ as equipes de desenvolvimento possuam diretrizes para codificação segura
- ✍✍ todos os acessos dos desenvolvedores ao ambiente de produção foram removidos.
- ✍✍ as áreas de desenvolvimento utilizem sistemas de controle de versão para os aplicativos migrados para o ambiente de produção
- ✍✍ as áreas de desenvolvimento utilizem sistemas automatizados para o controle da documentação gerada.

Pode-se constatar a importância do plano de contingência, ao observar que a VISANET executa periodicamente testes no seu Plano de Contingência, a fim de verificar a eficiência do plano quanto à retomada das funções críticas de negócio, após haver uma ruptura na continuidade das mesmas, bem como a atuação dos responsáveis pela recuperação dos recursos. São documentados também os testes realizados com o Plano de Contingência e atualizados, com as alterações necessárias detectadas após a realização do teste.

Constata-se que apesar de não automatizado totalmente, a área de Segurança da Informação já definiu o critério a ser adotado para concessão de acesso ao funcionário e/ou prestador de serviço.

A estratégia de Gerenciamento de Identidades consiste em possuir um repositório único, o qual contém todos os *userid*s dos funcionários e as informações que possibilitam sua identificação, sendo as informações deste repositório replicada para as *ACL*s dos demais aplicativos, de acordo com o perfil do funcionário. A remoção dos acessos também é feita por intermédio desse repositório, dessa forma à medida que a base é replicada e sincronizada com os demais aplicativos, a exclusão do usuário é automaticamente realizada. Pode-se

observar, conforme propõe CLARK (2003), que para viabilização do Gerenciamento de Identidades a VISANET deverá:

- ✍✍ remodelar o processo de concessão e remoção de acesso;
- ✍✍ adotar uma solução de *workflow*;
- ✍✍ mapear os perfis de acesso existentes de acordo com a função que o funcionário executa; e
- ✍✍ adotar um estrutura de diretórios.

Em relação a estrutura de diretórios constata-se que a extensa utilização de computação distribuída tem aumentado o desenvolvimento de diretórios distribuídos, os quais permitem sub-conjuntos de um diretório lógico a ser distribuído onde eles forem mais funcionais dentro da empresa. Metadiretórios, que compreende múltiplos diretórios, oferece uma visão única através da empresa e auxilia na conexão de múltiplos sistemas para melhor controle e gerenciamento.

Também foi constatado que a decisão pela utilização de uma solução de criptografia deve estar baseada em uma análise de risco efetuada pelo respectivo proprietário do sistema onde seja considerado o prejuízo financeiro e de imagem acarretado pela perda da confidencialidade e/ou integridade de uma determinada informação, versus o custo de se implementar uma solução de criptografia.

Foi constatado que área tecnologia avalia a forma como está implementada a integração entre ambas as plataformas, a fim de verificar a possibilidade de aprimorar o tráfego de informações entre estas, evitando dessa forma que haja a gravação e o transporte de mídias entre localidades distintas.

Constatou-se que muitas são as mudanças tecnológicas sendo implementadas constantemente neste tipo de negócio, e associados a eles observa-se, a ocorrência de tanto riscos dinâmicos quanto estáticos VAUGHAN (1996). No entanto, as implementações e operações de soluções de segurança da informação encontradas, ficam facilmente de serem geridas quando existe uma forte gestão centralizada de segurança de informação dando todo o suporte e

atenção por trás. Isto foi constatado quando comparamos o modelo proposto na fundamentação teórica e as devidas implementações realizadas pela VISANET.

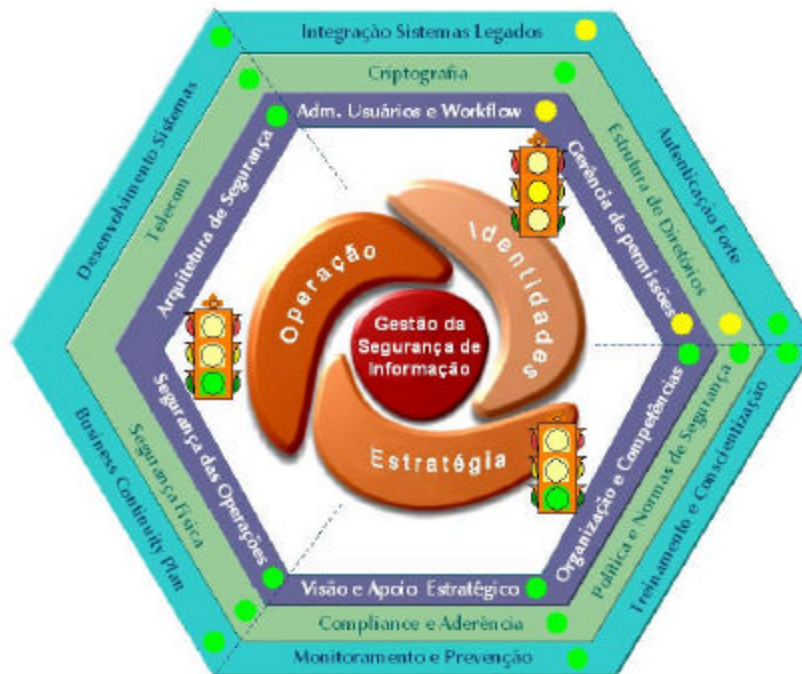


Figura 41: Aderência da VISANET ao modelo de gestão

(elaborado pelo autor)

Classificando de forma qualitativa, as cores⁹ representam o estágio de maturidade das soluções de segurança no determinado assunto. Conforme já comentamos as questões referentes ao alinhamento estratégico de segurança da informação estão muito bem estruturadas e portanto estão em verde. Pode-se notar, que as questões mais primordiais voltadas as questões técnicas da segurança da informação estão plenamente atendidas. Novos desafios voltados ao gerenciamento de identidades, estão ainda em um estágio mais inicial, mas possuem o devido direcionamento necessário, sendo portanto, uma questão de tempo de implementação.

⁹ Legenda:

Vermelho: com problemas

Amarelo: requer atenção

Verde: em conformidade

6. Conclusão

A informação é um fator crítico para os processos de negócios de uma empresa. A indisponibilidade, quebra de confidencialidade, e perda de integridade dessas informações podem acarretar prejuízos enormes e, dependendo do tipo do negócio, podem tirar a empresa do mercado. Assim, a empresa necessita de uma gestão de segurança da informação para proteger suas informações, que são manipuladas, armazenadas e processadas no ambiente computacional.

6.1. Conclusões

Este trabalho investigou, utilizando a metodologia do estudo de caso, como uma empresa da indústria de cartão de crédito construiu uma infraestrutura de gestão de risco em segurança de informação não só no âmbito tecnológico, mas também, no operacional e no mercadológico, estabelecendo uma relação transparente às demais áreas internas da organização, aos clientes e a todo o mercado.

O estudo de caso analisou o intento estratégico da VISANET e seus principais objetivos de negócio. Foi analisado a relação entre os principais processos de negócio e os quesitos de segurança da informação à situação da empresa. Através do estudo, foi possível observar a relação entre as implicações de negócio com os requisitos de segurança.

Foram comparados os resultados do estudo de caso com o modelo de gestão da segurança da informação proposto na fundamentação teórica. Foi possível concluir que, a gestão da segurança da informação na VISANET fora estruturada de forma totalmente aderente e específico ao seu negócio, atendendo totalmente o objetivo deste trabalho.

De forma surpreendente, observou-se que o modelo de gestão de risco em segurança da informação apresentado, apesar de ilustrativo e simples, é muito abrangente e contempla todos os componentes necessários para uma empresa estruturar e gerenciar suas questões relativas a segurança da informação. Este modelo, através deste trabalho foi elogiado pela área de segurança da VISANET por apresentar tais características.

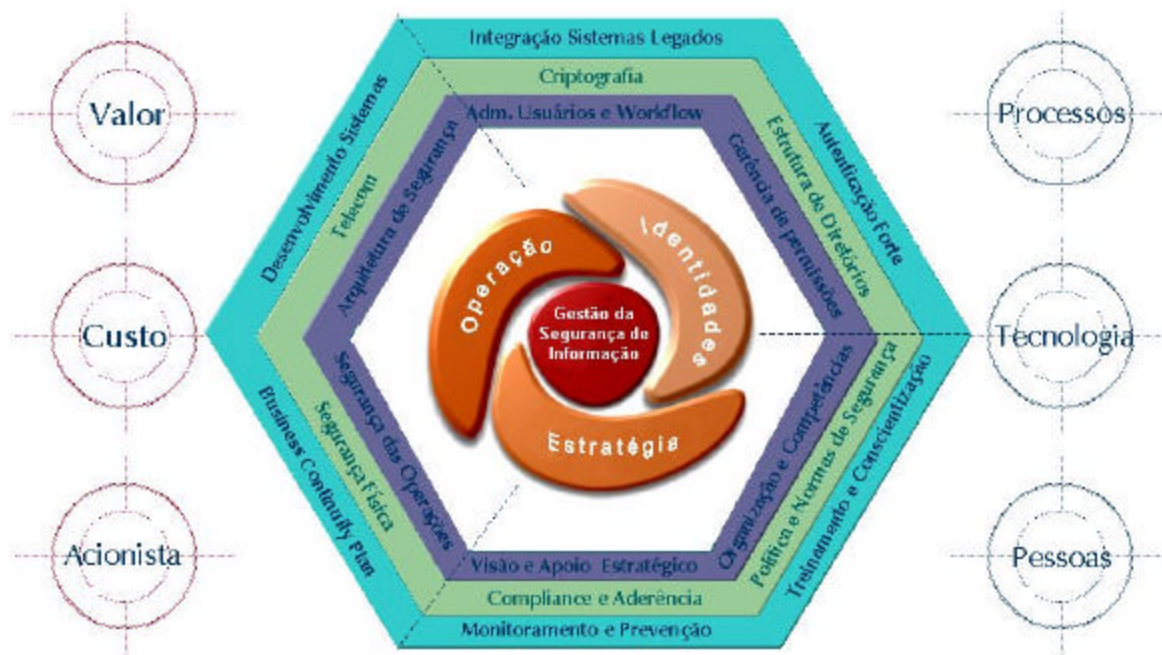


Figura 42: Modelo de gestão de risco em segurança da informação
(elaborado pelo autor)

Pode-se observar, através deste modelo, que a gestão da segurança da informação, não só deve considerar as questões de gestão interna e formas de implementações tecnológicas, mas também questões externas ao foco de área (ou no modelo: as áreas de interesse: alinhamento estratégico, segurança das operações e gerenciamento de identidades), como questões de negócio (criação do valor e gestão dos custos) e mercadológicas (administração das expectativas dos principais interessados, ou *stakeholders*: acionistas, clientes, investidores, fornecedores, etc).

Este trabalho foi satisfatório e conclusivo, uma vez que respondeu aos objetivos e questões propostos no início. A execução desta pesquisa demonstrou que as hipóteses H1 e H2 foram aceitas, ou seja que, a VISANET, empresa pertencente a indústria de cartão de crédito trata a gestão da segurança da informação de forma centralizada e especializada; e que a esta empresa executa uma análise de risco para a gestão da segurança da informação aderente e específico ao seu negócio.

Adicionalmente, foi constatado que a gestão de risco da segurança de informação sendo tratada centralizadamente, permite que não só as eventuais discussões técnicas quanto a aplicação das soluções tecnológicas, mas também os questionamentos em relação aos investimentos e implementações de soluções tecnológicas em segurança da informação por parte da alta administração e o resto da empresas, sejam evitadas através desta gestão centralizada e independente.

6.2. Limitações

As limitações deste trabalho são muitas, vista que o assunto é muito complexo e pouco explorado. Uma das limitações que merece destaque é o fato do estudo de caso ser de caso único, fazendo com que a análise do caso se restrinja apenas à situação encontrada na VISANET, e portanto, não pode ser ampliada para as outras empresas e concorrentes da indústria de cartão de crédito. O uso do caso único inviabiliza uma generalização estatística das conclusões.

Outra limitação foi o viés de concentração das informações obtidas nas entrevistas com o pessoal da área de segurança da informação. Este viés é devido ao assunto específico, uma vez que, ao tratarmos apenas dos questões referentes a segurança da informação, somente esta área possuía condições para respondê-las. Para atenuar esta limitação, foi utilizado também como fonte de evidências a observação pessoal e o exame de documentos e relatórios externos.

6.3. Sugestões para novas pesquisas

Este mercado de processamento de transações de cartão de crédito é bastante restrito, devido em grande parte à credibilidade associada a bandeira do cartão. Portanto, a sugestão mais evidente para pesquisas futuras seria a elaboração de novos estudos de caso, abordando com maior profundidade o assunto, sobre as demais participantes da indústria de cartão de crédito, que hoje seriam: a REDECARD, que processa as transações do MASTERCARD e a AMEX, processadora da AMERICAN EXPRESS.

Sugere-se ainda um estudo complementar, de modo a sintetizar as pesquisas sobre o tema de gestão de segurança da informação. Poderiam ser abordadas comparações do modelo de gestão de segurança da informação: entre as empresas da indústria de cartão de crédito no Brasil; entre as empresas da indústria de cartão de crédito no Brasil em relação ao mundo; entre as empresas da indústria de cartão de crédito em relação as demais indústrias no Brasil; e finalmente entre as indústrias no Brasil em relação ao mundo.

Seria conveniente elaboração de novos estudos, para o desenvolvimento e aprimoramento do modelo de gestão de risco em segurança da informação. Tanto os modelos analisados, quanto o modelo proposto, precisam serem explorados e desenvolvidos. O entendimento ampliado dos componentes do modelo de gestão de segurança é necessário para o bem e sobrevivência da organização.

Da mesma forma, que na teoria de gerenciamento de risco, existem diversas metodologias e técnicas, seria muito importante um estudo mais aprofundado destas aplicadas na avaliação de risco para a segurança da informação. Um tema interessante para um trabalho seria a elaboração de uma metodologia para avaliação de risco em segurança da informação, desenvolvendo métodos e modelos quantitativos e qualitativos. Por fim, esta metodologia em conjunto com um modelo de gestão poderia ser analisado e proposto a partir do ponto de vista dos próprios gestores de segurança da informação das empresas.

Finalmente seria bastante interessante e relevante a realização de estudos visando a criação de cursos acadêmicos multidisciplinares de formação em administração de empresas, tecnológica da informação, auditoria de sistemas e segurança da informação, de forma a preparar profissionais para exercer as funções de gerenciamento de risco em segurança da informação nas organizações.

7. Bibliografia

1. **ABECS – Associação Brasileira das Empresas de Cartão de Crédito e Serviços;** *Abecs Hoje*. Disponível em ABECS: <<http://www.abecs.org.br/hoje.htm>>; Acesso 10 de dezembro de 2002.
2. **ABU-MUSA, A.;** *Computer ccrimes: How can you protect your computerized accounting information system?*; Journal of American Academy of Business, Cambridge, Hollywood, Sep, 2002, v.2-1, p.91-101; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
3. **ABU-MUSA, A.;** *Security of computerized accounting information systems: A theoretical framework*; Journal of Americam Academy of Business, Cambridge, Hollywood, Sep, 2002, v.2-1, p.150-155; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
4. **ABU-MUSA, A.;** *Security of computerized accounting information systems: Na integrated evaluation approach*; Journal of American Academy of Business, Cambridge, Hollywood, Sep, 2002, v.2-1, p.141-149; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
5. **ALBERTIN, L. C.;** *Comércio Eletrônico*; Campus, 1999; ISBN 85-224-2139-0; p. 149-173.
6. **ALBERTS, C.; DOROFEE, A.;** *Managing Information Security Risks*; Addison- Wesley, 2002; ISBN 0-321-11886-3; p.10-25; 81-113.
7. **ALVEY, J.;** *IT security: Who`s investing in what?*; Public Utilities Fortnightly, Arlington, Jan, 2003, v. 141-1, p. 18-25; ISSN: 10785892; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
8. **ANSTEAD, M.;** *Taking a tough line on privacy*; Marketing, London, Apr, 2000, p. 31-34; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
9. **ANTHES, G.;** *Autoimmune computer systems*; Computerworld, Framingham, Dec, 2002, v. 36-50, p.38-40; ISSN: 00104841; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
10. **ATKINSON, A.; BANKER, R.; KAPLAN, R.; YOUNG, M.;** *Contabilidade Gerencial*. Atlas, 1999; ISBN 85-224-2350-4; p. 33-64.

11. **BEHAN, K. ; HOLMES, D.;** *Understanding Information Technology – Text, Readings, and Cases*; Prentice Hall, 1990 Second Edition; p. 237-242.
12. **BENITEZ, T.;** *Keeping watch*; Incentive, New York, Dec, 2002, v.176-12, p. 10-11; ISSN: 10425195; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
13. **BRADFORD, M.;** *Employee dishonesty risk requires careful approach*; Business Insurance, Chicago, Apr, 2002, v.36-16, p.12-14; ISSN: 00076864; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
14. **BRADNER, S.;** *What fools these mortals be*; Network World, Framingham, Dec, 2002, v. 19-49, p. 32-33; ISSN: 08877661; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
15. **BRAITHWAITE, T.;** *Securing E-Business Systems*; John Wiley and Sons, 2002; ISBN 0-471-07298-2; p. 109-145.
16. **BREIDENBACH, S.;** *How secure are you?*; Informationweek, Manhasset, Aug, 2000, i. 800, p.71-78; ISSN: 87506874; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
17. **BREIDENBACH, S.;** *The policy for protection*; Network World, Framingham, Oct, 2000, v.17-43, p.79-80; ISSN: 08877661; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
18. **BOYD, H.; WESTFALL, R.;** *Pesquisa Mercadológica – Textos e Casos*; 6ª Edição, Rio de Janeiro; Editora Getúlio Vargas.
19. **BOYTON, W.; KELL, W.;** *Modern Audintig*; John Wiley & Sons, 1996; ISBN 0-13-26849-5; p. 29-43.
20. **BROWN, J.;** *Instant messaging hidden threats*; Computing Canada, Willowdale, Sep, 2002, v.28-18, p. 6-7; ISSN: 03190161; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
21. **BYRNES, C.; KUTINICK, D.;** *Securing Business Information*; Addison-Wesley, 2001; ISBN 0-201-76735-X; p. 7-15.
22. **CARDNEWS;** *Evolução do Mercado*; Revista CardNews, Novembro de 2001; p. 49.
23. **CASTELLUCCIO, M.;** *Social engineering 101*; Strategic Finance, Montvale, Dec, 2002, v. 84-6, p. 57-58; ISSN: 1524833X; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

24. **CHELBA, M.;** *Marketing Digital*; Editora Futura, 1999; ISBN 85-7413-014-X; p. 59-78.
25. **CHOI, C.;** *Keyboard cops*; Scientific American, New York, Dec, 2002, v. 287-6, p. 36; ISSN: 00368733; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
26. **CHIDI, G.;** *Cybercrime plan*; CIO, Framingham, Mar, 2001, v.14-0, p.72; ISSN: 08949301; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
27. **CLARK, D.;** *Enterprise Security*; Addison- Wesley, 2003; ISBN 0-201-71972-X; p. 147-154.
28. **COBIT**; *Governance, Control and Audit for Information and Related Technology – Framework*, July 2000, 3rd Edition; ISBN 1-893209-14-8; p. 13-15.
29. **CONNOLLY, P.;** *The enemy within*; InfoWorld, San Mateo, Nov, 2002, v. 24-45, p. 26-27; ISSN: 01996649; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
30. **CORBITT, T.;** *Preventing fraud*; Management Services, Enfield, Dec, 2002, v.46-12, p.20-23; ISSN: 03076768; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
31. **CORRAL, C.;** *On-line security, payment services aid e-tailers stung by fraud*; Discount Store News, New York, Apr, 1999, v.38-8, p.20-25; ISSN: 00123587; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
32. **COSO**; *Committee os Sponsoring Organizations of Treadway Commission*; Internal Control, Integrated Framework, July 1994 Edition.
33. **CROWELL, W.;** *Trust, the e-commerce difference*; Credit Card Management, New York, Aug, 2001, v.14-5, p.80-82; ISSN: 08969329; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
34. **CULP, C.;** *The ART of Risk Management – Alternative Risk Transfer*; John Wiley & Sons, 2002; ISBN 0-471-12495-8; p. 199-217
35. **CUMMINGS, J.;** *From intrusion detection to intrusion prevention*; Network World, Framingham, Sep, 2002, v.19-38, p. 72-80; ISSN: 08877661; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

36. **CUMMINGS, J.;** *The people side of prevention*; Network World, Framingham, Sep, 2002, v.19-38, p.76-77; ISSN: 08877661; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
37. **DAVENPORT, T.; BECK, J.;** *The Attention Economy*; Havard Business School Press, 2001; ISBN 1-57851-441-X; p.84-85.
38. **DAVIS, J.;** *Consumer fears of online buying may be abated with new payment option*; Infoworld, Framingham, Oct, 2000, v. 22-43, p. 102-103; ISSN: 01996649; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
39. **D'AMICO, E.;** *Cyber crime is on the rise, but let's keep it quiet*; Chemical Week, New York, Sep, 2002, v.164-38, p.25-27; ISSN: 0009272X; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
40. **D'AMICO, E.;** *Industry praises law that shields data disclosure*; Chemical Week, New York, Jan, 2003, v.165-1, p.31-32; ISSN: 0009272X; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
41. **D'ANDREA, E.;** *Colaboradores; Segurança em Banco Eletrônico*. PricewaterhouseCoppers; 2000;
42. **DEMARIA, M.;** *Gone in 60 seconds*; Network Computing, Manhasset, Sep, 2002, v.13-20, p.77-90; ISSN: 10464468; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
43. **DINIZ, D.;** *O plástico avança*; Revista Exame; Finanças; 15/07/2002; Disponível em Portal Exame: <http://portalexame.abril.uol.com.br/pgMain.jhtml?ch=ch08&sc=sc0801&pg=pgart_0801_2> ; Acesso 29 de julho de 2002.
44. **DOHERTY, S.;** *Wanna buy the Brooklyn Bridge?*; Network Computing, Manhasset, Dec, 2002, v.13-25, p.16-18; ISSN: 10464468; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
45. **DOWD, K.;** *Beyond Value at Risk: the new science of risk management*; John Wiley & Sons, 1998; ISBN 0-471-97622-9; p. 3-5.
46. **DYKSTRA, G.;** *Where is DRM headed now?*; Information Today, Medford, Nov, 2002, v.19-10, p.29-30; ISSN: 87556286; cesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

47. **ECONOMIST**; *Leaders: How to worry wisely*; Digital security; The Economist, London, Oct, 2002, v.365-8296, p.13-16; ISSN: 00130613; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
48. **ECONOMIST**; *Science and Technology: Throttled at birth*; Computer viruses; The Economist, London, Nov, 2002, v. 365-8300, p. 74-75; ISSN: 00130613; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
49. **FERELLI, M.**; *Storage vulnerability*; Computer Technology Review, Los Angeles, Oct, 2002, v.22-10, p.12-14; ISSN: 02789647; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
50. **FERREIRA, A. B. H.**; *Novo Aurélio – O dicionário da Língua Portuguesa*; Nova Fronteira, 1999, 3ª ed.; ISBN 85-209-1010-6; p. 1772.
51. **FONSECA, B.**; *Security outfits fortify defenses*; InfoWorld, San Mateo, Nov, 2002, v. 24-45, p. 1-14; ISSN: 01996649; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
52. **FONTES, E.**; *Vivendo a segurança da informação*; Sicurezza Editora, 2000; ISBN 85-87297; p. 73-75.
53. **FRIEL, B.**; *NASA-Wide security vulnerability remediation program*; Government Executive, WASHINGTON, Nov, 2002, v.34-15, p. 42-43; ISSN: 00172626; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
54. **GARFINKEL, S.**; *The FBI's cyber-crime crackdown*; Technology Review, Cambridge, Nov, 2002, v.105-9, p.66-74; ISSN: 1099274X; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
55. **GITMAN, L. J.**; *Princípios de Administração Financeira*; Harbara Editora, 1997, 7ª ed.; ISBN 85-294-0060-7; p.17.
56. **GREENSTEIN, M. ; FEINMAN, T.**; *Security, Risk Management and Control*; McGraw-Hill Higher Education, 2000; ISBN 0-07-229289-X; p.171-188.
57. **GUERRY, B.**; *Access denied! Protecting community bank networks*; ABA Bank Compliance, Washington, Jan, 2003, v. 24-1, p. 4-11; ISSN: 08870187. Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

58. **HULME, G.;** *Guarding against threats from within*; Information Week, Manhasset, Dec, 2002, i. 920, p. 20-22; ISSN: 87506870; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
59. **HUNPHREYS,E.; MOSES, R.; PLATE, A.;** *Guide to Risk Assessment and Risk Management*; British Standards, 1998; ISBN 0-580-29551-6; p. 9-21.
60. **JOHNSON, M.;** *CyberWhoCares? IT should!*; Computerworld, Framingham, Dec, 2002, v.36-49, p. 24-25; ISSN: 00104841; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
61. **KALAKOTA, R.; OLIVA, R. A.; DONATH, B.;** *Move over, e-commerce*; Marketing Management, Chicago, v. 8-3, p. 22-33, 1999. ISSN: 10613846. Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>
62. **KALAKOTA, R.; ROBINSON, M.;** *E-Business – Estratégia para alcançar o sucesso no mundo digital*; Bookman, 2ª Ed, 2002. ISBN 0-201-72165-1;
63. **KUMAR, V.;** *Digital leakage*; The Internal Auditor, Altamonte Springs, Dec, 2002, v.59-6, p. 25-27; ISSN: 00205745; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
64. **KANELLAKIS, K.;** *Blurring the line between work and home*; Canadian HR Reporter, Toronto, Dec, 2002, v.15-21, p. G4-7; ISSN: 0838228X; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
65. **KEEGAN, C.;** *Cyber-terrorism risk*; Financial Executive, Morristown, Nov, 2002, v.18-8, p.35-37; ISSN: 08954186; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
66. **KING, J. L.;** *Operational Risk: Measure and Modelling*; John Wiley & Sons, 2001; ISBN 0-471-85209-0; p. 7-9, 53-63.
67. **KOLLER, G.;** *Risk Assessment and Decision Making in Business and Industry: a Practical Guide*; CRC Press, 1999; ISBN 0-8493-026804; p. 1-2, 37.
68. **KREWSKI, D.;** *Risk Assesment and Risk Management: a survey of recent models; Risk assessment and management*; Plenum Press, NY, 1987; ISBN 0-306-42683-8; p. 399-406.
69. **KRAUSE, J.;** *Hack attack*; ABA Journal, Chicago, Nov, 2002, v.88, p.50-55; ISSN: 07470088; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

70. **KRUTZ, R.; VINES, R.;** *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*; Wiley Press, 2001; ISBN 0-471-41356-9; p. 1-27, 215-245.
71. **LAUDON, K.; LAUDON, J. ;** *Management Information Systems*; Prentice Hall 7th Edition, 2001; ISBN 0-13-033066-3; p. 432-451.
72. **LOEB, M., GORDON, L.;** *Return on information security investments: Myths vs. realities*; Strategic Finance, Montvale, Nov, 2002, v.84-5, p.26-31; ISSN: 1524833X; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
73. **MACK, B.;** *Online privacy critical to research success*; Marketing News, Chicago, Nov, 2002, v. 36-24, p. 21-23; ISSN: 00253790; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
74. **MARLIN, S.;** *Public and private sectors ally to secure cyberspace*; Bank Systems & Technology, New York, Nov, 2002, v.39-11, p.8-10; ISSN: 10459472; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
75. **MARSHALL, C.;** *Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras*; Qualitymark Ed., 2002; ISBN 85-7303-357-6; p. 19-74.
76. **MASIE, E.;** *Byte wars*; E - Learning, Cleveland, Oct, 2002, v. 3-9, p.14-16; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
77. **MCCLURE, S.; SCAMBRAY, J.; KURTZ, G.;** *Hackers Expostos*. Makron Books, 2000; ISBN 85-346-1194-7.
78. **MCCOLLUM, T.;** *Security concerns prompt new initiatives*; The Internal, Altamonte Springs, Oct, 2002, v.59-5, p.14-15; ISSN: 00205745; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
79. **MCGEE, J.; PRUSAK, L.;** *Gerenciamento Estratégico da Informação*; Editora Campus, 1994; ISBN 85-7001-924-6; p. 5, 23-24.
80. **MILONE, M.;** *Hacktivismo: Securing the national infrastructure*; The Business Lawyer, Chicago, Nov, 2002, v.58-1, p.383-2002; ISSN: 00076899; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
81. **MYCHALCZUK, M.;** *Drowning in data*; Security Management, Arlington, Nov, 2002, v.46-11, p.70-74; ISSN: 01459406; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

82. **MUSASHI, M.;** *O livro de cinco anéis*; Ediouro Publicações, 2002; ISBN 85-00-0719-2; p. 80.
83. **NAKAMURA, E. T.; GEUS, P. L.;** *Segurança de Redes em Ambientes Cooperativos*; Berkeley Brasil, 2002; ISBN 85-7251-609-3; p. 28-29; 165-215.
84. **NBR ISO. IEC 17799 – Tecnologia da Informação.** Projeto 21:024.01-010:2001
85. **O`ROURKE, M.;** *Cyberattacks prompt response to security threat*; Risk Management, New York, Jan, 2003, v. 50-1, p.8-9; ISSN: 00355593; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
86. **PELTIER, T.;** *Information Security Risk Analysis*; Auerbach, 2001; ISBN 0-8493-0880-1; p. 3-47.
87. **PERERA, R., CHIDI, G.;** *Web law blocks growth*; InfoWorld, Framingham, Mar, 2001, v.23-10, p.36-37; ISSN: 01996649; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
88. **PHIFER, L., PISCITELLO, D.;** *Best practices for securing enterprise networks*; Business Communications Review, Hinsdale, Dec, 2002, v. 32-12, p. 32-37; ISSN: 01623885; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
89. **PIAZZA, P.;** *Bug hunters unite*; Security Management, Arlington, Dec, 2002, v.46-12, p.28-31; ISSN: 01459406; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
90. **PIAZZA, P.;** *Who's winning the cyberwars?*; Security Management, Arlington, Dec, 2002, v. 46-12, p. 70-78; ISSN: 01459406; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
91. **PLOTKIN, M., FAGAN, D.;** *Don't hack back*; Security Management, Arlington, Nov, 2002, v.46-11, p.56-62; ISSN: 01459406; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
92. **POPE, C.;** *Hack attacks*; Professional Engineering, Bury St. Edmunds, Nov, 2002, v.15-21, p.24-25; ISSN: 09536639; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
93. **PORTER, M.;** *Estratégia Competitiva*; Editora Campus, 1986; ISBN 85-7001-377-X; p. 22-30, 113, 267.

94. **PORTER, M.;** *Vantagem Competitiva*; Editora Campus, 1990; ISBN 85-7001-558-5; p. 150-158.
95. **PRAHALAD, C.K.; HAMEL, G.;** *Competindo pelo Futuro*; Editora Campus, 6ª Ed., 1995; ISBN 85-7001-945-9; p. 143.
96. **PRICEWATERHOUSECOOPERS.** *Risk Management Forecast 2001*. PricewaterhouseCoopers Press, 2000.
97. **OXFORD;** *Oxford learner's pocket dictionary*; Oxford University Press, 3rd. Ed., 1992; ISBN 0-19-431282-8; p.432.
98. **ROBERTS, S.;** *Companies' exposure to cyber terror growing*; Business Insurance, Chicago, Dec, 2002, v. 36-48, p.10-16; ISSN: 00076864; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
99. **ROGOSKI, R.;** *Safe and secure*; Health Management Technology, Atlanta, Dec, 2002, v. 23-12, p.14-18; ISSN: 10744770; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
100. **ROHAN, R.;** *Social engineering*; Black Enterprise, New York, Sep, 2002, v. 33-2, p.53-54; ISSN: 00064165; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
101. **ROMEO, J.;** *Keeping your Network safe*; HRMagazine, Alexandria, Dec, 2002, v.47-12, p.42-46; ISSN: 10473149; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
102. **ROTHKE, B.;** *Information Security Best Practice: 205 Basic Rules*; Security Management, Arlington, Sep, 2002, v. 46-9, p. 214-215; ISSN: 01459406; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
103. **SANTOS, P.;** *Gestão de Riscos Empresariais*; Novo Século Ed., 2002; CDD-658.155; p. 25.
104. **SAVAGE, M.;** *E&Y security unit counting on VARs*; CRN, Jericho, Jan, 2003; p. 5-14; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
105. **SCALET, S.;** *Fear Factor; A reality check on your top five concerns about reporting security incidents*; CIO, Framingham, Oct, 2002, v. 16-2, p.62-68; ISSN: 08949301; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

106. **SCHNEIER, B.**; *Segurança..Com*; Campus, 2001; ISBN 85-352-0755-4; p. 22-59; 303-314.
107. **SEEWALD, N.**; *CIDX forms cybersecurity unit*; Chemical Week, New York, Jan, 2003, v. 165-2, p. 20-21; ISSN: 0009272X; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
108. **SHERWIN, E., PAAR, R.**; *IT experts: Tighten cyber-security*; Best's Review, Oldwick, Oct, 2002, v. 103-6, p.86-88; ISSN: 15275914; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
109. **SHIPLEY, G.**; *Secure to the core*; Network Computing, Manhasset, Jan, 2003, v. 14-1, p. 34-40; ISSN: 10464468; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
110. **SPOSITO, R.**; *Visanet evita perda de 20 milhões de dólares*; Revista Info Corporate; Outubro de 2002; v1-1; p. 39-41.
111. **SPYMAN**; *Manual Completo do Hacker*; Book Express, 3ª Ed., 2000; p. 7-12; 49-53.
112. **SYMANTEC**; *Security Reference Handbook*; Symantec Corporation, 2002; p. 24-26.
113. **TAPSCOTT, D.**; *Plano de Ação para uma Economia Digital*; Makron Books, 2000; ISBN 85-346-1076-2; p. 229-243.
114. **TAPSCOTT, D.**; *Geração Digital*; Makron Books, 2001; ISBN 85-346-0726-5; p. 176.
115. **THIBODEAU, P.**; *Guidelines aim to secure government's IT systems*; Computerworld, Framingham, Nov, 2002, v. 36-45, p. 8-9; ISSN: 00104841; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
116. **TREMBLY, A.**; *Poor computer security leaves firms exposed to intellectual property losses*; National Underwriter, Erlanger, Nov, 2002, v. 106-47, p. 14-16; ISSN: 10426841; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
117. **TUESDAY, V.**; *Planning for a metro-area armageddo*; Computerworld, Framingham, Dec, 2002, v. 36-50, p.40-42; ISSN: 00104841; ; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.

118. **WADLOW, T.;** *Segurança de Redes*; Editora Campus, 2001; ISBN 0-201-43317-6; p. 4-57; 92-163.
119. **WETZEL, R.;** *Market drivers for e-business defense technology*; Business Communications Review, Hinsdale, Jan, 2003, v. 33-1, p.54-61; ISSN: 01623885; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
120. **VAUGHAN, E.;** *Risk Management*; New Baskerville: John Wiley & Sons. 1997; ISBN 0-471-10759; p. 3-67.
121. **VALLABHANENI, S.;** *CISSP Textbook*; SRV Professional Publications, 2002; ISBN 0-9715216-5-4; p. 154-161; 2-14; 53-116; 169-235; 238-285; 300-475.
122. **VERTON, D.;** *How will you secure your company data?*; Competerworld, Framingham, 2003, v. 37-1, p. 24-26; ISSN: 00104841; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>
123. **VERTON, D.;** *Hacking syndicates threaten banking*; Computerworld, Framingham, Nov, 2002, v.36-45, p.14-15; Acesso via Proquest Direct: <<http://proquest.umi.com/pqdweb>>.
124. **YIN, R.;** *Estudo de Caso – Planejamento e Métodos*; Bookman, 2001; ISBN 85-7307-852-9; p. 31-60.

8. Glossário

Access Control List – ACL – Lista de controle de acesso, responsável por especificar os níveis de privilégio que cada conta de usuário terá no sistema, diretório ou arquivo.

Ambiente Lotus Notes/Domino – Esse ambiente encontra-se em um servidor Windows NT devido ao seguinte fato: o Windows NT é o sistema operacional onde o Lotus Domino é instalado. O Lotus Notes utiliza o Lotus Domino para todas as operações com as bases e envio/recebimento de mensagens e réplicas.

Arquivos de log - São registros armazenados nos servidores, para que os administradores possam analisar a frequência em que o usuário se mantém conectado, tempo de conexão, modo em que ele estabelece sua conexão, etc.

Backup - Cópia de um arquivo ou conjunto de arquivos, de um dispositivo de armazenamento para outro com a finalidade de manter-se uma cópia de segurança caso haja alguma danificação do original.

Boot - É o processo pelo qual passa um computador quando é ligado. Há uma procura por determinados programas e arquivos que, via de regra, estão gravados no winchester: é conveniente ter de reserva um disquete de boot, ou seja, os arquivos usados na inicialização do sistema instalado no micro.

Browsers – São também conhecidos como navegadores como é o caso do Internet Explorer ou o Netscape Navigator, usados para abertura de páginas Internet.

Brute force – Este ataque utiliza-se de todos os valores de palavras possíveis, com caracteres alfanuméricos e especiais, testando a combinação utilizada na senha de um sistema.

Clear-text – Dados enviados sem nenhuma forma de criptografia que garanta sua confidencialidade, permitindo que qualquer pessoa que o intercepte, consiga ler seu conteúdo.

Common Gateway Interface - CGI - Aplicação servidora utilizada geralmente para processar solicitações do navegador (browser) através de formulários HTML, enviando o resultado em páginas dinâmicas HTML. Pode ser utilizado para conexão (gateway) com outras aplicações e bancos de dados do servidor. Exemplo de linguagens são: Perl, C e C++.

Confidencialidade – Garante que os dados trafegando na rede somente sejam abertos pelos seus respectivos destinatários. Utilizam-se chaves ou algoritmos criptográficas (vide glossário - algoritmos e chaves criptográficas).

Criptografia – Método que torna os dados ilegíveis para todos que não possuam a chave criptográfica correta. Esse método fornece confidencialidade às transferências de dados.

Dial-in – Tentativa de acesso discado.

Disponibilidade – Os dados devem ser mantidos disponíveis para todos que necessitem acessá-los.

Dispositivos – Equipamento.

Fake Mail – Falsas mensagens enviadas a partir de endereços existentes ou não, porém utilizando-se do domínio de determinada empresa, denegrindo a imagem da mesma com informações não verdadeiras, podendo ser usado também para spam.

File Transfer Protocol - FTP - Protocolo padrão da Internet de transferência de arquivos entre computadores.

Firewall – Hardware ou software que restringe o tráfego para uma rede privada a partir de uma rede não segura como a Internet. Pode restringir

também tráfego entre diferentes segmentos de redes locais para proteger dados sensíveis.

Hash fuctions – Funções matemáticas com duas propriedades muito importantes: anti-pré-imagem e livres de colisão. Anti-pré-imagem garante que mesmo de posse do resultado da função, não se consiga obter a função que gerou esse resultado e, livre de colisão garante que muito dificilmente a função obterá dois resultados iguais para duas fontes diferentes de dados.

Host – Qualquer dispositivo conectado à uma rede.

Hotfixes, patches e service packs – Atualizações de aplicativos para a solução de alguns bugs e vulnerabilidades encontradas após o lançamento dos mesmos.

Hubs – Dispositivo que propaga (regenera e amplifica) sinais elétricos em uma conexão de dados, para estender o alcance da transmissão, sem fazer decisões de roteamento ou de seleção de pacotes.

Hypertext Markup Language – HTML – A linguagem usada na Internet para criar páginas web com links para outros documentos, uso de formatação negrito, itálico entre outros. O código fonte para o que é visto na Internet é escrito em HTML.

Hyper Text Transfer Protocol HTTP— O protocolo mais utilizado na Internet para transferir informação dos servidores Web para os browsers. É o protocolo que negocia a entrega de documentos entre o browser e o servidor Web.

Integridade - Deve ser garantida a integridade dos dados de maneira a não permitir modificações por pessoas devidamente autorizadas. Para sua manutenção são utilizados algoritmos com funções hash (vide glossário – hash functions).

Internet - Significa a "rede das redes". Originalmente criada nos EUA, tornou-se uma associação mundial de redes interligadas, em mais de 70 países. Os computadores utilizam a arquitetura de protocolos de comunicação TCP/IP. Originalmente desenvolvida para o exército americano, hoje é utilizada em grande parte para fins acadêmicos e comerciais. Provê transferência de arquivos, login remoto, correio eletrônico, news e outros serviços.

Internet Control Message Protocol ICMP - Um protocolo de camada de rede Internet que provê pacotes de mensagens reportando erros e outras informações relevantes ao processamento de pacotes IP. Documentado na RFC 792.

Internet Protocol IP - Um protocolo de camada de rede que contém informação de endereçamento e alguns controles que permitem aos pacotes serem roteados. Documentado na RFC 791.

Logins genéricos - Logins que são utilizados por inúmeras pessoas não possibilitando responsabilização por ações efetuadas na rede.

Login/Logon - Comando inicial que o usuário deve executar para ter acesso à uma rede. Quando ele entra na rede, ele precisa executar seu logon, que é sua identificação na rede, seguido ou não de uma senha.

Não repúdio - Garantia de que o autor de determinada ação não possa negar a sua autoria.

Network Basic Input/Output System - NetBIOS - NetBIOS provê uma interface de comunicação entre o programa aplicativo e o meio físico utilizado. Todas as funções de comunicação da camada física à camada de sessão são manipuladas pelo NetBIOS, o software de suporte do adaptador de rede e o adaptador de rede. Uma sessão NetBIOS é uma conexão lógica entre quaisquer dois nomes em uma rede.

Plano de continuidade do negócios e/ou contingência - Planejamento de procedimentos e instalações que visem manter os sistemas tecnológicos

disponíveis, mesmo na ocorrência de problemas externos à eles, como por exemplo a falta de energia, ou um incêndio no prédio da empresa.

Port scanning - Técnica utilizada para obter conhecimento dos serviços ativos em hosts conectados à rede.

Porta - Uma abstração usada pela Internet para distinguir entre conexões simultâneas múltiplas para um único host destino. O termo também é usado para denominar um canal físico de entrada e saída de um dispositivo.

Recuperação Restore - Retorno do arquivo ou conjunto de arquivos a partir do dispositivo onde ele foi gravado na operação de backup para o local original.

Registry do Windows NT - Estrutura de configuração do Windows NT baseado em valores distribuídos em chaves. Contém toda configuração e alterações feitas no Windows NT.

Roteador - Dispositivo da camada de rede OSI que decide qual de vários caminhos o tráfego de rede utilizará baseado em algumas métricas de otimização. também chamado de gateway, roteadores repassam pacotes de uma rede para outra baseados em informações da camada de rede.

Security Accounts Manager - SAM - Gerenciador de usuários do Windows NT

Security Office - Departamento responsável por promover, planejar e implementar a segurança de dados.

Servidor - Numa rede, é um computador que administra e fornece programas e informações para os outros computadores conectados. No modelo cliente-servidor, é o programa responsável pelo atendimento a determinado serviço solicitado por um cliente. Referindo-se a equipamento, o servidor é um sistema que prove recursos tais como

armazenamento de dados, impressão e acesso dial-up para usuários de uma rede de computadores.

Sessão Nula – Conexão efetuada sem o uso de uma conta de usuário para identificação no sistema.

Sniffing.- Utilização de um programa chamado Sniffer, que captura todos os pacotes de informação que trafegam na rede possibilitando visualizar seu conteúdo, efetuar análises estatísticas do tráfego por tipo de protocolo de rede, podendo disponibilizar informações como contas de usuários e senhas que trafeguem sem serem criptografados.

Spoofing – Técnica de invasão que consiste em enganar o sistema, com a máquina intrusa se passando por uma máquina interna da rede.

Stack ou Buffer overflow – Método de ataque onde o invasor sobrecarrega a pilha do sistema, área de memória onde ficam armazenados alguns drivers e programas que estão ativos, fazendo com que o computador não consiga gerenciar estes programas e conseqüentemente trave..

Switchs – Dispositivo de rede que segmenta o tráfego de dados.

System Key – SYSKEY – Utilitário do Windows NT que permite a criptografia da Security Accounts Manager – SAM, com uma chave criptográfica de 128 bits.

TCP-Wrapper - Ferramentas que agem como filtros de endereços que podem acessar determinado serviço, por exemplo, se você precisa administrar seus roteadores remotamente e não quer que ele responda a todas as requisições de conexão Telnet, mesmo sabendo que você implementou o uso de uma senha de administrador que apenas um seleto grupo de funcionários conhece, você pode cadastrar apenas os endereços IP das máquinas de onde será possível efetuar essa conexão. Essa utilização aumenta muito o nível de segurança da sua rede, pois provê o serviço apenas para as estações que você entender que necessitem dele.

Telnet - Protocolo da Internet, que permite o login remoto, tornando possível a um microcomputador atuar como terminal de computadores de qualquer parte do mundo. O Telnet utiliza um programa cliente que permite usar um computador, que está longe, como se fosse o seu próprio micro.

Transfer Control Protocol -TCP - Protocolo Internet de camada de transporte orientado à conexão que executa controle de fluxo e erro fim a fim.

Transferência de zona - Transferência dos endereços da tabela de nomes de um servidor para outro. Uma falha na configuração do servidor de nomes - DNS pode permitir que qualquer usuário conectado à Internet possa obter uma cópia dessa tabela e até mesmo obter endereços da rede interna.

Userid - Identificação do usuário para o Lotus Notes. Cada usuário possui o seu Userid que é único.

Web - Literalmente, teia de alcance mundial. Baseada em hipertextos, integra diversos serviços Internet que oferecem acesso, através de hyperlinks, a recursos multimídia da Internet.

Anexo 1: Questionários

Direcionadores de Negócio

Entrevistado: Machado Jurnior - Riscos e Fraudes

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
2. Qual a missão, a visão, e os objetivos da diretoria executiva?
3. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Iniciativas de negócio

1. Quais são as estratégias relacionadas a segurança e privacidade da informação?
2. Quais são as estratégias para identificação de novos tipos de fraudes?

Operações do negócio

1. Quais são os processos críticos de negócio da Visanet?
2. Como é a utilização da informação no processo de negócio e transações?
3. Qual o grau de criticidade da informação utilizada no processo de negócio?

Direcionadores de Negócio

Entrevistado: Wanderley Barreto - Compliance e Processos

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
2. Qual a missão, a visão, e os objetivos da diretoria executiva?
3. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Operações do negócio

1. Quais são os processos críticos de negócio da Visanet?
2. Como é a utilização da informação no processo de negócio e transações?
3. Qual o grau de criticidade da informação utilizada no processo de negócio?
4. Quais os riscos e vulnerabilidades conhecidas relacionados ao negócio/processo?
5. O que assegura que os processos internos estão aderentes as regulamentações (compliance)?
6. Quais métricas são utilizadas para acompanhamento do desempenho dos negócios?

Aspectos legais/Regulamentos da indústria

1. Quais são as principais regulamentações legais e da indústria de cartão de crédito?
2. Quais são as principais regulamentações organizacionais?
3. Como é o processo de retenção de registro de atos ilegais (internos e externos)?
4. Quais são os principais litígios sofridos pela Visanet? Como é feito o controle sobre tais litígios?

Direcionadores de Negócio

Entrevistado: Andrea Marques - Desenvolvimento Organizacional

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
2. Qual a missão, a visão, e os objetivos da diretoria executiva?
3. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Cultura corporativa

1. Quais são as mudanças organizacionais previstas e qual o impacto na segurança e privacidade da informação?
2. Quais são as estratégias relacionadas ao envolvimento de terceiros nos processos produtivos?

Direcionadores de Negócio

Entrevistado: Herval Rossi - Tecnologia e Operações

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
2. Qual a missão, a visão, e os objetivos da diretoria executiva?
3. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Operações do negócio

1. Quais são os processos críticos de negócio da Visanet?
2. Como é a utilização da informação no processo de negócio e transações?
3. Qual o grau de criticidade da informação utilizada no processo de negócio?
4. Quais os riscos e vulnerabilidades conhecidas relacionados ao negócio/processo?
5. O que assegura que os processos internos estão aderentes as regulamentações (compliance)?

Tecnologia

1. Quais as principais tecnologias empregadas atualmente na organização?

2. Quais as principais iniciativas de negócio que estão direcionando as mudanças tecnológicas?
3. Quais as novas tecnologias que estão sendo introduzidas?
4. As funções e responsabilidades da informática estão claramente definidas?
5. Existe um comitê diretor de informática?
6. Quais os principais projetos e mudanças previstos a curto e longo prazo?
7. Quais as novas tecnologias estão sendo testadas e pesquisadas para possível implementação?
8. Qual a opinião da administração sobre a área de tecnologia no alcance dos objetivos da empresa?
9. Quais os controles adotados sobre a terceirização de recursos?
10. Quais os principais problemas tecnológicos que impactam no negócio da VisaNet?
11. Como são endereçadas os aspectos de segurança pela área de tecnologia?

Direcionadores de Negócio

Entrevistado: Walter Rabello - Marketing e Produtos

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
2. Qual a missão, a visão, e os objetivos da diretoria executiva?
3. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Iniciativas de negócio

1. Quais são as maiores iniciativas de negócio da organização?
2. Quais são os novos produtos/serviços oferecidos pela Visanet?
3. Quais são as estratégias de “go-to-market”?
4. Quais são as estratégias para uso da Internet?
5. Quais são as estratégias de E-commerce?
6. Quais são as estratégias relacionadas a segurança e privacidade da informação?

Direcionadores de mercado

1. Como são acompanhadas as tendências de mercado?
2. Qual o posicionamento da Visanet perante os concorrentes, mercado e seus clientes?

Direcionadores de Negócio

Entrevistado: Antonio Castilho - Vendas e Negócio

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
2. Qual a missão, a visão, e os objetivos da diretoria executiva?
3. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Iniciativas de negócio

1. Quais são as maiores iniciativas de negócio da organização?
2. Qual o impacto que a tecnologia ou a segurança tem sobre essas iniciativas?
3. Quais são os riscos decorrentes dessas iniciativas de negócio?
4. Quais são os novos produtos/serviços oferecidos pela Visanet?
5. Quais são as estratégias relacionadas a recursos humanos?
6. Quais são as estratégias de “go-to-market”?
7. Quais são as estratégias para uso da Internet?
8. Quais são as estratégias de E-commerce?

9. Quais são as estratégias relacionadas ao envolvimento de terceiros nos processos produtivos?
10. Quais são as estratégias relacionadas à implementação de sistemas e processos?
11. Quais são as estratégias relacionadas a segurança e privacidade da informação?
12. Quais são as estratégias para identificação de novos tipos de fraudes?

Direcionadores de mercado

1. Como são acompanhadas as tendência de mercado?
2. Qual o posicionamento da Visanet perante os concorrentes, mercado e seus clientes?

Direcionadores de Negócio

Entrevistado: Bartholomeu Ribeiro - Finanças e Administração

Informações sobre a diretoria executiva:

1. Qual a estrutura da diretoria executiva?
4. Qual a missão, a visão, e os objetivos da diretoria executiva?
5. Quais diretorias e gerências dão suporte ao negócio da Visanet ou são consideradas áreas de negócio?

Operações do negócio

7. Quais são os processos críticos de negócio da Visanet?
8. Como é a utilização da informação no processo de negócio e transações?
9. Qual o grau de criticidade da informação utilizada no processo de negócio?
10. Quais os riscos e vulnerabilidades conhecidas relacionados ao negócio/processo?
11. O que assegura que os processos internos estão aderentes as regulamentações (compliance)?
12. Quais métricas são utilizadas para acompanhamento do desempenho dos negócios?

Aspectos legais/Regulamentos da indústria

5. Quais são as principais regulamentações legais e da indústria de cartão de crédito?
6. Quais são as principais regulamentações organizacionais?
7. Como é o processo de retenção de registro de atos ilegais (internos e externos)?
8. Quais são os principais litígios sofridos pela Visanet? Como é feito o controle sobre tais litígios?